Information Technology & People

Number 5

Cybercrimes prevention: promising organisational practices
Guest Editors: Mahmood Hussain Shah, Paul Jones and Jyoti Choudrie

1125 Guest editorial

1130 Solutions for countering human deception in social engineering attacks
Curtis C. Campbell

1153 Prevention of cybercrimes in smart cities of India: from a citizen’s perspective
Sheshadri Chatterjee, Arpan Kumar Kar, Yogesh K. Dwivedi and Hatice Kizgin

1184 Preventing identity theft: identifying major barriers to knowledge-sharing in online retail organisations
Abdulrah Maitlo, Nisreen Ameen, Hamid Reza Peikari and Mahmood Shah

1215 Crime and social media
Simplice Asongu, Jacinta Nwachukwu, Stella-Maris Orim and Chris Pyke

1234 Shoplifting in mobile checkout settings: cybercrime in retail stores
John A. Aloysius, Ankur Arora and Viswanath Venkatesh

1262 Organizational practices as antecedents of the information security management performance: an empirical investigation
Daniel Pérez-González, Sara Trigueros Preciado and Pedro Solana-Gonzalez

1276 Online social network security awareness: mass interpersonal persuasion using a Facebook app
Ehinome Ikhalia, Alan Serrano, David Bell and Panos Louvieris

1301 The effect of cybercrime on open innovation policies in technology firms
Vanessa Ratten

1318 Cybersecurity economics – balancing operational security spending
Stale Ekelund and Zilia Iskoujina


www.emeraldinsight.com/loi/itp
Cybercrimes prevention: promising organisational practices

Contextualising the special issue

The growth of e-commerce worldwide has enabled many organisations to deliver products and services using innovative, efficient, fast and cost effective business models. The digital economy continues to grow and makes a considerable contribution to the world economy. However, this relatively rapid growth has also caused even faster growth in cybercrimes, mainly due to the ease of committing these crimes, lucrative returns and the slowness of prevention efforts. Cybercrimes represent an existential threat to e-commerce and the need to effectively control their growth is urgent. As the relevant legislation and capabilities of law enforcement agencies is failing to catch up with the fast changing nature of crimes, businesses need to adopt innovative preventative strategies. This special issue focuses on how both large organisations and SMEs are making effective use of cybercrime prevention strategies. It also presents new research approaches and methodologies contributing to the theory and practice in this important emerging research domain.

Bera (2019) gave worldwide figures for cybercrimes for the year 2018, stating that almost 700m people were victims of some type of cybercrime. Cybercriminals generate revenues of $1.5tn annually and cybercrime is estimated to cost $6tn businesses annually by 2021. Generally, when calculating cybercrimes losses, only reported direct losses are accounted for. The indirect losses such as reduction in sales, a reduction in market share, share price drop and other legal costs have a significant adverse impact on organisations; however, they are often overlooked. Many cybercrimes are not reported or are under reported by organisations because of possible reputational damage. Therefore, the figures given here could be under estimated below the real number of cybercrimes or the extent of damage. Nevertheless, these figures demonstrate how widespread these crimes are, with the resulting damages to the world economy in the trillions.

Doargajadthur and Dell (2019) identify that enhanced awareness of cybercrimes and alarming media reports about losses resulting from these crimes have intensified interest and attracted the attention of consumers, organisations, governments and researchers. Moreover, Vahdati and Yasini (2015) stressed that cybercrimes are the biggest threat to the survival of e-tailing. Whereas cybercrimes are a fast-evolving problem, prevention strategies and implementation have been slow amongst businesses. The losses caused by cybercrimes can damage both the finances and reputation of businesses (Vahdati and Yasini, 2015). These crimes and resulting fears also discourage many customers from buying goods online. Spanaki et al. (2019) and Tsouh and Holtkamp (2018) identified major challenges faced by consumers when they become victims of cybercrimes. These consumers faced issues such as credit problems (including rejection of loan applications), disruption to normal life routines and psychological difficulty in providing personal data to organisations and banks during an investigation.

Previous studies focused on issues related to the development and management of identity fraud policies (Njenga and Osimeo, 2013; Coulson-Thomas, 2017). Syed (2018) investigated the effects of data breaches on the reputation of organisations on social media. Moreover, Doherty and Tajuddin (2018) researched prevention approaches including identifying risks and sharing knowledge about information security with other organisations. The majority of these studies are, however, directed at internal fraud in banking and other public and private sectors; there is very limited literature available in terms of theories on cybercrime management.
Njenga and Osiero (2013) focused on fraud management policies and asserted that organisations should consider all stages in fraud management when developing an anti-fraud policy. Coulson-Thomas (2017) and Chen et al. (2015) suggested the importance of employees’ participation in fraud management plans, whereas Soomro et al. (2016) focused on identity fraud prevention. Jalali et al. (2019) suggested that organisations need to synchronise their fraud management plans and protocols with other partners in their value chain to ensure that there are no weak links for fraudsters to exploit. Furthermore, Yoon and Kim (2013) investigated information security behavioural intention and suggested that learning opportunities for IT users helps achieve improved security by eliminating previous mistakes and addressing user-related weaknesses in organisations.

Chen et al. (2015) and Kolkowska et al. (2017) researched the effectiveness of internal audits and recommended that organisations should develop regular audit processes for improved fraud detection and prevention. Some studies have suggested providing training that can create awareness of cybercrime-related problems (Singh et al., 2013; Chen et al., 2015). Al-Khoury (2014) focused on cybercrime-related difficulties and how these are having an impact on investments in online retailing. Khajouei et al. (2017) and Alsmadi and Prybutok (2018) researched frauds in mobile commerce which they claim are different compared to traditional e-commerce-related frauds in terms of methods used by the fraudsters.

The extant literature covered above investigated various organisational practices related to fraud which is encouraging; however, the fact that the cyber frauds are still growing in terms of number and resulting financial losses suggests that existing approaches are still inadequate, hence the need for further research. This special issue aims to serve this need. With the rest of this editorial, we consider the papers included in this special issue which are presented in the following order.

The study by Campbell investigated the three most significant issues related to social engineering and security approaches for counteracting social engineering attacks. The three most significant issues produced three target areas for implementing best practices in countering social engineering attacks. The findings offer fresh insights into blending security processes, practices and programmes, and aim to provide leaders with increased understanding in implementing counteractions.

Chatterjee, Kar, Dwivedi and Kizgin’s study identifies the factors influencing the citizens of India to prevent cybercrimes in the proposed smart cities of India. The study proposes a conceptual model identifying factors preventing cybercrimes. The study reveals that “awareness of cybercrimes” significantly influences actual usage of technology to prevent cybercrimes in the smart cities of India. The authors suggest that government initiatives and legal awareness have less impact towards the spreading of awareness of cybercrimes to the citizens of proposed smart cities.

Maitlo, Ameen, Peikari and Shah’s study considers barriers to effective knowledge sharing in preventing identity fraud in online retail organisations using a case study approach. The study proposes a framework based on a reconceptualization and extension of the knowledge sharing enablers framework. The findings suggest the major barriers to effective knowledge sharing for preventing identity fraud are poor leadership support, limited employee willingness to share knowledge, lack of employee awareness of knowledge sharing, inadequate learning/training opportunities, insufficient trust in colleagues, poor information-sourcing opportunities and information and communications technology infrastructure, inferior knowledge sharing culture, insufficient evaluation on performance and inadequate job rotation. The research offers solutions for removing existing barriers to knowledge sharing in preventing identity fraud.

Asongu, Nwachukwu, Orim and Pyke’s study complements the limited macroeconomic literature on the development outcomes of social media by examining the relationship between Facebook penetration and violent crime levels in a study of 148 countries using a
quantitative analysis. The study noted a negative relationship between Facebook penetration and crime. Furthermore, when the data set is decomposed into regions and income levels, the negative relationship is evident in the Middle East and North Africa, whereas a positive relationship is confirmed for Sub-Saharan Africa. Studies on the development outcomes of social media are sparse because of a lack of reliable macroeconomic data on social media.

Aloysius, Arora and Venkatesh’s study found that, in a smartphone checkout setting, intention to shoplift was driven by experiential beliefs and peer influence. Experiential beliefs and peer influence was recognised as having a stronger effect for prospective shoplifters when compared to experienced shoplifters. The findings also indicated that in an employee-assisted mobile checkout setting intention to shoplift was driven by experiential beliefs. Moreover, peer influence and experiential beliefs had a stronger effect for prospective shoplifters when compared to experienced shoplifters.

Pérez-González, Trigueros Preciado and Solana-González’s study expanded current knowledge regarding security organisational practices and analysed its effects on information security management performance. The authors propose a theoretical research model together with hypotheses. The results validate that information security knowledge sharing, information security education/training and information security visibility and security organisational practices have a positive effect on management performance. The consideration of organisational aspects of information security should be taken into account by academics, practitioners and policymakers in SMEs. The study further recognises the need to develop empirical research on information security focused on SMEs and the need to identify organisational practices that improve information security.

Ikhalia, Serrano, Bell and Louvieris employ mixed methods to evaluate a Facebook application including surveys, laboratory experiments and semi-structured interviews. The escalation of social engineering malware encourages a demand for end-user security awareness measures. Online social network (OSN) users have a higher propensity to malware threats due to the trust and persuasive factors that underpin OSN models. A Facebook video animation application (e.g. Social Network Criminal) creates security awareness and improves the threat avoidance behaviour of OSN users. Results validate the effectiveness of OSNs applications utilising a TTAT–MIP model – specifically the mass interpersonal persuasive (MIP) attributes. Practitioners are able to develop security awareness systems that more effectively leverage the intra-relationship model of OSNs. SNC enable persuasive security behaviour amongst employees and avoid potential malware threats. SNC support consistent security awareness practices by identification of new threats which may inspire creation of new security awareness videos. The structure of OSNs is making it easier for malicious users to undertake their activities without the possibility of detection. Thus, building a security awareness programme, using the TTAT–MIP model, organisations can proactively manage security awareness.

Ratten’s study examines the impact of open innovation on cybercrime in technology firms using semi-structured in-depth interviews. The study seeks to understand the role of open innovation in terms of technology scouting, horizontal collaboration and vertical collaboration on cybercrime activity. The study found that there is a dilemma most technology firm’s face in having a open innovation strategy and how to manage cybercrime. This means that a coopetition strategy is utilised that helps to balance the need to have open innovation but also protect intellectual property. Thus, managers of technology firms need to encourage open innovation as a strategy but manage the cybercrime that comes from sharing too much information in an online context.

Ekelund and Iskoujina demonstrate how to find the optimal investment level in protecting an organisations asset. This study integrates a case study of an international financial organisation with various methods and theories in security economics and mathematics. It combines theory and empirical findings to establish a new approach to
determining optimal security investment levels. The results indicate that optimal security investment levels can be found through computer simulation with historical incident data to find value at risk. By combining various scenarios, the convex graph of the risk cost function has been plotted, where the minimum of the graph represents the optimal investment level for an asset. The results can be used by business practitioners to assist them with decision making on investment to the increased protection of an asset. The originality of this research is in its novel way of combining theories with historical data to create methods to measure theoretical and empirical strength of a control (or set of controls) and translating it to loss probabilities and loss sizes.

In conclusion, the manuscripts collected here confirm the complexity of cybercrime threat with its implications for citizens, consumers, firms and their employees, public sector entities, cities, states, governments, technology and social media providers. Cybercrime represents an ongoing and significant threat driven by multiple agents. Several of the studies presented here offer recommendations and best practice frameworks to combat cybercrime. However, it is apparent that the cybercrime literature remains nascent and the academic community must endeavour to work with all parties to offer ongoing best practice.

Mahmood Hussain Shah  
School of Strategy and Leadership, Coventry University, Coventry, UK

Paul Jones  
School of Management, Swansea University, Swansea, UK, and

Jyoti Choudrie  
Hertfordshire Business School, University of Hertfordshire, Hatfield, UK

References


About the Guest editors
Dr Mahmood Hussain Shah is Senior Lecturer in e-business within the School of Strategy and Leadership, Coventry University, UK. Previously he has held academic posts at the University of Central Lancashire, Cranfield University and the University of Hertfordshire. He is acting as Consultant to several UK banks and online retailers on information security and e-banking management-related issues. His present research interests include identify theft prevention in online retailing and e-banking as well as in health information systems and IS strategy. He has published several books in the area of information security, e-banking and mobile technologies. He has also published many papers in high quality journals such as the *Computer and Human Behaviour*, *European Journal of Information Systems*, *International Journal of Simulation Modelling*, *Health Informatics* and the *International Journal of Information Management*.

Paul Jones is Professor of Entrepreneurship and Innovation at Swansea University and Head of the Business Department. He is currently Editor of the *International Journal of Entrepreneurial Behaviour and Research* and Associate Editor of the *International Journal of Management Education*. Professor Jones is an active Researcher and publishes widely on issues related to entrepreneurial behaviour and small business management. Paul Jones is the corresponding author and can be contacted at: W.P.Jones@Swansea.ac.uk

Jyoti Choudrie is Professor of Information Systems in Hertfordshire Business School. Professor Choudrie has maintained an active media profile in issues such as the digital divide, social inclusion, entrepreneurship, innovation and broadband development. She has also attained expertise in the non-adopters and adopters research area that has led her to understand the digital divide where her research influence lies. Professor Choudrie has published widely in international journals such as *Information Systems Frontiers*, *Journal of Business Research* and *Government Information Quarterly*, where her work is well cited. Professor Choudrie is presently researching older adults and information communication technologies where her interest is on the adoption and diffusion of technologies, with an emphasis on entrepreneurship for older adults. Professor Choudrie is also focused on examining and understanding the digital divide by considering internet access for older adults.
Solutions for counteracting human deception in social engineering attacks

Curtis C. Campbell
School of Advanced Studies, University of Phoenix, Tempe, Arizona, USA

Abstract
Purpose – The purpose of this paper is to investigate the top three cybersecurity issues in organizations related to social engineering and aggregate solutions for counteracting human deception in social engineering attacks.

Design/methodology/approach – A total of 20 experts within Information System Security Association participated in a three-round Delphi study for aggregating and condensing expert opinions. Three rounds moved participants toward consensus for solutions to counteract social engineering attacks in organizations.

Findings – Three significant issues: compromised data; ineffective practices; and lack of ongoing education produced three target areas for implementing best practices in countering social engineering attacks. The findings offer counteractions by including education, policies, processes and continuous training in security practices.

Research limitations/implications – Study limitations include lack of prior data on effective social engineering defense. Research implications stem from the psychology of human deception and trust with the ability to detect deception.

Practical implications – Practical implications relate to human judgment in complying with effective security policies and programs and consistent education and training. Future research may include exploring financial, operational and educational costs of implementing social engineering solutions.

Social implications – Social implications apply across all knowledge workers who benefit from technology and are trusted to protect organizational assets and intellectual property.

Keywords IT strategy, Security, Trust, Human–computer interaction (HCI), Phishing

Paper type Research paper

Introduction
Cybercrime and security breaches continuously generate news media headlines and have become routine reporting. One of the three most pressing risks to organizational performance is the threats of cyberattacks (FM Global, 2017). The cost of a cybersecurity breach to unlucky organizations varies from the millions to the trillions, depending on reports. In 2014, the estimated cost of cybercrime in the USA was around $100bn; however, by 2019, the estimated cost for cybercrime as projected at $2 trillion (Morgan, 2016). In the past decade, US government spending on cybercrime attack defense totaled $100bn, with $14bn budgeted for 2016 alone (Morgan, 2016). While there are projected costs for increasing cybercrime defense, there are bigger costs to protect the safety of the public and security of the nation, if efforts are not made (Shackelford et al., 2014).

Within cybercrime, there is a growing trend toward social engineering, a unique form of cyberattack, because of the simple low cost and high benefit in committing the crime. To bypass networks and technical controls, hackers utilize social engineering attacks through various forms of online communications, technology and deception techniques to persuade and trick individuals to grant access to the company network (Parmar, 2013). Social engineering attempts to influence workers to perform an action that may harm the organization (Hadnagy, 2014). By targeting individuals who often may not know the value of the information they are giving away (Mitnick and Simon, 2006), workers may...
misinterpret the intent that providing information carries little cost to the helper (Mitnick and Simon, 2006), failing to keep an otherwise secure computer system safe from malicious intent (Orgill et al., 2004).

Leveraging trust and the psychology of human behavior and decision making, social engineers aim to penetrate security networks by manipulating the human insider to obtain confidential information (Allsopp, 2009). While many companies are aware of external hacking or cyberattacks, many companies fail to address security controls internally at the employee level (Luo et al., 2013). Once compromised, organizations may lose data, competitive advantage and suffer financial losses. All it takes for cybercrime to be successful is one security exploit or vulnerability.

The escalation of cybercrime attacks targeting human deception supports researching counter defense approaches to social engineering in organizations. Different from direct network hacking, social engineering attacks exploit human decision making and trust to persuade the victim in inadvertently divulging sensitive information (Mitnick and Simon, 2006). These attacks revolve around an instant of decision making in whether or not to trust an action by opening or clicking a link. There is a relationship between an individual’s trust level and an individual’s performance in a computer-supported environment (Cheng et al., 2017).

Compared to the availability of the literature for IT security for cybercrime, the lack of peer-reviewed publications for social engineering defense for social engineering attacks justified the need for the study. Google Scholar returned 2.5m peer-reviewed articles for IT security in cybercrime published over the last decade. Refining the search to reflect literature relating specifically to social engineering attacks for the same period, Google Scholar returned 496,000 peer-reviewed articles, one-fifth of the quantity of references for the broad topic of IT security. Since 2016, Google Scholar reflected only 22,000 peer-reviewed, published articles on the topic of social engineering defense or prevention and 39,000 peer-reviewed articles related to social engineering attack success. The gap in the literature was specific to solutions to implement for countering social engineering attacks targeting human deception. It is this gap in the research in delivering effective social engineering defense and solutions to counteract attacks which served as the aim of the study.

Leaders must understand the psychology behind these targeted intrusions and account for why humans are easily deceived. Therefore, this study investigates the three most important issues related to social engineering and explores future solutions for counter defense. It provides an important contribution as it addresses the under-researched phenomenon of solutions for counter defense related to social engineering attacks that can be applied to any organization.

The specific problem is without organizational strategies or solutions to deliver effective countermeasures, the key cybersecurity risks of unauthorized access to classified, sensitive or personal data from social engineering attacks will continue to increase (LeClair and Keeley, 2015). Leaders may lack effective security strategies and solutions to eliminate human deception and the risk of success in social engineering attacks.

Review of the literature
In past few decades, the advent of the computer brought about the need for secure communication that was private. Secure communication led to data confidentiality, data integrity and authentication (Bellare and Rogaway, 2005). These led to the development of cryptography or encryption to block data from being deciphered on ATM cards, computer passwords and electronic commerce. During this period, information security processes and procedures were technical designs to prevent entry.

Over time, information security processes evolved from a technical design to behavioral factors (Dunkerley and Tejay, 2011). This evolution recognized the human individual in the
information security investment (Dunkerley and Tejay, 2011). Next came the advancement and adoption of the ease and familiarity of sharing information through technology.

Organizations began to implement technical controls and human-based controls to prevent gaps in computer systems (Dhillon et al., 2007). Technical controls included hardware or software for preventing and reducing cybercrime most commonly known as password tools, encryption, firewall and anti-virus software. Human-based controls included formal controls such as organizational policies for acceptable behavior, acceptable use and employee and supervisor responsibilities and informal controls such as ethical issues and attitude awareness, self-control, accountability and proper conduct (Dhillon et al., 2007).

Technical controls in security defense
From 1998 to 2007, technology developments for preventing intrusion dominated information security research (Wang, 2012). During that decade, the main research topics were information security assessment and management, information security economics, technical aspects of information security, development and monitoring of information systems (IS) and cryptographic technology design (Wang, 2012).

During that same time, global internet threats transitioned from disabling infrastructure to targeting people and organizations, endangering businesses and governments (Bhatia et al., 2011). Developments in technology included common security infrastructure and intrusion detection systems designed to detect multiple operating systems in information technology (Bhatia et al., 2011). Honeypot data collection technologies, computer or network services used as traps for detecting and detouring robot networks (botnets), were discussed along with their developmental importance for the future of IS (Bhatia et al., 2011).

Cryptography. Cryptography became a technical control for blocking secure communication with attackers (Rivest, 1990). It involved constructing and analyzing protocols that block attackers by changing information from a readable state to unreadable (Bellare and Rogaway, 2005). Over time, cryptography became known as encryption (Bellare and Rogaway, 2005) to describe a method for changing the readable state to a protected and unreadable state.

Non-technical controls in information security defense
Previously, security issues were addressed from a technical standpoint but later extended past technology to the information security management role (Soomro et al., 2016). The literature review for this study focused on the extension of non-technical factors of information security defense such as organizational factors, behavioral factors and environmental factors under management responsibility (Soomro et al., 2016). For successful security processes, specific managerial activities may play an important role (Soomro et al., 2016). However, non-technical factors of a successful implementation have received less attention from the research community.

Formal controls. Formal controls evolved from organizational measures such as acceptable behavior policies, procedures and standards for checks and balances (Beebe and Rao, 2005). Later, the IT security infrastructure expanded to include formal controls such as organizational risk management policies, IS security policies, standards, checklists and the technology aspects of security (Dunkerley and Tejay, 2011). Today, formal controls include physical security and information security, and the human’s knowledge is related to his or her technical expertise and user awareness of security policies and organizational regulations (Dunkerley and Tejay, 2011).

Organizational factors. The organizational areas of culture and security awareness also received attention (Dunkerley and Tejay, 2011). Organizational optimization is also
important in a successful information security implementation. Research in this area suggested that organizational goals and information security controls should be in balance to promote the delivery of value by the organization (Dunkerley and Tejay, 2011).

**Informal controls.** Informal controls include ethical issues and attitude awareness, self-control, accountability and proper conduct in organizations. In information security, informal controls in technology are a result of direct and easy access for individuals to interact with one another. Physical barriers have eroded as technological limitations and virtual borders are now completely open where one user can communicate around the globe with another in milliseconds (Bojanic and Budimir, 2011).

Overall, the advances of cyber-related technologies have caused social engineering efforts (Roberts and Jackson, 2008), creating new moral and ethical consequences, and the need for different psychological competence (Roberts and Jackson, 2008). Most major cyberattacks on US corporations within the past three years included social engineering (O'Harrow, 2012). Recent social engineering hacks include MacEwan University, defrauded out of $11.8m (Seals, 2017), Google and security giant, RSA Security (O'Harrow, 2012). Often, the human deception occurs without the individual realizing the manipulation. No matter how much funding and resources are spent on network security with firewalls, security appliances and encryption, the human sitting behind the phone or computer remains vulnerable to data theft from hackers using social engineering techniques.

Security trends require a holistic approach to cover the various vulnerabilities in an IS infrastructure (Ifinedo, 2012). This holistic approach would typically include organizational risk management policies, IS security policies, standards and checklists for organizational employees and the technology aspects of security (Dunkerley and Tejay, 2011). According to Ifinedo (2012), organizations that consider technical and non-technical aspects of information security are typically more successful in their efforts to secure their information assets.

**Theoretical framework**

To guide the research, two technical and two non-technical theories served as the analytical framework. The general deterrence theory and Dhillon’s theory of balanced control describe technical processes in implementing security measures (Lee et al., 2004) and balancing technical, formal and informal types of controls organizations may implement as protection and defense (Dhillon et al., 2007).

**General deterrence theory**

The general deterrence theory was developed to describe the technology and processes involved in implementing security measures to prevent computer abuse (Lee et al., 2004). The aim is general prevention using punishment or other consequence to deter the activity. Thus, using anti-virus software, enforcing password and computer security policies, organizations attempt to deter attacks from the outside and protect individuals from yielding to a message (Lee et al., 2004).

**Balanced control theory**

Dhillon’s balanced control theory posited that unintentional insider threats result from the imbalance of technical, formal and informal controls. The aim is to cover all technical options and human controls. The design of the IT security program includes technical systems, formal policies and company culture as opposed to a physical security-based monitoring. The principles surrounding Dhillon’s balanced control theory identified that balance is needed and that negative effects may result from an imbalance in the three controls (Dhillon et al., 2007).
Two non-technical theories to guide the research were the behavioral trust theory and the cognitive response theory. Both were useful in understanding trust in digital, automated communication (O’Harrow, 2012) and human factors that trigger thought processes in relation to information given (Petty et al., 2009). These theories guided an understanding of human factors that trigger deception. The challenge becomes understanding when behaviors are inappropriate and ascertaining which may result in unwanted risk or asset exposure (Manjak, 2006).

**Behavioral trust theory**
Individuals in organizations want to trust that digital communication is safe (O’Harrow, 2012). The behavioral trust theory supported reasons individuals were not able to recognize social engineering attempts. The behavioral theory of trust addressed trust in automated information and offered countermeasures for users’ uncertainties that result from trusting an application (Hoffman and Sollner, 2014).

**Cognitive response theory**
The cognitive response theory guided the research for human–computer interaction within IT security effectiveness. The cognitive response theory was developed to describe the processes involved in yielding to a message (Petty et al., 2009) where the individual depended on their own thoughts in relation to the information given. The theory contended that the impact relates to the extent the individual can explain or process their own thoughts regarding the information (Petty et al., 2009). Petty et al. (2009) indicated an individual response participated in the persuasion process by relating message elements to acquired and existing information (Petty et al., 2009). Petty’s research supported the concept that people’s reactions to other people, objects or messages can be positively or negatively affected depending on the compelling nature of their initial thoughts (Petty et al., 2009).

**Research question**
The gap in research for solutions and strategies to counteract social engineering attacks was the aim of the research paper. The research approach was an asynchronous, anonymous effort to gather cybersecurity experts’ opinions with the intent of reaching consensus on effective solutions and security approaches for countering social engineering attacks or preventing attacks within organizations. The intended outcome was a possible solutions-based framework for an effective IT security program. Therefore, one research question served as the basis for the study:

*RQ1.* What possible future solutions and strategies for social engineering defense can organizational leaders implement for preventing and inhibiting social engineering attacks?

**Research methodology and design**
To investigate the under-researched phenomenon, a qualitative method was selected for its exploratory approach. The Delphi design fits the purpose of aggregating and condensing experts’ opinions, ultimately seeking consensus of the three most likely future strategies and solutions for implementing social engineering defense for countering and preventing social engineering attacks. Since the Delphi design is an accepted form of structuring communication among experts to provide valuable contributions and solicit expert opinions (Linstone and Turoff, 2002), it provided the correct structure of gathering anonymous opinions into a desired outcome of group consensus for future strategies and solutions for inhibiting and preventing social engineering attacks (Skulmoski et al., 2007). The Delphi design is particularly appropriate for determining subjective judgments on a collective basis
and helping group participants to make decisions and develop agreement about the problem.

Delphi research has been perceived credible because experts’ collective responses may lead to suggested future best practices (Linstone and Turoff, 2002), and the research question sought leaders’ judgment and opinions on future best practices (possible effective approaches, solutions, strategies, policies and processes).

The validity of the Delphi design comes from the wisdom of crowd type research, stating group judgments under certain conditions are valid and reliable (Jorm, 2015). The strength of the Delphi is anonymity and confidentiality to prevent dominance by individuals and allows expert participants to interact, compare and even rethink opinions without influence and pressure of others (Sharkey and Sharples, 2001). Conducted through online surveys, the Delphi provided an interactive, iterative process that was anonymous, asynchronous and delivered aggregated, controlled feedback (Landeta, 2006). A unique characteristic of the Delphi is that the facilitator forges consensus into each stage of data collection, creating agreement in the decision process (Rayens and Hahn, 2003). Three Delphi rounds were used for generating responses (Loo, 2002).

Setting, population and sample
The geographic setting was across the USA, but the study, conducted in a virtual setting online, allowed participants the freedom to transfer their expert opinions asynchronously and electronically over the internet in three survey rounds, despite their time zone or location. The sampling method was purposive. Within the population of IT security professionals, a target population within the community of the Information System Security Association (ISSA) was selected based upon experience and expertise in IT security, certifications, social engineering publications, information security research and prior experience in IT security programs. Only ISSA members within the USA with ten years or more IT security leadership experience, CISSP or other IS security certifications, active membership status in ISSA for a minimum of five years and published articles or presentations on social engineering at the national ISSA conference level qualified for study participation. The population was appropriate for the focus of the study on potential social engineering solutions and strategies for IT leaders to deploy in enterprise organizations. Within the target population, a sample of 25 participants comprised the sampling frame. By confining the study population according to such criteria, the relevance of the findings was enhanced.

Materials and instruments
The Delphi design included a research question, feedback and participation of the expert panel on possible strategies and solutions for an effective defense in countering and preventing social engineering attacks. Electronic survey methods facilitated data collection by providing e-mail invitations to participants and featured e-mail notification for presenting questions. Two electronic software tools were used: Constant Contact secure e-mail platform, for anonymous e-mail distribution and Survey Monkey, software application for designing and implementing customizable, interactive surveys. The Constant Contact secure e-mail platform provided the instrument to send participants an e-mail notification including the survey hyperlink for each round. The e-mail did not include the population’s e-mail distribution list in the recipient header; therefore, no other participant contact information was given. Once the link was e-mailed to participants, they were able to independently click the link to go directly to the secure survey.

Survey Monkey provided user-friendly templates to create an expanded survey design to insert text for open-ended responses in Rounds 1 and 3. In Round 2, Survey Monkey provided a template for customizable drop and drag text boxes to automatically rank or sort responses in order. Through a secure web-based site, anonymity through internet delivery...
occurred by blocking participants’ computer IP address but allowed panelists’ responses to be collected without identifiers. Survey Monkey provided a secure section to export and add e-mail contacts for selection of participants, responses, monitoring and reporting and for review of rounds.

Round 1 included one open-ended question answered by the panelists to provide, in their expert opinion, the three most significant issues about social engineering organizations must address now and in the future. Automated survey notification alerts were sent to the researcher’s e-mail when a new Survey Monkey survey response was received. All responses were compiled and the top 10 responses were included in Round 2. Round 2 listed the top 10 responses in alphabetical order and requested panelists to rank issues in order of most important to least important with the option to provide comments for clarification. Round 3 survey was developed from calculations rating the top 3 most important ranked survey items from Round 2. It provided written text explanations for implementation asking participants to explain how they would implement the top 3 solutions. A summary of the data reduction is described in the data collection and analysis procedure section.

An informed consent form and letter of agreement addressed ethical procedures prior to the data collection. Participants who satisfied the requirements of an expert panelist received the informed consent form and letter of agreement before the first round of the Delphi research. The letter of agreement advised study participants of their anonymity, provided data collection explanation, and how data would be used, maintained and stored for research purposes. The letter informed participants that if the results of the research were published, names would be withheld and only general descriptions would be given pertaining to participant positions and experience. Each expert panelist signed, scanned and returned the informed consent agreement for assured individual privacy and compliance with the law (Cooper and Schindler, 2006).

The panel was requested to provide their opinions on significant issues related to social engineering and strategies as countermeasures for social engineering defense. The structure of the Delphi rounds began by seeking open-ended responses in Round 1, followed by ranking in Round 2, and an agreement or disagreement in Round 3 and elaboration of proposed solutions for implementation. Round 1 question was, “In your opinion, what are the three most significant issues related to social engineering that you believe organizations must address now, and especially in the future?” This question was designed to collect three short responses and the chance to comment why the panelist chose the responses. Those different explanatory comments were later analyzed using textual analysis. A total of 25 participants completed Round 1, but 2 participants were withdrawn because of inadequate responses, leaving 23 remaining experts, each providing three unique issues. In all, 69 issues were collated and combined based on similar words, meaning, themes and ideas. An Excel spreadsheet was created to keep track of how many times each solution was suggested, with the list consolidated into the top 10 most common issues for Round 2 prioritization.

In Round 2, 23 panelists were provided the list of top 10 issues the group had provided. The list was arranged in alphabetical order, with no information provided to the panelists as to which of the top 10 issues were noted most often. This was done to avoid the possibility of a group bias where participants might be swayed because of a majority opinion. The wording of the ten issues in the list reflected the most common wording by the panel members. Panelists were asked to take this list of ten items and then arrange them in order of importance with the most important ranked as No. 1 and the least important as No. 10, acknowledging that all ten issues were important. Panelists were instructed not to assign the same number to more than one issue, to ensure no duplicates. Out of 23 panelists, 21 completed Round 2 by ranking the issues in order of importance, and the rankings were entered into an Excel spreadsheet whereby averages were calculated for each of the ten issues. The averages provided an overall group ranking for the ten issues allowing the
issues to be sorted from lowest to highest averages (No. 1 being the most important). The top 3 issues receiving the lowest average score provided the top ranked, most important issues for Round 3.

In Round 3, panel members were given the top 3 ranked issues and asked to offer detailed, specific possible solutions that may resolve or correct these three issues with direction to expand and elaborate on any details they felt were important to the solutions. The texts from these responses of 15 panel members were included in textual analysis, and 115 explanations resulted (Table I).

NVivo 8 software, along with Saldana’s InVivo and Focused Coding methods, provided the thematic coding methods for analysis of the collective expert panel’s results from each round and prioritized data, with the top 3 responses categorized and coded from contextual comments (Saldana, 2013). Responses were further analyzed with Saldana’s (2013) InVivo First Cycle coding to determine if additional opportunities existed for coding or further reducing the data (Saldana, 2013). Additional opportunities for coding included second cycle coding using the Focused Coding method to reorganize and reanalyze data coded through the first cycle method (Saldana, 2013).

Findings

Round 1 survey question produced 69 significant issues related to social engineering which were recorded and analyzed into four areas associated with the research question: user awareness; security policy, program, practices and procedures; compromised data; and ongoing training and education. A total of 78 percent of panelists identified a compromised network from successful phishing attacks as one of the most significant issues related to social engineering attacks. A total of 69 percent of panelists included end-user awareness and compromised information as the most significant issues related to social engineering attacks. A total of 60 percent of panelists identified both bad employee practices and habits and compromised name/reputation and breach of information as the most significant issues. Subcategories were grouped into an alphabetized list for non-biased order interpretation of the list, and to prepare for Round 2, the researcher compiled the top 10 most mentioned significant issues.

The top 10 Round 2 responses in alphabetical order:

(1) Three most significant social engineering issues:

- awareness of the end user of social engineering threats and ever-changing techniques;
- bad practices and habits by employees;
- compromised data: compromised info including trade secrets, name and reputation, company records, compromised network with “hooks” leading to theft, blackmail or espionage;
- education (ongoing) on non-tech savvy employees, including executives and assistants;
- ineffective security practices or lack of security practices;

<table>
<thead>
<tr>
<th>Panelists</th>
<th>Comments</th>
<th>Text segments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Round 1: number of panelists = 23</td>
<td>23</td>
<td>69</td>
</tr>
<tr>
<td>Round 2: number of panelists = 21</td>
<td>21</td>
<td>10</td>
</tr>
<tr>
<td>Round 3: number of panelists = 15</td>
<td>115</td>
<td>112</td>
</tr>
</tbody>
</table>

Table I. Summary of participants and data for each survey round
lack of information around frequency of attacks;
- lack of practice on phishing programs;
- practicing good password management – including strong, changed, not repeated across systems;
- practice in user recognition and user reporting of suspicious e-mails; and
- prevention of employees clicking on phishing e-mails with a hidden link.

Round 2 survey served to rank and prioritize the top 10 issues in order of importance. Panelists assigned a numeric value according to a scale from 1 to 10. All rankings were added for each panelist, and then divided by the number of issues. This produced an overall average rating for each item based upon the order of ranked order of importance from the panelists. Table II shows the top 10 ranked responses with their average rating by highest rating to lowest rating. Issues with a lower average indicate a higher importance as the ranking order was based upon 1 (most important) and 10 (least important).

This served as the turning point for the study whereas the three most significant issues related to social engineering, on a 1–10 scale, were determined by panelists as: compromised organizational data; ineffective or lack of organizational security practices; and ongoing education and training of employees. Of 21 panelists, 9 ranked compromised data as the most significant or number 1 ranked issue. Of 21 panelists, 7 ranked ineffective or lack of security practices as the second highest ranked issue. Six panelists equally listed ongoing education and training of non-tech savvy employees, including executives and assistants, as the third highest ranked social engineering issue. Three panelists listed bad practices and habits by employees as the number 1 ranked significant issue facing organizations in social engineering attacks. Two panelists listed end-user awareness of ever-changing social engineering threats and techniques as the highest ranked or number 1 most significant issue while two panelists ranked practicing good password management as number 1 most significant.

Panelists were given the option to agree or disagree with the findings, and interestingly, the majority of panelists disagreed in the (ranked) order of importance of the related social

<table>
<thead>
<tr>
<th>Three most significant social engineering issues</th>
<th>Topic area</th>
<th>Average</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lack of information around frequency of attacks</td>
<td>User awareness</td>
<td>7.19</td>
</tr>
<tr>
<td>Prevention of employees clicking on phishing e-mails with a hidden link</td>
<td>User awareness</td>
<td>7.14</td>
</tr>
<tr>
<td>Lack of practice on phishing programs</td>
<td>Practice, programs, Policies, procedures</td>
<td>6.0</td>
</tr>
<tr>
<td>Practice in user recognition and user reporting of suspicious e-mails</td>
<td>Practice, programs, Policies, procedures</td>
<td>5.7</td>
</tr>
<tr>
<td>Practicing good password management – strong, changed, not repeated across systems</td>
<td>Practice, programs, Policies, procedures</td>
<td>5.5</td>
</tr>
<tr>
<td>Awareness of the end user of social engineering threats and ever-changing techniques</td>
<td>User awareness</td>
<td>5.2</td>
</tr>
<tr>
<td>Bad practices and habits by employees</td>
<td>Practices, programs, Policies, procedures</td>
<td>5.0</td>
</tr>
<tr>
<td>Education (ongoing) on non-tech savvy employees, including executives and assistants</td>
<td>Practices, programs, Policies, procedures</td>
<td>4.8</td>
</tr>
<tr>
<td>Ineffective security practices or lack of security practices</td>
<td>Practices, programs, Policies, procedures</td>
<td>4.1</td>
</tr>
<tr>
<td>Compromised data: compromised info, trade secrets, name and reputation, company records, compromised network</td>
<td>Compromised data</td>
<td>3.95</td>
</tr>
</tbody>
</table>

Table II.
Round 2 ranked responses by topic area and highest average to lowest average
engineering issues but agreed with the top 3 issues (topics). Findings showed that panelists preferred that the order of the second and third place ranked issue should be reversed. This was not surprising to the researcher given the second and third issues could overlap (Figure 1).

The 15 panelists’ responses reflected a distributed opinion of 6 experts in agreement and 7 experts in disagreement or the ranked order of importance. Disagreement responses included panelists’ preferences for re-ranking and reordering the top 3 issues with associated explanation. Two responses listed partial agreement or disagreement. Table III lists panelists’ agreement or disagreement and includes panelists’ explanations.

Despite non-consensus of the ranked order of the top 3 issues ranking, findings from Round 3 showed that panelists reached consensus of social engineering defense solutions of both technical and informal controls. Experts identified many challenges related to those solutions such as competing organizational priorities, management agreement and monitoring, limited resources and high costs contributing difficulty in implementing organizational solutions.

Findings included three possible solutions and strategies for preventing or inhibiting social engineering attacks in organizations: security solutions should implement balanced control in both technology and behavioral controls; security solutions should implement

---

**Notes:** Highest ranked issues related to social engineering. This figure displays the three highest ranked issues by panelists in order of importance.

---

<table>
<thead>
<tr>
<th>Agreement or disagreement with order of top 3 issues</th>
<th>Number of panelists</th>
<th>Panelist elaboration and reasons</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agreement</td>
<td>6</td>
<td>Based on impact to organization</td>
</tr>
<tr>
<td>Disagreement</td>
<td>7</td>
<td>Ongoing education received 5 votes for the number 1 ranking followed by ineffective security practices, with 2 votes for the number 1 ranking</td>
</tr>
<tr>
<td>Did not agree or disagree</td>
<td>2</td>
<td>Reasons included “apples and oranges” explanation and rebuttal with the statement of ineffective or lack of security practices in organizations</td>
</tr>
</tbody>
</table>

Table III. Consensus of agreement with ranked order of top 3 issues
user policies, programs, practices and procedures; and security solutions should educate and train user behavior continuously.

Panelists responded to the second question in Round 3 with proposed solutions and associated challenges for organizations to counter social engineering attacks. Of 15 panelists, 13 ranked both mandatory training and security practices and policies as the best solutions to counter social engineering attacks but listed challenges of limitations of resources, financial costs, time and the measure of precision or uniformity. To implement security practices and policies, panelists stated the challenge of reaching all employees. Of 15 panelists, 10 expressed security controls on corporate systems as the most effective solution to counter social engineering attacks. Panelists’ explanations of control measures as solutions included multiple facets of e-mail and gateway filtering, multifactor authentication, layering, user privilege control and remediation, access control, network monitoring, backups and perimeter controls.

Of 15 panelists, 5 included phishing campaigns as an effective solution to counter social engineering attacks. Repeated practice and rewards for recognition were included as key components of a successful campaign. Panelists included the challenge of losing employee trust over time with phishing campaign awareness and repeated practice.

Of 15 panelists, 4 listed security awareness, network monitoring, remedial training and consequences for user infractions as solutions to counter social engineering attacks. Panelists included the cost of resources as a challenge to implement security awareness. Management agreement and enforcement were noted as challenges to incorporate and force remedial training.

Of 15 panelists, 3 believed that testing and testers who continuously perform audits and tests were the solution to implement for countering social engineering. Panelists believed that users who fail testing should receive remedial training to understand the impact to the organization. The remaining 3 of 15 panelists included frequent password change management and audits of user machines as solutions with the challenge of time and resources to audit individual machines. Table IV shows panelists’ solutions with associated challenges.

**Theoretical framework alignment**

Findings showed that general deterrence theory and behavioral trust theory most closely aligned with the manipulations and methods behind social engineering attacks. Both explain false trust and lack of perceived risk in electronic information by the employee. Dhillon’s balanced control implementation theory most closely aligned with the future solutions provided in this study’s results.

Dhillon’s theory of balanced control implementation balances technical, formal and informal controls. The theory’s principles maintain balance from all controls, not just one IT security control. Findings for the top 3 solutions from panelists’ responses are synthesized with their supporting theories and discussed below.

**Finding 1: security solutions should implement balanced control in both technology and behavioral controls.** Panelists suggested that security solutions based on technology (perimeter security, restricting access, and authentication using technology permissions and parameters) would be best in enforcing security. Security solutions based on behavior concepts to change employee behavior were necessary. Explanations for balanced control were that behavioral control and technical control are layered, a term indicating multiple types of control, and balanced control involves systems and people working together. A second supporting explanation for a balanced control solution was explained as changing
employee thought patterns and behaviors in technology use. Panelists expressed that security solutions should incorporate both technology monitoring and people monitoring.

Dhillon’s theory of balanced control explained IT security effectiveness as a result of balanced technical, formal and informal controls. This balance, according to Dhillon et al. (2007), minimizes opportunity and constrains criminal behavior through technological and sociological influences (Beebe and Rao, 2005). Technical controls are software and hardware related and include firewalls, password protection and encryption. Formal controls include acceptable conduct and organizational policies outlining responsibilities and supervision. Informal controls include behavior related to conduct, ethics, accountability and ethical awareness (Dhillon et al., 2007). Dhillon’s theory supported Finding 2 for security effectiveness.

**Finding 2: security solutions should implement user policies, programs, practices and procedures.** Supporting comments for solutions related to the importance of having internal guidelines. One explanation of the solution was that strict policies and procedures must accompany best practices. A caveat included in the solution was a warning that consequences from not adhering to policies that should be enforced explaining policies direct employee actions, behavior and responses. A fourth explanation for the solution was that security programs to implement for social engineering should involve practices, regular testing, with continuing education.

Overall, general deterrence theory is based upon deterrence. Creating countermeasures in threat elimination, risk mitigation or curbing computer crime may dissuade individuals from committing unintentional acts from social engineering attempts (Schuessler, 2009). Findings recommended including consequences for not following countermeasures through the severity of punishment if caught. Suggestions included several levels of consequences for first, second and repeat offenders who did not follow policies, practices, training and reprimands. Current research adds that an information security program must include and be managed by a set of information policies, procedures and standards stemming from understanding the organizational mission (Landoll, 2017). Information security policies,

<table>
<thead>
<tr>
<th>Solution</th>
<th>Responses (n)</th>
<th>Responses (%)</th>
<th>Challenges</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mandatory training including concrete examples</td>
<td>13</td>
<td>86</td>
<td>Monitoring training and follow through on documentation. Not enough bandwidth. Challenge of no time, busy. Less precise and not uniformly effective. Requires supervisory motivation and commitment. Users may become tone-deaf to training</td>
</tr>
<tr>
<td>Security practices and policies</td>
<td>13</td>
<td>86</td>
<td>Getting the message to all employees</td>
</tr>
<tr>
<td>Security controls</td>
<td>10</td>
<td>66</td>
<td>Removing privileges may not always be possible. Requires overhead</td>
</tr>
<tr>
<td>Continuing education and communication</td>
<td>8</td>
<td>53</td>
<td>Not foolproof. Requires real expertise and resources. Student must be open to listen and read the communications</td>
</tr>
<tr>
<td>Phishing campaigns</td>
<td>5</td>
<td>33</td>
<td>Lose trust of employees. Employees may become tone-deaf to repeated campaigns</td>
</tr>
<tr>
<td>Remedial training</td>
<td>4</td>
<td>26</td>
<td>Management agreement. Needs to be anonymous</td>
</tr>
<tr>
<td>Consequences for infractions</td>
<td>4</td>
<td>26</td>
<td>Requires upper management agreement. Political suicide in many organizations</td>
</tr>
<tr>
<td>Security awareness</td>
<td>4</td>
<td>26</td>
<td>Not foolproof. Require resources to do frequently</td>
</tr>
<tr>
<td>Network monitoring</td>
<td>3</td>
<td>20</td>
<td>Management agreement</td>
</tr>
<tr>
<td>Security testing using testers</td>
<td>2</td>
<td>13</td>
<td>Time and resources</td>
</tr>
<tr>
<td>Audit user machines</td>
<td>2</td>
<td>13</td>
<td></td>
</tr>
<tr>
<td>Password change</td>
<td>2</td>
<td>13</td>
<td></td>
</tr>
</tbody>
</table>

Table IV. Panelists’ solutions and challenges by number and percentage of responses
procedures and standards are developed to be an integral part of the organizational mission with relevance to governance and oversight, budget support and compliance (Landoll, 2017). Countermeasures of duplication and training, backups and reprimands serve to eliminate or mitigate such risks (Schuessler, 2009).

*Making solutions should educate and train user behavior continuously.* Solutions provided by panelists emphasized that associated success in preventing social engineering attacks is a direct result of frequent, ongoing, dedicated and customized training. Employee-focused educational development was listed as a best practice to be incorporated. Results included educating employees on behavior, tactics and tricks to change thought patterns to help interpret the fake artifact from the real thing. Other supporting themes included policy and procedure-based training that combines written, visual and oral communication. Panelists repeated the theme of frequency of ongoing and continuous training and education. Finally, education and training should be supervisor-motivated to enforce completion and monitoring. Research showed that employee noncompliance with IS security policies is a key concern for organizations. Security solutions lose their efficacy, if users do not comply with security policies (Puhainen and Siponen, 2010). The literature added that there is a need for IS security training approaches that are theory-based and empirically evaluated (Puhainen and Siponen, 2010).

The behavioral trust theory explained the reasons that individuals are unable to recognize social engineering attempts. Founded on understanding human factors of trusting digital data, this theory may help in developing solutions to prevent social engineer attacks. Organizations may apply the behavior trust theory to evaluate continued education and training practices.

Three solution areas

Findings derived from thematic analysis of the panelists' responses were combined into three solution areas: compromised data; policies and procedures; and user awareness and training. Illustrated in Figure 2, the top 3 solution areas were matched to similar meaning to the issue and described below.

**Target area 1: compromised data.** Panelists ranked the importance of compromised data within the organization as the number 1 significant issue in social engineering attacks. The importance of protecting trade secrets, company records, compromised name or reputation, identify theft, blackmail or corporate espionage from compromised information were explained as components of compromised data. Panelists agreed that social engineering attackers targeting unintentional insider threats seek to compromise the organization through financial loss, disruption or information compromise (Greitzer et al., 2014).

**Solutions to address issue 1.** Panelists suggested security solutions based on perimeter security, restricting access and authentication using technology permissions and parameters to aid in enforcing security. Panelists discussed the importance of protecting proprietary data in organizations as the highest concern potentially causing the greatest harm to organizations. Those that disagreed with the ranking expressed that compromised data was an outcome of a successful engineering attack and was not a solution within itself or a reason for a failure.

**Target area 2: security practices: policies and procedures.** The second highest ranked issue was ineffective practices or lack of practices implemented in organizations to prevent...
social engineering attacks. Panelists identified lack of best practices in organizational policies and procedures as significant issues facing organizations related to countering social engineering attacks. Panelists noted that attackers succeed if one employee unintentionally succumbs. Panelists explained that an organization’s strategy to combat UIT attacks must be comprehensive and include up-to-date security practices (Greitzer et al., 2014) and security solutions enabling individuals (employees and managers) to recognize cybersecurity concerns and react accordingly and appropriately are essential (Ani et al., 2016). Panelists indicated that organizational leaders have responsibility for developing information security best practices through policies and procedures to keep up with the rapidly changing and sophisticated social engineering attacks that are well crafted to defeat even the best organizational countermeasures (Greitzer et al., 2014).

Solutions to address issue 2. Ineffective or lack of security practices including policies and procedures ranked the second highest and solutions included frequent, ongoing, dedicated and customized training as effective practices to implement. Panelists explained that ineffective or lack of organizational security practices causing potential breach to the network for accessing organizational data must be corrected. Comments showed that the most important issue in social engineering attacks resulting in compromised data is a consequence of lax security practices and procedures. Panelists provided solutions of identified practices and procedures including monitoring, authentication, password management, security programs and enforcing and rewarding practices on user reporting, user recognition and user practice. Panelists indicated that developing effective programs and practices throughout the organization is the balance of security and operational goals.

Target area 3: ongoing education, user awareness and training. The third highest ranked social engineering issue indicated the need to train people. Results agreed that organizational leaders have a responsibility to develop and maintain user awareness and training of social engineering attacks (CERT Insider Threat Team, 2013). Panelists noted the importance of user awareness since attacks involving direct communication and electronic interaction use human psychology to deceive victims for financial or other sabotage (Greitzer et al., 2014).

Solutions to address issue 3. Solutions included ongoing training and education as steps toward prevention and explained that the root cause of social engineering attacks stems from a lack of continuity in training or ongoing education. Many panelists explained that the key in implementing training and education was the frequency of the training and education, defined by panelists as ongoing and continuous. Educating non-tech savvy employees in the recognition and reporting of suspicious electronic or direct communication activity was identified as a necessary solution. The literature added to the panelists’ comments explaining key concerns are employee noncompliance with IS security policies, specifically in the approach of training. Current research showed that users who do not comply with IS security policies cause security solutions to lose their efficacy (Puhainen and Siponen, 2010). Of the different information security policy compliance approaches, the most commonly mentioned approach in the literature is training (Puhainen and Siponen, 2010).

Limitations
Limitations of the study existed since the findings were based on consensus according to an entire group’s judgment (Linstone and Turoff, 2002). The Delphi design has come under scrutiny for its limitations inherent to the research design in that results are dependent on the consensus. One limitation of the Delphi was the correct structure and importance of the first round’s questions (Delbecq et al., 1975). Since second and following questionnaires rely on the first questionnaire, a limitation may occur if an alignment regarding the first round does not reflect the key elements (Franklin and Hart, 2007).
A second limitation was forging consensus. The way consensus is determined is varied among researchers, and the lack of agreement among what constitutes consensus is one of the critiques of the Delphi design (Linstone and Turoff, 2002). Reaching consensus among the study’s experts was considered a limitation of this study. Although the participants reached consensus on the solutions and strategies, not all panelists agreed with the top 3 ranked order of the most significant issues, expressing the order of the second and third place ranked issue should be reversed.

A third limitation was sample size and the appropriate number of participants for the study. If the response rate is considered too low, this may result in the need to analyze the sample size in terms of potential limitation. While research suggested a sample size of 10–15 people (Hsu and Sandford, 2007), this study included a sample size of 25 who began the study and 15 which completed all three rounds.

Conclusion

Social engineering attacks have been part of most major cyberattacks on US corporations and are ballooning as one of the cybersecurity threats facing individuals, businesses and the nation today (LeClair and Keeley, 2015). Social engineering defense remains a weak link in managing IS security because it manipulates human nature, not technology controls (Luo et al., 2013). Technology tools and security software have prevented common technical attacks from penetrating organizations but have not prevented social engineering attacks targeting individuals. The problem of countering social engineering attacks served as the foundation of the study with the specific problem of what future solutions cybersecurity professionals may apply as counter defense in social engineering attacks.

The panel of security experts indicated that the three most significant issues related to social engineering were compromised organizational data, ineffective or lack of organizational security practices and ongoing education and training of employees in social engineering. To resolve these issues, the panel suggested coordinated security solutions with both technical and informal controls of layered security solutions of security authentication and education, continuing education and training, security practices, policies and procedures, frequent communication with varied media and employee education development and accountability.

Findings showed that panelists supported the value of a balanced controls program within information security to support employee development in recognizing human deception and security defense and to thwart entry into the privacy and security of the organization from one unintentional user access. Panelists noted that efforts to counter social engineering attacks must be ongoing and continuous through various techniques. Interestingly, information security leaders also identified many challenges related to implementing solutions such as competing organizational priorities, management agreement and monitoring, limited resources and high costs contributing difficulty in implementing organizational solutions.

Implications for future practice are related to solutions for dealing with human deception and the impact of implementing effective security policies and programs and consistent education and training. Directions for future research may include exploring the costs of implementing solutions from a financial and operational perspective in organizations. Future research may expand the knowledge for developing a comprehensive plan of action to include staffing and financial resources to advance the inclusion of social engineering education and training in information security policies and practices. Future researchers might consider exploring real costs to developing and implementing organizational solutions for different size organizations.

Second, a future quantitative study of statistical measurement of compliance with policies, program and training as compared to social engineering techniques regarding the
quantity of successful attempts may further the research. Third, the use of a quantitative research design to measure the financial impact of social engineering attacks would continue the research. Finally, future quantitative research may include testing the impact of variables of social engineering controls, policies and practices and education/training on the outcome (Babbie, 2013) of preventing a successful social engineering attack.

Cybercrime remains one of society’s most pressing issues, and while social engineering attacks represent a small segment of cybercrime, the impact can be devastating to organizations. The results of this study advanced the field of cybersecurity to include continuous types of security training, practices and procedures, frequent communication and employee development with accountability as organizational solutions to counter human deception to prevent or inhibit social engineering attacks. The study reinforced the need to include social engineering solutions as part of an organization’s overall strategic cybercrime plan.

References


Further reading


**Appendix 1**

<table>
<thead>
<tr>
<th>Significant issue topic area</th>
<th>n = number of panelists who mentioned</th>
<th>% of panelist responses</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>User awareness</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>End-user awareness of social engineering threat</td>
<td>16</td>
<td>69</td>
</tr>
<tr>
<td>User awareness to not click on files and links</td>
<td>16</td>
<td>69</td>
</tr>
<tr>
<td>Users not given enough information how (frequently) attacks happen</td>
<td>9</td>
<td>39</td>
</tr>
<tr>
<td>User recognition and reporting of suspicious e-mails</td>
<td>9</td>
<td>39</td>
</tr>
<tr>
<td><strong>Policy, program, practices, procedures</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bad employee habits and practices including sharing passwords</td>
<td>14</td>
<td>60</td>
</tr>
<tr>
<td>Lack of practice in a phishing (e-mail) program</td>
<td>13</td>
<td>56</td>
</tr>
<tr>
<td>Lack of security program or ineffective security program</td>
<td>12</td>
<td>52</td>
</tr>
<tr>
<td>Good password management process</td>
<td>10</td>
<td>43</td>
</tr>
<tr>
<td><strong>Compromised data and security breach</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Compromised network from successful phishing attack</td>
<td>18</td>
<td>78</td>
</tr>
<tr>
<td>Compromised information such as trade secrets, identity theft</td>
<td>16</td>
<td>69</td>
</tr>
<tr>
<td>Compromised name/reputation/breach of company records</td>
<td>14</td>
<td>60</td>
</tr>
<tr>
<td><strong>Training and education</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Training for preventing employees from clicking on phishing e-mails</td>
<td>13</td>
<td>56</td>
</tr>
<tr>
<td>Lack of training and education</td>
<td>12</td>
<td>52</td>
</tr>
<tr>
<td>Ongoing training for ever-changing social engineering techniques</td>
<td>12</td>
<td>52</td>
</tr>
<tr>
<td>Educating non-tech savvy employees</td>
<td>11</td>
<td>47</td>
</tr>
</tbody>
</table>

Table AII. Four topic areas from Round 1 by number and percentage of panelists

<table>
<thead>
<tr>
<th>Ranking</th>
<th>Social engineering issue</th>
<th>Rating</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Compromised data: trade secrets, name and reputation, records, network with “hooks”</td>
<td>4.0</td>
</tr>
<tr>
<td></td>
<td>leading to theft, blackmail or espionage</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Ineffective or lack of organizational security practices</td>
<td>4.1</td>
</tr>
<tr>
<td>3</td>
<td>Ongoing education of non-tech savvy employees, including executives and assistants</td>
<td>4.8</td>
</tr>
<tr>
<td>4</td>
<td>Bad practices and habits by employees</td>
<td>5.0</td>
</tr>
<tr>
<td>5</td>
<td>End-user awareness of ever-changing social engineering threats and techniques</td>
<td>5.2</td>
</tr>
<tr>
<td>6</td>
<td>Practicing good password management of strong, changed and not repeated across systems</td>
<td>5.5</td>
</tr>
<tr>
<td>7</td>
<td>Practice in user recognition and user reporting of suspicious e-mails</td>
<td>5.7</td>
</tr>
<tr>
<td>8</td>
<td>Lack of practice on phishing programs</td>
<td>6.0</td>
</tr>
<tr>
<td>9</td>
<td>Prevention of employees clicking on phishing e-mails with a hidden link</td>
<td>7.1</td>
</tr>
<tr>
<td>10</td>
<td>Lack of information around frequency of attacks</td>
<td>7.2</td>
</tr>
</tbody>
</table>

**Appendix 2**
### Appendix 3

<table>
<thead>
<tr>
<th>Panelist agreement</th>
<th>Order of issue preference 1st</th>
<th>Order of issue preference 2nd</th>
<th>Order of issue preference 3rd</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Disagree</td>
<td>Ineffective or lack of security practices</td>
<td>Ongoing education and training</td>
<td>Data compromise</td>
</tr>
<tr>
<td>2. Agree</td>
<td>Data compromise</td>
<td>Ineffective or lack of security practices</td>
<td>Ongoing education and training</td>
</tr>
<tr>
<td>3. Agree</td>
<td>Data compromise</td>
<td>Ineffective or lack of security practices</td>
<td>Ongoing education and training</td>
</tr>
<tr>
<td>4. Disagree</td>
<td>Ongoing education and training</td>
<td>No comment provided</td>
<td>No comment provided</td>
</tr>
<tr>
<td>5. Agree</td>
<td>Data compromise</td>
<td>Ineffective or lack of security practices</td>
<td>Ongoing education and training</td>
</tr>
<tr>
<td>6. Disagree</td>
<td>Ongoing education and training</td>
<td>Ineffective or lack of security practices</td>
<td>Compromised data</td>
</tr>
<tr>
<td>7. Agree</td>
<td>Compromised data</td>
<td>Ineffective or lack of security practices</td>
<td>Ongoing education and training</td>
</tr>
<tr>
<td>8. Disagree</td>
<td>Compromised data</td>
<td>Ongoing education and training</td>
<td>Ineffective or lack of security practices</td>
</tr>
<tr>
<td>9. Disagree</td>
<td>Ineffective or lack of security practices</td>
<td>Ongoing education and training</td>
<td>Compromised data</td>
</tr>
<tr>
<td>10. Disagree</td>
<td>Ongoing education and training</td>
<td>Ineffective or lack of security practices</td>
<td>Compromised data</td>
</tr>
<tr>
<td>11. Disagree</td>
<td>Ongoing education and training</td>
<td>Ineffective or lack of security practices</td>
<td>Compromised data</td>
</tr>
<tr>
<td>12. Agree</td>
<td>Compromised data</td>
<td>Ineffective or lack of security practices</td>
<td>Ongoing education and training</td>
</tr>
<tr>
<td>13. Neither agree or disagree</td>
<td>No comment provided</td>
<td>No comment provided</td>
<td>No comment provided</td>
</tr>
<tr>
<td>14. Neither agree or disagree</td>
<td>No comment provided</td>
<td>No comment provided</td>
<td>No comment provided</td>
</tr>
<tr>
<td>15. Agree</td>
<td>Compromised data</td>
<td>Ineffective or lack of security practices</td>
<td>Ongoing education training</td>
</tr>
</tbody>
</table>

**Table AIII.** Delphi Round 3 responses
Appendix 4

Round 3 Solutions for Countering Social Engineering Attacks

Figure A1. Round 3 code to theory generation
Appendix 5. Central themes from coding Delphi Round 3 responses

- Theme 1: layered security solutions.
- Theme 2: strict, mandatory solutions with consequences.
- Theme 3: security solutions structure.
- Theme 4: balanced control.
- Theme 5: privacy and security awareness implementation.
- Theme 6: security training.
- Theme 7: employee-focused and personalized solutions.

Appendix 6. Theoretical constructs

(1) Theoretical Construct 1: security solutions implement technology:
   - Supporting themes:
     - Layered security solutions include multiple systems.
     - Solutions include monitoring, auditing, testing, searching systems and networks.
     - Solutions are based on perimeter security, restricting access and authentication.
     - Technology parameters aid in enforcing change.

(2) Theoretical Construct 2: security solutions educate and train user behavior:
   - Supporting themes:
     - Solution is frequent, ongoing, dedicated, customized training.
     - Education development is employee focused.
     - Education is based on behavior, tactics, tricks and changing thought patterns.
     - Training is policy and procedure based.
     - Training involves variety of visual, written, oral communication.
     - Training and education should be supervisor motivated and monitored.
     - Education should be continuous and ongoing.

(3) Theoretical Construct 3: security solutions implement balanced control:
   - Supporting themes:
     - Behavioral control and technical control are layered.
     - Balanced control is systems and people working together.
     - Balanced control is changing through patterns and behaviors in technology.
     - Solutions incorporate people and systems monitoring.

(4) Theoretical Construct 4: personalizing security solutions for implementation:
   - Supporting themes:
     - Personalizing the risk and impact is key.
     - Personalizing empowers user recognition and responding.
     - Using personal remediation programs is effective.
     - Personalizing solutions reinforces learning.
     - Examples of feeling, showing, teaching, directing personalizes the program.
(5) Theoretical Construct 5: security solutions implement user policies, programs, practices:

- Supporting themes:
  - Strict policies and procedures must accompany best practices.
  - Consequences for not adhering to policies should be enforced.
  - Policies direct employee actions, behavior and responses.
  - Programs involve practices, regular testing, with continuing education.

(6) Theoretical Construct 6: communication drives effective security solutions:

- Supporting themes:
  - Communication by periodic bulletins, e-mail, meetings and dialog is needed.
  - Communication includes published campaigns with results, newsletters, cybersecurity guidelines for reading.

Corresponding author
Curtis C. Campbell can be contacted at: curtis@mprotechnologies.com

For instructions on how to order reprints of this article, please visit our website:
www.emeraldgrouppublishing.com/licensing/reprints.htm
Or contact us for further details: permissions@emeraldinsight.com
Prevention of cybercrimes in smart cities of India: from a citizen’s perspective

Sheshadri Chatterjee
Indian Institute of Technology Delhi, New Delhi, India

Arpan Kumar Kar
Department of Management Studies, Indian Institute of Technology Delhi, New Delhi, India

Yogesh K. Dwivedi
School of Business, Swansea University, Swansea, UK, and

Hatice Kizgin
School of Management, Swansea University, Swansea, UK

Abstract

Purpose – The purpose of this paper is to identify the factors influencing the citizens of India to prevent cybercrimes in the proposed Smart Cities of India.

Design/methodology/approach – A conceptual model has been developed for identifying factors preventing cybercrimes. The conceptual model was validated empirically with a sample size of 315 participants from India. Data were analyzed using structural equation modeling with SPSS and AMOS softwares.

Findings – The study reveals that the “awareness of cybercrimes” significantly influences the actual usage of technology to prevent cybercrimes in Smart Cities of India. The study reveals that government initiative (GI) and legal awareness are less influential in spreading of the awareness of cybercrimes (AOC) to the citizens of the proposed smart cities.

Research limitations/implications – The conceptual model utilizes two constructs from the technology adoption model, namely, perceived usefulness and ease of use. The study employs other factors such as social media, word of mouth, GIs, legal awareness and organizations constituting entities spreading awareness from different related literature works. Thereby, a comprehensive theoretical conceptual model has been proposed which helps to identify the factors that may help in preventing cybercrimes.

Practical implications – This study provides an insight to the policy maker to understand several factors influencing the AOC of the citizens of the proposed Smart Cities of India for the prevention of cybercrimes.

Originality/value – There are few existing studies analyzing the effect of AOC to mitigate cybercrimes. Thus, this study offers a novel contribution.

Keywords Smart city, Cyber security, Digital services, Cyber-infrastructure

Paper type Research paper

1. Introduction

The internet has emerged as an important infrastructure in our daily life in this journey toward digital transformation (Castiglione et al., 2018). In this journey, the Government of India (GoI) has announced the intention to create 100 smart cities in India (SCI). Smart Cities are construed to be datafied or internet cities (Gosgerove, 2011; Falconer and Mitcheli, 2012; Gupta, 2014; Chatterjee and Kar, 2017). The GoI is developing the SCI concept with a core of information communication technology (ICT activity). However, there are concerns that the SCI concept might be adversely affected by security problems (Thomsom et al., 2006; Chatturvedi et al., 2014; Dwivedi, Rana, Janssen, Lal, Williams and Clement, 2017; Dwivedi, Rana, Jeyaraj, Clement and Williams, 2017; Gcaza et al., 2017). It is expected that citizens of SCI would use high-speed internet for ensuring easy access to digital services (Chatterjee and Kar, 2017; Chhonker et al., 2017). As a result, this vulnerability might be increased. So, it is necessary to identify the perceived security determinants necessary for.
ensuring cyber security. The perceived security may affect the adoption and usage of IT services in SCI. Also, with the increase in ICT, the number of cybercrimes might be increased. Cybercrimes may be defined as “Criminal activity directly related to the use of computers, especially illegal trespass into the computer system or database of other, manipulation of theft of stored or on-line data, or sabotage of equipment and data” (Ompal et al., 2017, p. 166).

In India, the commission of cybercrimes is posing an increasing threat, especially for the citizens of SCI that require prevention. Now, before discussing preventive measures of cybercrimes in SCI, it is important to realize the conception of SC. We can designate a city to be “Smart” if the city has the capability of balancing social, economic and environmental developments in a sustainable way and if, with the help of government, the city can link up all democratic processes effectively (Caragliu et al., 2011). The SC authorities are expected to provide digital services to the citizens taking help of innovative technologies. These digital services would be available to the citizens for different sectors like smart transport, digital health care, smart energy, e-Education and even IoT technology (Chatterjee et al., 2018). The use of ICT is essential to ensure a balance among these developments (Tryfonas et al., 2001). The government is required to engage citizens effectively with modern technologies to improve society and their lived experience (Kickbusch and Gleicher, 2014). Realizing the fact that a country can leverage its national wealth through the adoption of modern technologies, the developed countries of the world have already done the needful to expedite the production of goods and services. They have created smart cities to improve the living standard of the inhabitants (Comin and Hobijn, 2010; Foster and Rosenzweig, 2010; Chatterjee and Kar, 2015).

The principal categories of cybercrimes are, for example, cybercrimes against society, cybercrimes against property, cybercrimes against individuals and cybercrimes against organizations (Brenner and Goodman, 2002). Now to combat the cybercrimes inimical for the progress and development of SCI, the citizens’ awareness regarding cybercrimes is very much instrumental (Muniandy and Muniandy, 2012). As the sense of awareness regarding cybercrimes grows, the citizens of SCI would become cautious regarding the menace of cybercrimes. Hence, this act of social engineering for developing awareness is a crucial issue (Mehta and Singh, 2013). Typical cybercrimes against society include currency forgery, cyberterrorism, illegal website amendments, revenue stamp forgery, etc. (Sproles and Byars, 1998). Cybercrimes against property include credit or debit card fraud, infringement of Intellectual Property Rights with software piracy, infringement of copyright, theft of coding, trademark breach and so on (Supriya, 2012). Cyberbullying, cyberdefamation, cyberstalking, e-mail spoofing, hacking, spamming (Parthasarathi, 2003; Joshi, 2016) and so on come under the category of cybercrimes against individuals. Cybercrimes against organizations include data theft of organizations, e-mail bombing, infringement of trade secret using cyberspace, logic bomb, unauthorized access to computers, virus attack and so on (Parthasarathi, 2003; Weerakkody et al., 2017). Cybercrimes are also said as “Internet Crimes” or “Computer Crimes,” and they include criminal activities actuated using computers (Kelly, 1999). These have become a great concern for SCI (Mohamed, 2003; Obuh and Babatope, 2011).

For addressing cybercrime challenges (Zhao et al., 2012), the citizens are required to use the preventive technologies if they are aware and conversant regarding the usefulness of the technology and if they do not feel difficulties in using the technologies (Davis, 1989). Thus, there comes the question of adoption capabilities of these technologies. Adoption behavior has been studied utilizing opposite inputs from other studies (Williams et al., 2009; Dwivedi, Rana, Janssen, Lal, Williams, Clement, 2017). For this, different adoption behaviors and models have been studied including the technology acceptance model (TAM). The inputs derived from these studies have helped to identify the factors responsible to enhance
citizens’ awareness regarding cybercrimes. It has helped to identify how the citizens of SCI would easily use these preventive technologies. With some recommendations, the study ends with a comprehensive conclusion.

This paper tries to find out the answers of the questions: Why there is a necessity to prevent cybercrime in SCI? What are different entities responsible for spreading awareness among the citizens of SCI regarding the menace of cybercrimes? How the actual use of preventive technologies can ensure the prevention of cybercrimes in SCI (PCS)? What are the perceived determinants influencing the citizens to prevent cybercrimes in SCI? Can we develop a theoretical model for PCS?

In subsequent sections, a detailed review on the background literature is presented followed by a section on how the conceptual theoretical model is developed. This is followed by a description of the research methodology, and then the results of our study have been elaborated. This is followed by the discussion on the implication to theorists and practitioners. The paper subsequently highlights the limitations with directions of future research. It concludes with the key takeaways for the readers.

2. Literature review
In the subsequent subsections, we explore the relevant existing literature surrounding smart cities, cybercrimes and the regulatory ecosystem surrounding cybercrimes in India.

2.1 Smart cities of India
In smart cities, there will be appreciable use of digital services by the citizens to perform their daily activities (Carlino, 2011). The citizens of SCI are expected to enjoy digital services including facilities of having smart buildings (Tagliabue et al., 2012; Gul and Patidar, 2015), advantages of smart water management (Van den Bergh and Viaene, 2015), smart education (Bakry, 2004) and so on. The citizens of SCI are expected to perform their daily commercial activities with the help of e-commerce platform (Alomari et al., 2012; Mansoori et al., 2018). These include digital payments, mobile banking and so on. The citizens are expected to use high-speed networks (Chatterjee et al., 2017a, b).

It is pertinent to mention here that shaping of SCI is still in the evolution stage. There is a limited literature considering the context of India regarding issues of cybercrimes in SCI. The citizens of proposed SCI are expected to depend on online platforms for performing their daily activities and hence they are required to be aware and cautious regarding their online activities (Rana et al., 2016). In India, it is experienced that most popular social platforms are Twitter, LinkedIn, Facebook and so on, though many citizens of SCI are expected to use these platforms simultaneously. Thus, social media (SM) would act as an effective factor for the citizens of SCI to improve their awareness regarding cybercrimes as it would be helpful for effective interactions through SM (Zhang and Benyoucef, 2016). The citizens of SCI are expected to interact directly with each other through word of mouth (WoM). It is expected that awareness related to cybercrimes might be increased through this direct interaction. However, WoM could act as a substantial determinant to enhance the awareness of cybercrimes (AOC) for the citizens of SCI. This is because information spread through WoM could motivate the citizens of SCI to realize the consequences of cybercrimes (Chu and Kim, 2011; Cheung and Lee, 2012; Cho et al., 2014).

2.2 Cybercrimes in smart cities of India
Cybercrime constitutes as an act committed or omitted in the contravention of law commanding or forbidding it and for this, there is provision of punishment (Aggarwal, 2015). There are diverse types of cybercrimes (Saini et al., 2012). These are described in Table I.
There are other cybercrimes like data crimes, network crimes, access crimes, virus dissemination related crimes and so on (Jankowitz, 1988; Spafford, 1989; Power, 2002). To develop awareness regarding cybercrimes, the authorities including GoI are required to be more up and doing so that affected citizens of SCI can get appropriate remedies (Belapure and Godble, 2011; Mohit, 2012; Singh, 2013). In the developing countries, it is observed that financial losses incurred by organizations are almost 80 percent due to computer breaches (Saini et al., 2012). Once the awareness of the citizens of SCI is increased by brushing up this psychology of social engineering (Aggarwal, 2015), they will be motivated to use modern preventive technologies provided they feel that these will fetch effective result and would not create constraint to use (Davis, 1989). The TAM that has been used here is considered as a special case of the theory of reasoned action (Fishbein and Ajzen, 1975). The development of effective awareness concerning to the realization of menace of cybercrimes may be achieved easily with the help of SM as an effective medium (Kim and Srivastava, 2007; Parise and Guinan, 2008; Kaplan and Haenlein, 2010). SM acts as an effective instrument in this context (Qualman, 2012; Lu et al., 2016).

The government should take appropriate initiatives and spread information through electronic and other media to increase the awareness of menace of cybercrimes. This would motivate the citizens of SCI to appropriately use technologies necessary to combat cybercrimes (Shareef et al., 2011; Zuiderwijk et al., 2015). The parts to be played by the organizations in different SCI for boosting up the AOC to the citizens of SCI are pivotal (Mitnick and Simon, 2011). Organizations should always keep them updated; otherwise, it would help the criminals to commit any crime in SCI (Abu-Musa, 2008). If the AOC can be improved among the citizens of SCI, it would effectively help mitigate cybercrimes in SCI (Mehta and Singh, 2013; Parmar and Patel, 2016; Zhang and Benyoucef, 2016).

<table>
<thead>
<tr>
<th>Cybercrimes</th>
<th>Explanation</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hackers</td>
<td>Out of curiosity or to be involved in competition with their friends or for education or otherwise, some individuals, called Hackers, used to have explored computer system of others</td>
<td>Thomas and Loader (2000)</td>
</tr>
<tr>
<td>Pranksters</td>
<td>These individuals used to have perpetrated tricks on others, especially not intending to cause any specific or long-lasting damage</td>
<td>Richards (1999)</td>
</tr>
<tr>
<td>Crackers</td>
<td>Just for a fun or for causing loss to others with ulterior motive, some individuals create virus. These individuals are called crackers</td>
<td>Chan et al. (1999)</td>
</tr>
<tr>
<td>Cyber terrorists</td>
<td>There exist several types of cyber terrorisms. It is, sometimes, a smart hacker who attempts to break a Government website or it may be a group of identical minded netizens who intend to crash a website with the help of flooding the website with traffic. Apparently, this action appears to be innocent, but it can invite many damages and it is still illegal</td>
<td>Longstaff and Schultz (1993)</td>
</tr>
<tr>
<td>Cyber bulls</td>
<td>It is a harassment committed by individuals with the help of internet. Unkind e-mail messages, vicious forum posts, posting fake bio-data on websites and so on come under this category</td>
<td>Adams (1996)</td>
</tr>
<tr>
<td>Salami attackers</td>
<td>For committing financial crimes, some individuals commit these attacks. The secret here is to make an insignificant charge so that in a particular case none will notice it, for example, an employee of a bank puts a program in the server of the bank and it goes on deducting small amount from every customer regularly</td>
<td>Philippsohn (2001)</td>
</tr>
<tr>
<td>Career criminals</td>
<td>There are individuals who earn part or all concerning to their income from crimes committed with the help of internet. “The FBI reported in 1995, that there were more than 30 Russian gangs operating in the United States. According to the FBI, many of these unsavory alliances use advanced information technology and encrypted communications to elude capture”</td>
<td>Bowen (2009)</td>
</tr>
</tbody>
</table>

Table I. Various kinds of cybercrimes
2.3 Cyber crime and regulatory ecosystem in India

To address cybercrimes in India, GoI has already framed Information Technology Act 2000 (IT Act, 2000). Some of its provisions have been amended in 2008 to make the act more stringent against cybercriminals. Most of the provisions of IT Act 2000 since amended are found to be non-bailable and cognizable. Ironically, it has been observed that some of the provisions of this act might be abused by the legal enforcement (LE) authorities. For example, the provisions were misused in the case of two girls who were punished wrongly by the LE authorities in Maharashtra, India (Shaheen, 2012) by the application of section 66A of IT Act 2000. Eventually, that section 66A of IT Act 2000 since amended was struck down as the Supreme Court of India held *inter alia* that this provision is violative of Article 19(2) of the Constitution of India in the Shreya Singhal case (*Shreya Singhal v. Union of India*, WP No. 167 of 2012, Supreme Court of India). The GoI is required to restructure the laws to see that provisions are not misused by the LE authorities. If these are done, this would also help the citizens of SCI to enhance their AOC.

The GoI should also make the citizens of SCI aware regarding the extent of punishments available for the delinquents (McConnell, 2000). This might motivate the citizens of SCI for taking legal remedies and would motivate them to appropriately use technologies for addressing cybercrimes in SCI (Holsapple and Lee-Post, 2006). Ironically, the individuals committing cybercrimes often escape punishment for want of appropriate evidence. It has thus become a challenge as to how appropriate evidential proofs of computer crimes committed in SCI can be collected to effectively prosecute the cybercriminals (Jiow, 2013).

3. Development of conceptual model

We have seen in the background studies that awareness regarding cybercrimes is pivotal for tackling and preventing cybercrimes in SCI (Mehta and Singh, 2013). Now, we try to find out different entities which could spread AOC among citizens of proposed SCI. Moreover, while developing the conceptual model, we would try to find out the major factors which might influence actual technology use (ATU) by the citizens of SCI to prevent cybercrimes.

Without the development of awareness regarding the menace of cybercrimes, the citizens would not be alert regarding its negative elements (Aggarwal, 2015). For this, many agencies are to take initiatives. Government through publicity campaign and by other means can help the citizens to improve their awareness (Gupta *et al.*, 2012). In a modern technological environment, SM plays a key role. Everyday activities can be supported through the effective use of SM. Through this, accurate information may be obtained by the citizens. Hence, this tool is considered effective to improve awareness (Ellison, 2007; Kim and Park, 2013). Citizens while interacting with each other, through conversation, can get a scope to develop their awareness regarding the menace of cybercrimes. Hence, WoM is an effective instrument to develop awareness (Hung and Lai, 2015). In smart cities, many organizations are expected to function. They may be banks, post offices, different financial institutions and so on. These institutions with the help of e-mail, short messaging services or otherwise can boost up the sense of awareness. Hence, the role of organizations in spreading awareness among citizens of SCI counts much (Belapure and Godbole, 2011; Mitnick and Simon, 2011). If any victim of cybercrime does not get an appropriate legal remedy, they will fail to have faith in legal system. Hence, the enhancement of LE toward addressing cybercrimes would increase awareness (Ali, 2016; Michael *et al.*, 2011). The enhancement of overall awareness of the citizens would help to get them motivated to use the preventive technology. It would also help to prevent cybercrimes (Pavlov and Fygenson, 2006). Again, if the citizens while using preventive technologies perceive that such use is neither fetching useful results, nor the use of technology is free from complexity, they would not be motivated to use that technology (Davis *et al.*, 1989; Park, 2009). Hence, perceived usefulness (PU) and ease of use would
motivate the citizens to use preventive technology which, in turn, will prevent cybercrimes (Longstaff and Schultz, 1993; Henderson and Divett, 2003; Park, 2009).

To visualize, all the factors instrumental to prevent cybercrimes in SCI mediating through two variables, namely AOC and ATU, are shown in Table II. It contains the factors, their corresponding explanations and the respective sources in the form of references.

3.1 Government initiative (GI)

The GoI as well as all state governments are required to take up meaningful initiatives for improving awareness among the citizens of SCI regarding the menace of cybercrimes. For this, on July 2, 2013, the GoI framed National Cyber Security Policy (2013) whose principal goal is to build up robust and effective and secured resilient cyberspace for citizens of SCI (Gupta et al., 2012). GoI should take appropriate initiatives to arrange different workshops, conferences and research-based programs to improve awareness. GoI should promote publicity campaign including seminars, radio and television programs and so on. National Awareness programs like National Information Security Awareness Program (NISAP) are to be promoted to realize cyber security requirements for the SCI citizens through effective training and academic programmes. Government should make the citizens of SCI aware regarding the fact that with more dependence on the internet, they are becoming more vulnerable to disruptions engineered through cyberspace (Gupta et al., 2012). Sincere GoI initiatives would improve the awareness of the citizens of SCI concerning to cybercrimes (Belapure and Godbole, 2011). Besides, the government should take up NISAP to make the citizens of SCI aware regarding the menace of cybercrimes (Raghav, 2012). From the above discussions, we can develop the following hypothesis:

\[ H1. \text{ Government initiative (GI) would positively impact AOC.} \]

3.2 Social media (SM)

If the citizens of proposed SCI interact among themselves via SM platforms, it would provide more accurate, transparent, and exhaustive information to each other which would enrich their knowledge (Wolfinbarger and Gilly, 2001; Alryalat et al., 2017). The interactions among citizens of SCI with the help of SM platform regarding dangers and consequences of cybercrimes would enhance their awareness about cybercrimes. It would enhance their belief that to prevent cybercrimes in SCI, the citizens are to take recourse to use appropriate technologies (Lu et al., 2016; Zhang and Benyoucef, 2016). The authorities are required to be vigilant to utilize these social platforms to enhance awareness regarding the menace of cybercrimes in proposed SCI (Ellison, 2007; Kim and Park, 2013; Alalwan et al., 2017). Advancement of technology also would motivate the citizens of SCI to use electronic platforms in a regular way and interactions among the citizens of SCI taking help of social platform would improve the extent of awareness regarding the menace of cybercrimes in SCI (Kim and Eastin, 2011; Shin, 2013). It is a fact that SM platforms are mainly concerned with affairs of transactions only; but at the same time, it also acts as an effective instrument for exchange of information through interactions. It would enhance the awareness of the citizens regarding cybercrimes and, in turn, such awareness would motivate the citizens to use technology to combat cybercrimes in proposed SCI (Devaraj et al., 2002; Yadav et al., 2013). However, the SM platform is used by SCI citizens in a more efficient way incurring lower costs compared to performing such interactions through traditional media and if used effectively would positively influence the citizens of SCI to appreciably enhance awareness regarding cybercrimes (Edelman, 2010; Mikalef et al., 2016). Based on the above discussion, the following hypothesis is provided:

\[ H2. \text{ SM will have a positive impact in enhancing the awareness of cybercrimes (AOC) of SCI toward cybercrimes.} \]
<table>
<thead>
<tr>
<th>Factors</th>
<th>Explanation</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>Government initiative (GI)</td>
<td>By NISAP (Part of National Cyber Security Policy), by making the citizens of SCI realize regarding needs of prevention of cybercrimes, the GoI should try to improve awareness among the citizens of SCI for the prevention of cybercrimes</td>
<td>Belapure and Godbole (2011), Gupta et al. (2012) and Raghav (2012)</td>
</tr>
<tr>
<td>Word of mouth (WOM)</td>
<td>Exchange of views by persons to persons through talks constitutes the affairs termed as WOM. It helps to form effective influence to improve awareness of cybercrimes of SCI regarding cybercrimes. It helps developing preventive measure against cybercrimes in SCI</td>
<td>Chu and Kim (2011), Cheung and Lee (2012), Wisman (2013), Zheng et al. (2013), Cho et al. (2014), King et al. (2014) and Hung and Lai (2015)</td>
</tr>
<tr>
<td>Organizations (ORG)</td>
<td>The role of organizations functioning in SCI is vital for forming awareness instrumental to prevent cybercrimes in SCI. The functions of the organizations should be flawless to develop trust among the citizens of SCI on these organizations. It would bring confidence of the citizens of SCI over these organizations and in that case the actions of the organizations would impact on the citizens of SCI to develop awareness of cybercrimes</td>
<td>Abu-Musa (2008), Gatzlaff and McCullough (2010), Belapure and Godbole (2011), Mitnick and Simon (2011) and Singh (2013)</td>
</tr>
<tr>
<td>Legal enforcement (LE)</td>
<td>Legal enforcement helps developing awareness among citizens of SCI which, in turn, would be helpful to prevent cybercrimes. The law enforcing authorities should be effective and efficient to enforce laws effectively</td>
<td>McConnell (2000), Mohamed (2003), Burns et al. (2004), Ali (2016), Michael et al. (2011) and Aggarwal (2015)</td>
</tr>
<tr>
<td>Awareness of cybercrimes (AOC)</td>
<td>It is associated with knowledge and attention of the users. This helps the users to know details about internet and its functionalities. This helps the citizens of SCI to improve their awareness of cybercrimes and its dangers. This would help to prevent cybercrimes in SCI</td>
<td>Aparna and Chauhan (2012), Mehta and Singh (2013), Arvais et al. (2014), Singaravelu and Pillai (2015), Narahari and Shah (2016) and Parmar and Patel (2010)</td>
</tr>
<tr>
<td>Perceived usefulness (PU)</td>
<td>It is perception of citizens of SCI for the prevention of cybercrimes. It includes many ingredients like effectiveness, performance, trust, risk perception and productivity. It motivates the citizens to actual use of technologies essential to prevent cybercrimes in SCI. It is associated with the sense of perceiving usefulness of the technology</td>
<td>Davis (1989), Davis et al. (1989), Henderson and Divett (2003), Aggelidis and Chatzoglou (2009), Park (2009) and Turner et al. (2010)</td>
</tr>
</tbody>
</table>

Table II. Summary of factors and sources (continued)
3.3 Word of mouth (WoM)
Exchange of views through person to person through WoM discussion acts as a self-leader capable of forming effective opinion among the citizens of SCI (Zheng et al., 2013). If persons in SCI speak with each other regarding dangers of cybercrimes, the citizens of SCI would improve their awareness regarding cybercrimes (Hung and Lai, 2015). WoM is concerned with direct interactions among the citizens. In the context of the SC, the direct interaction among the citizens of SCI would come under the remit of WoM. The interactions would be spread and if through any motivation whatsoever one feels the need of enhancement of awareness regarding cybercrimes, their opinion would be spread through WOM among the other citizens of SCI. In that case, it can be said that WoM would help motivate the citizens of SCI to realize the need of improving their AOC (Chu and Kim, 2011; Cho et al., 2014). WoM thus acts as an effective determinant to enhance the extent of awareness regarding cybercrimes. If one of the citizens wishes to spread the boon of possessing AOC, it would be spread by that person through interaction with others in the form of WoM. It would help to enhance the sense of awareness of the citizens of SCI regarding dangers and consequences of cybercrimes (Cheung and Lee, 2012; Wisman, 2013; King et al., 2014). In terms of the above discussions, the following hypothesis is formulated:

H3. WoM has a positive impact on the AOC among the citizens of SCI.

3.4 Organizations (ORG)
To make the citizens of SCI aware regarding the menace of cybercrimes, the role of organizations is vital (Singh, 2013). The organizations in SCI like banks, post offices and other financial institutions play a pivotal role to boost up awareness among the citizens of SCI through their day-to-day activities. Often, we find messages from the bank authorities cautioning not to disclose bank details to any other persons as it might jeopardize one’s commercial interests. Organizations are required to ensure security control and are to report to Indian Computer Emergency Response Team (Cert-in) regarding any security incidence (Belapure and Godbole, 2011). Besides, organizations’ duties are to always keep the concerned beneficiaries appraised regarding any possible future occurrence of cybercrimes. It would help the citizens of SCI to be cautious regarding the occurrence of

<table>
<thead>
<tr>
<th>Factors</th>
<th>Explanation</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>Perceived ease of use (PEU)</td>
<td>It is construed to be degree to which citizens of SCI would believe that some efforts are needed to learn for a technology essential to prevent cybercrimes in SCI. This ingredient includes factors like simplicity, compatibility and self-efficacy. This impacts on the actual use of technology to prevent cybercrimes in SCI.</td>
<td>Davis (1989), Davis, Bagozzi and Warshaw (1989) and Yi, Liao, Huang and Hwang (2009)</td>
</tr>
<tr>
<td>Actual technology usage (ATU)</td>
<td>This is related with the conception that users are involved with the use of the technology. This use of technology will help prevent cybercrimes in SCI.</td>
<td>Sorebo et al. (2007) and Abdul-Nasser (2012)</td>
</tr>
<tr>
<td>Prevention of cybercrimes in SCI (PCS)</td>
<td>The prevention of cybercrimes in SCI includes mechanisms required to increase awareness among the citizens of SCI and includes actual technology use. This would help to prevent cybercrimes in SCI.</td>
<td>Longstaff and Schultz (1993) and Abdul-Nasser (2012)</td>
</tr>
</tbody>
</table>

Table II.
cybercrimes. They would be aware regarding what to do and what not to do. In this way, organizations contemplated to be working in the SCI should act as an effective instrument to make the citizens of SCI aware of cybercrimes (AOC) (Mitnick and Simon, 2011). The organizations should be constantly seeking to update their internal processes so there would be no future re-occurrence of cybercrime. Such occurrence might adversely affect the citizens of SCI and a sense of lack of trust might grow in that case among the citizens (Abu-Musa, 2008). The organizations should preserve the data of their respective customers, so that there might not be any data breach since in that case, it would bring in adverse conception on the customers (Gatzlaff and McCullough, 2010). Thus, there is an effective role of the organizations which would be operating inside the SCI to boost awareness among the citizens regarding the menace of cybercrimes. In the light of above discussions, the following hypothesis is prescribed:

H4. Organizations (ORG) have positive impact on the AOC among the citizens of SCI.

3.5 Legal enforcement (LE)
The very nomenclature “Legal Enforcement” is associated with mechanism instrumental for the enforcement of law to address cybercrimes in the present context (Ali, 2016). It is a fact that in many developing countries, the laws for tackling the cybercriminals are not strong (McConnell, 2000). In many developing countries, it appears that the authorities are found to invest less amount to enforce laws to address cybercrimes. On the contrary, the authorities are found to invest more amount for the enforcement of laws to address other crimes of regular nature (Michael et al., 2011). Addressing cybercrimes in SCI with the help of proper enforcement of law requires a considerable amount of investment. Insufficient investment poses challenges to the LE authorities. This is because the nature of cybercrimes is assuming new forms (Mohamed, 2003). It is essential to combat cybercrimes in SCI with the help of enforcement of law (Burns et al., 2004). In this context, the role of IT authorities is important (Chatterjee et al., 2017a, b). The persons using the internet should be aware of the criminal activities occurring in the cyberspace. Online transaction techniques expected to be adopted in SCI would enable massive evolution in the use of the internet as it would change traditional business mechanisms (Ali, 2016). Data and information of the citizens of SCI are supposed to be protected from unauthorized illegal access. One is to know basic information of cyber enactments. Another is to know how those are enforced. Since the laws responsible to book the cybercriminals in India are not so stringent (McConnell, 2000) like other developing countries, the citizens of SCI possess less dependence on these laws. Hence, pragmatic LE against cybercrimes in SCI is essential. Once it is ensured, the awareness of the citizens regarding cybercrimes would be increased (Aggarwal, 2015). With all these inputs, the following hypothesis is provided:

H5. LE has a positive impact on the AOC among the citizens of SCI.

3.6 Perceived usefulness (PU)
This factor has been taken from the knowledge of the TAM (Davis, 1989; Davis et al., 1989). It effectively influences attitudes of the citizens of SCI to use technologies necessary to address and to prevent cybercrimes in SCI. It subsequently impacts the citizens of SCI for ATU to prevent cybercrimes. This model basically approached to identify the internal beliefs of citizens of SCI with the help of external variables. This has been identified by Davis in 1989 as PU. PU can be interpreted as a perception of citizens of SCI to the effect that the use of a technology will substantially improve the performance of citizens of SCI for the PCS. It is pertinent to mention here that PU includes effectiveness, performance,
trust, risk perception and productivity (Henderson and Divett, 2003; Aggelidis and Chatzoglou, 2009; Park, 2009; Turner et al., 2010). This variable PU is found to have an appreciable impact over ATU. Judged from the above discussions, the following hypothesis is developed:

\[ H6. \text{PU has positive impact on ATU.} \]

3.7 Perceived ease of use (PEU)
This belief has been lent from the TAM advanced by Davis (1989) and Davis et al. (1989). This factor influences the citizens to use a technology if the citizen finds that such use is not complex but easy on the contrary. This belief is construed to be a degree through which citizen believes that some efforts are needed to learn use of a technology necessary (Park, 2009). If the citizen perceives that the use of that technology would not pose any constraint, the citizen would feel easy and use the technology (Henderson and Divett, 2003). Again, the factor perceived ease of use (PEU) includes ingredients like simplicity, compatibility and self-efficacy (Yi et al., 2009). This belief is considered to have an impact on ATU, since the users feel comfortable in using technology. With these considerations, the following hypothesis is prescribed:

\[ H7. \text{PEU has a positive impact on ATU.} \]

3.8 Entities spreading awareness (ESA)
There are many entities which can address cybercrimes. However, studies of literature have revealed that so far as SCI is concerned, the entities which would be able to spread awareness among citizens of SCI most effectively for the prevention of cybercrimes are GI, SM (Edelman, 2010), WoM (Hung and Lai, 2015), organizations (Singh, 2013) and LE (Aggarwal, 2015). Therefore, in the context of developing AOC among the citizens of SCI, it has been considered that entities spreading awareness (ESA) in this context constitute these five ingredients like GI, SM, WOM, ORG and LE. Once the awareness of the citizens of proposed SCI toward consequences of cybercrimes increases, they would feel the need that to prevent cybercrimes, they are to use preventive technology. Then, they would be involved in ATU for the prevention of cybercrimes (Brown et al., 2003; Pavlou and Fygenson, 2006). With these inputs, the following hypothesis is developed:

\[ H8. \text{AOC of SCI has a positive impact on citizens’ behavior to ATU.} \]

3.9 Awareness of cybercrimes (AOC)
AOC is associated with the level of knowledge and attention which assists the users of internet (netizens) to conceptualize regarding what an internet is, how it can work and function, what are its environments, how transactions are to be done through internet safely, what are its uses and misuses, how remedies can be achieved in case of vulnerable threats, what are the laws available to address cybercrimes and so on. These ingredients will be able to assess the level of users’ awareness and extent of understandabilities of cybercrimes in SCI (Avais et al., 2014; Aggarwal, 2015). Improvement of awareness among the citizens of SCI regarding cybercrimes would be an effective issue to efficiently prevent cybercrimes (Aparna and Chauhan, 2012; Mehta and Singh, 2013; Singaravelu and Pillai, 2014; Parmar and Patel, 2016). The study in the city of Anand (Gujrat, India) revealed that 68 percent of the netizens did not hear the term “cyber cells” and do not know wherefrom remedies may be obtained to address cybercrimes save approaching police. In total, 15 percent know about IT Act, 2000 (India); 43 percent know that in case of being victims of cybercrimes, IT Act, 2000 (India) is the remedy, but they never referred to that;
24 percent heard about IT Act 2000 of India, but do not know what this act does; and 18 percent have hardly any idea about IT Act, 2000 of India (Narahari and Shah, 2016). It is pertinent to mention here that in Gujarat, through the public-private-partnership model, an SC known as GIFT city (Gujarat Industrial Finance Tec-city) is in operation partially. This is the first partially operated SC in India. It is the first international finance service center in India. That is why it is relevant to take up to assess the extent of awareness of the citizens of a city in the state of Gujarat. Judged from this important standpoint, the following hypothesis is formulated:

\[ H9. \text{ AOC positively affects PCS.} \]

3.10 Actual technology use and prevention of cybercrimes in SCI

The sense of ATU is associated with the conception that the citizens of SCI are involved with the use of technology (Sorebo et al., 2007). Once the citizens start adopting the preventive technologies and use those and once the awareness is increased, the citizens of SCI are expected to be able to prevent the cybercrimes in SCI (Longstaff and Schultz, 1993; Abdul-Nasser, 2012). With this conception, the following hypothesis is provided:

\[ H10. \text{ ATU has a positive impact on PCS.} \]

In developing the hypotheses, we have observed that some entities like GI, SM, WOM, ORG and LE act as effective and efficient factors to prevent cybercrimes in SCI. These five factors constitute ESA. These factors have an influence on developing AOC among the citizens of India. Again, this awareness impacts significantly and positively PCS (Burns et al., 2004; Kim and Eastin, 2011; Hung and Lai, 2015; Singh, 2013; Narahari and Shah, 2016). Again, we have seen as awareness is increased, the citizens of SCI would like to be involved in ATU instrumental to PCS (Shin, 2013). Besides, the citizens of SCI would use the preventive technologies for PCS only when they find the usefulness of that technology and when they would find ease to use that technology as provided in TAM, 1989 (Davis, 1989; Davis et al., 1989). All the inputs available here are shown in Table II as a summary.

With all these inputs including gathering knowledge from the hypotheses so developed, the following conceptual model is provided for PCS and it is shown in Figure 1.

---

**Figure 1.** Conceptual model connecting the constructs
4. Research methodology

We have developed the constructs with the help of inputs available from literature study as well as from studies of different adoption theories including the TAM (Davis, 1989). We have also analyzed different research studies dealing with the different issues of adoption as well as of awareness (Ali, 2016; Narahari and Shah, 2016; Dwivedi, Rana, Jeyaraj, Clement and Williams, 2017; Dwivedi, Rana, Janssen, Lal, Williams and Clement, 2017). We have developed the conceptual model shown in Figure 1. This model and the hypotheses are required to be validated with the help of standard statistical tools.

We are to frame some congenial questionnaires (items) with the help of the knowledge of constructs and with the help of existing different adoption theories and models with a special focus on the TAM (Davis, 1989). After developing the initial survey instrument, we have consulted with ten experts. They have adequate knowledge concerning to cybercrimes. They possess insights regarding the development of awareness among the citizens of SCI concerning the menace of cybercrimes. Out of these ten experts, four have been considered from academic areas and the remaining six have been considered from industries. Experts coming from academic sides are all PhD holders having knowledge of cyber security and SC. The remaining six experts from industries have all more than ten years’ experience in R&D sections dealing mainly with cybercrime protection mechanisms. We could initially prepare 41 questions. But, as per the opinion of these ten experts, nine questions have been rejected. According to their opinion, out of nine questions, some were not congenial to fetch accurate results. Some suffered from the defect of readability. Hence, we started our survey works with 32 questions covering six constructs. The questionnaires were serially oriented in such a fashion as initial questions were easy to respond. With progress, they required more deliberations. In preparing the questionnaires, we followed standard guidelines. Attention was given in structuring the questionnaires toward their layout, design and easiness. No ambiguous question was framed. The recitals of questionnaires are shown in Tables A1–AIV.

To target respondents for conducting the survey, we depended on the knowledge and information derived from the different participants attending eight different conferences and workshops in various parts of India. The theme of each conference was related to cyber security, information risk and smart cities. We targeted inhabitants of Mumbai, Gujrat, Pune, Bangalore and Delhi for conducting our survey works using convenience sampling. Here, the respondents were so selected as they could be accessed conveniently. Here in this study, we have selected these five cities since these conferences were held during October 2017–January 2018 in those places. The themes of these conferences were identical with the subject matter of this study. Thus, convenience sampling was considered appropriate. By the contacts with these participants in those workshops and conferences, we could gather a list of persons inhabiting in these cities having knowledge of cybercrimes and conception of SCI.

The total prospective respondents were 483 initially. Some of the e-mail addresses, telephone numbers or postal addresses of the prospective respondents were found inadequate and vague. They are 77 in number. So, we had to start with 406 respondents. The respondents were of different ages with different educational qualifications and professions. The 32 questionnaires were sent to 406 respondents partly through emails and partly through hardcopies. One-month time was given for responses. We eventually received 332 responses in time. The responses were given to those 10 experts for their opinion. They opined that out of those 332 responses, 17 responses were inappropriate and opined not to consider those. Hence, we began with 315 effective and useable responses for our study. This is within acceptable limit as we know that effective responses should be more than four times the questionnaires and preferably should be within ten times of the concerned questionnaires (Hinkin, 1995). Our effective responses were 315 against 32 questions. Hence, our survey approach is within a permissible range. The sample demographics of these 315 responses are shown in Table III.
To quantify the responses, we used a five-point Likert scale with marking strongly disagree as 1 to strongly agree as 5. The survey works including one-month time of responses were conducted for four months from October 2017 to January 2018.

5. Research results
In the subsequent subsections, we would discuss the results obtained from the survey. At first, an overview of the demographic profile is presented, followed by the reliability analysis. This is followed by the tests for multicollinearity and validation of the model, including structural equation modeling (SEM).

5.1 Respondents’ demographic profile
The result indicates that majority of the respondents was from comparatively younger generation, for example, 59.3 percent of the respondents have age group from 21 to 40 years. In terms of occupation, it appears that 46.7 percent respondents were from corporate sector. As per the education of the respondents, it appears that 58.4 percent representation came from graduate and postgraduate levels. The details are given in Table III.

5.2 Construct reliability test
To test the reliability of the constructs, Cronbach’s alpha of each construct was computed. It has been found that the value of each Cronbach’s alpha relating to each construct is more than 0.6, which is the lowest acceptable value of Cronbach’s alpha. The result confirms that constructs so developed are reliable (Hair et al., 1992). The results are shown in Table IV.

5.3 Test of multicollinearity
If the constructs so developed are found close to each other in their inner meaning, it is said that the identification of constructs suffers from the multicollinearity defect. It creates difficulties to apply regression analysis. For this, the variance inflation factor (VIF) of each construct is to be computed. It appears that each value of VIF lies between 3.3 and 5, which confirms that the constructs do not suffer from the multicollinearity defect (Kock and Lynn, 2012). The results are shown in Table V.
5.4 Computations of LF, AVE, CR and MSV

To assess if each questionnaire (item) can explain its own construct, we need to find out the loading factor (LF) of each item concerning to its own construct. The lowest permissible value of LF in this context is 0.707 (Borroso et al., 2010). To examine the reliability of each construct, we have estimated average variance extracted (AVE) of each construct, composite reliability (CR) of each construct and maximum shared variance (MSV) of each construct (Fornell and Larcker, 1981). Acceptable lowest values of AVE and of CR are 0.5 and 0.7, respectively, and each MSV should be less than its corresponding AVE (Urbach and Ahlemann, 2010; Hair et al., 2011). The entire result is shown in Table VI. The values so estimated show that they are within permissible limit. Hence, they confirm reliability of the items. It reconfirms the reliability of the constructs so identified.

It appears that values of AVE range from 0.694 to 0.753, LFs range from 0.799 to 0.915 and CR values range from 0.711 to 0.801. It also appears that each value of MSV is less than the corresponding value of AVE relating to each construct.

5.5 Discriminant validity test

If it is seen that each item concerning to its own construct is strongly associated with that construct and weakly related with other constructs, it is said that the discriminant validity has been established (Fornell and Larcker, 1981). To test this, we have computed average variance (AV) of each construct. It is square root of the corresponding AVE. We have found that values of AV are all greater than the correlation coefficients of the construct with the other constructs. This confirms that discriminant validity has been established (Barclay and Smith, 1997). The values of AV are shown in diagonal positions of Table VII, and the values of correlation coefficients are shown in off-diagonal positions of Table VII.

There is another procedure for establishing discriminant validity test. In that case, LF of each item corresponding to its own construct should be greater than the cross-LFs of that item corresponding to other constructs. In that case, we are to find out item-wise LFs and cross-LFs. We have computed those. The entire results are shown in Tables AI–AIV. It appears that the LFs are all greater than their cross-LFs. In this way, we have been able to reconfirm the discriminant validity test.

<table>
<thead>
<tr>
<th>Construct</th>
<th>Value of Cronbach’s $\alpha$</th>
<th>No. of item</th>
</tr>
</thead>
<tbody>
<tr>
<td>Entities spreading awareness (ESA)</td>
<td>0.896</td>
<td>17</td>
</tr>
<tr>
<td>Perceived usefulness (PU)</td>
<td>0.821</td>
<td>3</td>
</tr>
<tr>
<td>Perceived ease of use (PEU)</td>
<td>0.962</td>
<td>3</td>
</tr>
<tr>
<td>Awareness of cybercrimes (AOC)</td>
<td>0.799</td>
<td>3</td>
</tr>
<tr>
<td>Actual technology use (ATU)</td>
<td>0.811</td>
<td>3</td>
</tr>
<tr>
<td>Preventing cybercrimes in SCI (PCS)</td>
<td>0.867</td>
<td>3</td>
</tr>
</tbody>
</table>

Table IV. Estimation of Cronbach’s $\alpha$

<table>
<thead>
<tr>
<th>Construct</th>
<th>Estimation of VIF</th>
</tr>
</thead>
<tbody>
<tr>
<td>Entities spreading awareness (ESA)</td>
<td>3.8</td>
</tr>
<tr>
<td>Perceived usefulness (PU)</td>
<td>4.2</td>
</tr>
<tr>
<td>Perceived ease of use (PEU)</td>
<td>4.3</td>
</tr>
<tr>
<td>Awareness of cybercrimes (AOC)</td>
<td>4.7</td>
</tr>
<tr>
<td>Actual technology use (ATU)</td>
<td>4.9</td>
</tr>
<tr>
<td>Preventing cybercrimes in SCI (PCS)</td>
<td>4.6</td>
</tr>
</tbody>
</table>

Table V. Estimation of VIF
5.6 Structural equation modeling

SEM estimates the relationship prevalent among the latent variables. Computation of different parameters has been done with the application of AMOS 22. It helps to confirm whether the structure is correct and in order, and whether the structure has been able to represent the data. The results are shown in Table VIII.
Table VIII shows that all fit indices are within their acceptable limits. Thus, we have been able to establish the relative adequacy of the model fit. The detailed results containing paths, hypotheses, \( \beta \)-values and \( p \)-values are shown in Table IX.

After validation through standard statistical tools, the model is represented in Figure 2. It is the validated model.

<table>
<thead>
<tr>
<th>Fit index</th>
<th>Recommended value</th>
<th>Value in the model</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \chi^2/\text{degree of freedom (df)} )</td>
<td>( \leq 3.000 ) Chin and Todd (1995) and Gefen (2000)</td>
<td>2.013</td>
</tr>
<tr>
<td>Goodness of fit index (GFI)</td>
<td>( \geq 0.900 ) Hoyle (1995)</td>
<td>0.903</td>
</tr>
<tr>
<td>Adjusted goodness of fit index (AGFI)</td>
<td>( \geq 0.800 ) Segars and Grover (1993)</td>
<td>0.869</td>
</tr>
<tr>
<td>Comparative fit index (CFI)</td>
<td>( \geq 0.900 ) Hoyle (1995)</td>
<td>0.962</td>
</tr>
<tr>
<td>Tucker Lewis index (TLI)</td>
<td>( \geq 0.950 ) Hu and Bentler (1999)</td>
<td>0.957</td>
</tr>
<tr>
<td>Root mean square error (RMSE)</td>
<td>( \leq 0.080 ) Hu and Bentler (1999)</td>
<td>0.026</td>
</tr>
</tbody>
</table>

Table IX.
Detailed results relating to the research model

<table>
<thead>
<tr>
<th>Path</th>
<th>Hypothesis</th>
<th>Path coefficient (( \beta )-value)</th>
<th>( p )-value</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>GI → AOC</td>
<td>H1</td>
<td>0.012</td>
<td>ns (( p &gt; 0.05 ))</td>
<td>Not supported</td>
</tr>
<tr>
<td>SM → AOC</td>
<td>H2</td>
<td>0.512</td>
<td>**(( p &lt; 0.01 ))</td>
<td>Supported</td>
</tr>
<tr>
<td>WOM → AOC</td>
<td>H3</td>
<td>0.611</td>
<td>**(( p &lt; 0.01 ))</td>
<td>Supported</td>
</tr>
<tr>
<td>ORG → AOC</td>
<td>H4</td>
<td>0.502</td>
<td>**(( p &lt; 0.01 ))</td>
<td>Supported</td>
</tr>
<tr>
<td>LE → AOC</td>
<td>H5</td>
<td>0.017</td>
<td>ns (( p &gt; 0.05 ))</td>
<td>Not supported</td>
</tr>
<tr>
<td>PU → ATU</td>
<td>H6</td>
<td>0.479</td>
<td>***(( p &lt; 0.001 ))</td>
<td>Supported</td>
</tr>
<tr>
<td>PEU → ATU</td>
<td>H7</td>
<td>0.019</td>
<td>ns (( p &gt; 0.05 ))</td>
<td>Not supported</td>
</tr>
<tr>
<td>AOC → ATU</td>
<td>H8</td>
<td>0.627</td>
<td>***(( p &lt; 0.001 ))</td>
<td>Supported</td>
</tr>
<tr>
<td>AOC → PCS</td>
<td>H9</td>
<td>0.459</td>
<td>***(( p &lt; 0.001 ))</td>
<td>Supported</td>
</tr>
<tr>
<td>ATU → PCS</td>
<td>H10</td>
<td>0.666</td>
<td>***(( p &lt; 0.001 ))</td>
<td>Supported</td>
</tr>
</tbody>
</table>

Notes: ns, \( p > 0.05 \); **\( p < 0.01 \); ***\( p < 0.001 \)

Figure 2.
Structural model with path weights and level of significance

Notes: ns, \( p > 0.05 \); **\( p < 0.01 \); ***\( p < 0.001 \)
6. Discussions
From studies of literature, we considered that GI and effect of LE would influence the citizens of SCI toward improvement of their AOC (Ali, 2016). We hypothesized accordingly H1 and H5. We also considered that PEU would impact ATU (Henderson and Divett, 2003). We hypothesized accordingly H7. But, after validation, it appears that our assumptions based on literature review have been contradicted. H1, H5 and H7 have not been supported. Studies of literature helped us to hypothesize that SM, WoM, organizations have significant impacts on AOC (Kim and Park, 2013; Wisman, 2013; Singh, 2013). These presumptions corresponding to H2, H3 and H4, respectively, were found correct after validation. Impact of PU on ATU, impact of AOC on ATU, impact of AOC on PCS and impact of ATU on PCS have been considered through literature review (Davis, 1989; Sorebo et al., 2007; Abdul-Nasser, 2012; Aggarwal, 2015). This consideration received support from the validation results. H6, H8, H9 and H10 have been supported.

We have conceptually hypothesized ten hypotheses and developed a model shown in Figure 1. But, while we examined its validity through statistical tools, we found that out of the ten hypotheses, three hypotheses were not supported. These are impact of GI on AOC (H1) since the path coefficient (β-value) is found to be low (0.012) having no significance level (p > 0.05). Again, the impact of LE on AOC (H5) was not supported since the path coefficient (β-value) was found low like 0.017 having no significance level (p > 0.05). Besides, result also shows that the impact of PEU has no significant impact on ATU (H7), as the corresponding path coefficient (β-value) is low like 0.019 with no significance level (p > 0.05). Thus, out of ten hypotheses, it is seen that seven hypotheses have been supported like SM→AOC (H2) as its path coefficient (β-value) is as high as 0.512 with significance level p < 0.01. Again, WOM→AOC (H3) has been supported as its path coefficient (β-value) is 0.611 with significance level p < 0.01. ORG→AOC (H4) has been supported since the concerned path coefficient (β-value) is 0.502 with significance level p < 0.01. The PU→ATU (H6) has been supported since the path coefficient (β-value) is 0.479 having significance level p < 0.001. Again, AOC→ATU (H8) has been supported since the path coefficient (β-value) is 0.627 with significance level p < 0.01. AOC→PCS (H9) has been supported as the concerned path coefficient (β-value) is 0.459 with significance level p < 0.001. Again, ATU→PCS (H10) has been supported as the corresponding path coefficient (β-value) is 0.666 with significance level p < 0.001. Thus, H2, H5, H4, H6, H8, H9 and H10 have been supported, while H1, H5 and H7 have not been supported. The result shows that GI, SM, WOM, ORG and LE can explain AOC to the extent of 56 percent, as the concerned R² value is 0.56. Besides, PU, PEU and AOC can explain ATU to the tune of 62 percent as the concerned R² value is 0.62. Moreover, PCS can be explained by AOC and ATU to the tune of 80 percent as the corresponding R² is 0.80. Studies highlight that out of the determinants GI, SM, WOM, ORG and LE constituting the construct ESA impacting AOC, the factor WOM has the strongest impact on AOC and GI has the weakest impact over AOC, since the corresponding path coefficients (β-values) are 0.611 and 0.012, respectively. The influence of PU on ATU is appreciable, whereas the impact of PEU on ATU is insignificant since the corresponding path coefficients (β-values) are 0.479 and 0.019, respectively. Influences of AOC and ATU on PCS have been studied. It is found that out of these two constructs influencing PCS, the influence of ATU is more than the influence of AOC since the corresponding path coefficient (β-values) of ATU→PCS is more (0.666) than that of AOC→PCS (0.459). The reason for such variation of influence by several factors on AOC, ATU and PCS will be explained in the subsequent sections.

6.1 Theoretical implications
Our study has proposed and tested a theoretical model with AOC and ATU as two variables representing the individual context. Through analysis of our theoretical model, it appears
that it has good performances since eventually it could explain 80 percent of the PCS. This is because that while developing the theoretical model, we selected better-suited measures instead of directly using any standard model. We had analyzed the contexts exhaustively. Inclusion of AOC as a construct has added more theoretical value to the model because this construct effectively influences PCS directly.

Again, in considering the factors that would affect AOC, we did not consider many factors as it is found in other studies. The factors like ethics, attitude and awareness were taken into consideration (Ali, 2016) to explain awareness. But in the context of improvement of AOC, we did not consider those factors in the context of our theoretical mode (Mohit, 2012). We have developed our theoretical model with consideration of five factors like GI, WOM, SM, ORG and LE. These five factors constitute ESA. This construct ESA appreciably impacts AOC. Again, AOC, in turn, impacts PCS. It is our goal in this study. It has path coefficient ($\beta$-value) 0.459 with significance level $p < 0.001^{***}$. While considering the factors affecting ATU, we took help of the TAM (Davis, 1989) and considered that PU and PEU would impact ATU. While considering impact on ATU, we did not consider factors like performance, effectiveness, trust, risk perception, simplicity, compatibility and self-efficacy of the technology, though some researchers gave much stress on some of these factors (Lewis and Weigert, 1985; Kim, 2005). Since PU includes performance, effectiveness, trust and risk factors (Park, 2009) and PEU includes simplicity, compatibility and self-efficacy (Yi et al., 2009), the consideration of these factors separately was redundant.

This proposed theoretical model considers only some important and simple salient factors to explain PCS. Therefore, it is expected that this model will be used by the authorities and policy makers with ease. The explanatory power of this theoretical model is 80 percent. This high explanatory power of this theoretical model is presumably due to its simplicity and due to the inclusion of AOC and ATU as mediating variables. The theoretical proposed model has been able to explain 80 percent of the PCS. This indicates that the non-consideration of any type of moderator influencing individuals’ behavioral pattern could not adversely affect the efficiency of this proposed theoretical model. Criticism may be there for the non-inclusion of the moderators in our proposed model. It may be argued that, in that case, the explanatory power might have been more than 80 percent. Policy makers and authorities would be able to apply this theoretical model to combat cybercrimes in SCI.

7. Conclusion
In this study, we have identified some factors that would impact on improving AOC among the citizens of SCI. Among the awareness factors constituting ESA, it appears that GI has an insignificant impact on the AOC among the citizens of SCI. This lack has been criticized by the researchers. They opined that this is owing to slow working bureaucratic systems that fail to account emerging problems. This is owing to the lack of preparedness to face various technologies being used by the efficient cyber criminals (Hinduja, 2004; Moitra, 2005). Besides, the LE has no significant effects on AOC among citizens of SCI. The laws which help to punish the delinquents for commission of cybercrimes are not so forceful (McConnell, 2000). The laws are also found not befitting and not up to date to address the cybercrimes. This is because that a new nature of crimes is emerging based on updated technologies (Correia and Bowling, 1999; Atoum et al., 2014). This is due to the reluctance of police people to investigate cybercrimes with the help of existing cyber laws. They are found more agile to act against crimes of traditional nature (Goodman, 1997). LE against cybercrimes is not gaining momentum due to the lack of intimate connection between investigators and prosecutors (Davis, 2012). The concerned authorities are to brush up these defects effectively.

It is recommended to update the authorities for gaining better understanding to address the rapidly evolving cybertechnologies adopted by the cyber criminals (Gogolin and Jones, 2010). For this, attention is to be focused on updating existing laws commensurate with the
advancement of technologies. Efficiencies of specialized task force expected to work in SCI are to be enhanced. Effective promotion on cybercrime research activities is to be ensured. Effective utilization of civic resources available in SCI is to be made. Gathering the sad experience of the 9/11 attack, experts opined that cyber terrorists may attempt to damage information infrastructure and to damage key websites of different countries (Levi and Wall, 2004; Davis, 2012). Such untoward attack by cyber criminals may damage the very growth of SCI. It is imperative for the authorities to formulate a comprehensive plan toward the best to make all the stakeholders of SCI prepared for the worst.

It is necessary to adopt technological, legal and organizational pragmatic approaches to make the citizens of SCI aware for the prevention of cybercrimes. To detect crimes of traditional nature, the identification of fingerprints and DNA helps a lot. This is not available to detect cybercriminals. For this, it is suggested that IT facilities in SCI are to be appropriately enhanced for analyzing cybercrimes and detecting cybercriminals’ behavioral pattern (De Vel et al., 2001). Once these are achieved, the citizens of SCI will realize that laws are being able to punish the cybercriminals effectively and quickly. Then, the citizens of SCI will be influenced by the LE and their AOC will be increased. Besides, our findings show that AOC mediates the effect of ESA which constitutes GI, WOM, ORG, LE, SM on ATU. This ATU impacts PCS. AOC has a direct effect on PCS.

Besides utilizing the idea of TAM, we have been able to substantiate that at least PU has a direct effect on ATU by the citizens of SCI. This, in turn, helps to prevent cybercrimes. Thus, our empirical investigation highlights that proposed theoretical model may serve as a meaningful weapon to prevent cybercrimes. When SCI will be operational, this model would act as an effective instrument to combat cybercrimes in SCI. The citizens of SCI would then unhesitatingly use ICT to meet their needs.

Finally, when the entire results are summarized, we have reached the following key findings:

- prevention of cybercrimes in India, especially in the SC context, is important for successfully delivering digital services in SCI;
- entities such as WoM and SM are key contributors for spreading AOC among the citizens of SCI;
- the use of preventive technologies plays a significant role in the prevention of cybercrimes if the citizens can realize that the technologies are useful;
- the research studies highlight that the key determinants AOC and ATU being the mediating variables have maximum influence on PCS; and
- finally, a theoretical model is developed for the prevention of cybercrimes.

7.1 Practical and policy implications

The purpose of this study is to identify the factors that will be able to prevent cybercrimes. This has become necessary because in SCI, the citizens are expected to use ICT to meet their needs (Tryfonas et al., 2001). The government is also expected to take initiatives to involve the citizens to use ICT to make them smarter (Kickbusch and Gleicher, 2014). This would enhance the living standard of the citizens of SCI (Foster and Rosenzweig, 2010). The citizens of SCI would not use technology with the help of ICT if they feel that in using ICT, they would become victims of cybercrimes (Thomson et al., 2006). Hence, they are to be made aware regarding the cybercrimes and its consequences. In making the citizens aware, there are various factors that would improve awareness for the prevention of cybercrimes. These factors constitute ESA. This has been included in our model.
The result of the model shows that GI has an insignificant impact on AOC. For this, \( H1 \) was not supported while validating the conceptual model. The government or the policy makers need to significantly improve their initiatives to make the citizens of SCI aware regarding cybercrimes to help preventing cybercrimes. The SM has a significant impact on the citizens of SCI toward improvement of their awareness regarding cybercrimes. So, the SM can be used extensively to improve awareness of the citizens of SCI for preventing cybercrimes. WoM has a significant impact on AOC as is evident from the result. Thus, WoM acts as a significant ingredient that helps spreading AOC among the citizens of SCI. In smart cities, all the organizations are expected to use electronic media extensively for spreading their business activities. Thus, it is seen that organizations may also play a pivotal role to enhance AOC. It is seen that LE does not affect AOC in a significant way. Thus, government and policymakers are to improve enforcement of laws to increase AOC amongst the citizens of SCI.

Improvement of AOC would enhance the use of preventive technologies by the citizens of SCI to prevent cybercrimes. Actual usage of preventive technologies by the citizens of SCI would ensure PCS as is evident from the result. It is seen from the result that the PEU has an insignificant influence on the AUT, but, on the other side, PU has a positive impact on AUT. In practice, it is evident that citizens of SCI think that technology can play a pivotal role in protecting cybercrimes in SCI. This, in turn, encourages citizens of SCI to use technology for the prevention of cybercrimes. The citizens think that the use of technology to prevent cybercrimes is difficult to learn as is found from the result. Thus, the policy makers and the SC authorities need to make the citizens aware and the citizens should be trained to use different smart techniques with ease to prevent cybercrimes. This would enhance the ATU by the citizens of SCI to prevent cybercrimes. However, it is expected that the authorities will be able to use the proposed theoretical model to effectively prevent cybercrimes.

7.2 Societal implications

GoI has taken sincere initiatives to create 100 SCIs. For this, works are going on in full swing. When the SCI will be operational, the citizens would be involved in digital activities. The society would evolve as “digital society” or “cyber society.” In cyber society, there will be innumerable cyber activities. This could invite influx of cybercrimes. With passage of time, the number of commission of cybercrimes is expected to be increased. Hence, there is a need of prevention of cybercrimes. The citizens of SCI are to be made aware regarding the menace of cybercrimes. Increase of awareness among the citizens of the society would help to prevent cybercrimes. This article has provided effective mechanisms for the development of awareness among the prospective citizens regarding cybercrimes in terms of \( H1-H4 \). This development of awareness has a positive impact on the prevention of cybercrimes.

Besides, the citizens of the cyber society by developing AOC would be motivated to use the preventive technologies against cybercrimes. Thus, the use of preventive technologies in digital society is essential. Citizens of SCI are expected to use these preventive technologies if they feel that these preventive technologies would make them secured. Hence, societal needs in this context are to avail such preventive technologies which are useful and can be operated with ease. In this study, this has been confirmed through \( H6, H8, H9 \) and \( H10 \).

7.3 Limitations and directions for future research

We have taken appropriate precautions while undertaking the analysis to come to the findings. However, our findings of this study are to be interpreted cautiously in the light of specific limitations. We have used the sense of adoption from TAM (Davis, 1989). But, it may be argued that we have developed the model without the consideration of some citizen-specific factors. These are experience, voluntariness, age factor and gender factor. This might be available in other adoption-related standard models. These are important
moderators as they moderate behavioral patterns (Venkatesh et al., 2003). We did not consider this because we have found no prior studies on which they depended on these moderators. These studies did not give any concrete information concerning contribution of these moderators also. The absence of consideration of these moderators is presumed to not have undermined our results completely. However, it may be construed as a limitation. The future researchers may consider the effects of these moderators.

Apart from the factors we have considered having impact on AOC in SCI, the future researchers may consider other additional factors like risk factors, trust factor and so on, as is found to have been nurtured in other studies (Williams et al., 2009). The result of the study was arrived at by having inputs from a mixed sample of citizens. They had different professions. They had varied educational qualifications as it appears from the demographics of the people shown in the concerned table. The inputs were utilized to validate the conceptual model and the hypotheses. It is suggested that the future researchers should only pick and choose those personalities who had specific knowledge regarding ICT exclusively in handling cybercrimes in SCI. Here, we have not considered such representations exclusively. It is not known if all the respondents in our survey works have adequate knowledge to handle for the prevention of cybercrimes. We have considered representations of the people of some of the metropolitan cities of India where there exist or there would be smart cities. But, GoI has proposed 100 smart cities across the various parts of India. Hence, we ought to have considered representations from other cities. It would have helped to provide our results in a generic form. This gap was not filled up. This is left for the future researchers to nurture. Finally, in our study, we could explain the ultimate construct PCS to the tune of 80 percent ($R^2 = 0.80$). It is left for the future researchers to identify and test other boundary conditions in addition to provide a more comprehensive and richer realization.

References


Further reading


### Prevention of cybercrimes

<table>
<thead>
<tr>
<th>Item/construct</th>
<th>Statement</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Entities spreading awareness (ESA)</strong></td>
<td></td>
</tr>
<tr>
<td>ESA1</td>
<td>Spreading awareness on cyberthreats is important to prevent cybercrimes</td>
</tr>
<tr>
<td>ESA2</td>
<td>Various entities should be involved for spreading awareness on cybercrimes</td>
</tr>
<tr>
<td>ESA3</td>
<td>I get information on cyberthreats from different government initiatives</td>
</tr>
<tr>
<td>ESA4</td>
<td>Government initiatives are effective to make citizens aware of cyberattacks</td>
</tr>
<tr>
<td>ESA5</td>
<td>Government is doing an excellent job by spreading awareness on cybercrimes</td>
</tr>
<tr>
<td>ESA6</td>
<td>I use social media extensively for gathering information</td>
</tr>
<tr>
<td>ESA8</td>
<td>Social media provides vital information on different cyberthreats</td>
</tr>
<tr>
<td>ESA9</td>
<td>Social media is an important instrument combating cybercrime</td>
</tr>
<tr>
<td>ESA10</td>
<td>I know how to use internet securely</td>
</tr>
<tr>
<td>ESA11</td>
<td>All the inhabitants of smart cities of India would use social media extensively</td>
</tr>
<tr>
<td>ESA12</td>
<td>I learn on cyberthreats from other people</td>
</tr>
<tr>
<td>ESA13</td>
<td>My friends and relatives discuss about the menace of cyberattacks with me</td>
</tr>
<tr>
<td>ESA14</td>
<td>I am aware of IT Act in India and its provisions</td>
</tr>
<tr>
<td>ESA15</td>
<td>Legal enforcement is essential to spread awareness on cyberthreats among citizens</td>
</tr>
<tr>
<td>ESA16</td>
<td>Organizations in the smart cities would play important roles in cyber awareness</td>
</tr>
<tr>
<td>ESA17</td>
<td>My organization makes me aware about different cyberthreats</td>
</tr>
<tr>
<td><strong>Perceived usefulness (PU)</strong></td>
<td></td>
</tr>
<tr>
<td>PU1</td>
<td>Proper application of technology can help to prevent cybercrimes</td>
</tr>
<tr>
<td>PU2</td>
<td>I use different techniques to protect myself from different cybercrimes</td>
</tr>
<tr>
<td>PU3</td>
<td>Citizens of smart cities would use technology extensively to prevent cybercrimes</td>
</tr>
<tr>
<td><strong>Perceived ease of use (PEU)</strong></td>
<td></td>
</tr>
<tr>
<td>PEU1</td>
<td>I find it easy to use different tools and technologies for the protection of cyberthreats</td>
</tr>
<tr>
<td>PEU2</td>
<td>I expect most of the citizens of smart cities would find it easier to use different tools and technologies to protect themselves from cybercrimes</td>
</tr>
<tr>
<td>PEU3</td>
<td>I perceived that in future the technology to protect from cybercrimes would become easier to use by the citizens</td>
</tr>
<tr>
<td><strong>Awareness of cybercrimes (AOC)</strong></td>
<td></td>
</tr>
<tr>
<td>AOC1</td>
<td>I am aware of various kinds of cyberthreats</td>
</tr>
<tr>
<td>AOC2</td>
<td>It is important for me to know about different cybercrimes</td>
</tr>
<tr>
<td>AOC3</td>
<td>All the citizens in smart cities should be aware of different cybercrimes</td>
</tr>
<tr>
<td><strong>Actual technology use (ATU)</strong></td>
<td></td>
</tr>
<tr>
<td>ATU1</td>
<td>Citizens of the smart cities should be trained how to use technology efficiently to prevent cybercrimes</td>
</tr>
<tr>
<td>ATU2</td>
<td>I have proper training to use different tools and technologies for protecting myself from various kinds of cybercrimes</td>
</tr>
<tr>
<td>ATU3</td>
<td>All the citizens in smart cities need to use different technologies extensively for preventing cybercrimes</td>
</tr>
<tr>
<td><strong>Preventing cybercrimes in SCI (PCS)</strong></td>
<td></td>
</tr>
<tr>
<td>PCS1</td>
<td>Cybercrimes can be prevented by making citizens aware</td>
</tr>
<tr>
<td>PCS2</td>
<td>Technology plays a vital role in preventing cybercrimes in smart cities of India</td>
</tr>
<tr>
<td>PCS3</td>
<td>I believe authorities would take sufficient measures for preventing cybercrimes in smart cities of India</td>
</tr>
</tbody>
</table>

Table AI. Items and questionnaire
Table AII. Computations of loadings and cross-loadings

<table>
<thead>
<tr>
<th></th>
<th>ESA</th>
<th>PU</th>
<th>PEU</th>
<th>AOC</th>
<th>ATU</th>
<th>PCS</th>
</tr>
</thead>
<tbody>
<tr>
<td>ESA1</td>
<td>0.872</td>
<td>0.432</td>
<td>0.462</td>
<td>0.491</td>
<td>0.417</td>
<td>0.451</td>
</tr>
<tr>
<td>ESA2</td>
<td>0.866</td>
<td>0.401</td>
<td>0.462</td>
<td>0.500</td>
<td>0.416</td>
<td>0.402</td>
</tr>
<tr>
<td>ESA3</td>
<td>0.915</td>
<td>0.506</td>
<td>0.417</td>
<td>0.417</td>
<td>0.411</td>
<td>0.426</td>
</tr>
<tr>
<td>ESA4</td>
<td>0.844</td>
<td>0.413</td>
<td>0.431</td>
<td>0.419</td>
<td>0.490</td>
<td>0.417</td>
</tr>
<tr>
<td>ESA5</td>
<td>0.911</td>
<td>0.333</td>
<td>0.437</td>
<td>0.418</td>
<td>0.491</td>
<td>0.471</td>
</tr>
<tr>
<td>ESA6</td>
<td>0.867</td>
<td>0.412</td>
<td>0.421</td>
<td>0.417</td>
<td>0.498</td>
<td>0.433</td>
</tr>
<tr>
<td>ESA7</td>
<td>0.810</td>
<td>0.451</td>
<td>0.496</td>
<td>0.416</td>
<td>0.496</td>
<td>0.344</td>
</tr>
<tr>
<td>ESA8</td>
<td>0.812</td>
<td>0.424</td>
<td>0.311</td>
<td>0.412</td>
<td>0.492</td>
<td>0.390</td>
</tr>
<tr>
<td>ESA9</td>
<td>0.876</td>
<td>0.416</td>
<td>0.359</td>
<td>0.490</td>
<td>0.501</td>
<td>0.311</td>
</tr>
<tr>
<td>ESA10</td>
<td>0.835</td>
<td>0.382</td>
<td>0.491</td>
<td>0.399</td>
<td>0.490</td>
<td>0.317</td>
</tr>
<tr>
<td>ESA11</td>
<td>0.888</td>
<td>0.501</td>
<td>0.371</td>
<td>0.463</td>
<td>0.493</td>
<td>0.361</td>
</tr>
<tr>
<td>ESA12</td>
<td>0.871</td>
<td>0.362</td>
<td>0.401</td>
<td>0.461</td>
<td>0.492</td>
<td>0.409</td>
</tr>
<tr>
<td>ESA13</td>
<td>0.800</td>
<td>0.492</td>
<td>0.388</td>
<td>0.490</td>
<td>0.490</td>
<td>0.416</td>
</tr>
<tr>
<td>ESA14</td>
<td>0.842</td>
<td>0.302</td>
<td>0.492</td>
<td>0.417</td>
<td>0.493</td>
<td>0.437</td>
</tr>
<tr>
<td>ESA15</td>
<td>0.861</td>
<td>0.399</td>
<td>0.498</td>
<td>0.416</td>
<td>0.420</td>
<td>0.333</td>
</tr>
<tr>
<td>ESA16</td>
<td>0.799</td>
<td>0.471</td>
<td>0.500</td>
<td>0.311</td>
<td>0.490</td>
<td>0.462</td>
</tr>
<tr>
<td>ESA17</td>
<td>0.820</td>
<td>0.490</td>
<td>0.490</td>
<td>0.408</td>
<td>0.496</td>
<td>0.411</td>
</tr>
<tr>
<td>PU1</td>
<td>0.417</td>
<td>0.799</td>
<td>0.401</td>
<td>0.405</td>
<td>0.499</td>
<td>0.426</td>
</tr>
<tr>
<td>PU2</td>
<td>0.416</td>
<td>0.886</td>
<td>0.382</td>
<td>0.393</td>
<td>0.491</td>
<td>0.431</td>
</tr>
<tr>
<td>PU3</td>
<td>0.438</td>
<td>0.812</td>
<td>0.309</td>
<td>0.390</td>
<td>0.501</td>
<td>0.437</td>
</tr>
<tr>
<td>PEU1</td>
<td>0.496</td>
<td>0.411</td>
<td>0.872</td>
<td>0.411</td>
<td>0.502</td>
<td>0.490</td>
</tr>
<tr>
<td>PEU2</td>
<td>0.501</td>
<td>0.417</td>
<td>0.810</td>
<td>0.416</td>
<td>0.490</td>
<td>0.411</td>
</tr>
<tr>
<td>PEU3</td>
<td>0.309</td>
<td>0.424</td>
<td>0.844</td>
<td>0.417</td>
<td>0.496</td>
<td>0.431</td>
</tr>
<tr>
<td>AOC1</td>
<td>0.412</td>
<td>0.416</td>
<td>0.419</td>
<td>0.886</td>
<td>0.411</td>
<td>0.437</td>
</tr>
<tr>
<td>AOC2</td>
<td>0.424</td>
<td>0.419</td>
<td>0.418</td>
<td>0.812</td>
<td>0.407</td>
<td>0.431</td>
</tr>
<tr>
<td>AOC3</td>
<td>0.504</td>
<td>0.492</td>
<td>0.496</td>
<td>0.872</td>
<td>0.431</td>
<td>0.492</td>
</tr>
<tr>
<td>ATU1</td>
<td>0.302</td>
<td>0.311</td>
<td>0.491</td>
<td>0.411</td>
<td>0.800</td>
<td>0.390</td>
</tr>
<tr>
<td>ATU2</td>
<td>0.409</td>
<td>0.317</td>
<td>0.317</td>
<td>0.417</td>
<td>0.864</td>
<td>0.361</td>
</tr>
<tr>
<td>ATU3</td>
<td>0.399</td>
<td>0.492</td>
<td>0.333</td>
<td>0.438</td>
<td>0.871</td>
<td>0.317</td>
</tr>
<tr>
<td>PCS1</td>
<td>0.421</td>
<td>0.407</td>
<td>0.433</td>
<td>0.496</td>
<td>0.416</td>
<td>0.380</td>
</tr>
<tr>
<td>PCS2</td>
<td>0.457</td>
<td>0.398</td>
<td>0.411</td>
<td>0.416</td>
<td>0.401</td>
<td>0.388</td>
</tr>
<tr>
<td>PCS3</td>
<td>0.450</td>
<td>0.390</td>
<td>0.407</td>
<td>0.490</td>
<td>0.419</td>
<td>0.911</td>
</tr>
</tbody>
</table>

Note: The loadings have been shown in this table in italics

Table AIII. Statement of hypothesis and remarks

<table>
<thead>
<tr>
<th>Hypothesis</th>
<th>Statement</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>H1</td>
<td>Government initiatives (GI) would positively impact the awareness of cybercrimes (AOC)</td>
<td>Not supported</td>
</tr>
<tr>
<td>H2</td>
<td>Social media (SM) will have a positive impact to enhance awareness of cybercrimes (AOC) of SCI toward cybercrimes</td>
<td>Supported</td>
</tr>
<tr>
<td>H3</td>
<td>Word of mouth (WOM) has a positive impact on the awareness of cybercrimes (AOC) among the citizens of SCI</td>
<td>Supported</td>
</tr>
<tr>
<td>H4</td>
<td>Organizations (ORG) have a positive impact on the awareness of cybercrimes (AOC) among the citizens of SCI</td>
<td>Supported</td>
</tr>
<tr>
<td>H5</td>
<td>Legal enforcement (LE) has a positive impact on the awareness of cybercrimes (AOC) of the citizens of SCI</td>
<td>Not supported</td>
</tr>
<tr>
<td>H6</td>
<td>Perceived usefulness (PU) has a positive impact on actual technology use (ATU)</td>
<td>Supported</td>
</tr>
<tr>
<td>H7</td>
<td>Perceived ease of use (PEU) has a positive impact on actual technology use (ATU)</td>
<td>Supported</td>
</tr>
<tr>
<td>H8</td>
<td>Awareness of cybercrimes (AOC) of SCI has a positive impact on citizens’ behavior to actual technology use (ATU)</td>
<td>Supported</td>
</tr>
<tr>
<td>H9</td>
<td>Awareness of cybercrimes (AOC) positively affects the prevention of cybercrimes (PCS) in SCI</td>
<td>Supported</td>
</tr>
<tr>
<td>H10</td>
<td>Actual technology use (ATU) has a positive impact on the prevention of cybercrimes in SCI (PCS)</td>
<td>Supported</td>
</tr>
<tr>
<td></td>
<td>$\beta$-value</td>
<td>Hypothesis</td>
</tr>
<tr>
<td>----------------------</td>
<td>---------------</td>
<td>------------</td>
</tr>
<tr>
<td>Effect on AOC</td>
<td></td>
<td></td>
</tr>
<tr>
<td>By GI</td>
<td>0.012</td>
<td>$H_1$</td>
</tr>
<tr>
<td>By SM</td>
<td>0.512</td>
<td>$H_2$</td>
</tr>
<tr>
<td>By WOM</td>
<td>0.611</td>
<td>$H_3$</td>
</tr>
<tr>
<td>By ORG</td>
<td>0.502</td>
<td>$H_4$</td>
</tr>
<tr>
<td>By LE</td>
<td>0.017</td>
<td>$H_5$</td>
</tr>
<tr>
<td>Effect on ATU</td>
<td></td>
<td></td>
</tr>
<tr>
<td>By AOC</td>
<td>0.627</td>
<td>$H_8$</td>
</tr>
<tr>
<td>By PU</td>
<td>0.479</td>
<td>$H_6$</td>
</tr>
<tr>
<td>By PEU</td>
<td>0.019</td>
<td>$H_7$</td>
</tr>
<tr>
<td>Effect on PCS</td>
<td></td>
<td></td>
</tr>
<tr>
<td>By AOC</td>
<td>0.459</td>
<td>$H_9$</td>
</tr>
<tr>
<td>By ATU</td>
<td>0.666</td>
<td>$H_{10}$</td>
</tr>
</tbody>
</table>

Corresponding author
Yogesh K. Dwivedi can be contacted at: ykwivedi@gmail.com

For instructions on how to order reprints of this article, please visit our website:
www.emeraldgrouppublishing.com/licensing/reprints.htm
Or contact us for further details: permissions@emeraldinsight.com
Preventing identity theft

Identifying major barriers to knowledge-sharing in online retail organisations

Abdullah Maitlo
Computer Science Department, Shah Abdul Latif University, Khairpur, Pakistan

Nisreen Ameen
Lord Ashcroft International Business School, Anglia Ruskin University – Cambridge Campus, Cambridge, UK

Hamid Reza Peikari
Department of Management, Isfahan (Khorasgan) Branch, Islamic Azad University, Isfahan, Iran, and

Mahmood Shah
School of Strategy and Leadership, Coventry University, Coventry, UK

Abstract

Purpose – Knowledge-sharing (KS) for preventing identity theft has become a major challenge for organisations. The purpose of this paper is to fill a gap in the literature by investigating barriers to effective KS in preventing identity theft in online retail organisations.

Design/methodology/approach – A framework was proposed based on a reconceptualisation and extension of the KS enablers framework (Chong et al., 2011). A qualitative case study research method was used for the data collection. In total, 34 semi-structured interviews were conducted in three online retail organisations in the UK.

Findings – The findings suggest that the major barriers to effective KS for preventing identify theft in online retail organisations are: lack of leadership support; lack of employee willingness to share knowledge; lack of employee awareness of KS; inadequate learning opportunities; lack of trust in colleagues; insufficient information-sourcing opportunities and information and communications technology infrastructure; a weak KS culture; lack of feedback on performance; and lack of job rotation.

Practical implications – The research provides solutions for removing existing barriers to KS in preventing identity theft. This is important to reduce the number of cases of identity theft in the UK.

Originality/value – This research extends knowledge of KS in a new context: preventing identity theft in online retail organisations. The proposed framework extends the KS enablers framework by identifying major barriers to KS in the context of preventing identity theft.

Keywords Qualitative method, Case study

Paper type Research paper

1. Introduction

Information has become an increasingly valuable asset, and hackers are frequently accessing and abusing the sensitive information of organisations and individuals for financial gain (Liu et al., 2011). The total direct cost of retail crime increased by 6 per cent more than in 2016 to just over £700m in 2017 (BRC, 2017). Identity theft is one of the fastest-growing online crimes (Abdullah et al., 2016) and it affects the online retail industry (Rahman et al., 2018; Sayles, 2012; Tian et al., 2018). It refers to stealing someone’s whole identity, their personal information or their bank card details (Abdullah et al., 2016). The major challenges associated with identity-related offences include credit problems for consumers (such as aggravation by debt collectors and the rejection of loan applications), disruption to normal life (such as reputation damage) and the psychological difficulty of providing personal data to organisations and banks during an investigation (Kirk, 2014; Spanaki et al., 2018; Tsou and Holtkamp, 2018). Enhanced awareness of identity theft and media reports of these crimes have intensified interest and attracted the attention of consumers, organisations, governments and researchers...
(Almerdas, 2014; Chakraborty et al., 2016; Doargajudhur and Dell, 2018; Walt et al., 2018). Such incidents can have numerous consequences; for example, loss of customer confidence, damage to an organisation’s reputation, legal issues and financial losses (Kerr et al., 2013). In 2017, 175,000 cases of identity theft were recorded: an increase of 125 per cent over ten years (Cifas, 2018; Hughes, 2018). Fraudsters continued to focus on online applications, with 88 per cent of identity fraud cases being internet-enabled (Cifas, 2018).

To prevent such security threats and attacks, organisations have several options. These include identifying the risks and sharing knowledge about information security (Doherty and Tajuddin, 2018; He and Johnson, 2015; Liu et al., 2011; Naicker and Van Der Merwe, 2018). Having sufficient information and knowledge to handle threats is crucial for recognising and reducing risks (Safa et al., 2015). Therefore, organisations need to collect and share knowledge on security risks and find solutions for reducing them (Feledi et al., 2013). Knowledge-sharing (KS) is the process through which individuals share their expertise and experiences with others to find new ideas or deal with challenges and problems (Ortiz et al., 2017). Sharing knowledge with employees can avoid similar security solutions being created more than once and leads to more effective security measures (Feledi et al., 2013). Indeed, KS plays a vital role in increasing the knowledge of individuals within organisations (Charband and Navimipour, 2016; Hwang et al., 2018; Zhang et al., 2018).

Table AI contains the most relevant and frequently cited studies that have investigated KS. The information illustrates that although numerous studies have explored KS in specific contexts, the findings cannot be generalised. Previous studies have reported diverse barriers to KS, which implies that these barriers differ according to the business and knowledge context (Pirkkalainen and Pawlowski, 2014; Tjøfjåt et al., 2017). As a result, the authors have called for more research into KS barriers in new contexts (Blagov et al., 2017). Thus, due to the specific nature of the knowledge shared, it has been suggested that KS in the context of information security is different from KS in other contexts (Tamjidyamcholo et al., 2014).

KS can help in the context of handling online identity theft (Feledi et al., 2013; He and Johnson, 2015; Liu et al., 2011; Safa et al., 2015). However, there is a lack of research on the effective sharing of knowledge on security and best practices (He and Johnson, 2015; Khakurel et al., 2018; Ochieng et al., 2018). The need for research into barriers to knowledge management in the context of information security has been highlighted by previous studies (Gal-Or and Ghose, 2005; Gordon et al., 2003; Liu et al., 2011; Tamjidyamcholo et al., 2014). There is a general lack of knowledge about which barriers to KS are most important in organisations (Riege, 2005); this is even more pressing in the context of information security, where few studies have investigated KS (Flores et al., 2014; Safa and Von Solms, 2016). More specifically, very little work has been done regarding KS in the prevention of identity theft (Abdullah et al., 2016).

Individuals and groups need to enhance their knowledge about issues of identity theft and how to protect themselves, and companies need to implement KS processes to prevent identity theft in their own organisations. However, existing barriers to these KS processes present major obstacles to enhancing the knowledge of employees working in online retail organisations. In large organisations, employees have fewer opportunities to share their knowledge face to face; therefore, KS barriers are more severe in larger online retail organisations than in small- and medium-sized enterprises (Tamjidyamcholo et al., 2014). This calls for more research in larger organisations. Hence, the main aim of this research is to bridge the gap in the literature by investigating the existing barriers affecting KS processes in large online retail organisations. The KS enablers framework proposed by Chong et al. (2011) includes KS implementation issues; hence, it was adopted as the underlying theoretical framework for this study.

This research makes theoretical and practical contributions. First, it bridges a gap in the literature by providing a comprehensive framework for a full understanding of the barriers to KS for preventing identity theft in online retail organisations. Second, it contributes to the
existing literature by reconceptualising and extending the KS enablers framework proposed by Chong *et al.* (2011) in the context of identity theft in retail organisations in the UK. Three new factors related to the context of this study are added to the framework: lack of employee willingness to share knowledge, lack of employee awareness and lack of trust in colleagues. Third, the research has several practical implications. Sharing lessons learned and knowledge about the practice of preventing identity theft can help organisations reconsider their processes and evaluate whether their security procedures are addressing the concerns raised. Indeed, this study seeks to provide practical guidelines for overcoming diverse KS barriers more successfully in the context of preventing identity theft.

The remainder of this paper is organised into the following sections: a review of the literature; a discussion of the research methods employed; a presentation of the findings; a discussion of their importance; the theoretical contributions, limitations recommendations for future research; and, finally, the conclusion.

2. Literature review

Binder and Gill (2005) explain that it is difficult to measure the effectiveness of methods of preventing identity theft. Nevertheless, Duffin *et al.* (2006) argue that one of the most effective ways to prevent identity theft is to adopt effective organisational preventive control measures, which are often linked to the company’s employees. Kerr *et al.* (2013) explain that sanctions and sentencing play an important role in preventing further cases of identity fraud. Meanwhile, Button and Gee (2013) highlight the importance of creating an anti-fraud culture in the organisation that encourages honesty and trust. Interestingly, national culture is also highlighted as an important influence on organisational culture (Button and Gee, 2013). In addition, Button *et al.* (2014) emphasise the importance of education and training in the prevention of identity fraud.

The review of the literature finds that the online retail industry acknowledges the importance of KS (Charband and Navimipour, 2016; Kozlowski *et al.*, 2016; Lai *et al.*, 2016; White and Fisher, 2008). However, many online retail organisations face difficulties with collecting, integrating and developing appropriate information and practices (Bhatt *et al.*, 2010; Jonsson and Kalling, 2007). Furthermore, even when knowledge is shared, convincing people to provide and use stored knowledge resources is a challenge (Ardichvili *et al.*, 2003; Suppiah and Singh Sandhu, 2011). A critical examination of the factors that influence KS reveals that they fall into three categories: individual (Alamahamid *et al.*, 2010; Lee and Al-Hawamdeh, 2002; Riege, 2005; Wang *et al.*, 2015), organisational (Islam *et al.*, 2012; Ives *et al.*, 1997; Kim and Lee, 2004; Martin *et al.*, 2010) and technological (Alavi and Leidner, 2001; Argote *et al.*, 2003). These three overarching factors are highlighted by many investigators (e.g. Islam *et al.*, 2012; Ives *et al.*, 1997; Kim and Lee, 2004; Martin *et al.*, 2010; Salleh, 2010).

It can be argued that many of the obstructions to successful KS methods are related to individuals, as KS has a human element as its core (Donate and Guadamillas, 2015). People are complicated, with different psychological needs (Donate and Guadamillas, 2015). Table I shows that existing studies have identified nine main barriers to KS in organisations and have highlighted different areas related to each of these barriers. However, there is a lack of research on the main barriers to KS in the context of identity theft. On the other hand, several factors have been identified as enablers for knowledge management in public organisations (Chong *et al.*, 2011). These enablers are knowhow and skill in information and communications technology (ICT), job training, job rotation, feedback on performance, learning opportunities, information-sourcing opportunities, leadership support, a KS culture, ICT infrastructure and software, knowledge-management technologies and the KS process (Chong *et al.*, 2011). If these enablers are absent, the process of KS cannot take place (Chong *et al.*, 2011).
<table>
<thead>
<tr>
<th>Barrier</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>Lack of employee willingness</em></td>
<td></td>
</tr>
<tr>
<td>The accomplishment of KS efforts depends largely on the willingness of</td>
<td>Hislop (2002)</td>
</tr>
<tr>
<td>employees</td>
<td></td>
</tr>
<tr>
<td>Individuals’ positive behaviour and attitude affect KS and benefit the</td>
<td>Chang and Chuang (2011);</td>
</tr>
<tr>
<td>organisation</td>
<td>Sheehan (2016)</td>
</tr>
<tr>
<td>Employees who are satisfied with their jobs and committed to their</td>
<td>Robertson and O’Malley</td>
</tr>
<tr>
<td>companies are willing to share knowledge, and they believe that the</td>
<td>Hammersley (2000)</td>
</tr>
<tr>
<td>advantages for the organisation are to their benefit</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><em>Lack of individual employee awareness</em></td>
<td></td>
</tr>
<tr>
<td>Individual employee awareness is important for successfully implementing</td>
<td>Ismail and Yusof (2010)</td>
</tr>
<tr>
<td>the KS process in an organisation</td>
<td></td>
</tr>
<tr>
<td>Individual employee awareness is considered to be a tool for improving</td>
<td>Daneshgar (2001)</td>
</tr>
<tr>
<td>co-operation, sharing and knowledge in a collective process</td>
<td></td>
</tr>
<tr>
<td>Awareness is considered to be a key component for the efficient</td>
<td>Cong and Pandya (2003),</td>
</tr>
<tr>
<td>implementation of a KS programme for employees</td>
<td>Safa et al. (2016)</td>
</tr>
<tr>
<td>Individual awareness is essential for successfully implementing the KS</td>
<td>Safa et al. (2016)</td>
</tr>
<tr>
<td>process in an organisation</td>
<td></td>
</tr>
<tr>
<td>Providing awareness of KS is a major challenge in the process of KS in</td>
<td>Zahedi et al. (2016)</td>
</tr>
<tr>
<td>an organisation</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><em>Inadequate learning opportunities</em></td>
<td></td>
</tr>
<tr>
<td>An employee learning environment describes procedures that increase</td>
<td>Mohammad Hossein and Nadalipour (2016)</td>
</tr>
<tr>
<td>skills and capabilities in routine work</td>
<td>Harteis et al. (2008)</td>
</tr>
<tr>
<td>Learning opportunities increase the progress in working outcomes by</td>
<td></td>
</tr>
<tr>
<td>illuminating mistakes made and weaknesses in organisations</td>
<td></td>
</tr>
<tr>
<td>Organisations provide various training opportunities to their employees</td>
<td>Dymock and McCarthy (2006)</td>
</tr>
<tr>
<td>Training is a learning opportunity to enhance technological skills for</td>
<td>Hortovanyi and Ferincz (2015)</td>
</tr>
<tr>
<td>computer use and KS</td>
<td></td>
</tr>
<tr>
<td>Companies also provide training to enhance the working knowledge of</td>
<td>De Grip and Sauer mann (2013)</td>
</tr>
<tr>
<td>their employees</td>
<td>Lui (2013), Smith (2012)</td>
</tr>
<tr>
<td>Lack of a learning environment in any organisation is a barrier to</td>
<td></td>
</tr>
<tr>
<td>enhancing the knowledge of individuals and teams</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><em>Lack of trust in KS</em></td>
<td></td>
</tr>
<tr>
<td>Trust in others is one of the main elements in the process of KS</td>
<td>Bäläu and Utz (2016),</td>
</tr>
<tr>
<td></td>
<td>Hashim and Tan (2015),</td>
</tr>
<tr>
<td></td>
<td>Uso ro et al. (2007)</td>
</tr>
<tr>
<td>Social exchange arises when individuals co-operate in a KS process.</td>
<td>Lee et al. (2010), Liebowitz (1999), White (2001)</td>
</tr>
<tr>
<td>In this process, trust is significant and essential to sharing</td>
<td></td>
</tr>
<tr>
<td>knowledge</td>
<td>Bov et al. (2002), Hsu et al. (2007), Jones and George (1998),</td>
</tr>
<tr>
<td>Trust is the backbone of a KS process in any organisation. Employees</td>
<td>Ridings et al. (2002) Roth and Broad (2008), Safa et al. (2016),</td>
</tr>
<tr>
<td>will work efficiently if they have the trust of others working with</td>
<td>Hsu et al. (2007), Ruten et al. (2016), Safa et al. (2016)</td>
</tr>
<tr>
<td>them</td>
<td>Scott Holste and Fields (2010)</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>*Various empirical studies support the importance of trust when sharing</td>
<td></td>
</tr>
<tr>
<td>knowledge in an organisation</td>
<td>Pervaiz et al. (2016)</td>
</tr>
<tr>
<td>Trust is closely linked to KS</td>
<td></td>
</tr>
<tr>
<td>Trust and sincerity could support strong KS performance through</td>
<td></td>
</tr>
<tr>
<td>successful communication promptness by providing a mandate to the</td>
<td></td>
</tr>
<tr>
<td>members of organisations for sharing the knowledge that they possess</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><em>Lack of feedback on performance in identity-theft prevention</em></td>
<td></td>
</tr>
<tr>
<td>Feedback on learning and access to learning resources are significant</td>
<td>Abdullah et al. (2009)</td>
</tr>
<tr>
<td>and point toward a strong role in KS</td>
<td></td>
</tr>
</tbody>
</table>

(continued)
The KS enablers framework developed by Chong et al. (2011) forms the basis of the framework proposed in this paper. It was selected for three main reasons. First, the framework integrates the main factors that are significant for KS in the existing literature (as shown in Table I). Second, the framework was among the first to address the lack of knowledge on the topic of KS in an organisational context. Third, the framework is comprehensive in terms of identifying the KS enablers at the organisational, technological and individual levels. Although the existing literature offers other frameworks, such as the KS enablers frameworks proposed by Allameh and Zare (2011), Kanaan et al. (2013) and

<table>
<thead>
<tr>
<th>Barrier</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Evaluation and feedback are paramount. The need to create a system for</strong></td>
<td>Omotayo (2015)</td>
</tr>
<tr>
<td><strong>evaluating attempts made to use knowledge management is important</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Lack of an efficient ICT infrastructure and insufficient information-sourcing opportunities</strong></td>
<td>Bhatt et al. (2010), Khan et al. (2016)</td>
</tr>
<tr>
<td>IT resources and the substantial procedures are important for making</td>
<td></td>
</tr>
<tr>
<td>organisational learning or knowledge available by expediting KS among the</td>
<td></td>
</tr>
<tr>
<td>skilled workforce</td>
<td></td>
</tr>
<tr>
<td>The knowledge-management technology infrastructure includes the following</td>
<td>Holtsapple (2013), Martin (2000)</td>
</tr>
<tr>
<td>elements: intranet, communication networks, e-mail, data warehousing and</td>
<td></td>
</tr>
<tr>
<td>the decision support system. It is necessary for KS in the organisation</td>
<td></td>
</tr>
<tr>
<td>KS requires different technologies, such as the internet, intranets and</td>
<td></td>
</tr>
<tr>
<td>groupware, which connect organisations at the intra-organisational and inter-</td>
<td></td>
</tr>
<tr>
<td>organisational level, and throughout the world</td>
<td></td>
</tr>
<tr>
<td><strong>Lack of leadership support</strong></td>
<td>Bass and Stogdill (1990), Maethel and Hoegl (2016)</td>
</tr>
<tr>
<td>Leadership has an important role in managing the KS process in any organisation</td>
<td></td>
</tr>
<tr>
<td>Leadership is accountable for practising strategic planning for efficient use of</td>
<td>Boerner et al. (2007)</td>
</tr>
<tr>
<td>means and promoting learning culture and KS</td>
<td></td>
</tr>
<tr>
<td>Leadership is required to bring about an unrestricted culture and to build an</td>
<td>Chuang et al. (2016)</td>
</tr>
<tr>
<td>environment for KS</td>
<td></td>
</tr>
<tr>
<td>Senior management must provide support to promote the significance of KS</td>
<td>Mittal and Rajib (2015)</td>
</tr>
<tr>
<td>and signify KS approaches</td>
<td></td>
</tr>
<tr>
<td>Senior executives and others in the management team need to use the knowledge</td>
<td>Aga et al. (2016), Barnes (2001)</td>
</tr>
<tr>
<td>of others before taking action, and reward those who share their knowledge</td>
<td></td>
</tr>
<tr>
<td><strong>Weak KS culture</strong></td>
<td>McDermott and O'Dell (2001)</td>
</tr>
<tr>
<td>Organisational culture refers to the shared values, beliefs and performances</td>
<td></td>
</tr>
<tr>
<td>of people in an organisation</td>
<td></td>
</tr>
<tr>
<td>Organisational culture is one of the main elements considered in the organisation for KS among individuals and teams</td>
<td>Syed-Ikhsan and Rowland (2004)</td>
</tr>
<tr>
<td>Culture is considered to be a significant aspect of KS because it controls the</td>
<td>Stoddart (2001)</td>
</tr>
<tr>
<td>effects of other related variables (such as existing technology and management techniques) on the achievement of knowledge management</td>
<td></td>
</tr>
<tr>
<td><strong>Lack of job rotation</strong></td>
<td>Agra et al. (2016), Huang and Pan (2014), Kane et al. (2005), Ortega (2001), Santos et al. (2016)</td>
</tr>
<tr>
<td>KS among individuals is concerned with how to establish communication among workers inside the organisation. Job rotation plays a major role in enhancing the knowledge of employees. Therefore, job rotation is vital to enhancing the knowledge of individuals and teams within and outside any department in the organisation. Employee learning, employer learning and employee motivation are the advantages of job rotation in any organisation. Job rotation enables individuals to learn from various departments, reduces employee exhaustion caused by tedious or boring tasks and increases individuals’ confidence and job satisfaction</td>
<td></td>
</tr>
</tbody>
</table>

Table I.

The KS enablers framework developed by Chong et al. (2011) forms the basis of the framework proposed in this paper. It was selected for three main reasons. First, the framework integrates the main factors that are significant for KS in the existing literature (as shown in Table I). Second, the framework was among the first to address the lack of knowledge on the topic of KS in an organisational context. Third, the framework is comprehensive in terms of identifying the KS enablers at the organisational, technological and individual levels. Although the existing literature offers other frameworks, such as the KS enablers frameworks proposed by Allameh and Zare (2011), Kanaan et al. (2013) and
Hussein et al. (2016), these frameworks do not account for these four levels in an organisational context or integrate them into one framework. Therefore, the framework proposed in this study is based on Chong et al.'s (2011) framework in order to identify the challenges organisations face in terms of KS for identity theft prevention.

Table I provides a summary of the literature reviewed. It identifies nine main barriers to KS in different contexts. Based on an analysis of the studies in Table I, it can be argued that the knowledge-management enablers identified by Chong et al. (2011) do not cover all the barriers to KS, as additional factors were identified in the literature. Indeed, the review of the literature reveals three challenges that were not integrated into Chong et al.’s (2011) framework: lack of employee willingness to share knowledge, lack of employee awareness and lack of trust in colleagues.

The nine barriers proposed in the framework for this study are discussed in the following sections.

2.1 Inadequate learning opportunities
Learning opportunities enhance progress in achieving outcomes by eliminating previous mistakes and removing weaknesses in organisations (Harteis et al., 2008; Yoon and Kim, 2013). Accordingly, insufficient training and learning is a large barrier to KS (Jaegersberg and Ure, 2011; Kukko, 2013; Pirkkalainen and Pawlowski, 2013; Riege, 2005; Sun and Scott, 2005). Sun and Scott (2005) highlight that a lack of learning opportunities at the individual, group and organisational levels is a major challenge for KS. Job training can be grouped into two types. The first is general training, which impacts on general human capital and enhances productivity in all job types; examples include training to enhance computer skills and language courses (Hortovanyi and Ferincz, 2015). Knowledge and general skills can be transferred to job holders in similar companies, such as businesses competing in the same industry sector, and to similar jobs in the same profession (Hortovanyi and Ferincz, 2015). The second category of job training is firm-specific training, which enhances knowledge solely in the employee’s current organisation (De Grip and Sauermann, 2013). This type of training is provided to enhance knowledge of machinery, workplace infrastructure and procedures that are only used in the company where the employee is working; it is provided to impart knowledge of particular characteristics of the organisation’s products and customers (De Grip and Sauermann, 2013).

2.2 Lack of feedback on performance
Feedback is important for the assessment of employees’ activities in organisations (Steelman and Wolfeld, 2018). For a long time, companies have observed their employees; however, current developments in electronic technology are advancing performance monitoring (Alder and Ambrose, 2005; Yu et al., 2018). Feedback can be provided for various purposes: on the outcome of activities or processes; to provide direction when employees move away from their primary goals; to establish new goals or adjust existing goals; or to provide guidance on performing activities (Hollenbeck et al., 2018). Furthermore, feedback encourages critical reflection on situations and tasks, which helps to bring about new approaches (Gabelica et al., 2012). Feedback can also help organisations to understand employees’ level of awareness of KS and of identifying and preventing identity theft (Chong et al., 2011).

2.3 Lack of an efficient ICT infrastructure and insufficient information-sourcing opportunities
An effective ICT infrastructure enables employees to generate, store and share knowledge with other employees, teams and departments (Dong et al., 2016; Syed-Ikhsan and Rowland, 2004). The ICT infrastructure includes the intranet, communication networks, emails, data warehousing and a decision-support system (Stankosky, 2005). Technologies that have been
developed with knowledge management in mind comprise document-management and workflow systems, innovative knowledge bases and expert systems for creating communal memory, data-extraction and data-filtering systems. These technologies include the internet and groupware that connects organisations on the intra-organisational and inter-organisational levels and throughout the world (Holsapple, 2013; Martin, 2000). Technology is important for creating, storing, retrieving, transmitting and sharing knowledge in a collaborative environment (Okere, 2017). In any organisation, an effective KS process requires well-structured information-sourcing opportunities and a good IT infrastructure. When an organisation does not have an efficient ICT infrastructure to document and transfer its information and knowledge, KS is challenged (Okere, 2017; Sun and Scott, 2005; Yang et al., 2012).

2.4 Lack of leadership support in KS
Leadership plays an important role in managing the KS process in any organisation (Bass and Stogdill, 1990; Muethel and Hoegl, 2016). This is because leaders are accountable for developing strategies for encouraging and making the best use of a learning culture and KS (Boerner et al., 2007). Leaders are required to develop an unrestricted culture and build an environment that supports KS (Chuang et al., 2016). Riege (2005, 2007) speculates that a lack of efficient leadership in KS is a barrier at the organisational level. KS in organisations is voluntary and people may need training to share their knowledge; therefore, continuous support and clear, effective guidelines are required (Mittal and Rajib, 2015). To create an environment of KS in an organisation, it is vital for leaders to emphasise their long-term commitment and support for sharing knowledge. Moreover, managers can facilitate KS in the organisation by developing policies to support the process (Mittal and Rajib, 2015). Senior executives and managers can also support KS by revealing the breadth of their own knowledge, using the knowledge of others when taking action (Aga et al., 2016; Mueller and Kamoche, 2000), and rewarding others who share their knowledge (Barnes, 2001).

2.5 Weak KS culture
Organisational culture refers to the shared values, beliefs and performance of people in an organisation (Hara and Foon Hew, 2007; McDermott and O’Dell, 2001). It plays a significant role when organisations employ new strategies for KS (McLaughlin et al., 2008; Syed-Ikhsan and Rowland, 2004). Furthermore, organisational culture controls the effects of related factors, such as existing technology and management techniques for effective KS. Jones et al. (2006) group organisations into two main categories: first, stability-oriented organisations, which ignore the need for change and the transfer of knowledge; and, second, change-oriented organisations, which welcome any change created by KS. Nation, culture and the diversity of spoken languages in the organisation have been identified as KS barriers (Riege, 2005). In addition, McDermott and O’Dell (2001) highlight that organisations should create a culture of tolerance and learning from mistakes to improve KS.

2.6 Lack of job rotation
Some experiences are hard to code and document (Ardichvili et al., 2003). In such cases, job rotation can be a good solution (Abdullah et al., 2016). Job rotation enables employees to work in different situations and to learn about and experience the related problems and solutions for themselves, expanding their knowledge boundaries. It can also help employees learn from each other (Riege, 2007). Hence, an organisation that does not use job rotation may find it difficult to enhance the knowledge of individual employees and teams (Aga et al., 2016; Huang and Pan, 2014; Ortega, 2001). There are three reasons for adopting job rotation in any organisation (Eriksson and Ortega, 2006). The first is employee learning, which makes employees more efficient and resourceful. The second is employer learning: when employees
work in different roles, employers learn about the weaknesses and strengths of individuals in
the organisation. The third is employee motivation, as working in a new environment can
reduce boredom and inspire individuals to learn new things.

2.7 Lack of employee willingness to share knowledge
The tendency for individuals not to share knowledge has been identified as a barrier to KS
in the context of social software (Pirkkalainen and Pawlowski, 2014). One of the main
limitations is insufficient motivation to share or receive knowledge (Hong et al., 2011);
indeed, it is the most challenging barrier for KS in the context of information security
(Tamjidyamcholo et al., 2014). When individuals do not anticipate any significant benefits
from sharing knowledge, they are reluctant to play an active role in the process. Additional
factors that contribute to a lack of willingness to share knowledge include geographical
distance, bureaucracy, language barriers, resistance to change, conflict avoidance and loss

2.8 Lack of employee awareness of KS
Lack of awareness has also been identified as a barrier to KS (Kukko, 2013; Richter, 2013;
Riege, 2005, 2007; Pirkkalainen and Pawlowski, 2013, 2014). Therefore, employee awareness of
knowledge-transfer processes is an important element of KS (Ismail and Yusof, 2010).
Employees may be aware of the problems but not the solutions (Hong et al., 2011). According
to Riege (2007), employees should be aware of the requirements and knowledge gaps of the
other employees, teams and organisations who are receiving the knowledge. Employees,
including senior managers, must be aware of the importance (Van den Hooff et al., 2003) of an
effective KS culture in an organisation. However, in many organisations, raising awareness of
the benefits of KS is a challenge (Zahedi et al., 2016). Communicating about the company’s
security policy and developing awareness programmes are two means of raising employee
awareness of KS in the context of information security (Flores et al., 2014).

2.9 Lack of trust in colleagues
Trust in others is a key element in the process of KS (Ardichvili et al., 2003; Hashim and Tan,
2015; Riege, 2005; Sun and Scott, 2005; Usero et al., 2007). Conversely, it is speculated that the
lack of trust is a barrier to distributive KS (Pirkkalainen and Pawlowski, 2014). From the
perspective of the social exchange theory, Homans (1958) claims that individual employees
exchange knowledge and ideas through a process of social interchange. Social interchange is
categorised by indeterminate personal responsibilities, fundamental rewards and trust
(Huang et al., 2011). In KS, social exchange occurs when individuals co-operate in the process
of knowledge transfer. The lack of trust can take the form of interpersonal distrust, distrust in
the organisation (McLaughlin et al., 2008; Riege, 2005; Sun and Scott, 2005), distrust in the
team’s values (Sun and Scott, 2005) and distrust in the knowledge received from other
employees (Hong et al., 2011; Riege, 2007). Kukko (2013) maintains that the lack of trust is
more likely to arise when an organisation recruits new employees.

To summarise, the extensive review of the literature (Table I) has revealed three main
findings. First, nine factors are necessary to facilitate effective KS: adequate learning
opportunities; feedback on performance; sufficient information-sourcing opportunities and an
efficient ICT infrastructure; leadership support; a strong KS culture; job rotation; employee
willingness; employee awareness; and trust in colleagues. If these factors are not present, KS is
hindered in organisations. Second, organisations lack effective KS processes in the context of
information security. Third, there is a need for research that identifies the barriers to KS in the
prevention of identity theft in online retail organisations. Despite the large number of studies
on KS, there is a lack of research in the context of preventing identity theft. Therefore, this
study investigates the existing barriers to KS in preventing identity theft in online retail organisations and suggests effective solutions for removing those barriers. It aims to find simple but comprehensive answers to the following questions, which have not yet been addressed in the literature:

**RQ1.** What are the major barriers to KS for the prevention of identity theft in online retail organisations?

**RQ2.** How can organisations overcome these barriers?

3. Research methodology

The main sources of data are documentation, archival records, interviews, direct observations and participant observation (Yin, 1994, 2011). This research adopted a case study approach, which is appropriate when a researcher seeks to gain a comprehensive understanding of a situation (Merriam, 2001). According to Yin (1994), the case study design must have five components: the research question, its propositions, its units of analysis, a determination of how the data are linked to the propositions and criteria to interpret the findings. Yin (1994, 2011) points out that case studies are the preferred strategy when “how” and “why” questions are posed. Therefore, this approach is suitable for this study given that its key purpose is to gain an understanding of factors that influence how effectively employees share knowledge about identity theft, rather than to make generalisations or prove underlying hypotheses.

The case study approach includes data collection, data analysis, and reporting and presenting the results of the analysis (Yin, 2011). This research used several data-collection methods: analysis of internal documents from the selected organisations (including memos and survey reports); analysis of the organisations’ websites; an investigation of news about the organisations in print and electronic media; and interviews with employees.

Both internal and external documents from the online retail organisation were analysed. During site visits, 60 short memos and e-mail conversations and 45 internal policy and working procedure documents were collected from the case companies. The set of internal procedure documents included secure communication, network security, computer protection and data encryption. Using the archival analysis method, these documents were examined in order to understand the organisation’s existing KS processes for identity-theft prevention. The analysis focussed on any evidence of identity theft, reasons for stealing data from individuals and the organisation, the steps taken to overcome these problems, and existing KS policies and processes for preventing identity theft. The external documents investigated included news reports on the organisations published in print and digital media, including Cifas, CCR Magazine, the BBC, CNN, The Guardian, The Telegraph and others. These reports were examined for any evidence of or clues about identity theft and its prevention. Furthermore, the websites of the selected organisations were studied, focussing on publications about KS and the prevention of identity theft.

The qualitative method used also included interviews. These are effective for illuminating issues and arriving at explanations; for example, by exploring meaning (Gillham, 2000). Researchers may use this approach to scrutinise issues related to a variety of employee operations (Creswell, 2013). Therefore, interviews were conducted with individual employees to identify how they experienced concerns about KS in the context of preventing identity theft. Initially, the researchers conducted a review of the related literature to assess the extent of the work on KS for the purpose of preventing identity theft and to identify the role of individual employees in sharing knowledge to prevent identity theft. Based on this analysis, a list of interview questions was developed. The interview questions were underpinned by the KS enablers framework proposed by Chong et al. (2011). A pilot study was conducted using eight semi-structured interviews with PhD research students in a relevant field at a UK university.
Following the pilot study, irrelevant and duplicated questions were removed, the sequence of questions was altered, and the wording was amended to ensure clarity for participants.

The researchers conducted thirty-four semi-structured interviews with employees in three online retail companies in the UK: Company X, Company Y and Company Z (renamed for anonymity). These companies were selected because they sell and purchase products and services online. The employees ranged from senior managers to support staff, and they were working in teams and groups. A total of 14 interviews were conducted in various departments in Company X. At Company Y, the researchers conducted 12 face-to-face interviews and one telephone interview. In addition, seven interviews were conducted with employees working at Company Z. Appendix 2 presents information about each of the three companies. Tables AII–AIV present details of the interview participants from each company. The semi-structured interviews were conducted face to face or over the phone and lasted for between 45 and 75 min. In some cases, additional questions were asked to clarify the interviewees’ responses and obtain clear data for analysis. The sequence of the questions was also altered during the interviews depending on the responses of the interviewees. Before the data collection started, a confidentiality agreement was signed with the management of the company. The researchers obtained consent from each interview participant via e-mail.

Thematic analysis was conducted using a qualitative coding process (Braun and Clarke, 2006). The data collected from employees in the three UK companies were coded to establish patterns. NVivo software and manual coding were used for the thematic analysis. Various nodes (codes) were generated from group participants’ interview responses, which were based on the themes that emerged in the literature review. These themes included ICT infrastructure, employee willingness to share knowledge, employee awareness, trust of colleagues, job rotation, feedback on performance, information-sourcing opportunities, leadership support and KS culture. Once this had been completed, the data (i.e., all the grouped responses) were printed along with the interview transcripts and analysed manually. This involved a critical reading of all the responses in each node and sub-node.

4. Findings

This section presents the main findings of this study with reference to each of the nine barriers identified in the literature.

4.1 Lack of employee willingness to share knowledge

The findings indicate that in two of the organisations studied, a lack of willingness to share knowledge is a barrier to KS for the prevention of identity theft. Employees in Company X only shared knowledge within their own department for the purpose of preventing identity theft; they were not willing to share information with colleagues working in non-technical departments. One participant from the company stated: “I can only share any type of knowledge with the people I work with. I don’t discuss it with people who work in other areas of the business” (R06, Company X).

Similarly, employees in Company Z were willing to share knowledge in their own department only. One respondent stated: “I am happy to discuss with my friends who work here, but I won’t share any type of knowledge outside this department”. Another respondent expanded on this: “I don’t share it [knowledge] with others and I am not willing to share knowledge with them. It is not the policy of the company” (R10, Company Z).

However, in Company Y employees were willing to share knowledge with colleagues in other departments: “I am happy to share the knowledge with other people in the company. It helps to increase the knowledge of others, and mine too” (R10, Company Y). Therefore, at Company Y, unwillingness to share knowledge for the purpose of preventing identity theft is not a barrier.
One reason employees at Companies X and Z were unwilling to share knowledge outside their own departments was the absence of a supportive environment for this activity. No rewards or incentives were offered for sharing knowledge with others; therefore, individuals were unwilling to share it.

4.2 Lack of employee awareness
In all three companies, there was a lack of awareness of the existence of KS for the purpose of preventing identity theft. A participant from Company X said: “I don’t know about the KS for ID theft prevention” (R11, Company X). Participants from Company Y and Company Z were also unaware of their companies’ knowledge-transfer process for preventing identity theft:

I do not know about the process of KS. Actually, nobody told me about it. (R09, Company Y)

I am not aware about ID theft prevention KS. Actually, we don’t do it. (R03, Company Z)

I am not aware of ID theft. Well, I don’t know about those problems. (R07, Company Z)

Therefore, this study did not find any evidence of KS for the purpose of preventing identity theft. This implies that there is a lack of focus on creating a supportive environment that would enhance employees’ awareness of identifying and preventing identity theft.

4.3 Inadequate learning opportunities
The three companies provided various learning opportunities to their employees, including training. However, the participants from Company Y had not received any training on identity theft:

There is no mention of ID theft. (R06, Company Y)

I do not think there is a specific training for that here that we receive. (R02, Company Y)

There is no training for ID theft prevention in the company. (R05, Company Y)

All the companies provided training to new employees about the company’s ICT infrastructure and its working procedures; for example, how to interact with the company’s computerised systems, what the working procedures are and how to deal with customer data. However, training on using effective methods to prevent identity theft was lacking in all three companies. Training on identity theft was provided only to employees from technical departments, and it was limited to the technical aspects of preventing identity theft.

4.4 Lack of trust in colleagues
In Company X, employees trusted colleagues in their own department but did not trust individuals or teams outside their department. Respondents from the company were reluctant to share their knowledge of identity-theft prevention with these colleagues: “I cannot share knowledge with people who are not here in this department. I don’t trust others outside my working unit” (R14, Company X). Due to this lack of trust at an inter-departmental level, employees from non-technical departments were not able to obtain the advantages from the KS process that would enable them to prevent identity theft within the company. Therefore, the lack of trust among colleagues was a barrier to the process of KS for the purpose of preventing identity theft in Company X.

Although KS for identity-theft prevention was not a focus in Company Y either, individuals trusted each other enough to share knowledge about routine jobs and day-to-day activities. One respondent said: “I trust people working there with me. I would
like to discuss […] anybody working here in the company” (R10, Company Y). Employees were willing to share knowledge with colleagues inside or outside their own departments. Illustrating this, one participant stated: “There are no particular restrictions on sharing knowledge with other departments” (R13, Company Y). The findings from the interviews suggest that while there is no evidence of a lack of trust in Company Y. However, the company does lack a supportive environment for KS to prevent identity theft. Therefore, there is a need to enhance the KS process with a focus on preventing identity theft.

The interview responses from employees in Company Z showed that they trusted each other at a departmental level, sharing knowledge with individuals and teams in their own departments. However, employees working in technical departments did not trust employees working in non-technical departments. Therefore, there was a lack of trust among colleagues in Company Z.

### 4.5 Lack of an efficient ICT infrastructure and insufficient information-sourcing opportunities

In all three companies, the existing ICT infrastructure was efficient and various information-sourcing opportunities were available to employees. However, none of the companies used those information-sourcing opportunities to enable KS for the purpose of preventing identity theft. Employees in each company used the ICT infrastructure for their routine work and to communicate business tasks, but there was no focus on using that infrastructure to prevent identity theft. Therefore, none of the companies studied used information-sourcing opportunities or the ICT infrastructure to prevent identity theft. This represents a barrier to KS for preventing identity theft in online retail organisations.

### 4.6 Lack of leadership support in KS

The management of Company Y appeared to be supportive and to share information with employees, regularly sending group emails about general issues and task completion. One participant stated: “A cascade of information is done via email, and so there are regular email briefings that come out” (R03, Company Y).

Employees expected the company leadership to provide guidance and education in the following areas: identity-theft issues; how to prevent identity theft; and how to protect personal and organisational knowledge from those who are not authorised to access it. The participants said that they needed KS resources to be made available to them and for business systems to be enhanced for the prevention of identity theft. One participant stated that they expected the following support:

Support regarding training, education and guidance. Moreover, just making resources available, making business systems robust enough to protect from ID theft and promote KS from that perspective. (R01, Company Y)

The participants also said they needed a company policy on identity-theft issues and protecting identity:

If there is a policy in the organisation about KS or ID theft, then certainly everyone will be expected to comply with it. I think there will be top support, high-level support certainly. (R08, Company Y)

Although the company leadership was supportive for KS among employees, the management team did not focus on issues related to preventing identity theft. Most of the employees interviewed stated that they required education to increase their awareness of identity-theft issues and to secure their own – and the organisation’s – knowledge. Employees needed support from management to be able to create a KS environment and build a culture of KS for the purposes of preventing identity theft.
4.7 Weak KS culture
As described previously, the research revealed that Company X lacked a supportive culture for sharing knowledge at the inter-departmental level for preventing identity theft: employees share this information within their own departments only. Hence, a weak KS culture in the company acted as a barrier to the use of KS to prevent identity theft.

On the other hand, Company Y had a strong culture of KS. Employees were trusted and shared knowledge with each other in their department. One participant responded: “I trust my friends, actually we help each other in our department” (R03, Company Y). Another participant from Company Y said: “We have a good culture of information sharing. We are quite good at trusting others. Well, I can trust all the employees here working in this company, and I should do it as others trust me” (R11, Company Y). Nevertheless, the analysis of the data revealed an absence of a culture that supports KS for preventing identity theft in Company Y. This is because employees were not sharing their knowledge of preventing identity theft. Therefore, a weak KS culture was also a barrier in Company Y.

Company Z had a culture of KS at the departmental level. A respondent from the company stated: “I share what I do here in my department. Others also do it here” (R05, Company Z). However, employees did not share their knowledge with colleagues in other departments: “Actually, we do not discuss with others who do not work with us” (R02, Company Z). Therefore, Company Z had a weak culture of KS, which was a barrier to the process of preventing identity theft.

4.8 Lack of feedback on performance
The findings highlighted that feedback on performance was important in the companies. One participant stated: “That is the bulk of the managers’ job; we have performance management” (Company Y). However, none of the three organisations had a process for evaluating employees’ performance on KS for the purpose of preventing identity theft:

We are not evaluating the performance for ID theft prevention KS. And there is no feedback for that. Or I can say our evaluation is not about KS to prevent ID theft. (R04, Company Y)

ID theft prevention is not in that criteria. It is the evaluation of our job we do here, not the KS for it. (R10, Company Y)

No ID theft is mentioned in our performance review. (R04, Company Z)

As for ID theft prevention and KS, we are not evaluated on that. (R04, Company Z)

Managers in the companies arranged monthly one-to-one meetings with advisors to obtain information on employees’ performance. The three companies evaluated the performance of their employees twice a year. The respondents stated that there was only one tool for evaluating employees’ performance: an e-learning system providing information about evaluating performance in general. However, the participants stated that it is vital to provide feedback on the performance of work activities.

4.9 Lack of job rotation
The research did not find any job-rotation processes in Company X, and all the participants from the company confirmed that there was no job rotation. Not rotating jobs creates a barrier to the process of KS and does not enhance the knowledge of employees or teams. It leaves individuals to learn from their own experiences only, rather than also learning from those of others.

On the other hand, Company Y frequently used job rotation. This meant that employees were able to increase their knowledge while working in different teams and departments in the company. Employees learned about new systems and gained knowledge from the
experiences of colleagues in other departments. They learned from doing new tasks as part of a different role:

I am happy to work in new environment and with new people. I learn from them and it leaves me no chance of failure. So I am happy with it. (R11, Company Y)

It is useful for gaining knowledge of different areas in the company. (R07, Company Y)

However, Company Y did not rotate jobs specifically for the purpose of increasing employees’ knowledge of preventing identity theft. Therefore, there is still a barrier to KS in the context of preventing identity theft.

The investigation of Company Z’s internal documents revealed no evidence of job rotation in the company. This was confirmed by an interview participant, who stated: “We do not have any policy of job rotation in the company here” (R05, Company Z). Furthermore, another respondent did not see the value of job rotation: “I gain knowledge from my things I experience here and I do not need to go anywhere and ask how to do my work” (R07, Company Z). These responses revealed that employees were learning from their own experiences only, with some of them doing the same job for many years.

5. Discussion

The primary aim of this research was to investigate the main barriers to KS for the purpose of preventing identity theft. There were two main research questions:

RQ1. What are the major barriers to KS for the prevention of identity theft in online retail organisations?

RQ2. How can organisations overcome these barriers?

By answering these questions, this research sought to fill the gap in the literature and help online retail organisations to prevent identity theft by improving their KS practices. Identity theft is becoming an increasing concern, with rising numbers of cases. Through the extensive literature review (see Table I), nine main barriers were identified. Data were collected from 34 semi-structured interviews and an examination of the internal documents of the companies under study. The research has extended the KS enablers framework proposed by Chong et al. (2011) by identifying nine major barriers to sharing knowledge in the context of preventing identity theft.

To answer the first research question, based on the findings from analysing the data collected in this research, the framework shown in Figure 1 is proposed. This framework includes the major barriers to KS for the prevention of identity theft in online retail organisations. It is based on the reconceptualisation and extension of the KS enablers framework proposed by Chong et al. (2011). The proposed framework includes three additional barriers to KS: lack of employee willingness to share knowledge, lack of employee awareness and lack of trust in colleagues. It proposes additional relationships between these barriers by acknowledging the central role of leadership support in the process.

In response to the second research question, the findings have revealed that leadership support plays a central role in increasing employee awareness of KS and encouraging them to share their knowledge for the purpose of preventing identity theft. Leadership support is also key to creating a supportive culture of KS for the prevention of identity theft, providing an efficient ICT infrastructure, supporting trust among colleagues, providing feedback on performance related to preventing identity theft, and providing training and support (learning opportunities). This agrees with previous studies which have highlighted that leadership support is an important enabler for KS in organisations (Chong et al., 2011; Muethel and Hoegl, 2016; Jones et al., 2006). It is also consistent with previous studies which explained that the lack of efficient leadership can undermine an effective KS culture, the
efficiency of the ICT infrastructure, training and learning opportunities, individuals' motivation to share knowledge, and their trust in each other (Aga et al., 2016; Riege, 2005, 2007; Sun and Scott, 2005). Hence, there is a need to carefully select the right individuals to work in the organisation at the recruitment stage (Kukko, 2013). A lack of leadership support can inhibit the creation of a culture that encourages KS. Leadership teams need to foster a culture that is not restrictive and build a supportive environment for KS (Chuang et al., 2016). Without a supportive culture, individuals are discouraged from sharing their knowledge. A KS culture is a significant factor because it controls the effects of other related variables, such as the available technology and techniques for effective KS.

Leadership support influences job satisfaction and willingness to commit to the organisation among employees. The results of this research have confirmed the findings in the literature on the significance of employees' willingness to share knowledge. In addition, the findings have revealed a lack of awareness of KS among employees in the companies under study. These findings are consistent with those of previous studies that investigated how a lack of awareness can affect KS. For example, employees may be unaware of the value of the knowledge available to them or of the benefits of sharing that knowledge (Kukko, 2013). They may not be aware of the solutions to problems associated with identity theft (Hong et al., 2011), the purpose and use of knowledge (Riege, 2007) or the knowledge available from other employees (Riege, 2007). Indeed, the management may be unaware of the importance of this knowledge (Van den Hooff et al., 2003).

The findings indicate that in the companies studied, there is a lack of opportunity for employees to learn about KS in the context of preventing identity theft. Employees should be given opportunities to learn about the core knowledge to be transferred and the skills required to use ICT to share their knowledge. Such factors were found to be important in previous studies (e.g. Ardichvili et al., 2003; Pirkkalainen and Pawlowski, 2013). Hence, the lack of efficient ICT can discourage KS in the organisation. Moreover, an inefficient ICT infrastructure reduces employees' motivation and willingness to share knowledge and hinders learning opportunities.

The findings have revealed a lack of job rotation in two of the studied companies. Job rotation plays a vital role in enhancing individuals' knowledge (Aga et al., 2016;
Huang and Pan, 2014; Ortega, 2001). It is especially important for positions that require employees to gain new knowledge through personal experience (Abdullah et al., 2016; Ardichvili et al., 2003); for example, jobs that involve dealing with changing conditions in a turbulent environment. In addition, feedback on performance in preventing identity theft can be provided for various purposes: bringing the outcomes of activities or processes into focus; providing information when workers move away from primary goals; helping them to set new goals or adjust their current goals; and guiding their performance of activities. It also promotes critical reflection and brings about new approaches (Gabelica et al., 2012).

6. Theoretical contributions and practical implications

This study provides theoretical contributions and has practical implications. There are three main theoretical contributions. First, this research has bridged a gap in the literature by providing a comprehensive framework for a full understanding of the barriers to KS for preventing identity theft in online retail organisations. Although the topic of KS has been discussed in previous studies in various contexts, this study is the first to address barriers to KS in the context of preventing identity theft. Second, the proposed framework has extended the KS enablers framework developed by Chong et al. (2011) by identifying additional barriers to KS in the context of preventing identity theft. Third, the results revealed that the most significant barriers to KS in preventing identity theft are lack of employee willingness to share knowledge, lack of employee awareness and lack of trust in colleagues. These three additional barriers have been integrated into the framework.

The findings also have important implications for practitioners. First, the findings are useful for managers who wish to identify an organisation’s key barriers to KS for preventing identity theft. This is important to reduce the number of cases of identity theft in the UK and increase customers’ trust in the companies they deal with. Second, the three online retail companies studied demonstrated weaknesses in the context of KS for preventing identity theft. Hence, these companies should consider improving their current practices by following the specific recommendations set out in Table AV. Third, the recommendations may be useful to other online retail companies. As this research presents the results of a qualitative study, the recommendations apply most specifically to the organisations under scrutiny. However, online retail companies often have similar organisational structures and business processes, allowing some generalisation of the findings to other companies.

7. Limitations and future work

The findings of this study are based on three online retail companies in the UK. Therefore, further research is required using an empirical method and focussing on larger numbers of organisations. This study is limited by the use of the case study approach, the small number of interviews conducted, the number of internal company documents examined, and the lack of availability of existing literature and data from the organisations due to confidentiality concerns. Therefore, future research can adopt quantitative research methods to test the validity of the research outcomes across the whole online retail sector. The researchers carried out this study in the UK’s online retail sector. Further research is recommended for the expansion of this study to include other countries.

8. Conclusion

This study has provided important contributions in terms of theory and practice. In terms of theory, the research extended the model proposed by Chong et al. (2011) by integrating three new barriers to KS in the context of identity fraud preventions in online retail organisations. These are lack of employee willingness to share knowledge, lack of employee awareness and lack of trust in colleagues. In addition, the research highlighted the key role of leadership in
this process. The research has several further implications in terms of practice, and recommendations were provided to managers who wished to reduce the number of cases of identity theft in online retail organisations. Future research can collect data from more companies, use a larger number of interviews and collect quantitative data through questionnaires to ensure the generalisability of the findings.

References


Further reading


### Appendix 1. Summary of studies on KS in different contexts

<table>
<thead>
<tr>
<th>Source</th>
<th>Context</th>
<th>Method</th>
<th>KS barrier</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pirkkalainen and Pawlowski (2014)</td>
<td>General knowledge among global knowledge workers</td>
<td>Systematic literature review</td>
<td>Cultural; technical; social; organisational/contextual</td>
</tr>
<tr>
<td>Tjoflåt et al. (2017)</td>
<td>Nurses in an exchange programme between Madagascar and Norway</td>
<td>Qualitative, descriptive design, including focus group interviews and semi-structured interviews</td>
<td>Language</td>
</tr>
<tr>
<td>Jaegersberg and Ure (2011)</td>
<td>General knowledge in solar-energy SMEs</td>
<td>Interview</td>
<td>Communication; lack of training and skills</td>
</tr>
<tr>
<td>Hong et al. (2011)</td>
<td>General knowledge in finance companies</td>
<td>Interview/case study</td>
<td>Individual (including internal resistance, trust, motivation and awareness); organisational (including language, conflict avoidance, bureaucracy and distance)</td>
</tr>
<tr>
<td>Makela et al. (2007)</td>
<td>Multinational corporations</td>
<td>Interview/case study</td>
<td>National-cultural background; similarity of organisational status and shared language</td>
</tr>
<tr>
<td>Sánchez et al. (2013)</td>
<td>Transfer of tacit knowledge</td>
<td>Conceptual paper</td>
<td>Culture</td>
</tr>
<tr>
<td>Jones et al. (2006)</td>
<td>General KS in enterprise resource planning implementation</td>
<td>Qualitative (case study)</td>
<td>Cultural (including orientation to change, control, co-ordination, responsibility, orientation to collaboration, basis of truth and rationality, motivation, orientation to work, orientation and focus, nature of time horizon)</td>
</tr>
<tr>
<td>Ardichvili et al. (2003)</td>
<td>Virtual KS communities</td>
<td>Qualitative (case study)</td>
<td>Lack of employee willingness (due to job security concerns, accuracy of knowledge, importance of knowledge, losing face and credit among colleagues)</td>
</tr>
<tr>
<td>Sun and Scott (2005)</td>
<td>General KS in numerous ways, including individual–team, team–organisation and organisation–organisation</td>
<td>Delphi technique</td>
<td>Competency; individual imperative; team climate; relationships and norms; organisational climate and relationships; organisational system and structure; inter-organisational imperatives; relation climate and relationships; inter-organisational systems and structures</td>
</tr>
<tr>
<td>Pirkkalainen and Pawlowski (2013)</td>
<td>Social networking software for global social knowledge management</td>
<td>Interview/case study</td>
<td>Lack of resources; lack of time; lack of knowledge and awareness; lack of training; lack of trust; lack of motivation; lack of ICT skills; insufficient ICT infrastructure; geographical and cultural differences</td>
</tr>
<tr>
<td>Leal-Rodriguez et al. (2012)</td>
<td>Knowledge-innovation in healthcare</td>
<td>Path modelling analysis</td>
<td>Cultural</td>
</tr>
</tbody>
</table>

(continued)
<table>
<thead>
<tr>
<th>Source</th>
<th>Context</th>
<th>Method</th>
<th>KS barrier</th>
</tr>
</thead>
<tbody>
<tr>
<td>Okere (2017)</td>
<td>Project-management knowledge in the construction sector</td>
<td>Interview/case study</td>
<td>Lack of standardisation; lack of integrated computer network system; lack of need for KS IT</td>
</tr>
<tr>
<td>Yang et al. (2012)</td>
<td>Project management</td>
<td>Quantitative (structural equation modelling)</td>
<td>Technological (including loss of documents, slow compatibility, lack of simultaneous document editing, absence of electronic signature recognition system); organisational (including ambiguous job instructions, lack of motivation, excessive centralised communication)</td>
</tr>
<tr>
<td>Blagov et al. (2017)</td>
<td>Educational programme management</td>
<td>Case study</td>
<td>No physical proximity to colleagues; fear of asking foolish questions; knowledge as power; lack of appreciation and attention</td>
</tr>
<tr>
<td>Lilleoere and Hansen (2011)</td>
<td>Pharmaceutical research and development</td>
<td>Case study</td>
<td>Attitude toward KS behaviour; controllability of KS practices; KS self-efficacy; subjective norm toward KS practices</td>
</tr>
<tr>
<td>Kuo and Young (2008)</td>
<td>Virtual professional community of teachers</td>
<td>Quantitative (structural equation modelling)</td>
<td>Intention to KS; trust; organisational support</td>
</tr>
<tr>
<td>Safa and Von Solms (2016)</td>
<td>General security knowledge among general, non-security expert employees</td>
<td>Quantitative (structural equation modelling)</td>
<td>Organisational structure; co-ordinating information-security process; information security management</td>
</tr>
<tr>
<td>Tamjidyamcholo et al. (2014)</td>
<td>Virtual professional community of security experts</td>
<td>Quantitative (structural equation modelling)</td>
<td>Social capital; security awareness; threat appraisal; source credibility</td>
</tr>
<tr>
<td>Flores et al. (2014)</td>
<td>Security KS among organisations in the USA and Sweden</td>
<td>Quantitative (structural equation modelling)</td>
<td>Lack of economic returns; expectation to receive knowledge of the same value; trust; motivating individuals to engage in KS</td>
</tr>
<tr>
<td>Ortiz et al. (2017)</td>
<td>General KS behaviour among members of a social network</td>
<td>Quantitative (structural equation modelling)</td>
<td>Lack of economic returns; expectation to receive knowledge of the same value; trust; motivating individuals to engage in KS</td>
</tr>
<tr>
<td>Feledi et al. (2013)</td>
<td>Information security KS between organisations using web technologies</td>
<td>Qualitative (experts' evaluation of web portal)</td>
<td>Affect; social factors; facilitating conditions; perceived consequences</td>
</tr>
<tr>
<td>He and Johnson (2015)</td>
<td>Generic security template to share security knowledge in the context of healthcare</td>
<td>Interview/case study</td>
<td>Learning efforts; comprehension of knowledge</td>
</tr>
<tr>
<td>Ardichvili (2008)</td>
<td>Virtual (online) communities of practice</td>
<td>Conceptual paper</td>
<td>Procedural or use of technology-related factors; interpersonal factors; cultural norms</td>
</tr>
<tr>
<td>Sharma et al. (2012)</td>
<td>Unspecified</td>
<td>Interpretive structural modelling</td>
<td>Lack of top management commitment; lack of proper understanding of knowledge management</td>
</tr>
<tr>
<td>Hew and Hara (2007)</td>
<td>Teachers' online KS</td>
<td>Online observation and semi-structured telephone interviews</td>
<td>Lack of knowledge; competing priorities</td>
</tr>
<tr>
<td>Santos et al. (2012)</td>
<td>Complex research and development projects</td>
<td>Semi-structured interviews</td>
<td>Codification process; inadequate information technology; lack of initiative and strategy by employees; lack of time and resources</td>
</tr>
</tbody>
</table>

Table AI.
Appendix 2. Case descriptions
The selected companies were all reputable online retailers in the UK. The companies included large, medium and small organisations with multiple branches in different cities in the UK. A brief description of each selected company follows.

Company X
The company is a leading multi-brand retailer with annual sales of approximately £2bn and numerous active customers receiving millions of products every year. More than three-quarters of sales are processed online, one-third of these being from mobile devices. Approximately 1m customers visit the website every day.

Company Y
The company is a corporate organisation with multiple child companies selling online train tickets, processing online payments and maintaining online travel schedules. More than 3,000 employees joined the company in the year 2015. The company manages the information of 1.3 billion passengers, including payment-processing and travel information. The company’s online database is one of the largest in Europe, and it stores passengers’ travel schedules, payment processes and other details.

Company Z
The company provides services and consultancy to retail companies and their customers. Since it was set up in 2008 as a contact centre, it has been providing services and consultancy to more than 200,000 client companies and individual customers. They attempt to understand clients’ sales strategies and then execute them through telephonic and direct e-mail contact. The company is expert at taking new products to market and enhancing awareness among prospects. It provides various services, such as outbound sales, inbound sales, customer service and customer retention, to maximise the revenue of its clients and their customers.
### Appendix 3. Interview participants

<table>
<thead>
<tr>
<th>Code</th>
<th>Department</th>
<th>Responsibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>C1-R01</td>
<td>Group security</td>
<td>Performance management</td>
</tr>
<tr>
<td>C1-R02</td>
<td>Fraud prevention</td>
<td>Actioning referrals; speaking to genuine customers who have been the victims of identity theft and resolving their issues</td>
</tr>
<tr>
<td>C1-R03</td>
<td>Fraud prevention</td>
<td>Looking at online applications for credit; dealing with victims of identity theft; attending to calls from victims and explaining what they should do</td>
</tr>
<tr>
<td>C1-R04</td>
<td>Group security</td>
<td>Internal consultancy</td>
</tr>
<tr>
<td>C1-R05</td>
<td>Group security</td>
<td>Investigating and preventing fraud and theft</td>
</tr>
<tr>
<td>C1-R06</td>
<td>Group security</td>
<td>Detecting and managing threats; vulnerability scanning</td>
</tr>
<tr>
<td>C1-R07</td>
<td>Group security</td>
<td>Group security head of technical services and training</td>
</tr>
<tr>
<td>C1-R08</td>
<td>Group security</td>
<td>Information security specialist: making sure that customer data is safe; encrypting sensitive information</td>
</tr>
<tr>
<td>C1-R09</td>
<td>Group security</td>
<td>Head of different departments; consulting with managers of various departments, especially group security, information security and fraud prevention</td>
</tr>
<tr>
<td>C1-R10</td>
<td>Fraud prevention</td>
<td>Investigating fraud and theft within the business</td>
</tr>
<tr>
<td>C1-R11</td>
<td>Intelligence unit</td>
<td>Supporting the regional loss-prevention managers and providing the information they require</td>
</tr>
<tr>
<td>C1-R12</td>
<td>Group security</td>
<td>Analysing data; putting packages together and sending them out to regional directors</td>
</tr>
<tr>
<td>C1-R13</td>
<td>Group security</td>
<td>Leading on intelligence and technical issues</td>
</tr>
<tr>
<td>C1-R14</td>
<td>Physical security</td>
<td>Investigating identity theft (hijacked accounts; fraudulent set-up of accounts); investigating the web during the process of fraud being committed</td>
</tr>
</tbody>
</table>

Table AII.
Interview participants, Company X
<table>
<thead>
<tr>
<th>Code</th>
<th>Department</th>
<th>Responsibility</th>
<th>Experience (years)</th>
</tr>
</thead>
<tbody>
<tr>
<td>C2-R01</td>
<td>Group business services</td>
<td>Looking after the Microsoft estate, including cloud infrastructure; making sure that anything entered conforms to the correct standards</td>
<td>15</td>
</tr>
<tr>
<td>C2-R02</td>
<td>Asset management</td>
<td>Supporting IBM infrastructure, IBM officer application service infrastructure and IBM WebSphere Messaging infrastructure</td>
<td>1</td>
</tr>
<tr>
<td>C2-R03</td>
<td>Information management</td>
<td>Managing data migration, data security, hardware and software set-up</td>
<td>5</td>
</tr>
<tr>
<td>C2-R04</td>
<td>IT</td>
<td>Managing the technical team</td>
<td>2</td>
</tr>
<tr>
<td>C2-R05</td>
<td>Project and programme services</td>
<td>Training, e-learning, research and development</td>
<td>16</td>
</tr>
<tr>
<td>C2-R06</td>
<td>Supply chain</td>
<td>Managing the delivery of work streams; working on a desktop-transformation programme</td>
<td>2 months</td>
</tr>
<tr>
<td>C2-R07</td>
<td>PMPS</td>
<td>Managing communication in the company; sending out communication emails to individuals and teams</td>
<td>1</td>
</tr>
<tr>
<td>C2-R08</td>
<td>Desktop transformation programme</td>
<td>Supporting the regional loss-prevention managers and providing the information they require</td>
<td>1</td>
</tr>
<tr>
<td>C2-R09</td>
<td>Supply chain</td>
<td>Commercialising excess capacity in the supply chain, including selling goods and services to third parties</td>
<td>2</td>
</tr>
<tr>
<td>C2-R10</td>
<td>Supply chain</td>
<td>Commercialising excess capacity in the supply chain, including selling goods and services to third parties</td>
<td>1</td>
</tr>
<tr>
<td>C2-R11</td>
<td>Corporate functions</td>
<td>Delivering business changes and new technology to time, to cost and to quality</td>
<td>5</td>
</tr>
<tr>
<td>C2-R12</td>
<td>Maintenance and development</td>
<td>Maintaining the company’s ICT infrastructure</td>
<td>3</td>
</tr>
<tr>
<td>C2-R13</td>
<td>Information security</td>
<td>Securing information; managing information-security issues</td>
<td>2</td>
</tr>
</tbody>
</table>

Table AIII. Interview participants, Company Y

<table>
<thead>
<tr>
<th>Code</th>
<th>Department</th>
<th>Responsibility</th>
<th>Experience (years)</th>
</tr>
</thead>
<tbody>
<tr>
<td>C3-R01</td>
<td>Information technology</td>
<td>Managing the company website; updating web content; handling the back end of the database</td>
<td>7</td>
</tr>
<tr>
<td>C3-R02</td>
<td>Information technology</td>
<td>Looking after the IT infrastructure; administrating existing systems, including the network and hardware</td>
<td>5</td>
</tr>
<tr>
<td>C3-R03</td>
<td>Information security</td>
<td>Handling information on the company’s security issues; managing firewalls and secure lines</td>
<td>5</td>
</tr>
<tr>
<td>C3-R04</td>
<td>Call centre</td>
<td>Contacting customers; providing sales advice</td>
<td>3</td>
</tr>
<tr>
<td>C3-R05</td>
<td>Call centre</td>
<td>Contacting customers; providing sales advice</td>
<td>1</td>
</tr>
<tr>
<td>C3-R06</td>
<td>Human resources</td>
<td>Managing human resources</td>
<td>7</td>
</tr>
<tr>
<td>C3-R07</td>
<td>Call centre</td>
<td>Contacting customers; providing sales advice</td>
<td>3</td>
</tr>
</tbody>
</table>

Table AIV. Interview participants, Company Z

1213 Preventing identity theft
### Appendix 4. Barriers and recommendations

<table>
<thead>
<tr>
<th>Barrier</th>
<th>Company X</th>
<th>Company Y</th>
<th>Company Z</th>
<th>Recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lack of employee willingness</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Companies should provide rewards and incentives to employees to increase their willingness to share knowledge to prevent identity theft.</td>
</tr>
<tr>
<td>Lack of employee awareness</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Companies should enhance employee awareness of the prevention of identity theft and have a culture of knowledge sharing within the company.</td>
</tr>
<tr>
<td>Inadequate learning opportunities</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Companies should provide enhanced learning opportunities to increase employee and team awareness of sharing knowledge of identity theft prevention within the company.</td>
</tr>
<tr>
<td>Lack of trust in colleagues</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Companies should increase levels of trust at the inter-departmental level; employees need to trust others to share their knowledge of identity-theft prevention within companies.</td>
</tr>
<tr>
<td>Lack of an efficient ICT infrastructure and insufficient information-sourcing opportunities</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Companies should use existing information-sourcing opportunities and ICT infrastructure to share knowledge of identity-theft prevention within the company. Further information-sourcing opportunities are required to enhance the knowledge of employees.</td>
</tr>
<tr>
<td>Lack of leadership support</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Company leadership teams should support the implementation of a KS process to prevent identity theft in the company.</td>
</tr>
<tr>
<td>Weak KS culture</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Companies need to build a company-wide KS culture in order to prevent identity theft.</td>
</tr>
<tr>
<td>Lack of job rotation</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Companies need to develop a process of job rotation across departments within the organisation.</td>
</tr>
<tr>
<td>Lack of feedback on performance</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Companies should focus on providing feedback on employees’ performance in the prevention of identity theft.</td>
</tr>
</tbody>
</table>

**Table AV.**

Barriers to KS for preventing identity theft in organisations

**Corresponding author**

Nisreen Ameen can be contacted at: nisreen.ameen@pgr.anglia.ac.uk

---

For instructions on how to order reprints of this article, please visit our website: [www.emeraldgrouppublishing.com/licensing/reprints.htm](http://www.emeraldgrouppublishing.com/licensing/reprints.htm)

Or contact us for further details: permissions@emeraldinsight.com
Crime and social media

Simplice Asongu
Development Finance Centre, Graduate School of Business,
University of Cape Town, Cape Town, South Africa

Jacinta Nwachukwu
Lancashire School of Business and Enterprise,
University of Central Lancashire, Preston, UK

Stella-Maris Orim
School of Engineering, Environment and Computing,
Coventry University, Coventry, UK, and

Chris Pyke
Lancashire School of Business and Enterprise,
University of Central Lancashire, Preston, UK

Abstract
Purpose – The purpose of this paper is to complement the scant macroeconomic literature on the development outcomes of social media by examining the relationship between Facebook penetration and violent crime levels in a cross-section of 148 countries for the year 2012.
Design/methodology/approach – The empirical evidence is based on ordinary least squares (OLS), Tobit and quantile regressions. In order to respond to policy concerns on the limited evidence on the consequences of social media in developing countries, the data set is disaggregated into regions and income levels. The decomposition by income levels included: low income, lower middle income, upper middle income and high income. The corresponding regions include: Europe and Central Asia, East Asia and the Pacific, Middle East and North Africa (MENA), Sub-Saharan Africa and Latin America.
Findings – From OLS and Tobit regressions, there is a negative relationship between Facebook penetration and crime. However, quantile regressions reveal that the established negative relationship is noticeable exclusively in the 90th crime quantile. Further, when the data set is decomposed into regions and income levels, the negative relationship is evident in the MENA while a positive relationship is confirmed for Sub-Saharan Africa. Policy implications are discussed.
Originality/value – Studies on the development outcomes of social media are sparse because of a lack of reliable macroeconomic data on social media. This study primarily complemented three existing studies that have leveraged on a newly available data set on Facebook.
Keywords Technology, Information exchange, Social media, Interactive media, Social networking, Knowledge-based community
Paper type Research paper

1. Introduction
In every corner of the earth, there are a growing number of citizens who considerably rely on social media for information and discussion. The knowledge gained could either moderate their position on some conflicting interests or consolidate their radical standpoint. Discussions may be within personal networks as well as individuals without any prior ties with whom offline interactions would have been impossible owing to, inter alia: distances and asymmetric daily schedules (Barbera, 2015). In the light of the growing relevance of social media platforms in everyday corporate and household activities, a recent World Bank report on digital dividends has recommended more research on the socio-economic and development consequences of social media (World Bank, 2016).

JEL Classification — K42, D83, O30, D74
The authors are indebted to the editor and reviewers for constructive comments.
In response to above policy concern, the positioning of this study on the relationship between social media and crime is motivated by the growing cost of crime and violence on the one hand and gaps in the literature, on the other. These two issues are substantiated below in this order.

First, a substantial part of annual global wealth is increasingly being spent by governments in the prevention and mitigation of violence, crimes, political instability with consequent externalities (Asongu, 2018; GPI, 2016; Anderson, 2015; Asongu and Kodila-Tedika, 2017). According to the attendant policy and scholarly literature, the underlying annual global wealth spent is about $14.3 trillion and represents the combined gross domestic product of the following advanced countries, namely: Brazil, Canada, France, Germany, Spain and the UK. This policy effort can be considerably improved with evidential insights into the relationship between social media and crime across the world. Unfortunately, the extant macroeconomic contemporary literature on this interconnection is rare because of a lack of appropriate data.

Second, the existing literature on crimes can be summarised in two main strands, notably: studies on crime and literature on the relationship between social media and crime. The former strand has largely focused on: risk evaluations in decisions on sentencing (Kopkin et al., 2017); assessment of parallels between mass incarceration and mass deportation (Tanya, 2017); determinants of drug use after sentencing (Rao et al., 2016); the relevance of legal origins in cross-country consequences of crime (D’Amico and Williamson, 2015); the role of restorative justice in crime prevention (Woods, 2015); the imprisonment of adolescents that are traumatised (Mallet, 2015); drivers and deterrents of juvenile delinquency after sentencing (Olashore et al., 2017); the relationship between inequality, imprisonment and public health (Wilderman and Wang, 2017) and strategies designed to support families and children whose parents have been imprisoned (Kjellstrand, 2017). The strand of literature on the association between social media and crime has focused on: developing social media-based suicide prevention messages (Robinson et al., 2017); the use of Twitter to monitor mental health discussions (McClellan et al., 2017); examining suicide risks and emotional distress in Chinese social media (Chen et al., 2017); social media and the emerging suicide death rate among military personnel (Bryan et al., 2018) and the designing of microblog direct messages used in the engagement of users of social media who have suicide intentions (Tan et al., 2017).

Notably, the foregoing literature has the shortcoming of being too exploratory and country-specific. For instance, the study by Robinson et al. (2017), Tan et al. (2017) and Chen et al. (2017) were focused on China while, Bryan et al. (2018) was concerned with the USA. The present study addresses this country-specific shortcoming by employing a global data set of 148 countries on the one hand, and on the other, decomposing the data set into regions and income levels, in order to increase the policy relevance of the study. The disaggregation is also motivated by the imperative of articulating developing countries, in order to address a concern by the World Bank which maintains that the development consequences of social media, especially in developing countries have not been substantially researched and documented (World Bank, 2016[1]).

In the light of the observation of the World Bank, a reason for the scant empirical analyses on the macroeconomic consequences of social media is the lack of relevant data. As far as we have reviewed, only three studies have employed a recent Facebook penetration data set to assess the association between social media usage and development outcomes. Kodila-Tedika (2018) has investigated the link between Facebook penetration and the governance of natural resources, Jha and Sarangi (2017) have examined if Facebook penetration influences corrupt behaviour, while Jha and Kodila-Tedika (2018) have investigated if democracy is promoted by Facebook penetration.

The current study improves this strand of literature by evaluating the strength of the connection between Facebook penetration and crime. The empirical evidence is based on ordinary least squares (OLS), Tobit and quantile regressions and data from 148 countries for the year 2012. From OLS and Tobit regressions, there is a negative relationship
between Facebook penetration and crime. From quantile regressions, the established negative relationship is apparent exclusively in the 90th quantile. When the data set is decomposed into regions and income levels, the negative relationship is obvious in the Middle East and North Africa (MENA) while a positive relationship is established for Sub-Saharan Africa.

The results of our empirical analyses have significantly improved the narratives in the aforementioned exploratory and country-specific studies in three key ways. First, they complemented the description by Tan et al. (2017) and other country-specific studies by confirming the policy relevance of the negative association between social media and crime. This global dimension can lead to the adoption of more holistic policies that are applicable to a wide variety of countries. Second, the findings improve exploratory studies (e.g. Robinson et al., 2017) by establishing that the hypothetical negative relationship between social media and crime withstands empirical scrutiny within the framework of Facebook penetration. Third, contrary to the previous studies, our findings do not support a “one size fits all implications for policy” because they are articulated along two main dynamics: on the one hand, income levels and regions and on the other hand, initial levels of crime. Accordingly, beyond the emphasis on income levels and regions, the fact that the estimated negative relationship is exclusively apparent at the highest quantile of the crime distribution is an indication that blanket policies on the nexus between Facebook penetration and crime cannot be effective unless on initial levels of crime and tailored differently across countries with low, intermediate and high initial levels of crime.

Overall, the findings are broadly consistent with the existing literature. According to Chen et al. (2017), social media can be used to effectively assess emotional distress and suicide risk. Robinson et al. (2017) concluded that social media could potentially be an important mechanism for the prevention and moderation of distress as well as suicidal behaviour and thoughts. This is consistent with the position of Bryan et al. (2018) who subsequently found that certain sequences in the content of social media could predict the cause and timeline of death by suicide. The conclusions of Bryan et al. (2018) are in line with Tan et al. (2017) who reported that whereas web-based interventions can be effective in the prevention of online suicide, it is also imperative to increase user engagement with online information and discussion groups.

The rest of the study is structured as follows. Section 2 dwells on the theoretical underpinning whereas the data and methodology are covered in Section 3. The empirical results are presented in Section 4 while Section 5 concludes.

2. Theoretical underpinnings

The theoretical connection between social media and crime can be elucidated from three main perspectives, notably: a wound culture theory (WCT) if Facebook penetration positively affects crime; social control and conflict management theories in a scenario where Facebook penetration reduces crime; and irrespective of the direction of effect (i.e. whether positive or negative), both strands of theoretical underpinnings rely on technology acceptance models (TAM). The three theoretical frameworks are expanded in chronological order.

The WCT can be used to elicit some negative socio-economic signals such as crimes, political instability and violence. The WCT was developed by Mark Seltzer (1998) and later summarised by Gibson (2006) as follows:

Serial killing has its place in a public culture in which addictive violence has become not merely a collective spectacle but one of the crucial sites where private desire and public fantasy cross. The convening of the public around scenes of violence – the rushing to the scene of the accident, the milling around the point of impact – has come to make up a wound culture; the public fascination with torn and open bodies and torn and open persons, a collective gathering around shock, trauma, and the wound. (p. 19)
According to the WCT, the desire to inflict harm on humans in society is both literal (via mutilation) and figuration (via criticism). The relevance of crime is considered within the theoretical framework as a common focus which enables citizens to engage in wound appreciation: “One discovers again and again the excitations in the opening of private and bodily and psychic interiors; the exhibition and witnessing, the endlessly reproducible display, of wounded bodies and wounded minds in public. In wound culture, the very notion of sociality is bound to the excitations of the torn and open body, the torn and exposed individual, as public spectacle” (Seltzer, p. 137). The author has further observed that the wound theory has considerable implications in the formation of citizenry attitude: “The spectacular public representation of violated bodies, across a range of official, academic, and media accounts, in fiction and in film, has come to function as a way of imagining and situating our notions of public, social, and collective identity (Seltzer, p. 21). Social media can be used to fuel the wound culture because it is a mechanism by which information is exchanged to either increase contention or hatred among users or improve harmony and moderation among them. In the latter scenario, conflict management and social control models are more relevant.

Social control and conflict management models (CMM) have been used to substantiate theoretical underpinnings in the recent conflict management literature (Asongu and Kodila-Tedika, 2017), namely: the CMM of Thomas-Kilmann (1992) and the social control theory (SCT) by Black (1990). The SCT maintains that relationships between organisations, groups and individuals typically affect the exercise of one among five fundamental channels of social control, notably: self-help, settlement, avoidance, tolerance and negotiation. Conversely, the CMM argues that strategic ambitions that are very likely to centre on a two dimensional matrix (of cooperation and assertiveness), when merged with collaboration could result in five principal styles in the management of conflicts, namely: avoidance, compromise, collaboration, competition and accommodation. These theoretical insights are broadly in line with the conflict management literature (Borg, 1992; Volkema and Bergmann, 1995; Akinwale, 2010; Asongu and Kodila-Tedika, 2017). Social media provides the platforms which underpin the conflict management and social control theories herein discussed.

The effectiveness of either the WCT or social control theories depends on TAM. In accordance with recent social media (Nikiforova, 2013; Lee and Lowry, 2015; Cusick, 2014) and information technology (Yousafzai et al., 2010; Asongu et al., 2018) studies, TAM are dominated by three principal theories which justify the adoption and use of specific types of communication tools. They are the: theory of reasoned action (TRA), theory of planned behaviour (TPB) and TAM.

Consistent with the TRA, the underpinning hypothesis is that, when the acknowledgement of actions come into play, customers display rational features (Fishbein and Ajzen, 1975; Ajzen and Fishbein, 1980; Bagozzi, 1982). Given the context of the study, these rational traits could motivate new ideas, notably: either to the resolution of conflicts or in the perception of crime as a solution to conflicts. The TPB is an extension of the TRA which articulates the absence of a difference between customers who are conscious of the ramifications of their actions and those that are lacking in this consciousness (Ajzen, 1991). The theory is in accordance with social media because crime prevention or crime propagation can be done by users with or without, adequate certainty on the soundness of the information being shared. Concerning the TAM, the principal driver behind a customer’s motivation to adopt a specific technology is traceable to preferences and the will of a client to adopt and use a specific means of communication (Davis, 1989).

Hence, the selection of social media platform by a user is contingent on the relevance of the social media network in attenuating or fuelling crime.

The three strands of theories, which were discussed in the previous paragraphs, are also relevant to the positioning of this study because: Facebook penetration entails the adoption
and usage of a specific type of social media (which is consistent with TAM) and Facebook can either be used to fuel or deter crime. On the one hand, the use of Facebook to fuel crime is consistent with WCT while the use of the Facebook to mitigate crime is in line with the SCT and the CMM. On the other, the common features among TAM merit contextualisation. Accordingly, the TRA, TPB and TAM articulate the perspective that the use and adoption of particular types of communication mechanisms encompass a multitude of traits, namely: the formation of customer belief and the composite elements which entail, utilitarian, behavioural, psychological and social characteristics. In what follows, these common features are contextualised.

Within the specific context of this study, the utilitarian view is apparent when a social media platform is adopted by an individual because he/she presumes that such a platform is relevant in enhancing his/her opportunities for fuelling or preventing crime; with regard to the behavioural view, even in a scenario where personal motivation is not apparent, an individual can still take the decision to use social media if he/she already has some degree of awareness that adopting social media for crime-related purposes is a social norm; psychological and personal motivations can also be important in the decision of an individual to adopt a social media platform for crime-related concerns if the person is motivated by private potential rewards in crime prevention and/or crime instigation by means of social media; and the importance of belief formation in an individual is consolidated by the view that it is an accepted social norm that social media can either be used to prevent crime or instrumented to fuel crime.

In the light of the above concepts, the decision by an individual to adopt Facebook for a crime-related ambition can be inspired by both idiosyncratic (or individual) and systemic (or social) factors as well as the potential advantages of using the social media platform to realise his/her crime-related objective.

The choice of variables in the conditioning information set is consistent with wound culture (i.e. for the WCT), conflict management (i.e. for the CMM) and social control (i.e. for the SCT). These control variables which are discussed in the data section include: access to weapons, homicide rate, prison incarcerations, violent demonstrations and conflict intensity.

3. Data and methodology

3.1 Data

The study focuses on a cross-section of 148 countries for the year 2012. The selected geographic and temporal scopes are due to data availability constraints. The data come from variables sources, notably: the Uppsala Conflict Data Program Battle-Related Deaths Data set; qualitative assessments by Economic Intelligence Unit (EIU) analysts’ estimates; the operations of Criminal Justice Systems; the International Institute for Strategic Studies the Institute for Economics and Peace; the United Nations Office on Drugs and Crime Surveys on Crime Trends, Quintly and the United Nations Committee on Contributions. The selection of these sources is motivated by the recent literature on crime and violence (Asongu and Acha-Anyi, 2018; Asongu, 2018). Moreover, to the best of our knowledge, the sources are used by authoritative scholarly and policy reports and data sets on crime and peace. These include: reports on the global peace index and the global terrorism database.

The dependent variable is the level of violent crime from the qualitative assessment by the EIU analysts’ estimates while the data on Facebook penetration (which is a proxy of social media usage) is from Quintly, which is a social media benchmarking and analytics Solution Company[2]. This data on social media are consistent with the recent literature on the consequences of social media on development outcomes (Jha and Sarangi, 2017;
Jha and Kodila-Tedika, 2018; Kodila-Tedika, 2018). It confirms the authenticity of our source of data on Facebook penetration. However, as in the case of these other previous studies, the findings are interpreted as simple correlations without causal inferences. This is due to, the cross-sectional nature of the data set. This caveat is also disclosed in the concluding section. In summary, in the absence of panel data, the use of cross-sectional data to inform scholars and policy makers on the relationships between a new phenomenon (such as social media penetration) and social outcomes (such as crime), is a useful initial scientific activity.

Five main control variables are adopted in this study. They are: access to weapons; homicide; incarcerations; violent demonstrations and conflict intensity. The selection of the variables to be included in the conditioning information set is supported by the findings of recent studies on the determinants of conflicts, crime, incarcerations and violence (Asongu and Acha-Anyi, 2018; Asongu and Kodila-Tedika, 2016, 2017; GPI, 2016; Freytag et al., 2011; Blanco and Grier, 2009). They commonly advised that variables which are most likely to be associated with crime (as documented in the attendant literature) should be used as control variables. In accordance with the existing literature, we expect these variables to positively influence the crime rate. This is essentially because they reflect conditions that are favourable to criminality and violence. The choice of these control variables is also consistent with the aforementioned theories because they are by definition concomitant with wound culture, conflict management and social control. Table AI provides the definitions of variables while Table AII discloses the summary statistics (in Panel A) and the sampled countries (in Panel B). A correlation matrix is also provided in Table AIII.

Secondary data are used for the study. Hence, contrary to the requirement of discussing how the data are collected as it is the case of primary data, the study defines the variables, justifies the reliability of their sources and articulates how the choice of the variables are in conformity with the existing literature and the problem statement being investigated. The interested reader is advised to obtain further information on how data on each variable was collected by referring to the original sources identified in the previous paragraph.

3.2 Methodology

3.2.1 Ordinary least squares. Borrowing from the recent literature based on cross-sectional observations, the OLS estimation strategy is considered because the underlying assumptions are in agreement with the nature of the data set. The latest articles have advised the use of this estimation approach on cross-sectional data (Andrés, 2006; Asongu, 2013a; Kodila-Tedika and Asongu, 2015). The following equation illustrates the relationship between Facebook penetration and crime:

\[ C_i = \alpha_1 + \alpha_2 F_i + \alpha_3 X_i + \epsilon_i, \]

where \( C_i \) and \( F_i \) represent the crime and Facebook penetration indicator for country \( i \) in that order, \( \alpha_1 \) is a constant, \( X \) is a vector of control variables, and \( \epsilon_i \) the error term. \( X \) contains the following five variables: access to weapons; homicide; incarcerations; violent demonstrations; and conflict intensity.

3.2.2 Tobit regressions. The level of violent crime as rated by the EIU analysts’ varies from 0 to 5. Theoretically, the OLS approach could be complemented with Tobit regressions because the dependent variable has a restricted range (Kumbhakar and Lovell, 2000; Koetter et al., 2008; Ariss, 2010; Coccorese and Pellecchia, 2010). Moreover, a double-censored Tobit approach is the same as estimating with a linear regression technique because the two likelihood functions coincide (Coccorese and Pellecchia, 2010; Asongu and Nwachukwu, 2016; Ajide et al., 2019).
The standard Tobit model (Tobin, 1958; Carson and Sun, 2007) is represented as follows:

\[ y_{it}^* = \alpha_0 + \beta X_{it} + \epsilon_{it} \]  
(2)

where \( y_{it}^* \) is a latent response variable, \( X_{it} \) is an observed \( 1 \times k \) vector of explanatory variables and \( \epsilon_{it} \) is i.i.d. \( N(0, \sigma^2) \) and is independent of the \( X_{it} \) variables. Instead of observing \( y_{it}^* \) we observe \( y_{it} \):

\[ y_{it} = \begin{cases} 
  y_{it}^*, & \text{if } y_{it}^* > \gamma \\
  0, & \text{if } y_{it}^* \leq \gamma, 
\end{cases} \]  
(3)

where \( \gamma \) is a non-stochastic constant. In other words, the value of \( y_{it}^* \) is missing when it is less than or equal to \( \gamma \).

3.2.3 Quantile regressions. The OLS and Tobit regressions discussed in the previous two sections are based on the conditional mean of the dependent variable. In order to address this static concern, the quantile regression approach is adopted to estimate parameters throughout the conditional distribution of the dependent variable (Koenker and Bassett, 1978). While mean effects in the previous two estimation techniques are relevant, the quantile regression technique articulates lower, intermediate and higher levels of crime. The quantile regression strategy is increasingly being employed in the empirical literature in order to provide more policy implications. Most notable studies are in: health (Asongu, 2014a), finance, (Asongu, 2014b) and corruption (Billger and Goel, 2009; Asongu, 2013b; Okada and Samreth, 2012).

The \( \theta \)th quantile estimator of crime is obtained by solving for the following optimisation problem, which is presented without subscripts in the following equation for the purpose of simplicity and readability:

\[
\min_{\beta \in \mathbb{R}^k} \left[ \sum_{i \in \{y_i \geq x_i \beta\}} \theta |y_i - x_i \beta| + \sum_{i \in \{y_i < x_i \beta\}} (1-\theta) |y_i - x_i \beta| \right],
\]  
(4)

where \( \theta \in (0, 1) \). Contrary to OLS method which is fundamentally based on minimising the sum of squared residuals, the QR approach focuses on minimising the weighted sum of absolute deviations for different quantiles such as the median or 90th quantile (with \( \theta = 0.50 \) or 0.90, respectively). The conditional quantile of the crime rate or \( y_i \) given \( x_i \) is shown as follows:

\[ Q_{y_i}(\theta/x_i) = x_i \beta \theta, \]  
(5)

where, unique slope parameters are modelled for each \( \theta \)th specific quantile. This formulation is analogous to \( E(y/x) = x/\beta \) in the OLS slope where parameters are assessed only at the mean of the conditional distribution of the crime rate. For Equation (5) the dependent variable \( y_i \) is crime whereas \( x_i \) is a vector contain in the following control variables: a constant term, access to weapons; homicide; incarcerations; violent demonstrations; and conflict intensity.

4. Empirical analysis

4.1 Presentation of results

The empirical results pertaining to OLS and Tobit regressions are presented in Table I. Findings reported on the left-hand side (LHS) and right-hand side (RHS) are, respectively, from OLS and Tobit regressions. The following outcomes are observable from the table.
### Table I.
Ordinary least squares and negative binomial regressions

<table>
<thead>
<tr>
<th>Dependent variable: crime</th>
<th>Ordinary least squares</th>
<th>Tobit regressions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Constant</td>
<td>3.322*** (0.000)</td>
<td>3.426*** (0.000)</td>
</tr>
<tr>
<td>Facebook penetration</td>
<td>-0.027*** (0.000)</td>
<td>-0.010* (0.056)</td>
</tr>
<tr>
<td>Access to Weapons</td>
<td>0.570*** (0.000)</td>
<td>0.687*** (0.000)</td>
</tr>
<tr>
<td>Homicide</td>
<td>0.412*** (0.000)</td>
<td>0.493*** (0.000)</td>
</tr>
<tr>
<td>Incarcerations</td>
<td>-0.047 (0.559)</td>
<td>-0.022 (0.821)</td>
</tr>
<tr>
<td>Violent</td>
<td>0.294*** (0.000)</td>
<td>0.378*** (0.000)</td>
</tr>
<tr>
<td>Demonstrations</td>
<td>-0.017 (0.432)</td>
<td></td>
</tr>
<tr>
<td>Conflict Intensity</td>
<td>0.193** (0.010)</td>
<td></td>
</tr>
<tr>
<td>Fisher</td>
<td>15.36*** 65.84*** 41.01***</td>
<td>33.38*** 78.44*** 97.57*** 123.06***</td>
</tr>
<tr>
<td>Adjusted $R^2$</td>
<td>0.202 0.419 0.496 0.576</td>
<td>0.069 0.162 0.202 0.255</td>
</tr>
<tr>
<td>LR $\chi^2$</td>
<td>37.20***</td>
<td>97.57*** 123.06***</td>
</tr>
<tr>
<td>Pseudo $R^2$</td>
<td>0.193***</td>
<td>0.378*** 0.207***</td>
</tr>
</tbody>
</table>

**Notes:** *,**,***Significant at 10, 5 and 1 per cent levels, respectively.
First, Facebook penetration is negatively correlated with the crime rate. The negative relationship is robust to the first-three specifications on the LHS and the first-two specifications on the RHS. It is important to note that the best specification is the third because concerns of multicollinearity are less noticeable. Putting aside the concern of multicollinearity, univariate regressions depict a negative correlation between the two variables of interest. However, the magnitude of negative relationship decreases as the number of variables in the conditioning information set is increased. This change is normal because in the real world, Facebook penetration and crime do not interact in isolation, but the connection is contingent on other determinants of crime. Moreover, as more control variables are added to the specifications, the coefficient of adjustment (i.e. adjusted $R^2$) increases. The significant determinants of crime (or control variables) in the conditioning information set have the expected positive signs.

Table II provides the quantile regressions results which are based on the third specification of OLS and Tobit regressions in Table I. As discussed previously, this third specification in Table I provides our best Facebook estimator because issues of multicollinearity are more apparent in the fourth specification. Consistent differences in the estimated Facebook coefficients between the OLS/Tobit and quantiles regressions (in terms of sign, magnitude and significance) provides justification for our decision to employ the three separated estimation methods in this study. The main finding in the quantile regression in Table II is that, the established negative relationship between Facebook penetration and crime is highest in the 90th quantile. Again, the significant control variables display the expected signs.

### 4.2 Extension with fundamental characteristics

As an extension of our empirical analysis, a recent concern raised by a World Bank report is addressed in this section. This relates to the poor coverage in the literature of the importance of social media in development outcomes, especially for developing countries (World Bank, 2016). In order to articulate the relevance of our analysis for developing nations, the data set is disaggregated into regions and income levels. This decomposition by regions and income groups is in accordance with the World Bank’s classification of income groups and a recent stream of development studies (Narayan et al., 2011; Beegle et al., 2016; Asongu and Nwachukwu, 2017; Machila et al., 2017; Asongu and Le Roux, 2017[3]. The decomposition by income levels comprises: low income, lower middle income, upper middle income and high income. The corresponding regions include: Europe and Central Asia, East Asia and the Pacific, MENA, Sub-Saharan Africa and Latin America (Table III).

<table>
<thead>
<tr>
<th>Dependent variables: crime</th>
<th>Q.10</th>
<th>Q.25</th>
<th>Q.50</th>
<th>Q.75</th>
<th>Q.90</th>
</tr>
</thead>
<tbody>
<tr>
<td>Constant</td>
<td>0.614 (0.328)</td>
<td>0.348 (0.473)</td>
<td>0.743 (0.100)</td>
<td>1.428* (0.077)</td>
<td>1.952*** (0.001)</td>
</tr>
<tr>
<td>Facebook penetration</td>
<td>-0.008 (0.168)</td>
<td>-0.003 (0.533)</td>
<td>-0.005 (0.344)</td>
<td>-0.007 (0.421)</td>
<td>-0.018*** (0.003)</td>
</tr>
<tr>
<td>Access to weapons</td>
<td>0.038*** (0.008)</td>
<td>0.364*** (0.001)</td>
<td>0.445*** (0.000)</td>
<td>0.449*** (0.014)</td>
<td>0.399*** (0.001)</td>
</tr>
<tr>
<td>Homicide</td>
<td>0.154* (0.066)</td>
<td>0.315*** (0.000)</td>
<td>0.278*** (0.003)</td>
<td>0.389*** (0.018)</td>
<td>0.356*** (0.002)</td>
</tr>
<tr>
<td>Incarcerations</td>
<td>-0.034 (0.830)</td>
<td>-0.011 (0.914)</td>
<td>-0.029 (0.780)</td>
<td>-0.160 (0.309)</td>
<td>0.023 (0.819)</td>
</tr>
<tr>
<td>Pseudo $R^2$</td>
<td>0.264</td>
<td>0.248</td>
<td>0.293</td>
<td>0.310</td>
<td>0.376</td>
</tr>
<tr>
<td>Observations</td>
<td>148</td>
<td>148</td>
<td>148</td>
<td>148</td>
<td>148</td>
</tr>
</tbody>
</table>

Notes: OLS, ordinary least squares. $R^2$ for OLS and Pseudo $R^2$ for quantile regression. Lower quantiles (e.g. Q 0.1) signify nations where crime is least. *,**,**,**Significant at 10, 5 and 1 per cent levels, respectively.

Table II. Quantile regressions
Table III.

Comparative evidence on social media and political instability

<table>
<thead>
<tr>
<th>Dependent variable: crime</th>
<th>Ordinary least squares (OLS)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Income levels</td>
<td>Regions</td>
</tr>
<tr>
<td>Constant</td>
<td>0.513 (0.429)</td>
</tr>
<tr>
<td>Facebook penetration</td>
<td>-0.003 (0.421)</td>
</tr>
<tr>
<td>Control variables</td>
<td>Yes</td>
</tr>
<tr>
<td>Fisher Adjusted R²</td>
<td>5.87***</td>
</tr>
<tr>
<td>Observations</td>
<td>42</td>
</tr>
</tbody>
</table>

| Income levels | Regions | HI | UMI | LMI | LI | ECA | EAP | MENA | SSA | LA |
| Control variables | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| Fisher Adjusted R² | 0.061 (0.931) | 1.094 (0.489) | 0.345 (0.742) | 0.493 (0.671) | 0.753 (0.220) | -0.314 (0.850) | 0.582 (0.740) | -0.336 (0.784) | -1.134 (0.677) |
| Observations | 42 | 34 | 39 | 33 | 47 | 15 | 17 | 38 | 22 |

| Income levels | Regions | HI | UMI | LMI | LI | ECA | EAP | MENA | SSA | LA |
| Control variables | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes | Yes |
| Fisher Adjusted R² | 17.47*** | 14.69*** | 11.04*** | 11.60*** | 37.10*** | 9.48*** | 12.94*** | 17.92*** | 121.2*** |
| Observations | 42 | 34 | 39 | 33 | 47 | 15 | 17 | 38 | 22 |

| Notes: HI, high income countries; UMI, upper middle income countries; LMI, little middle income countries; LI, low income countries; ECA, Europe and Central Asia; EAP, East Asia and the Pacific; MENA, Middle East and North Africa; SSA, Sub-Saharan Africa; LA, Latin America. *,**,***Significant at 10, 5 and 1 per cent levels, respectively. |
4.3 Discussion
The negative relationship between social media and violent crime can be elucidated from two main perspectives: friendly interactions for ideological moderation and ideological harmonisation. These two perceptions are expanded in chronological order.

First, a possible reason for the negative association between Facebook penetration and crime is because the information sharing platform does not exclusively connect people with problems in the society – the kind of disputes that could motivate them to resort to crime as a means to resolving them. Hence, diverse information on how to solve corresponding issues may provide Facebook users with avenues and solutions to the concerns that otherwise would have been resolved through violence and crime.

The consumption of conflicting information from social media (Kaplan and Haenlein, 2010) is not exclusively limited to interactions between acquaintances, co-workers, family and friends. This narrative is consistent with the literature maintaining that selectivity of information is restricted because users of social media platforms are exposed to all types of information on conflict resolution and crime prevention from friends and acquaintances (Brundidge, 2010). As recently explained by Barberá (2015), in accordance with the Pew Research Centre, as of 2013, approximately half of the users of social media (i.e. Facebook and Twitter), received information from a plethora of sites while about 78 per cent of the underlying users were exposed incidentally to information. In summary, a social media platform is a mechanism by which friendly interactions and ideological moderation can assuage violent intensions. The medium of exchange and moderation has been generally supported by the mainstream literature on this channel. Most notably: Burke and Kraut (2014) who concluded that there is a considerable overlap between offline and personal networks; Gilbert and Karahalios (2009) and Jones et al. (2013) who remarked that social media interactions facilitate the consolidation of interpersonal relationships; Mutz (2006) who asserted that online information sharing platforms promote ties between social media users; Messing and Westwood (2014) who suggested that friendly recommendations by social media users are indications that reduce conflicting situations; and Barberá (2015) who proposed that individuals are more likely to use information from people sharing the same social media platform even if they disagree with them. Such diversity in views provides a gateway to ideological moderation.

Second, ideological moderation is facilitated by social media because users of social media are exposed to information from people with different ideologies and network heterogeneity (Mutz, 2006; Barberá, 2015). This is contrary to a contending proposition in the literature that the exchange of information on social media is often between users of the same belief (Conover et al., 2012; Colleoni et al., 2014; Smith et al., 2014; Barberá and Rivero, 2014). The position supported by findings in this study is that exposure to social media can moderate violent dispositions because of among others reasons relating to: “political tolerance” (Mutz, 2002), “greater awareness of rationales for oppositional views” (Mutz, 2002, p. 114), a learning framework of socialisation (Stoker and Jennings, 2008) and mitigation in overconfidence in ideological positions (Iyengar et al., 2012; Ortoleva and Snowberg, 2015).

5. Concluding implications and future research directions
The study has examined the relationship between Facebook penetration and violent crime in a cross-section of 148 countries for the year 2012. The empirical evidence is based on three estimation methods: OLS, Tobit and quantile regressions. From OLS and Tobit regressions, there is a negative relationship between Facebook penetration and crime. From quantile regressions, the established negative relationship is apparent exclusively in the 90th quantile. When the data set is disaggregated into regions and income levels, the negative relationship is noticeable in the MENA while a positive relationship is confirmed for Sub-Saharan Africa.

The findings have also contributed to the policy literature on the concern that the literature on the consequences of social media is sparse, especially in developing countries.
World Bank, 2016). Furthermore, when existing levels of crime are taken into account in the modelling exercise, the fact that social media is most effective in countries where the crime rate is highest. Such, is an indication that blanket policies on the interconnections between Facebook penetration and crime rates are ineffective unless the application is tailored distinctly across countries with high, intermediate and low levels of crime.

The findings of the study also have implications on the social theory literature because they complement the existing studies on the importance of social networks in the behaviour of citizens (Tufekci and Wilson, 2012; Bond et al., 2012; Vaccari et al., 2013). As discussed in Section 4.3, our findings also clarify the relevance of social media in modulating violent tendencies owing to information diversity, ideological moderation and ideological harmonisation, when messages are disseminated via social media platforms such as the Facebook (McCharg, 2006; Klofstad, 2009; Barberá, 2015).

In the light of the above, it is also worthwhile to emphasise that, with the exception of the Sub-Saharan African region, the findings in this study challenge the mainstream wisdom that social media fuels violence. The corresponding caveat is that, the established negative link between Facebook penetration and crime is not causal. However, in the absence of panel data, the use of cross-sectional data to inform scholars and policy makers on the interconnections between a new phenomenon (such as social media) and social outcomes (such as crime), is a worthwhile initial empirical exercise.

In the light of the above shortcomings, improving the findings with panel data in the assessment of whether the relationships extend to causality is advisable. Moreover, examining the feasibility of the suggested channels of association (i.e. ideological moderation and ideological harmonisation) is another interesting future research area.

Notes
1. The positioning and design of this paper is consistent with the extant recent empirical and theoretical studies on the relevance of information technology in: enhancing conditions for human development (Afutu-Kotey et al., 2017; Bongomin et al., 2018; Asongu and Bouteng, 2018; Gosavi, 2018; Hubani and Wiese, 2018; Minkoua Nzie et al., 2018; Issahaku et al., 2018; Abor et al., 2018; Muthanja and Chipeta, 2018; Asongu and Nwachukwu, 2018a, b) and improving society with opportunities for human emancipation (Kreps and Kimppa, 2015; Tatnall, 2015; Lennerfors et al., 2015; Patrignani and Whitehouse, 2015; Aricat, 2015; Lahtiranta et al., 2015; Tchamyou, 2017, 2018; Tchamyou and Asongu, 2017).
2. The data were accessed from its website (www.quintly.com/facebook-countrystatistics?period=1year).
3. There are four main World Bank income groups: high income, $12,276 or more; upper middle income, $3,976–$12,275; lower middle income, $1,006–$3,975; and low income, $1,005 or less.

References

Akinwale, A.K. (2010), “Integrating the traditional and the modern conflict management strategies in Nigeria”, Department of Sociology, Faculty of Social Sciences, University of Ibadan, Ibadan.


Further reading


Appendix 1

Variables | Definition of variables and sources
--- | ---
Violent crime | Level of violent crime  
Qualitative assessment by EIU analysts
Facebook penetration | Facebook penetration (2012), defined as the percentage of total population that uses Facebook. From Quintly
Access to weapons | Ease of access to small arms and light weapons  
Qualitative assessment by EIU analysts
Homicides | Number of homicides per 100,000 people  
United Nations Office on Drugs and Crime (UNODC) Surveys on Crime Trends and the Operations of Criminal Justice Systems (CTS); EIU estimates
Incarceration | Number of jailed population per 100,000 people  
World Prison Brief, International Centre for Prison Studies, University of Essex
Violent demonstrations | Likelihood of violent demonstrations  
Qualitative assessment by EIU analysts
Conflict intensity | Conflict Intensity, GPI

Notes: UCDP, Uppsala Conflict Data Program; IEP, the Institute for Economics and Peace; EIU, the Economic Intelligence Unit; UNPKF, United Nations Peacekeeping Funding; GDP, gross domestic product; IISS, the International Institute for Strategic Studies; GPI, global peace index

Table A. Definition of variables

Table AI.
Panel A: summary statistics

<table>
<thead>
<tr>
<th>Variables</th>
<th>Mean</th>
<th>SD</th>
<th>Minimum</th>
<th>Maximum</th>
<th>Observers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Violent crime</td>
<td>2.774</td>
<td>1.109</td>
<td>1.000</td>
<td>5.000</td>
<td>148</td>
</tr>
<tr>
<td>Facebook penetration</td>
<td>19.868</td>
<td>18.566</td>
<td>0.038</td>
<td>97.636</td>
<td>148</td>
</tr>
<tr>
<td>Access to weapons</td>
<td>3.118</td>
<td>1.077</td>
<td>1.000</td>
<td>5.000</td>
<td>148</td>
</tr>
<tr>
<td>Homicides</td>
<td>2.799</td>
<td>1.170</td>
<td>1.183</td>
<td>5.000</td>
<td>148</td>
</tr>
<tr>
<td>Incarceration</td>
<td>2.209</td>
<td>0.902</td>
<td>1.174</td>
<td>5.000</td>
<td>148</td>
</tr>
<tr>
<td>Violent demonstrations</td>
<td>2.950</td>
<td>0.983</td>
<td>1.000</td>
<td>5.000</td>
<td>148</td>
</tr>
<tr>
<td>Conflict intensity</td>
<td>2.432</td>
<td>1.164</td>
<td>1.000</td>
<td>5.000</td>
<td>148</td>
</tr>
</tbody>
</table>

Panel B: sampled countries (148)
Afghanistan; Albania; Algeria; Angola; Argentina; Armenia; Australia; Austria; Azerbaijan; Bahrain; Bangladesh; Belarus; Belgium; Benin; Bhutan; Bolivia; Bosnia and Herzegovina; Botswana; Brazil; Bulgaria; Burkina Faso; Burundi; Cambodia; Cameroon; Canada; Central African Republic; Chad; Chile; China; Colombia; Costa Rica; Croatia; Cyprus; Czech Republic; Democratic Republic of the Congo; Denmark; Djibouti; Dominican Republic; Ecuador; Egypt; El Salvador; Equatorial Guinea; Eritrea; Estonia; Ethiopia; Finland; France; Gabon; Georgia; Germany; Ghana; Greece; Guatemala; Guinea; Guyana; Haiti; Honduras; Hungary; Iceland; India; Indonesia; Iraq; Ireland; Israel; Italy; Jamaica; Japan; Jordan; Kazakhstan; Kenya; Kuwait; Kyrgyz Republic; Laos; Latvia; Lebanon; Lesotho; Libya; Lithuania; Macedonia (FYR); Madagascar; Malawi; Malaysia; Mali; Mauritania; Mauritius; Mexico; Moldova; Mongolia; Montenegro; Morocco; Mozambique; Namibia; Nepal; the Netherlands; New Zealand; Nicaragua; Niger; Nigeria; Norway; Oman; Pakistan; Panama; Papua New Guinea; Paraguay; Peru; the Philippines; Poland; Portugal; Qatar; Republic of the Congo; Romania; Russia; Rwanda; Saudi Arabia; Senegal; Serbia; Sierra Leone; Singapore; Slovak; Slovenia; Somalia; South Africa; South Korea; Spain; Sri Lanka; Swaziland; Sweden; Switzerland; Tajikistan; Tanzania; Thailand; The Gambia; Togo; Trinidad and Tobago; Tunisia; Turkey; Turkmenistan; Uganda; Ukraine; United Arab Emirates; the UK; the USA; Uruguay; Uzbekistan; Venezuela; Vietnam; Yemen and Zambia

Notes: SD, standard deviation; Observers, Observations
### Appendix 3

**Corresponding author**
Simplice Asongu can be contacted at: asongusimplic@yahoo.com

<table>
<thead>
<tr>
<th></th>
<th>Weapons</th>
<th>Homicide</th>
<th>Incarcerations</th>
<th>Demonstrations</th>
<th>Conflict intensity</th>
<th>Facebook</th>
<th>Crime</th>
</tr>
</thead>
<tbody>
<tr>
<td>Weapons</td>
<td>1.000</td>
<td>0.527</td>
<td>-0.105</td>
<td>0.525</td>
<td>0.605</td>
<td>-0.545</td>
<td>0.636</td>
</tr>
<tr>
<td>Homicide</td>
<td>1.000</td>
<td>0.186</td>
<td>0.256</td>
<td>-0.160</td>
<td>-0.071</td>
<td>0.121</td>
<td>-0.028</td>
</tr>
<tr>
<td>Incarcerations</td>
<td>1.000</td>
<td>-0.160</td>
<td>0.531</td>
<td>1.000</td>
<td>-0.531</td>
<td>-0.473</td>
<td>0.552</td>
</tr>
<tr>
<td>Demonstrations</td>
<td>1.000</td>
<td>-0.473</td>
<td>0.563</td>
<td>1.000</td>
<td>-0.449</td>
<td>Facebook</td>
<td>Crime</td>
</tr>
</tbody>
</table>

**Notes:** Weapons: access to weapons; Homicide: homicide rate; Incarcerations: incarceration rate; Demonstrations: violent demonstrations; Facebook: Facebook penetration; Crime: violent crime

**Table AIII.** Correlation matrix

For instructions on how to order reprints of this article, please visit our website: www.emeraldgrouppublishing.com/licensing/reprints.htm

Or contact us for further details: permissions@emeraldinsight.com
Shoplifting in mobile checkout settings: cybercrime in retail stores

John A. Aloysius
Department of Supply Chain Management, Sam M. Walton College of Business, University of Arkansas, Fayetteville, Arkansas, USA, and
Ankur Arora and Viswanath Venkatesh
Department of Information Systems, Sam M. Walton College of Business, University of Arkansas, Fayetteville, Arkansas, USA

Abstract

Purpose – Retailers are implementing technology-enabled mobile checkout processes in their stores to improve service quality, decrease labor costs and gain operational efficiency. These new checkout processes have increased customer convenience primarily by providing them autonomy in sales transactions in that store employee interventions play a reduced role. However, this autonomy has the unintended consequence of altering the checks and balances inherent in a traditional employee-assisted checkout process. Retailers, already grappling with shoplifting, with an estimated annual cost of billions of dollars, fear that the problem may be exacerbated by mobile checkout and concomitant customer autonomy. The purpose of this paper is to understand the effect of mobile checkout processes in retail stores on cybercrime in the form of shoplifting enabled by a technology transformed the retail environment.

Design/methodology/approach – The authors conducted an online survey of a US sample recruited from a crowdsourced platform. The authors test a research model that aims to understand the factors that influence the intention to shoplift in three different mobile checkout settings – namely, smartphone checkout settings, store-provided mobile device checkout settings, and employee-assisted mobile checkout settings – and compare it with a traditional fixed location checkout setting.

Findings – The authors found that, in a smartphone checkout setting, intention to shoplift was driven by experiential beliefs and peer influence, and experiential beliefs and peer influence had a stronger effect for prospective shoplifters when compared to experienced shoplifters; in a store-provided mobile devices checkout setting, experiential beliefs had a negative effect on shoplifters’ intention to shoplift and the effect was weaker for prospective shoplifters when compared to experienced shoplifters. The results also indicated that in an employee-assisted mobile checkout setting, intention to shoplift was driven by experiential beliefs and peer influence, and experiential beliefs had a stronger effect for prospective shoplifters when compared to experienced shoplifters.

Originality/value – This study is the among the first, if not first, to examine shoplifters’ intention to shoplift in mobile checkout settings. We provide insights into how those who may not have considered shoplifting in less favorable criminogenic settings may change their behavior due to the autonomy provided by mobile checkout settings and also provide an understanding of the shoplifting intention for both prospective and experienced shoplifters in different mobile checkout settings.

Keywords Smartphone, Mobile checkout, Prospective shoplifters, Employee-assisted mobile checkout, Store-provided mobile device

Paper type Research paper

1. Introduction

“I take full responsibility for the mistake I have made – shoplifting. I know that this goes beyond me letting my school down. I let the entire country down,” said Codey Riley, one of the three UCLA Bruins basketball players accused of shoplifting in China (ESPN, 2017). These players did not belong to economically disadvantaged sections of society. This is not the only such incident when celebrities or financially advantaged people have committed such an act. Even wealthy celebrities, such as Megan Fox who stole from Walmart when she was a teen, Britney Spears who stole a one-dollar lighter from a gas station and Lindsay Lohan who stole a $2,500 necklace from a jewelry store (Tinubu, 2018), have been found to shoplift.
It is evident from these stories that shoplifting is committed not just due to financial need, but there could be other reasons for shoplifting, such as to satisfy psychological needs, due to societal influences, to satisfy the desire to possess expensive objects or for enjoyment and entertainment (Krasnovsky and Lane, 1998).

Shoplifting is defined as the act of stealing from a store by a customer when the store is open for business (Francis, 1979). It is one of the most prevalent crimes in our society. According to the National Association for Shoplifting Prevention (NASP), there are approximately 27m shoplifters in the USA and thus it is estimated that 1 in every 11 people shoplift. Out of those shoplifters, 25 percent are juveniles and 75 percent are adults (NASP, 2018). Shoplifting happens in all types of retail stores, i.e., department stores, drug stores, supermarkets, thrift shops, specialty shops, music stores and convenience stores, with supermarkets particularly prone to shoplifting as they carry a broad selection of items catering to the needs of people (Luo et al., 2015). According to a recent survey, 90 percent of retail crime was due to shoplifting by customers, and the remainder was due to dishonest employees, cargo theft at the supplier, or due to administrative errors (Jack L. Hayes International, Inc., 2017). Estimates of the annual losses in retail stores from shoplifting across the globe have ranged in the billions of dollars, with the US retail industry losing nearly $50bn in 2016 (Reilly, 2017). There are big losses from shoplifting in other countries as well, with even the much smaller New Zealand retail market reporting over $800m in financial losses in 2017 (RetailNZ, 2017), and the Japanese retail market suffering a loss of approximately 450bn yen in 2016 (Yamato et al., 2017).

Over the past few years, retailers have invested in technology-enabled self-checkout processes to enhance customer experience. Retailers are making mobile applications more user-friendly to create a better shopping experience and to ease transaction processing for customers (Roth et al., 2009). Retailers have also integrated mobile technologies in the form of mobile checkout processes into their sales operations to create a better shopping experience for customers (Aloysius et al., 2016; Chandra et al., 2010). Although mobile checkout has brought benefits to both retailers and customers in the form of customer satisfaction and convenience (Fernandes and Pedroso, 2016; Venkatesh et al., 2017; Vuckovac et al., 2017), self-service scenarios have also been attributed to a form of cybercrime known as shoplifting using technology (Knapton, 2016; Phillips et al., 2005; Taylor, 2016). Self-scanning technologies have generated losses of more than 122 percent of the average (University of Leicester, 2016). Over the past few years, the evolution of technology has brought new ways of conducting cybercrime. Our research aims to understand thus a new type of cybercrime in the form of shoplifting aided by technology that will add to the literature on criminology.

Shoplifting has serious implications not only for the retail industry, but also for society as a whole. Sales tax revenues lost due to shoplifting could be utilized for the betterment of society (Potdar et al., 2018). The losses incurred by retailers due to shoplifting result in an increase in the price of merchandise and customers ultimately have to pay to cover the cost of stolen goods. Therefore, there are compelling practical reasons to investigate the factors that play a role in promoting and/or driving the act of shoplifting in retail stores.

The literature on shoplifting in the criminology as well as the retailing/marketing fields has provided a rich understanding of the motivational beliefs that are articulated for various types of shoplifters (Blum et al., 2018; Cameron, 1964; Cox et al., 1990; Grant, 2006; Krasnovsky and Lane, 1998; Moore, 1984). The shoplifting literature has also provided insights into the prevention mechanisms ranging from social influence (Cox et al., 1993), fear appeals (Vermeir et al., 2017) and control (Hirtenlehner and Hardie, 2016), to implementation of technology, i.e., in the form of video cameras, and image analysis to electronic article surveillance (EAS) systems (McCarty, 2017; Yamato et al., 2017). Although these studies have given us an understanding of the motivations and beliefs and have provided effective means of preventing...
shoplifting, the literature lacks an understanding of the new form of cybercrime resulting from emerging customer-facing technologies used by retailers in the stores. Such a new context can result in changes to our theories (see Johns, 2006) – and technology-specific theories have been shown to outperform general theories (see Hong et al., 2014). Although some studies do discuss the role of self-service technologies tied to shoplifting (Phillips et al., 2005; Taylor, 2016), there is a need for a deeper understanding of the motivations and beliefs driving intention to shoplift in mobile checkout settings that feature increased autonomy to customers. Further, empirical work has mostly studied experienced shoplifters with a history of criminal shoplifting behavior and how their impulsive desire to steal, societal influences and desire to possess wealthy objects motivate them to commit shoplifting (Blum et al., 2018; Cameron, 1964; Cox et al., 1990; Grant, 2006; Krasnovsky and Lane, 1998; Moore, 1984). The literature lacks an understanding of prospective shoplifters, who do not have prior shoplifting experience, but do not have a moral repugnance toward shoplifting and could thus be enticed into shoplifting in the right circumstances – here, mobile checkout settings. Given the emerging mobile technology-driven changes to retail shopping processes, there is a need for more theory-driven investigations of the underlying factors that can lead to a new form of cybercrime tied to shoplifting in a mobile technology-enabled checkout context and ultimately, to retail losses.

Our work aims to understand shoplifting intention among customers in different mobile checkout settings using a multi-theoretic lens to allow us to tap into related yet distinct aspects that drive shoplifting intention: theory of planned behavior (TPB; Ajzen, 1991) and situational action theory (SAT; Wikström, 2006). TPB provides a framework to understand the determinants of intention to shoplift. Underlying TPB is the core argument that an individual’s intention to perform a behavior determines the actual performance of the behavior. Beyond that, TPB states that an individual’s attitude toward performing the behavior, subjective norm, and perception of behavioral control drive an individual's intention to perform the behavior. TPB will thus help us understand the link between shoplifter beliefs and shoplifting intention in different mobile checkout settings. SAT hypothesizes that human action is influenced by the settings in which he or she takes part. In mobile checkout technologies, customers have either reduced or no engagement with store employees in comparison to traditional fixed location employee-assisted checkout. These mobile checkout settings could act as criminogenic settings for shoplifters. SAT will help us understand the influence of environment settings in the form of mobile checkout settings on shoplifting intention. SAT is a general theory of crime that explains criminal behavior by integrating persons’ crime propensity and criminogenic settings, and an environment conducive to crime, to which an individual is exposed. Integrating these two theoretical lenses will strengthen our understanding of the emerging scenarios by integrating environmental factors in the form of mobile checkout settings with beliefs and how these beliefs drive shoplifting intention. Different types of customer-friendly checkout mechanisms implemented in retail stores could not only contribute to customer satisfaction, but also function as a driver of shoplifting. To the best of our knowledge, no prior research has been conducted to understand the influence of technology in driving shoplifting intention. Against this backdrop, the overall goal of this work is to investigate the beliefs instrumental in shoplifting intention in different mobile checkout settings among experienced shoplifters and prospective shoplifters. Given the role that technology can play in creating situations – e.g. store processes – store processes that facilitate shoplifting, the specific objectives of this work are to:

(1) understand the factors driving shoplifting intention in different mobile checkout scenarios;

(2) compare the effect of factors driving shoplifting intentions for experienced and prospective shoplifters in different mobile checkout settings; and
(3) empirically validate the model with data gathered from experienced and prospective shoplifters.

This work is expected to contribute to the literature in different ways. First, it will enrich our understanding of the drivers of shoplifting in the context of the new, emerging mobile checkout scenarios, which become the criminogenic settings, and how conducive they are to shoplifting. Second, we will contribute to the shoplifting literature by understanding shoplifting intention among both experienced shoplifters, and among prospective shoplifters who possess the beliefs and desire to shoplift but never had the exposure to criminogenic settings in the form of mobile checkout settings that bestow the customer with a high degree of autonomy. Third, our work will extend the shoplifting literature by integrating two theoretical lenses to provide a holistic understanding of the factors influencing experienced and prospective shoplifters, not to mention the subtle differences across these two sets of shoplifters. Lastly, our work will complement research on cybercrime by understanding how the use of technology in the retail industry can work to shoplifters’ advantage.

2. Theory
2.1 Literature review
The first incident of shoplifting was examined in 1838 by two French physicians – Jean-Etienne Esquirol and C.C. Marc. They coined the term “Kleptomania” to describe shoplifting as an involuntary and irresistible action (Abelson, 1989). Shoplifting is committed either by professional criminals to resell stolen items for monetary benefits or by respectable citizens who do not resell the items they steal but have chronic impulsivity to shoplift (Cameron, 1964). The complexity of factors associated with motivations and characteristics of shoplifters resulted in various extensions of Cameron’s typology and researchers have delineated several types of shoplifters based on personality and social class (Goldman, 1991; Moore, 1984; Schlueter et al., 1989). The literature on shoplifting has studied different gender and age groups to understand the factors driving customers to shoplift, such as peer pressure, psychological needs, experiential beliefs and monetary benefits (Blum et al., 2018; Cameron, 1964; Cox et al., 1990; Grant, 2006; Krasnovsky and Lane, 1998; Moore, 1984). Much of the IS literature in retail settings has dealt with the relationship between technology and customer satisfaction (e.g. Aloysius et al., 2016; Fernandes and Pedroso, 2016; Venkatesh et al., 2017; Vuckovac et al., 2017), and the benefits of technology in preventing shoplifting (Yamato et al., 2017). The literature on cybercrime has dealt with various kinds of cybercrime: from cyberbullying (Lowry et al., 2016) to hacking and spreading of malicious software (Bossler and Holt, 2009; Choi, 2008) to cyber-trespassing (Maimon and Louderback, 2019) to cyber-deception (Jajodia et al., 2017) to digital piracy (Lowry et al., 2017) to cyber porn (Lewis, 2018). Although there have been attempts to define and classify cybercrime (e.g. Wall, 2007), such efforts tend to evolve over time following the evolution of technology and how people use that technology. Jahankhani et al. (2014) provide a typology of cybercrime that includes a category defined by “using a computer as the instrumentality of the crime (e.g. fraudulent use of automated teller machine (ATM) cards and accounts, credit card and telecommunication fraud).” The extant research does not consider a form of crime in this category – the emerging form of cybercrime tied to shoplifting using technology, such as mobile phones and store devices, used either by employees or customers. Although shoplifting has featured in some research related to cybercrime, it was mostly descriptive (Rempala and Okdie, 2017).

Shoplifting is one means of customer product acquisition (Cox et al., 1990) and has been defined as the act of acquiring products through stealing as a customer misbehavior (Cox et al., 1990; Fullerton and Punj, 1993; Tonglet, 2001). Thus, we define shoplifters as the category of customers engaging in an act of misbehavior of stealing merchandise from...
stores either for fun, money or to satisfy their psychological impulses (Cameron, 1964; Cox et al., 1990; Moore, 1984). Ray (1987) argued that customers who are more likely to perceive shoplifting in retail stores as not a bad thing are more likely to engage in the act of shoplifting. We define experienced shoplifters as those who have engaged in prior shoplifting. Thus, shoplifters could be experienced as they have shoplifted in the past or could be customers who have a desire to shoplift but, in the past, were deterred due to less favorable retail settings that caused a feeling of apprehension toward being detected. We delineate people who have not shoplifted in the past into prospective shoplifters and honest customers. We define prospective shoplifters as those who have not previously shoplifted, but have the desire to shoplift and could commit shoplifting given conducive retail store settings. We define honest customers as those who have not previously committed shoplifting and have high repugnance toward shoplifting in retail stores.

2.2 Criminogenic settings
A setting is defined as an environment to which a person is exposed. Mobile checkout technologies in retail stores can be criminogenic settings as customers have either no engagement or limited engagement with store employees in comparison to traditional fixed location employee-assisted checkout and customers have increased autonomy in the transaction process during checkout (Aloysius et al., 2016). Mobile checkout settings in retail stores are forms of self-service technology checkout settings in which the customer purchases a product without direct contact with a store employee or with minimal interaction with an employee (Fernandes and Pedroso, 2016; Tseng and Yazdanifar, 2015; Vuckovac et al., 2017). We studied three types of mobile checkout scenarios (Aloysius et al., 2013) that have been implemented by retailers to speed up customer transaction processing and create better customer-store engagement (Fernandes and Pedroso, 2016; Tseng and Yazdanifar, 2015; Venkatesh et al., 2017; Vuckovac et al., 2017). SAT assumes that human action is influenced by the settings in which an individual takes part. Settings are termed as criminogenic when they are conducive to crime. This theory in the context of mobile checkout settings helps us to understand the context in which shoplifting could take place.

2.2.1 Smartphone checkout settings. This process requires the use of a smartphone to scan products by opening an app on the phone and making the payment through a mobile wallet. Technology failure, no employee engagement and lack of scanning knowledge by the customer could create problems, preventing the smooth operation of this process.

2.2.2 Store-provided mobile device checkout settings. This process requires the use of a store-provided mobile device by a customer to scan products in the basket and the basket is assigned an electronic ID. The customer uses a self-service lane and the basket ID is used for payment. This process requires registration of the customer at the store before they can use the store mobile device. Technology failure, no employee engagement and lack of knowledge about scanning on the part of the customer could create problems preventing the smooth operation of this process.

2.2.3 Employee-assisted mobile checkout settings. A store employee is equipped with a mobile device to scan the products in a customer’s basket and uses a mobile credit card machine to accept payment on the shop floor. Customers do not need to go to fixed checkout terminals for transaction processing. During busy periods, an employee-assisted mobile checkout setting could create problems for customers having to find a store employee to process a transaction.

2.2.4 Fixed location checkout settings. In this process that has been the traditional mode of checkout for about 100 years, a store employee at a fixed checkout terminal (point-of-sale terminal) helps customers to scan products in their basket and payment is done either by
cash or using a credit or debit card machine at the terminal. During busy periods, fixed location checkout settings could create inconvenience to customers as they have to wait in line for sales transactions to be processed by the server.

2.3 Research model
Mobile checkout settings in retail stores are forms of autonomous technology checkout settings in which a customer purchases a product either without any direct contact with a store employee or with minimal interaction with an employee (Fernandes and Pedroso, 2016; Tseng and Yazdanifar, 2015; Vuckovac et al., 2017). Such checkout settings provide autonomy and convenience to customers, as they do not need to stand in line at fixed registers for scanning and payment. We examine intention to shoplift in these mobile checkout settings. Figure 1 shows our conceptual model. TPB provides a framework to understand the determinants of intention to shoplift. TPB posits that intention, an indication of individual’s readiness to perform a given behavior and is considered to be a direct determinant of behavior (Ajzen, 1991), is determined by three factors: attitude, “an individual’s positive or negative feelings (evaluative affect) about performing the target behavior” (Fishbein and Ajzen, 1975, p. 216); subjective norm, “the person’s perception that most people who are important to him think he should or should not perform the behavior in question” (Fishbein and Ajzen, 1975, p. 302); and perceived behavioral control, “the perceived ease or difficulty of performing the behavior” (Ajzen, 1991, p. 188). It is typical for beliefs underlying these core constructs to be identified for particular contexts including the prediction of technology-related behaviors (e.g. Brown and Venkatesh, 2005; Venkatesh and Brown, 2001). For the shoplifting context, we conceptualized attitude, subjective norm, and perceived behavioral control in the form of experiential beliefs, peer influence, and technology self-efficacy and define intention to shoplift as an individual’s willingness to shoplift; experiential beliefs as the extent to which a customer views shoplifting in mobile

![Conceptual model](image-url)
checkout settings as fun or exciting (Ray, 1987); peer influence as the extent to which a customer is influenced by peers to shoplift (Cox et al., 1990); and technology self-efficacy as the belief in one’s ability to complete a checkout process using technology (McDonald and Siegall, 1992).

We also used SAT to understand how motivations and beliefs drive people to engage in an act of shoplifting behavior in different criminogenic settings – here, mobile checkout settings (Wikström, 2006). Situational action theory states that interaction between persons’ crime propensity and criminogenic exposure guide actions. Therefore, SAT will provide insights into drivers of intention of shoplifters in different mobile checkout settings. Although we do not examine actual behavior in our research, but as shown in Figure 1, we study intention, which is a predictor of actual behavior (Ajzen and Fishbein, 1980; Venkatesh et al., 2016; Yang et al., 2016), including shoplifting (Tonglet, 2001).

2.4 Hypotheses development

2.4.1 Experiential beliefs. TPB posits that beliefs, such as the experiential belief identified here, underlying attitude influences intention to perform a behavior. Mobile checkout settings, namely smartphone bestow a high level of autonomy to shoplifters. Such autonomous checkout settings will foster a feeling of fun or excitement that shoplifters want to experience (Ray, 1987). Fernandes and Pedroso (2016), in their study on self-service technologies in retail stores, argued that customers find it enjoyable and entertaining when they scan items themselves. For example, customers could make a scanning motion without activating their mobile phone app. Therefore, we argue that shoplifters, both experienced and prospective, are more likely to derive pleasure from the entertainment in autonomous mobile checkout settings as they pretend to scan the items and are able to carry out more items from the store than for which they actually pay. Thus, we posit that:

**H1a.** Experiential beliefs will have a positive relationship with intention to shoplift in smartphone checkout settings for both experienced and prospective shoplifters.

Store-provided mobile checkout settings require registration in order to use a store device for scanning. Such checkout settings are likely to induce fear in the minds of the shoplifters. Research has shown that shoplifting behavior is influenced by apprehension risks (Cox et al., 1990; Dahlback, 1998; Ray, 1987). Shoplifters are likely to have negative feeling toward store-provided mobile checkout settings. In TPB terms, this is a negative evaluative effect that undermines the positive effect of experiential beliefs. Thus, we posit that:

**H1b.** Experiential beliefs will have a negative relationship with intention to shoplift in store-provided mobile device checkout settings for both experienced and prospective shoplifters.

In employee-assisted mobile checkout settings, a store employee helps a customer to checkout by scanning the items on the floor. In such checkout settings, employees sometimes find it hard to manage foot traffic. Shoplifters could take advantage of such situations and walk away from the store without paying for the items. A shoplifter might have an accomplice engage with a store employee and stand between the store employee and the shoplifter so that they mask the act of concealment. This will have a positive evaluative effect on shoplifters and such affect is likely to excite and add to the hedonic motivation of shoplifters (Holbrook and Hirschman, 1982). Thus, we posit that:

**H1c.** Experiential beliefs will have a positive relationship with intention to shoplift in employee-assisted mobile checkout settings for both experienced and prospective shoplifters.
2.4.2 Peer influence. TPB argues that peer influence can play a key role in the intention to engage in specific behaviors. Peer influence is a strong motivational factor to engage in shoplifting (Cox et al., 1990; Tonglet, 2001). Individuals tend to adopt bad habits of friends known as "deviant social influence" (Johnson, 1979). Peer influence is thus likely to influence both experienced and prospective shoplifters in mobile checkout settings as yielding to the influence will help them gain status among their peers (Johnson, 1979). Thus, we posit that:

H2a. Peer influence will have a positive relationship with intention to shoplift in smartphone checkout settings for both experienced and prospective shoplifters.

H2b. Peer influence will have a positive relationship with intention to shoplift in store-provided mobile device checkout settings for both experienced and prospective shoplifters.

H2c. Peer influence will have a positive relationship with intention to shoplift in employee-assisted mobile checkout settings for both experienced and prospective shoplifters.

2.4.3 Technology self-efficacy. TPB posits that perceived ease or difficulty of performing the behavior and the concomitant control is a direct determinant of intention to perform a behavior. Technology self-efficacy will be vital in mobile checkout settings for scanning and payment. Lack of technological expertise or the confidence in one’s ability could be a challenge in order to use the mobile devices for checkout (Aloysius et al., 2013). Ease of use of mobile devices, which is determined by self-efficacy (Venkatesh and Davis, 1996; Venkatesh, 2000) will contribute to the use of mobile checkout settings (see Venkatesh et al., 2012). Criminals use technical knowledge to find vulnerabilities in technology in cyber deception (Jajodia et al., 2017). Shoplifters could make use of their technical proficiency by either finding loopholes in store-provided mobile devices or retail stores’ mobile apps on their own smartphones. We can thus expect both experienced and prospective shoplifters to be influenced by their technology self-efficacy. Thus, we posit that:

H3a. Technology self-efficacy will have a positive relationship with intention to shoplift in smartphone checkout settings for both experienced and prospective shoplifters.

H3b. Technology self-efficacy will have a positive relationship with intention to shoplift in store-provided mobile device checkout settings for both experienced and prospective shoplifters.

In the case of employee assisted checkout settings, store employee uses a store-provided mobile device for checkout. In such settings, shoplifters’ technology self-efficacy becomes moot and will not play a part in helping shoplifters in checkout.

2.4.4 Interaction effect: intention to shoplift in smartphone checkout settings. As noted earlier, smartphone checkout settings bestow a high level of autonomy to the shoplifters as shoplifters do not have to interact with a store employee for checkout. When individuals use a technology for the first time, they tend to be more excited because of the novelty associated with the use of the technology (Holbrook and Hirschman, 1982). Innovativeness in the form of shoplifting and using a smartphone will act in concert (see Holbrook and Hirschman, 1982). Prospective shoplifters who desire to shoplift but never found the environment conducive to shoplifting are more likely to experience greater highs compared to experienced shoplifters to whom although the technology is novel, shoplifting itself is not. Thus, we posit that:

H4. Experiential beliefs will have positive relationship with intention to shoplift in smartphone checkout settings such that the effect will be stronger for prospective shoplifters than it will be for experienced shoplifters.
Shoplifters tend to mimic other shoplifters when their peers steal with impunity (Nettler, 1989). Peer influence will be greater on prospective shoplifters than on experienced shoplifters. This is because experienced shoplifters, having already engaged in shoplifting, will be less influenced by the peers than prospective shoplifters will be. There is significant accumulated evidence that the impact of peer pressure on intention is greater when the behavior is newer (see Venkatesh and Davis, 2000; Venkatesh et al., 2003; Venkatesh et al., 2012). Thus, we posit that:

H5. Peer influence will have a positive relationship with intention to shoplift in smartphone checkout settings such that the effect will be stronger for prospective shoplifters than it will be for experienced shoplifters.

Higher technology self-efficacy among experienced shoplifters is likely to lead to higher intention to shoplift because they will be more comfortable with leveraging a smartphone to shoplift. In contrast, a prospective shoplifter, despite comparable technology self-efficacy, will be more apprehensive about the act of shoplifting itself. Thus, we posit that:

H6. Technology self-efficacy will have a positive relationship with shoplifting intention in smartphone checkout settings such that the effect will be stronger for experienced shoplifters than it will be for prospective shoplifters.

2.4.5 Interaction effect: intention to shoplift in store-provided mobile device checkout settings. Store-provided mobile checkout settings require customers to reveal their identity in the registration process in order to use the store device for checkout. It will be easy for retail stores to track a shoplifter in such checkout settings. Shoplifters are more likely to develop a negative feeling toward engaging in shoplifting in store-provided mobile device checkout settings for fear of being caught. Research has shown that shoplifting behavior is influenced by apprehension risks (Cox et al., 1990; Dahlback, 1998; Ray, 1987). In TPB terms, this is a negative evaluative effect that undermines the positive effect of experiential beliefs. Prospective shoplifters, given the lack of shoplifting experience, can be expected to have greater apprehension and fear, thus dampening the effect of experiential beliefs more in their case than in the case of experienced shoplifters. Thus, we posit that:

H7. Experiential beliefs will have a positive relationship with shoplifting intention in store-provided mobile device checkout settings such that the effect will be weaker for prospective shoplifters than it will be for experienced shoplifters.

In autonomous mobile device checkout settings, such as this, the more pressure put on by the peers, the more likely for shoplifters, both experienced and prospective, to engage in shoplifting in order to comply with the peers. Registration process to use store-device for checkout will induce apprehensions among both experienced and prospective shoplifters. As fear is shown to be more salient in curbing actions of novice criminals than experienced criminals (Cusson, 1993; Copes and Tewksbury, 2011), such apprehension risks are likely to be more salient to deter prospective shoplifters when compared to experienced shoplifters in store-provided mobile device checkout settings. Thus, we posit that:

H8. Peer influence will have a positive relationship with shoplifting intentions in store-provided mobile device checkout settings such that the effect will be stronger for experienced shoplifters than it will be for prospective shoplifters.

Technology self-efficacy is important to operate a store-provided mobile device for scanning and checkout. High self-efficacy will help shoplifters exploit the vulnerabilities associated with the technology used in store-provided mobile devices (see Jajodia et al., 2017). SAT states that interaction between persons’ crime propensity and criminogenic exposure guide action. Prospective shoplifters have constrained their actions in traditional checkout
settings owing to the fear of being caught when engaging in shoplifting (Cox et al., 1990; Ray, 1987). They are more likely to perceive higher risk of being apprehended in trying to interfere with store-devices for the purpose of shoplifting. Thus, prospective shoplifters have lower intention to shoplift in store-provided checkout settings when compared to experienced shoplifters. Thus, we posit that:

\begin{align*}
H9. \text{ Technology self-efficacy will have a positive relationship with shoplifting intention in store-provided mobile device checkout settings such that the effect will be stronger for experienced shoplifters than it will be for prospective shoplifters.}
\end{align*}

2.4.6 Interaction effect: intention to shoplift in employee-assisted mobile checkout settings.

Shoplifters require distraction or diversion to cover an act of theft. In retail stores, employees sometimes find it hard to manage foot traffic, and shoplifters could take advantage of such situations and walk away from the store without paying for the items. The advantage of bypassing store employees when store employees are busy handling other customers will make the task easy for shoplifters. Prospective shoplifters will have a greater urge to perform an action that would help fulfill their desire of experiencing the act of shoplifting for the first time (Schroeder, 2006) and given the task of shoplifting is made easier, they are more likely than experienced shoplifters to have higher intention to shoplift or hide items from employees who, in times of high traffic, may not be able to spot the hidden items. Thus, we posit that:

\begin{align*}
H10. \text{ Experiential beliefs will have a positive relationship with shoplifting intention in employee-assisted mobile checkout settings such that the effect will be stronger for prospective shoplifters than it will be for experienced shoplifters.}
\end{align*}

Such checkout settings provide a criminogenic environment for shoplifters to imitate the deviant behaviors of their peers (Johnson, 1979). The logic for this hypothesis is the same as the logic for \( H8 \). Thus, we posit that:

\begin{align*}
H11. \text{ Peer influence will have a positive relationship with shoplifting intention in employee-assisted mobile checkout settings such that the effect will be stronger for experienced shoplifters than it will be for prospective shoplifters.}
\end{align*}

2.4.7 Interaction effect: intention to shoplift in fixed location checkout settings.

Prior research on shoplifting behavior was conducted in fixed location checkout settings (Cox et al., 1990; Moore, 1984; Tonglet, 2001). Peer influence was found to be a determinant for shoplifters to engage in shoplifting in fixed location checkout settings (Cox et al., 1990; Tonglet, 2001). In such checkout settings, payment is done either by cash or using a credit or debit card machine at the terminal. The fear of getting caught will restrain prospective shoplifters from shoplifting in fixed location checkout settings (Cox et al., 1990; Dahlback, 1998) more than it does experienced shoplifters. On the contrary, experienced shoplifters will comply with their peers in such checkout settings. Thus, we posit that:

\begin{align*}
H12. \text{ Peer influence will have a positive relationship with shoplifting intention in fixed-location checkout settings such that the effect will be stronger for experienced shoplifters than it will be for prospective shoplifters.}
\end{align*}

3. Methods

3.1 Participants and data collection

Our study is a type of mixed-methods research study. We followed a sequential mixed-methods research approach (Creswell et al., 2003). A mixed-methods study provides holistic understanding of the phenomena of interest (Venkatesh et al., 2013). Before designing our
survey, we reached out to the NASP for insight into shoplifting in the environment of mobile checkout. In a focus group with shoplifters conducted by the NASP, one of the authors observed the discussion that suggested interest in shoplifting in mobile checkout settings. The findings from the qualitative study gave us impetus to conduct a quantitative study to get a deeper understanding of the role of technology in facilitating shoplifting in mobile checkout settings. For this, we conducted an online survey using crowdsourced platform – M-turk. All survey research is subject to limitations based on the method used to recruit subjects – whether it is a mailing, e-mail list, visitors to a physical location or otherwise. Recent literature (e.g. Goodman and Paolacci, 2017) has listed the advantages as well as the limitations of a crowdsourced data collection platform such as M-Turk and consistent with recommendations in that literature we took the precautions to ensure validity of our results. Prior to analyzing the data, we screened all responses for completeness and accuracy. We excluded those respondents who did not correctly answer reverse-coded filler items and/or took less than two minutes to complete the survey. Two minutes were used as a quality threshold based on the number of questions and we felt that those respondents who spent less than two minutes paid inadequate attention to the questions. We also included social desirability measures (Haghighat, 2007) to ensure the reliability of responses, as shoplifting is a sensitive subject and thus may be subject to dishonest reporting. Thus, we feel our sample was appropriate to understand the intention to shoplift in mobile checkout settings. We did not feel the need to compare early vs late responses because all responses were collected during a single week and we did not send out reminders (see Hair et al., 1998). To collect data, we presented customers with all the four checkout scenarios present in our research model. All respondents were provided with information about the different checkout scenarios and for better clarity, we also included images of mobile checkout scenarios to further illustrate the processes defined in each of the mobile checkout scenarios. Our sample comprised 472 participants. Table AI provides information on the respondent demographics.

3.2 Measurement

Most questions were adapted from prior studies and contextualized for shoplifting in mobile checkout settings. The items used in our study are listed in Table AII. In predicting intention to shoplift, we control for various individual-level variables, i.e., gender, age, ethnicity, education, geography, employment, annual household income, urge to shoplift, shoplifting experience, shoplifting team size and social desirability score. These were controlled because they are known influences on the intention to shoplift.

4. Data analysis and results

4.1 Reliability and validity of the scales

We used Smart-PLS, version 3.2.8 to analyze our data. Factor loadings, average variance extracted, and reliabilities were examined to assess validity and reliability. We observed that Cronbach’s α was higher than 0.70 for all scales. Thus, we concluded that our scales were reliable. The measurement model indicated that items measuring each construct loaded onto a single factor and all cross-loadings were less than 0.40. Thus, the evidence suggests that the scales exhibited discriminant validity. Tables AIII and AIV provide reliability and validity statistics.

4.2 Categorization of shoplifters

We first categorized the data into shoplifters, i.e., those who had committed shoplifting in the past and non-shoplifters who never shoplifted, using the corresponding survey question on past shoplifting. Ray (1987) argues that customers who do not have a repugnance toward shoplifting in retail stores are more likely to shoplift. Based on the responses on opinions
about shoplifting in retail stores measured on a seven-point Likert-type scale adapted from Ray (1987), we identified prospective shoplifters as those who may desire to shoplift in retail stores but have never shoplifted. We computed a median split of the observations from non-shoplifters for opinions about shoplifting in retail settings and checked the differences in the intention to shoplift across different mobile checkout settings between prospective shoplifters, who have less repugnance toward shoplifting in retail stores, and honest customers, who view shoplifting as bad in retail stores. After categorization, the sample comprised 146 experienced shoplifters, 126 prospective shoplifters and 200 honest customers. In comparing prospective shoplifters (opinions about shoplifting in retail stores: \( M = 3.81, \ SD = 0.88 \) with honest customers (opinions about shoplifting in retail stores: \( M = 1.56, \ SD = 0.61 \)), we found that prospective shoplifters have higher shoplifting intention in smartphone checkout settings \( t(216.55) = 2.08, \ p < 0.05 \), store-provided mobile device checkout settings \( t(182.45) = 2.88, \ p < 0.01 \), and employee-assisted mobile checkout settings \( t(178.46) = 2.36, \ p < 0.05 \). We compared shoplifting intention in fixed location checkout settings between experienced and prospective shoplifters, and found that experienced shoplifters have a higher intention to shoplift in fixed location checkout settings \( t(232.18) = 5.462, \ p < 0.001 \). We further found that for experienced shoplifters, intention to shoplift in mobile checkout settings compared to fixed location checkout settings showed no statistically significant differences \( t(145) = 0.374, \ p > 0.05 \). Prospective shoplifters showed higher shoplifting intention in mobile checkout settings compared to fixed location checkout settings \( t(125) = 1.962, \ p < 0.05 \). The results provided support for our belief that mobile checkout settings may entice prospective shoplifters to shoplift. We included social desirability measures (Haghighat, 2007) to ensure the reliability of responses as shoplifting is a sensitive subject and thus may be subject to dishonest reporting. These items are included in Appendix 4. The proportion of the respondents who admitted to shoplifting is consistent with previous studies on shoplifting (see Farrington, 1999; Klemke, 1992; Tonglet, 2001). We compared the social desirability scores of experienced and prospective shoplifters and found scores to be consistent across both types of shoplifters \( t(263.634) = 0.767, \ p > 0.05 \).

4.3 Hypotheses tests: structural model tests
To test our research model, we used Smart-PLS v 3.2.8. To study the main effects of experiential beliefs, peer influence, and technology self-efficacy on intention to shoplift in mobile checkout settings and fixed-location checkout settings, we analyzed experienced shoplifter data that had a sample size of 146 and prospective shoplifter data that had a sample size of 126. To examine the interaction effects, we analyzed the data pooled across both experienced and prospective shoplifters that had a sample size of 272. Tables I–III show the results for predicting intention to shoplift in mobile checkout settings.
shoplift in mobile checkout settings, and Table IV shows the results for predicting intention to shoplift in fixed location checkout settings.

### 4.3.1 Mobile checkout settings

Table I shows the results for predicting intention to shoplift in smartphone checkout settings. Models 1–3 explain shoplifting intention in smartphone checkout settings. Model 1 examined the main effects for experienced shoplifters and explained 56 percent of the variance. Model 2 examined the main effects for prospective shoplifters and explained 54 percent of the variance. Model 3 examined the

<table>
<thead>
<tr>
<th>Study variables</th>
<th>Models</th>
<th>Store-provided mobile device</th>
<th></th>
<th>Store-provided mobile device</th>
<th></th>
<th>Store-provided mobile device</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>4: Experienced</td>
<td>5: Prospective</td>
<td>6: Interaction</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Experiential beliefs</td>
<td>-0.293**</td>
<td>-0.755*</td>
<td>-0.606**</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Peer influence</td>
<td>0.490***</td>
<td>0.011</td>
<td>0.260**</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Technology self-efficacy</td>
<td>0.073</td>
<td>-0.089</td>
<td>0.017</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pros_Exp</td>
<td></td>
<td></td>
<td>-0.084*</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Notes:** Pros_Exp, prospective or experienced shoplifter. *p < 0.05; **p < 0.01; ***p < 0.001

### Table II.
Structural model results for store-provided mobile device checkout settings

<table>
<thead>
<tr>
<th>Study variables</th>
<th>Models</th>
<th>Employee-assisted mobile</th>
<th></th>
<th>Employee-assisted mobile</th>
<th></th>
<th>Employee-assisted mobile</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>7: Experienced</td>
<td>8: Prospective</td>
<td>9: Interaction</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Experiential beliefs</td>
<td>0.281</td>
<td>0.771***</td>
<td>0.449***</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Peer influence</td>
<td>0.794***</td>
<td>0.017</td>
<td>0.426***</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Technology self-efficacy</td>
<td>Pros_Exp</td>
<td></td>
<td>0.065</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Experiential beliefs × Pros_Exp</td>
<td></td>
<td></td>
<td>0.565***</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Peer influence × Pros_Exp</td>
<td></td>
<td></td>
<td>-0.328***</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Technology self-efficacy × Pros_Exp</td>
<td></td>
<td></td>
<td>0.529</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Adj. $R^2$</td>
<td>0.529</td>
<td>0.616</td>
<td>0.573</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Notes:** Pros_Exp, prospective or experienced shoplifter. **p < 0.01; ***p < 0.001

### Table III.
Structural model results for employee-assisted mobile checkout settings

<table>
<thead>
<tr>
<th>Study variables</th>
<th>Models</th>
<th>Fixed location checkout settings</th>
<th></th>
<th>Fixed location checkout settings</th>
<th></th>
<th>Fixed location checkout settings</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>10: Experienced</td>
<td>11: Prospective</td>
<td>12: Interaction</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Experiential beliefs</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Peer influence</td>
<td>0.707***</td>
<td>0.630</td>
<td>0.659***</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pros_Exp</td>
<td></td>
<td></td>
<td>0.114*</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Technology self-efficacy</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Experiential beliefs × Pros_Exp</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Peer influence × Pros_Exp</td>
<td></td>
<td></td>
<td>-0.601*</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Technology self-efficacy × Pros_Exp</td>
<td></td>
<td></td>
<td>0.500</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Adj. $R^2$</td>
<td>0.500</td>
<td>0.397</td>
<td>0.525</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Notes:** Pros_Exp, prospective or experienced shoplifter. *p < 0.05; ***p < 0.001
interaction effects of experiential beliefs and type of shoplifters, peer influence and type of shoplifters, and technology self-efficacy and type of shoplifters, and explained 60 percent of the variance. The results indicated that the experiential beliefs and peer influence had positive, significant effects on intention to shoplift in smartphone checkout settings for both experienced and prospective shoplifters, thus supporting $H1a$ and $H2a$. The results indicated that technology self-efficacy had a positive, significant effect on intention to shoplift in smartphone checkout settings for only experienced shoplifter, thus partially supporting $H3a$. The interaction effect of experiential beliefs and type of shoplifters was significant. Figure 2 shows that high experiential beliefs lead to higher shoplifting intention in smartphone checkout settings among prospective shoplifters, thus supporting $H4$. The interaction effect of peer influence and type of shoplifters was significant. Figure 3 shows that high peer influence leads to higher shoplifting intention in smartphone checkout settings among prospective shoplifters, thus supporting $H5$. The interaction effect of technology self-efficacy and type of shoplifters was significant. Figure 4 shows that high technology self-efficacy leads to higher shoplifting intention in smartphone checkout settings among experienced shoplifters, thus supporting $H6$.

Figure 2. Interaction effect of type of shoplifter and experiential beliefs on intention to shoplift in smartphone checkout settings

Figure 3. Interaction effect of type of shoplifter and peer influence on intention to shoplift in smartphone checkout settings
Table II shows the results for predicting intention to shoplift in store-provided mobile device checkout settings. Models 4–6 explain shoplifting intention in store-provided mobile device checkout settings. Model 4 examined the main effects for experienced shoplifters and explained 54 percent of the variance. Model 5 examined the main effects for prospective shoplifters and explained 65 percent of the variance. Model 6 examined the interaction effects of experiential beliefs and type of shoplifters, peer influence and type of shoplifters, and technology self-efficacy and type of shoplifters, and explained 60 percent of the variance. The results indicated that the experiential beliefs had negative, significant effects on intention to shoplift in store-provided mobile device checkout settings for both experienced and prospective shoplifters, thus supporting $H_{1b}$. The results indicated that peer influence had a positive, significant effect on intention to shoplift in store-provided mobile device checkout settings for only experienced shoplifter, thus partially supporting $H_{2b}$. The interaction effect of experiential beliefs and type of shoplifters was significant. Figure 5 shows that high experiential beliefs lead to lesser shoplifting intention in store-provided mobile device checkout settings and effect is weaker among prospective shoplifters, thus supporting $H_7$. The interaction effect of peer influence and type of shoplifters was significant. Figure 6 shows that high peer influence leads to higher shoplifting intention in store-provided mobile device checkout settings.
checkout settings among experienced shoplifters, thus supporting $H_{8}$. The results indicated that $H_{3b}$ and $H_{9}$ were not supported.

Table III shows the results for predicting intention to shoplift in employee-assisted mobile checkout settings. Models 7–9 explain shoplifting intention in employee-assisted mobile checkout settings. Model 7 examined the main effects for experienced shoplifters and explained 53 percent of the variance. Model 8 examined the main effects for prospective shoplifters and explained 62 percent of the variance. Model 9 examined the interaction effects of experiential beliefs and type of shoplifters, and peer influence and type of shoplifters, and explained 57 percent of the variance. The results indicated that the experiential beliefs had positive, significant effects on intention to shoplift in employee-assisted mobile checkout settings for only prospective shoplifters, thus partially supporting $H_{1c}$. The results indicated that peer influence had a positive, significant effect on intention to shoplift in employee-assisted mobile checkout settings for only experienced shoplifter, thus partially supporting $H_{2c}$. The interaction effect of experiential beliefs and type of shoplifters was significant. Figure 7 shows that high experiential beliefs lead to higher shoplifting intention in employee-assisted mobile checkout settings and effect is stronger.
among prospective shoplifters, thus supporting $H_{10}$. The interaction effect of peer influence and type of shoplifters was significant. Figure 8 shows that high peer influence leads to higher shoplifting intention in employee-assisted mobile checkout settings among experienced shoplifters, thus supporting $H_{11}$.

4.3.2 Fixed location checkout settings. Table IV shows the results for predicting intention to shoplift in fixed location checkout settings. Models 10–12 explain the intention to shoplift in fixed location checkout settings. Model 10 examined the main effects for experienced shoplifters and explained 50 percent of the variance. Model 11 examined the main effects for prospective shoplifters and explained 39 percent of the variance. Model 12 examined the interaction effects of peer influence and type of shoplifters, and explained 52 percent of the variance. The interaction effect of peer influence and type of shoplifters was significant. Figure 9 shows that high peer influence leads to higher shoplifting intention in fixed location checkout settings and effect is stronger among experienced shoplifters, thus supporting $H_{12}$.

Table V summarizes the support for the hypotheses.

Table V

<table>
<thead>
<tr>
<th></th>
<th>Exp</th>
<th>Pros</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low peer influence</td>
<td></td>
<td></td>
</tr>
<tr>
<td>High peer influence</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Figure 8.** Interaction effect of type of shoplifter and peer influence on intention to shoplift in employee-assisted mobile checkout settings.

**Figure 9.** Interaction effect of type of shoplifter and peer influence on intention to shoplift in fixed location checkout settings.
5. Discussions and implications

We found support for our proposed model linking shoplifters’ experiential beliefs, peer influence, and technology self-efficacy to their shoplifting intention in mobile checkout settings. We found that both experienced and prospective shoplifters have a higher shoplifting intention when retail stores allow customers to use their own smartphones for mobile checkout. Our model explained about 50 percent of the variance in shoplifting intention among experienced and prospective shoplifters in various mobile checkout settings. We found that shoplifters are reluctant to shoplift when they had to use a store-provided mobile device for scanning and checkout even if they have skills and knowledge to use a store-provided mobile device. We found that experiential beliefs resulted in higher shoplifting intention among prospective shoplifters in employee-assisted mobile checkout settings.

5.1 Theoretical implications

This work makes several key contributions. This work contributes to the importance of shoplifting in criminology. Although prior research in criminology has studied factors leading to shoplifting in retail markets, extant empirical literature was limited in that it mainly studied shoplifters who had been apprehended. To the best of our knowledge, our research is the first to study prospective shoplifters who desire to shoplift but never had favorable criminogenic settings in retail stores. Mobile checkout settings provide autonomy to the customers in which...
customers can scan products and process payments without needing to go to fixed terminals for sales transactions. We extend the literature by studying the motivations among both experienced and prospective shoplifters in different criminogenic settings. Also, to the best of our knowledge, no research has studied the influence of technology on shoplifters to commit shoplifting. The model proposed here complements and advances prior work on shoplifting. Retailers have invested in mobile checkout settings for customer satisfaction and competitive advantage. Our work not only leverages ideas from the literature highlighting mobile checkout settings, but also contextualizes the exploitation of mobile checkout settings by shoplifters and how these settings play a role among different shoplifters in their shoplifting intention by developing arguments and providing empirical evidence. Thus, our work contributes to the literature on the dark side of technology by bringing to light the potential downside of emerging mobile checkout settings engendering special type of cybercrime in the form of shoplifting using technology.

5.2 Practical implications
One of our key findings is the higher shoplifting intention in mobile checkout settings than fixed location checkout settings. The use of smartphone checkout settings for scanning and payment was found to be conducive to shoplifting both for experienced and prospective shoplifters. Mobile checkout settings are instrumental in reducing the costs associated with manual processing of purchase transactions. These mobile checkout processes have not only resulted in cost savings and improvements in service quality, but also created an opportunity for customers to exploit technology in committing cybercrime in the form of shoplifting. Shoplifters can easily use mobile technologies to their advantage because of the vulnerabilities associated with the technology. Our findings revealed that in autonomous mobile checkout settings both experienced and prospective shoplifters express intention to shoplift. Technology undoubtedly helps the business in terms of cost savings, surveillance mechanisms, and operational efficiency, but our findings highlight the adverse effects that arise with the implementation of technology. We caution retailers to put in place extra measures such as separate exit inspections for smartphone checkout settings, audible feedback associated with a successful scan in store mobile devices used for checkout so that unrecorded scans do not go undetected, use of data analytics to trigger extra checks for customers who were convicted before, warning messages provided in mobile applications and emails to the dishonest customers engaged in the shoplifting, use of corralling at checkout to separate customers based on the mode of checkout they choose to use, inspection check points to match the items in the basket with the receipt, higher employee engagement to monitor customers for any malicious acts, and use of electronic article surveillance (EAS) protocols to help retailers detect unpaid merchandise when it exits the store (Aloysius et al., 2013), to implementation of technology, i.e., in the form of video cameras, image analysis, to EAS systems (McCarty, 2017; Yamato et al., 2017). Our work is one of the initial steps in providing insights that could help reduce losses incurred by retailers from one form of cybercrime, shoplifting enabled by technology.

5.3 Limitations and future research
There are a few limitations of our study that must be acknowledged. First, we collected cross-sectional data. We only measured intention but this concern is alleviated given that extant previous research has shown intention to be a strong predictor of behavior (Venkatesh et al., 2016). Future research could measure behavior over different intervals of time to see whether intention results in shoplifting. Second, we did not study how technology failure and employee shirking could assist shoplifters. Technology failure could help shoplifters as failed scans will help customers to get merchandise without payment. Employees could collude with shoplifters because they are not directly responsible for
monitoring transactions. Future research could extend our work by incorporating technology failure and employee shirking behavior in the model. Third, our study was conducted in the USA. Future research could study shoplifters from different countries and we could thus extend our model by examining its generalizability across cultures. Fourth, future research could add another dimension to cybercrime related to shoplifting by studying the hacking of mobile applications and devices used in mobile checkout settings. Finally, our work did not make use of different typologies of shoplifters having different needs. Future research could include other kinds of shoplifters—e.g., impulsive shoplifters, nonrational shoplifters (Moore, 1984). This will help in enhancing our understanding of various types of shoplifters and their reactions when exposed to mobile checkout settings.

6. Conclusion
We found support for our model that shoplifters have higher shoplifting intention in the context of mobile checkout settings. The intention among shoplifters can vary depending on the kind of mobile checkout settings retailers have in place. Shoplifters showed higher intention when they used their own smartphone for checkout and were less likely to shoplift using store-provided mobile devices. Peer influence played a role in influencing shoplifting intention in all three different mobile checkout settings, namely smartphone, store-provided mobile device and employee-assisted mobile checkout settings. This work contributes to our understanding of shoplifting and use of technology by shoplifters to their advantage by identifying, justifying, and empirically testing determinants of shoplifting intention. Our model can serve as a platform for future research and our findings can help retailers in taking necessary steps to curb the losses due to shoplifting in mobile checkout settings. This work complements prior work on the dark side of technology use by adding another component to the literature on cybercrime, i.e., focusing on the context of shoplifting using technology.

References


<table>
<thead>
<tr>
<th></th>
<th>$n$</th>
<th>%</th>
<th></th>
<th>$n$</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Gender</strong></td>
<td></td>
<td></td>
<td><strong>Geography</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Men</td>
<td>240</td>
<td>50.8</td>
<td>Rural</td>
<td>189</td>
<td>40</td>
</tr>
<tr>
<td>Women</td>
<td>232</td>
<td>49.2</td>
<td>Urban</td>
<td>283</td>
<td>60</td>
</tr>
<tr>
<td><strong>Age</strong></td>
<td></td>
<td></td>
<td><strong>Employment</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Under 25</td>
<td>50</td>
<td>10.6</td>
<td>Full-time</td>
<td>309</td>
<td>65.5</td>
</tr>
<tr>
<td>25–29</td>
<td>90</td>
<td>19.1</td>
<td>Part-time</td>
<td>74</td>
<td>15.7</td>
</tr>
<tr>
<td>30–39</td>
<td>175</td>
<td>37.1</td>
<td>Retired</td>
<td>18</td>
<td>3.8</td>
</tr>
<tr>
<td>40–49</td>
<td>87</td>
<td>18.4</td>
<td>Unemployed</td>
<td>71</td>
<td>15</td>
</tr>
<tr>
<td>50–59</td>
<td>41</td>
<td>8.7</td>
<td>Annual household income</td>
<td></td>
<td></td>
</tr>
<tr>
<td>60 and over</td>
<td>29</td>
<td>6.1</td>
<td>Less than $20k</td>
<td>64</td>
<td>13.6</td>
</tr>
<tr>
<td><strong>Ethnicity</strong></td>
<td></td>
<td></td>
<td>$20k–$40k</td>
<td>110</td>
<td>23.3</td>
</tr>
<tr>
<td>African-American</td>
<td>29</td>
<td>6.1</td>
<td>$40k–$60k</td>
<td>107</td>
<td>22.7</td>
</tr>
<tr>
<td>Asian/Pacific Islander</td>
<td>35</td>
<td>7.4</td>
<td>$60k–$80k</td>
<td>91</td>
<td>19.3</td>
</tr>
<tr>
<td>Caucasian</td>
<td>366</td>
<td>77.5</td>
<td>$80k–$100k</td>
<td>42</td>
<td>8.9</td>
</tr>
<tr>
<td>Hispanic/Latino</td>
<td>30</td>
<td>6.4</td>
<td>More than $100k</td>
<td>58</td>
<td>12.3</td>
</tr>
<tr>
<td>Native American</td>
<td>5</td>
<td>1.1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Others</td>
<td>7</td>
<td>1.5</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Education</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>College or school dropout</td>
<td>50</td>
<td>10.6</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Undergraduates</td>
<td>258</td>
<td>54.7</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Graduates</td>
<td>125</td>
<td>26.5</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Others</td>
<td>39</td>
<td>8.3</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Table AI.**
Demographic statistics of the respondents

**Note:** Sample $n = 472$
## Appendix 2

<table>
<thead>
<tr>
<th>Constructs (measurement source)</th>
<th>Items</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Items measured on seven-point Likert-type scale</strong></td>
<td><strong>Intention to shoplift in smartphone checkout settings (Ajzen, 1991)</strong>&lt;br&gt;I intend to shoplift in a store that has smartphone checkout settings&lt;br&gt;I predict I would shoplift in a store that has smartphone checkout settings&lt;br&gt;I plan to shoplift in a store that has smartphone checkout settings</td>
</tr>
<tr>
<td><strong>Intention to shoplift in store provide mobile device checkout settings (Ajzen, 1991)</strong></td>
<td>I intend to shoplift in a store that has store-provided mobile device checkout settings&lt;br&gt;I predict I would shoplift in a store that has store-provided mobile device checkout settings&lt;br&gt;I plan to shoplift in a store that has store-provided mobile device checkout settings</td>
</tr>
<tr>
<td><strong>Intention to shoplift in employee-assisted mobile checkout settings (Ajzen, 1991)</strong></td>
<td>I intend to shoplift in a store that has store employee-assisted mobile checkout settings&lt;br&gt;I predict I would shoplift in a store that has store employee-assisted mobile checkout settings&lt;br&gt;I plan to shoplift in a store that has store employee-assisted mobile checkout settings</td>
</tr>
<tr>
<td><strong>Intention to shoplift in fixed location checkout settings (Ajzen, 1991)</strong></td>
<td>I intend to shoplift in a store that does not have mobile checkout settings&lt;br&gt;I predict I would shoplift in a store that does not have mobile checkout settings&lt;br&gt;I plan to shoplift in a store that does not have mobile checkout settings</td>
</tr>
<tr>
<td><strong>Experiential beliefs (Ray, 1987)</strong></td>
<td>I will shoplift just for fun&lt;br&gt;I will shoplift for excitement&lt;br&gt;I will shoplift just to see what it's like&lt;br&gt;I will shoplift to see if I could get away with it</td>
</tr>
<tr>
<td><strong>Peer influence (Cox et al., 1990)</strong></td>
<td>Will you shoplift because friends are doing it?&lt;br&gt;Will you shoplift because friends dare you to do it?&lt;br&gt;Will you shoplift because you want to please friends?&lt;br&gt;Will you shoplift because your friend needs the item?&lt;br&gt;Will you shoplift because your friend can't legally buy the item?&lt;br&gt;Will you shoplift because your friend might be embarrassed to buy the item?&lt;br&gt;Will you shoplift because your friend is told that he/she can't have the item?&lt;br&gt;Do your friends encourage you to shoplift?</td>
</tr>
<tr>
<td><strong>Technology self-efficacy (McDonald and Siegall, 1982)</strong></td>
<td>In general, I could complete the checkout using the technology if I could call someone for help if I got stuck&lt;br&gt;In general, I could complete the checkout using the technology if someone else had helped me get started&lt;br&gt;In general, I could complete the checkout using the technology if I had lot of time to complete the checkout for which technology was provided&lt;br&gt;In general, I could complete the checkout using the technology if someone showed me how to do it first&lt;br&gt;In general, I could complete the checkout using the technology if I had used technology before this one for checkout&lt;br&gt;In general, I could complete the checkout using the technology if I had just the built-in help facility for assistance</td>
</tr>
</tbody>
</table>

*(continued)*

Table AII. Scales used
Appendix 3

<table>
<thead>
<tr>
<th>Constructs (measurement source)</th>
<th>Items</th>
</tr>
</thead>
</table>
| Opinion about shoplifting in retail stores (Ray, 1987) | People shoplift in retail stores because items are overpriced  
The shoplifted items will never be missed in retail stores |

*Items measured on a five-point scale with 0 denoting "none" and 4 denoting "extreme"*

Urge to shoplift from retail stores during past one week (Grant and Kim, 2002)

| If you had urges to steal during the past WEEK, on average, how strong were your urges?  
During the past WEEK, how many times did you experience urges to steal?  
During the past WEEK, how many hours (add up hours) were you preoccupied with your urges to steal?  
During the past WEEK, how much were you able to control your urges? Please circle the most appropriate numberα |

Table AII.  
Note: “These items were reverse coded

### Table AIII. Reliability and validity statistics of the scales

<table>
<thead>
<tr>
<th>Scale</th>
<th>Cronbach’s α</th>
<th>Average variance extracted</th>
<th>Range of the loadings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intention to shoplift in smartphone checkout settings</td>
<td>0.939</td>
<td>89.1</td>
<td>0.923–0.967</td>
</tr>
<tr>
<td>Intention to shoplift in store-provided mobile device checkout settings</td>
<td>0.957</td>
<td>92.1</td>
<td>0.948–0.975</td>
</tr>
<tr>
<td>Intention to shoplift in employee-assisted mobile checkout settings</td>
<td>0.952</td>
<td>91.2</td>
<td>0.952–0.957</td>
</tr>
<tr>
<td>Intention to shoplift in fixed location checkout settings</td>
<td>0.966</td>
<td>93.6</td>
<td>0.964–0.976</td>
</tr>
<tr>
<td>Experiential beliefs</td>
<td>0.960</td>
<td>89.2</td>
<td>0.931–0.950</td>
</tr>
<tr>
<td>Peer influence</td>
<td>0.953</td>
<td>75.5</td>
<td>0.796–0.902</td>
</tr>
<tr>
<td>Technology self-efficacy</td>
<td>0.944</td>
<td>68.3</td>
<td>0.839–0.900</td>
</tr>
</tbody>
</table>
Appendix 4

Social desirability questionnaire (Haghighat, 2007)

Please check the appropriate box below:

Q1. Would you smile at people every time you meet them? □ Yes □ No
Q2. Do you always practice what you preach to people? □ Yes □ No
Q3. If you say to people you will do something, do you always keep your promise no matter how inconvenient it might be? □ Yes □ No
Q4. Would you ever lie to people? □ Yes □ No
Q5. Would you ever laugh at a dirty joke people may make? □ Yes □ No

Corresponding author
Viswanath Venkatesh can be contacted at: vvenkatesh@vvenkatesh.us

Table AIV. Loadings and cross-loadings

<table>
<thead>
<tr>
<th>Construct</th>
<th>Items</th>
<th>IM</th>
<th>ISM</th>
<th>IEA</th>
<th>IC</th>
<th>ExB</th>
<th>PI</th>
<th>TSE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Smartphone checkout settings</td>
<td>IM1</td>
<td>0.97</td>
<td>0.14</td>
<td>0.30</td>
<td>0.21</td>
<td>0.21</td>
<td>0.15</td>
<td>0.25</td>
</tr>
<tr>
<td></td>
<td>IM2</td>
<td>0.96</td>
<td>0.22</td>
<td>0.30</td>
<td>0.21</td>
<td>0.19</td>
<td>0.16</td>
<td>0.19</td>
</tr>
<tr>
<td></td>
<td>IM3</td>
<td>0.93</td>
<td>0.15</td>
<td>0.20</td>
<td>0.24</td>
<td>0.22</td>
<td>0.17</td>
<td>0.29</td>
</tr>
<tr>
<td>Store-provided mobile device checkout settings</td>
<td>ISM1</td>
<td>0.14</td>
<td>0.98</td>
<td>0.21</td>
<td>0.15</td>
<td>0.13</td>
<td>0.19</td>
<td>0.26</td>
</tr>
<tr>
<td></td>
<td>ISM2</td>
<td>0.17</td>
<td>0.95</td>
<td>0.19</td>
<td>0.17</td>
<td>0.14</td>
<td>0.23</td>
<td>0.20</td>
</tr>
<tr>
<td></td>
<td>ISM3</td>
<td>0.15</td>
<td>0.96</td>
<td>0.22</td>
<td>0.15</td>
<td>0.19</td>
<td>0.14</td>
<td>0.27</td>
</tr>
<tr>
<td>Employee-assisted mobile checkout settings</td>
<td>IEA1</td>
<td>0.30</td>
<td>0.10</td>
<td>0.96</td>
<td>0.25</td>
<td>0.30</td>
<td>0.20</td>
<td>0.36</td>
</tr>
<tr>
<td></td>
<td>IEA2</td>
<td>0.30</td>
<td>0.07</td>
<td>0.95</td>
<td>0.28</td>
<td>0.30</td>
<td>0.15</td>
<td>0.33</td>
</tr>
<tr>
<td></td>
<td>IEA3</td>
<td>0.18</td>
<td>0.09</td>
<td>0.96</td>
<td>0.25</td>
<td>0.20</td>
<td>0.24</td>
<td>0.40</td>
</tr>
<tr>
<td>Fixed location checkout settings</td>
<td>IC1</td>
<td>0.30</td>
<td>0.09</td>
<td>0.21</td>
<td>0.98</td>
<td>0.17</td>
<td>0.09</td>
<td>0.32</td>
</tr>
<tr>
<td></td>
<td>IC2</td>
<td>0.26</td>
<td>0.04</td>
<td>0.28</td>
<td>0.96</td>
<td>0.15</td>
<td>0.17</td>
<td>0.33</td>
</tr>
<tr>
<td></td>
<td>IC3</td>
<td>0.30</td>
<td>0.08</td>
<td>0.29</td>
<td>0.96</td>
<td>0.15</td>
<td>0.14</td>
<td>0.32</td>
</tr>
<tr>
<td>Experiential beliefs</td>
<td>ExB1</td>
<td>0.28</td>
<td>0.10</td>
<td>0.18</td>
<td>0.39</td>
<td>0.95</td>
<td>0.34</td>
<td>0.29</td>
</tr>
<tr>
<td></td>
<td>ExB2</td>
<td>0.24</td>
<td>0.08</td>
<td>0.20</td>
<td>0.40</td>
<td>0.95</td>
<td>0.25</td>
<td>0.30</td>
</tr>
<tr>
<td></td>
<td>ExB3</td>
<td>0.25</td>
<td>0.19</td>
<td>0.18</td>
<td>0.42</td>
<td>0.94</td>
<td>0.23</td>
<td>0.30</td>
</tr>
<tr>
<td></td>
<td>ExB4</td>
<td>0.25</td>
<td>0.07</td>
<td>0.16</td>
<td>0.33</td>
<td>0.93</td>
<td>0.29</td>
<td>0.22</td>
</tr>
<tr>
<td>Peer influence</td>
<td>PI1</td>
<td>0.10</td>
<td>0.22</td>
<td>0.15</td>
<td>0.14</td>
<td>0.24</td>
<td>0.88</td>
<td>0.36</td>
</tr>
<tr>
<td></td>
<td>PI2</td>
<td>0.12</td>
<td>0.21</td>
<td>0.14</td>
<td>0.17</td>
<td>0.25</td>
<td>0.90</td>
<td>0.33</td>
</tr>
<tr>
<td></td>
<td>PI3</td>
<td>0.17</td>
<td>0.15</td>
<td>0.18</td>
<td>0.15</td>
<td>0.14</td>
<td>0.88</td>
<td>0.32</td>
</tr>
<tr>
<td></td>
<td>PI4</td>
<td>0.20</td>
<td>0.14</td>
<td>0.08</td>
<td>0.15</td>
<td>0.15</td>
<td>0.85</td>
<td>0.24</td>
</tr>
<tr>
<td></td>
<td>PI5</td>
<td>0.18</td>
<td>0.14</td>
<td>0.15</td>
<td>0.09</td>
<td>0.16</td>
<td>0.89</td>
<td>0.25</td>
</tr>
<tr>
<td></td>
<td>PI6</td>
<td>0.16</td>
<td>0.15</td>
<td>0.15</td>
<td>0.12</td>
<td>0.19</td>
<td>0.90</td>
<td>0.37</td>
</tr>
<tr>
<td></td>
<td>PI7</td>
<td>0.15</td>
<td>0.17</td>
<td>0.17</td>
<td>0.22</td>
<td>0.17</td>
<td>0.84</td>
<td>0.30</td>
</tr>
<tr>
<td></td>
<td>PI8</td>
<td>0.28</td>
<td>0.15</td>
<td>0.14</td>
<td>0.21</td>
<td>0.20</td>
<td>0.80</td>
<td>0.26</td>
</tr>
<tr>
<td>Technology self-efficacy</td>
<td>TSE1</td>
<td>0.19</td>
<td>0.18</td>
<td>0.27</td>
<td>0.25</td>
<td>0.23</td>
<td>0.25</td>
<td>0.86</td>
</tr>
<tr>
<td></td>
<td>TSE2</td>
<td>0.15</td>
<td>0.14</td>
<td>0.23</td>
<td>0.18</td>
<td>0.21</td>
<td>0.24</td>
<td>0.84</td>
</tr>
<tr>
<td></td>
<td>TSE3</td>
<td>0.28</td>
<td>0.26</td>
<td>0.37</td>
<td>0.29</td>
<td>0.32</td>
<td>0.36</td>
<td>0.86</td>
</tr>
<tr>
<td></td>
<td>TSE4</td>
<td>0.18</td>
<td>0.16</td>
<td>0.25</td>
<td>0.24</td>
<td>0.17</td>
<td>0.21</td>
<td>0.87</td>
</tr>
<tr>
<td></td>
<td>TSE5</td>
<td>0.23</td>
<td>0.23</td>
<td>0.38</td>
<td>0.33</td>
<td>0.28</td>
<td>0.34</td>
<td>0.90</td>
</tr>
<tr>
<td></td>
<td>TSE6</td>
<td>0.29</td>
<td>0.28</td>
<td>0.42</td>
<td>0.36</td>
<td>0.32</td>
<td>0.38</td>
<td>0.87</td>
</tr>
</tbody>
</table>

Notes: IM – smartphone checkout settings; ISM – store-provided mobile device checkout settings; IEA – employee-assisted mobile checkout settings; IC – fixed location checkout settings; ExB – experiential beliefs; PI – peer influence; TSE – technology self-efficacy

For instructions on how to order reprints of this article, please visit our website:
www.emeraldgrouppublishing.com/licensing/reprints.htm
Or contact us for further details: permissions@emeraldinsight.com
Organizational practices as antecedents of the information security management performance
An empirical investigation
Daniel Pérez-González, Sara Trigueros Preciado and Pedro Solana-Gonzalez
Department of Business Administration, University of Cantabria, Santander, Spain

Abstract
Purpose – The purpose of this paper is to expand current knowledge about the security organizational practices and analyze its effects on the information security management performance.
Design/methodology/approach – Based on the literature review, the authors propose a research model together with hypotheses. The survey questionnaires were developed to collect data, which then validated the measurement model. The authors collected 111 responses from CEOs at manufacturing small- and medium-sized enterprises (SMEs) that had already implemented security policies. The hypothesized relationships were tested using the structural equation model approach with EQS 6.1 software.
Findings – Results validate that information security knowledge sharing, information security education and information security visibility, as well as security organizational practices, have a positive effect on the information security management performance.
Research limitations/implications – The consideration of organizational aspects of information security should be taken into account by academics, practitioners and policymakers in SMEs. Besides, the work helps validate novel constructs used in recent research (information security knowledge sharing and information security visibility).
Practical implications – The authors extend previous works by analyzing how security organizational practices affect the performance of information security. The results suggest that an improved performance of information security in the industrial SMEs requires innovative practices to foster knowledge sharing among employees.
Originality/value – The literature recognizes the need to develop empirical research on information security focused on SMEs. Besides the need to identify organizational practices that improve information security, this paper empirically investigates SMEs’ organizational practices in the security of information and analyzes its effects on the performance of information security.
Keywords SMEs, Security organizational practices, Information security knowledge sharing, Information security visibility, Information security education, Performance of information security management
Paper type Research paper

1. Introduction
Digital interrelations fostered by the internet, IoT, cloud computing and other technologies, in which people and companies act as interconnected and interdependent nodes, have meant that information security has a strategic importance (Doherty and Fulford, 2005; Chen et al., 2008; Cram et al., 2017), especially in business environments, where the competitiveness of organizations depends on their ability to manage the information (Drucker, 2002; Gordon and Loeb, 2006; Preston and Karahanna, 2009; Soomro et al., 2016).

Global spending on IT security in 2017 has increased to $86.3bn at a growth rate of 8 percent, which doubles the rate of IT budgets over the last two years (Gartner, 2017). Organizations are increasingly focusing on implementing information security
products such as anti-virus, intrusion detection and prevention systems, database/contents security, total security systems and public key infrastructure (Venter and Eloff, 2003; Cavusoglu et al., 2009). Indeed, despite the prevalence of technical security measures, studies have reported that internal security incidents continue to happen and create more damage and losses than security incidents caused by outsiders (Baskerville et al., 2014).

In this sense, experts growingly argue that the main cause for information security incidents lies mainly with employees’ behavioral and organizational factors rather than technical issues per se, which implies a turn to internal problems attributed to the organizational practices and users of information systems (Siponen et al., 2014; Soomro et al., 2016; Doherty and Tajuddin, 2018; Moody et al., 2018).

The literature on information security in companies has mainly focused on technological issues, and to a lesser extent on strategies, security standards and policies. Recent research indicates the need of a more holistic approach to understand information security management (Siponen et al., 2016; Cram et al., 2017; Doherty and Tajuddin, 2018).

In this sense, the literature points out the need for works that identify the organizational factors that affect the security of information. Thus, the works that describe a great variety of factors of organizational type are incipient and with a predominant qualitative analysis. These factors are business size, sector, information security policy, information security education, training, culture, behavior and compliance with security policy, awareness, knowledge and visibility (Flores et al., 2014; Singh et al., 2014; Cram et al., 2017; Doherty and Tajuddin, 2018). The literature highlights the need to advance in the field of knowledge not only describing but also organizing the factors and analyzing in an empirical way the effect they have on the performance of information security management. It is especially necessary to do it in small- and medium-sized enterprises (SMEs) where there is a greater lack of work despite the fact that they are the most numerous business organizations in the developed economies, having an important contribution for the employment and productivity (OECD, 2009; Flores et al., 2014; Safa and Von Solms, 2016).

At present, the literature points out in different qualitative and revision studies a great variety of organizational factors, emphasizing especially their transversality, being common to all organizations regardless of size and sector, and having already been categorized through constructs in previous studies: information security education, information knowledge sharing and information security visibility (Singh et al., 2014; Soomro et al., 2016; Choi et al., 2018).

To address these issues, this paper aims to examine (empirically theorize and test) how companies can improve the performance of information security through organizational practices such as information security education, information knowledge sharing and information security visibility, in the specific context of industrial SMEs. The remainder of this paper is organized as follows. The next section presents the referential background and hypotheses. Following that, the research methods, drawing from a large sample consisting of industrial SMEs, are described. Then, the data analysis and results are presented. Finally, the paper ends with a discussion on the research findings, concluding remarks, limitations and future research guidelines.

2. Theoretical background and hypotheses

The analysis of the information security is a complex subject due to its multidisciplinary character (Flores et al., 2014; Safa and Von Solms, 2016; Hwang et al., 2017). According to Soomro et al. (2016), a more holistic approach is needed for information security management. Siponen et al. (2014) suggest that information security issues should be considered in a management perspective.
In this sense, information security is a field which has been treated in literature especially by academics and information professionals. However, it is a relatively modern concept in the focus of business management (Dhillon and Backhouse, 2001; Gordon and Loeb, 2006) and has acquired a greater impact from the generalized use of internet in business and the possibilities that the technologies based on web allow in all enterprise process.

In this line, the analysis of the literature on information security in organizations shows that the treatment of this subject has evolved from technical to management approaches. Thus, the first references that studied the information security in companies were primarily focused on describing the information security from a technological approach and seeking technical tools to improve it (Kim et al., 2005; Kwon et al., 2007).

A major advance in the study of information security, with a focus on the company, has been produced in recent years with works without forgetting the technical aspects, considering organizational variables, analyzing issues related to compliance with the standards of information security, developing models and systems of information security management, and analyzing its certification (Siponen and Willison, 2009; May and Dhillon, 2010). These studies are important because they relate information security strategy to business processes and give rise to the consideration of information security as a process, whose development must start from the strategic level to the rest of the organization (Siponen and Willison, 2009; Werlinger et al., 2009; May and Dhillon, 2010; Singh et al., 2014).

Thus, it is especially important to identify the organizational aspects that are indicated in the information management security (Table I). In this sense, the works that identify organizational factors that can affect the information security performance are recent. These works are varied in: methodology, mainly theoretical approaches and case studies; units of analysis, in general large organizations, and present a wide variety of factors deriving from the literature review itself, with the need to advance in this topic of study by organizing the factors and empirically analyzing their effects on the performance of information security management.

According to Soomro et al. (2016), the quantity of articles in the last years shows that the research trend in exploring the management role in information security is growing. This approach is under construction and within this approach the organizational role in information security is becoming increasingly important and is gaining the attention of researchers. This research is an attempt to contribute to filling the gap in the literature by focusing on the organizational practices. Specifically, the review of the literature stands out as the most cited cross-cutting for any organization and constitutes practices at the operational level, executed by all employees, which are as follows: information security knowledge sharing, information security education and information security visibility.

Information security knowledge sharing

In relation to the above, recent studies place the focus of research on the role of shared knowledge in information security. Experts face similar problems in this domain and they should provide proper solutions for them, preventing the development of the same solutions for similar problems by means of sharing knowledge. This practice leads to the avoidance of time-wasting and extra costs (Feledi et al., 2013). Sharing previous relevant experiences in the domain of information security is a valuable resource in information security awareness. (Rhee et al., 2009; Safa and Von Solms, 2016).

In this context, information security knowledge sharing not only increases the level of awareness as an effective approach, but also reduces the cost of information security in organizations. Information security knowledge sharing refers to collaboration with others by sharing our experiences, ideas and knowledge in order to safeguard information assets in organizations (Flores et al., 2014). It includes periodic meetings of knowledge sharing, mail list, wikis and specific web spaces to share knowledge.
Therefore, this discussion leads to the following hypotheses:

**H1.** The organizational practice of information security knowledge sharing is positively related to the performance of information security management.

**Information security education**

Within the traditional organizational practices to improve the security of business information, security education is within the context of the organization itself, as reflected in the main information security standards (ISO/IEC 27001, 2005; ITIL; COBIT; NIST Special Publication 800). Such standards coincide in pointing out the fundamental role that information security education has as an organizational factor that must ensure in the personnel a sufficient knowledge in security and contributes to reduce incidents, and thus has been treated in the literature (Siponen, 2000; Lee et al., 2004; D’Arcy et al., 2009). Information security education refers to a program or efforts to make employees

<table>
<thead>
<tr>
<th>References</th>
<th>Key factors/findings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Whitman (2004)</td>
<td>Information security needs higher levels of awareness, education and policy</td>
</tr>
<tr>
<td>Chang and Ho (2006)</td>
<td>Quantify the impacts of organizational culture traits on the effectiveness of implementing ISM</td>
</tr>
<tr>
<td>Hagen and Albrechtsen (2008)</td>
<td>Awareness-creating activities are applied by the organizations to a considerably lesser extent, but at the same time these are assessed as being more effective organizational measures than technical-administrative ones</td>
</tr>
<tr>
<td>Ma et al. (2009)</td>
<td>Information security training is possibly the most important measure for its effectiveness, as it increases awareness and understanding</td>
</tr>
<tr>
<td>Puhakainen and Siponen, (2010)</td>
<td>Information security policy compliance training has a positive effect on employees’ behavior regarding compliance</td>
</tr>
<tr>
<td>Albrechtsen and Hovden, (2010)</td>
<td>Employee participation and knowledge creation incorporate positive changes toward information security awareness and behavior</td>
</tr>
<tr>
<td>Flores et al. (2014)</td>
<td>Authors present an empirical investigation on what behavioral information security governance factors drive the establishment of information security knowledge sharing in organizations</td>
</tr>
<tr>
<td>Parsons et al. (2014)</td>
<td>Awareness training and education have positive impact on employee attitude and behavior toward information security policy</td>
</tr>
<tr>
<td>Singh et al. (2014)</td>
<td>The paper categorizes various organizational ISM functions into ten factors. Spanning across three levels (strategic, tactical and operational), these factors cover various management issues of organizational ISM</td>
</tr>
<tr>
<td>Safa and Von Solms (2016)</td>
<td>Information security knowledge sharing (ISKS) forms and decreases the risk of information security incidents</td>
</tr>
<tr>
<td>Soomro et al. (2016)</td>
<td>Development and execution of information security policy, awareness, compliance training, development of effective enterprise information architecture, IT infrastructure management, business and IT alignment and human resources management had a significant impact on the quality of management of information security</td>
</tr>
<tr>
<td>Hwang et al. (2017)</td>
<td>The authors found that security systems, security education and security visibility decrease instances of non-compliance</td>
</tr>
<tr>
<td>Choi et al. (2018)</td>
<td>The paper identifies a set of organizational insiders’ perceived components of effective information security practices (organizational mission statement; common understanding of information security; awareness of threats; knowledge of information security incidents, routines and policy; relationships between employees; circulation of stories; role of punishment provisions; and training), based on which more successful information security strategies can be developed</td>
</tr>
<tr>
<td>Moody et al. (2018)</td>
<td>This paper reviews 11 theories that have served the majority of previous information security behavior models. It empirically compares these theories and proposes a unified model, called the unified model of information security policy compliance (UMISPC), which integrates elements across these extant theories</td>
</tr>
</tbody>
</table>

Table I. Literature review organizational factors in information security management

<table>
<thead>
<tr>
<th>References</th>
<th>Key factors/findings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Whitman (2004)</td>
<td>Information security needs higher levels of awareness, education and policy</td>
</tr>
<tr>
<td>Chang and Ho (2006)</td>
<td>Quantify the impacts of organizational culture traits on the effectiveness of implementing ISM</td>
</tr>
<tr>
<td>Hagen and Albrechtsen (2008)</td>
<td>Awareness-creating activities are applied by the organizations to a considerably lesser extent, but at the same time these are assessed as being more effective organizational measures than technical-administrative ones</td>
</tr>
<tr>
<td>Ma et al. (2009)</td>
<td>Information security training is possibly the most important measure for its effectiveness, as it increases awareness and understanding</td>
</tr>
<tr>
<td>Puhakainen and Siponen, (2010)</td>
<td>Information security policy compliance training has a positive effect on employees’ behavior regarding compliance</td>
</tr>
<tr>
<td>Albrechtsen and Hovden, (2010)</td>
<td>Employee participation and knowledge creation incorporate positive changes toward information security awareness and behavior</td>
</tr>
<tr>
<td>Flores et al. (2014)</td>
<td>Authors present an empirical investigation on what behavioral information security governance factors drive the establishment of information security knowledge sharing in organizations</td>
</tr>
<tr>
<td>Parsons et al. (2014)</td>
<td>Awareness training and education have positive impact on employee attitude and behavior toward information security policy</td>
</tr>
<tr>
<td>Singh et al. (2014)</td>
<td>The paper categorizes various organizational ISM functions into ten factors. Spanning across three levels (strategic, tactical and operational), these factors cover various management issues of organizational ISM</td>
</tr>
<tr>
<td>Safa and Von Solms (2016)</td>
<td>Information security knowledge sharing (ISKS) forms and decreases the risk of information security incidents</td>
</tr>
<tr>
<td>Soomro et al. (2016)</td>
<td>Development and execution of information security policy, awareness, compliance training, development of effective enterprise information architecture, IT infrastructure management, business and IT alignment and human resources management had a significant impact on the quality of management of information security</td>
</tr>
<tr>
<td>Hwang et al. (2017)</td>
<td>The authors found that security systems, security education and security visibility decrease instances of non-compliance</td>
</tr>
<tr>
<td>Choi et al. (2018)</td>
<td>The paper identifies a set of organizational insiders’ perceived components of effective information security practices (organizational mission statement; common understanding of information security; awareness of threats; knowledge of information security incidents, routines and policy; relationships between employees; circulation of stories; role of punishment provisions; and training), based on which more successful information security strategies can be developed</td>
</tr>
<tr>
<td>Moody et al. (2018)</td>
<td>This paper reviews 11 theories that have served the majority of previous information security behavior models. It empirically compares these theories and proposes a unified model, called the unified model of information security policy compliance (UMISPC), which integrates elements across these extant theories</td>
</tr>
</tbody>
</table>
aware of the environment, policy and manual of an organization’s security (Hwang et al., 2017). It includes organized and coordinated way talks, tailored educational materials, specific training and knowledge evaluation. Based on this discussion, the following hypothesis is proposed:

\[ H2. \text{ Information security education efforts are positively related to the performance of Information security management.} \]

Education in security information in the enterprise environment is important. Nevertheless, successful organizational education requires more actions aimed at complementing shared knowledge and education, for example, through the visibility of the subject.

**Information security visibility**

Hwang et al. (2017) defined security visibility as the degree of organizational efforts to provide employees with a positive view of information security policies. The literature suggests that when organizations encourage the visibility of information security technologies, procedures, activities and control methods, employees are able to voluntarily form a security culture (AlHogail, 2015; Faily and Fléchais, 2010; Lacey, 2010).

Information security policies, activities, incidents and practices should be visible and continuously advertised to employees in order for them to make decisions that are consistent with the organization’s desirable direction. Such visibility has an impact on the compliance of employees who are required to adhere to information security policies (Siponen et al., 2010; Hwang et al., 2017). Among others, posters, notices, press releases and bulletin boards are also included. Thus, the following hypothesis is suggested:

\[ H3. \text{ Information security visibility in organizations is positively related to the performance of information security management.} \]

### 3. Research methodology

#### Data and sample

The organizations selected for this study are industrial SMEs from Cantabria, in the north of Spain, where economic, technological development and IT use are similar to other OECD regions and to the Europa average (OECD, 2017; European Commission, 2018). In this sense, this region has been selected because its social, economic and innovation variables are located within the average of Europe and the OECD. This situation facilitates the comparison with other regions (Fritsch and Wyrwich, 2018; Rodríguez-Pose and Wilkie, 2019).

With respect to SMEs, this kind of firms has been selected due to the relevance they have in the economy, representing more than 95 percent of companies of development economies (OECD, 2016). In contrast, there are insufficient works that analyze the organizational practices in information security and their effects on the security of information of this type of companies (Dutot et al., 2014). At the same time, international organizations’ reports suggested that the industrial sector is behind the implementation of new IT development in its information security processes, and therefore, there is some space for improvement (OECD, 2016). Besides, in developed countries, there is an urgent need for improving the competitiveness of this sector (OECD, 2016).

To ensure a minimum firm complexity, in which IT may be relevant, the population considered in this study was industrial SMEs, with ten employees or more, located in the region of Cantabria. A total of 478 SMEs were identified, for this purpose, the official database of the Cantabria Institute of Statistics (ICANE) (2016) was used. All the SMEs identified were invited by e-mail to participate in the study. A personal interview was conducted to the companies that showed interest. In total, 111 valid questionnaires were obtained, yielding a response rate of 23.2 percent. The sample characteristics are presented in Table II.
Data collection was conducted following two phases. First, a pilot study was performed, and, following that, a questionnaire was conducted. Five SMEs were randomly selected from a database to perform the pilot study. Based on these responses and the subsequent interviews with the participants in the pilot study, minor modifications were made to the questionnaire for the next phase of data collection. Responses from these five pilot study firms were not included in the final sample. The survey was administered to the CEO of the companies via personal interview and the company was the unit of analysis for this study. All answers were treated anonymously and confidentially. The technical research summary is presented in Table III.

**Measures**

Measurement items were introduced on the basis of a careful literature review. Constructs and associated indicators in the measurement model are listed in Table AI and discussed below. To facilitate future research, scales of measure tested by previous studies were used. Scales were measured on a five-point Likert scale with anchors from strongly disagree (1) to strongly agree (5). All the variables were operationalized as multi-item constructs.

The information security knowledge sharing measured the level at which an organization has established processes to capture and share knowledge about information security among organizational members through formal and informal information flows (Belsis et al., 2005; Zakaria, 2006; Flores et al., 2014). Items for this variable are based on Flores et al. (2014).

### Sample characteristics

<table>
<thead>
<tr>
<th>Intervals</th>
<th>% in total</th>
<th>% in total</th>
<th>Average value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Employees</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10–49</td>
<td>80.1</td>
<td>89</td>
<td>46</td>
</tr>
<tr>
<td>50–249</td>
<td>199</td>
<td>22</td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td>100</td>
<td>111</td>
<td></td>
</tr>
<tr>
<td><strong>Sales (€)</strong></td>
<td></td>
<td></td>
<td>€1.1m</td>
</tr>
<tr>
<td>0 ≤ 500,000</td>
<td>28</td>
<td>31</td>
<td></td>
</tr>
<tr>
<td>500,001 ≤ 1m</td>
<td>47.7</td>
<td>53</td>
<td></td>
</tr>
<tr>
<td>&gt; 1m</td>
<td>24.3</td>
<td>27</td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td>100</td>
<td>111</td>
<td></td>
</tr>
<tr>
<td><strong>Age (years)</strong></td>
<td></td>
<td></td>
<td>23</td>
</tr>
<tr>
<td>0 ≤ 9</td>
<td>7.2</td>
<td>8</td>
<td></td>
</tr>
<tr>
<td>10 ≤ 20</td>
<td>55</td>
<td>61</td>
<td></td>
</tr>
<tr>
<td>&gt; 20</td>
<td>37.8</td>
<td>42</td>
<td></td>
</tr>
<tr>
<td>Total</td>
<td>100%</td>
<td>111</td>
<td></td>
</tr>
</tbody>
</table>

Table II. Sample characteristics

---

**Information security management performance**

---

<table>
<thead>
<tr>
<th>Pilot study</th>
<th>Random sampling five SMEs from a database, February 2016</th>
</tr>
</thead>
<tbody>
<tr>
<td>Quantitative study (survey)</td>
<td>478 SMEs from the industrial with 10 employees or more</td>
</tr>
<tr>
<td>Universe</td>
<td>All the companies that formed the universe were contacted</td>
</tr>
<tr>
<td>Sampling procedure</td>
<td>Survey administrated to the CEO via personal interview</td>
</tr>
<tr>
<td>Collection of information</td>
<td>Was the company</td>
</tr>
<tr>
<td>Unit of analysis</td>
<td>111 valid questionnaires (response rate of 23.2%)</td>
</tr>
<tr>
<td>Date of field work</td>
<td>8.16%</td>
</tr>
<tr>
<td>Sampling error</td>
<td>95.5% (K = 1.96) for the most unfavorable case p = q = 0.5</td>
</tr>
<tr>
<td>Level of trust</td>
<td>February to July 2016</td>
</tr>
</tbody>
</table>

Table III. Research technical summary
Information security education assessed the extent to which companies used education activities or efforts to make employees aware of the environment, policy and manual of an organization’s security (Lee et al., 2004; Hwang et al., 2017). This variable was operationalized based on Hwang et al. (2017).

Information security visibility measured the degree of organizational efforts to provide employees with a positive view of information security policies (AlHogail, 2015; Faily and Flechais, 2010; Lacey, 2010). Security visibility scale is based on Siponen et al. (2010) and Hwang et al. (2017).

The information security performance measured the degree in which the information security program achieves its goals and the information is sufficiently protected. This includes preventing multiple cybercrime options, among other viruses, malware, hackers, Trojan, phishing or ransomware. The variable was operationalized following the items used in previous studies, such as Straub (1990), Knapp et al. (2007), Khan et al. (2011), Zhang et al. (2012) and Trigueros-Preciado et al. (2013).

Instrument validation

The measures from the data set were refined by assessing their unidimensionality and reliability. First, an initial testing of unidimensionality was made using principal component factor analyses. In each analysis, eigenvalues were greater than 1, lending preliminary support to a claim of unidimensionality in the constructs. Next, a confirmatory factor analysis was performed to assess the required convergent validity, discriminant validity and reliability of the constructs. This study uses EQS 6.1 to estimate the measurement model. The measurement model presented a good fit to the data ($\chi^2(21) = 32.479$, $p = 0.152$; CFI = 0.96; IFI = 0.96; GFI = 0.95; RMSEA = 0.06). All traditionally reported fit indexes were within the acceptable range. This study calculated reliability of measures, using Bagozzi and Yi’s (1998) composite reliability index, and Fornell and Larcker’s (1981) average variance extracted index.

For all the measures, both indexes were higher than the evaluation criteria, namely, 0.7 for composite reliability and 0.5 for the average variance extracted. With regard to convergent, all estimated standard loadings are significant ($p < 0.01$) and of acceptable magnitude (see Table IV), suggesting good convergent validity. Furthermore, Cronbach’s $\alpha$ values of all indicators exceed the recommended value of 0.6 (Hair et al., 1999).

<table>
<thead>
<tr>
<th>Construct</th>
<th>Indicator</th>
<th>S. loadings</th>
<th>t-value</th>
<th>Cronbach’s $\alpha$</th>
<th>Reliability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information security knowledge sharing</td>
<td>ISKS1</td>
<td>0.92</td>
<td>–</td>
<td>0.87</td>
<td>CR = 0.89</td>
</tr>
<tr>
<td></td>
<td>ISKS2</td>
<td>0.88</td>
<td>16.32</td>
<td></td>
<td>AVE = 0.72</td>
</tr>
<tr>
<td></td>
<td>ISKS3</td>
<td>0.74</td>
<td>9.18</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security education</td>
<td>SE1</td>
<td>0.84</td>
<td>–</td>
<td>0.84</td>
<td>CR = 0.85</td>
</tr>
<tr>
<td></td>
<td>SE2</td>
<td>0.68</td>
<td>8.42</td>
<td></td>
<td>AVE = 0.65</td>
</tr>
<tr>
<td></td>
<td>SE3</td>
<td>0.88</td>
<td>10.73</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security visibility</td>
<td>SV1</td>
<td>0.65</td>
<td>–</td>
<td>0.81</td>
<td>CR = 0.81</td>
</tr>
<tr>
<td></td>
<td>SV2</td>
<td>0.89</td>
<td>6.49</td>
<td></td>
<td>AVE = 0.60</td>
</tr>
<tr>
<td></td>
<td>SV3</td>
<td>0.82</td>
<td>6.46</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information security effectiveness</td>
<td>ISE1</td>
<td>0.86</td>
<td>–</td>
<td>0.90</td>
<td>CR = 0.90</td>
</tr>
<tr>
<td></td>
<td>ISE2</td>
<td>0.77</td>
<td>14.08</td>
<td></td>
<td>AVE = 0.58</td>
</tr>
<tr>
<td></td>
<td>ISE3</td>
<td>0.73</td>
<td>9.64</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>ISE4</td>
<td>0.64</td>
<td>6.77</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table IV. Measurement model: confirmatory analysis, scale reliability and convergent validity

Notes: CR, composite reliability; AVE, average variance extracted. Fit statistics for measurement model: $\chi^2(21) = 32.479$, $p = 0.152$; CFI = 0.96; IFI = 0.96; GFI = 0.95; RMSEA = 0.06. (-): Fixed items
To assess the discriminant validity, Fornell and Larcker’s (1981) criterion was used. This criterion involves that the square root of average variance extracted for each construct (diagonal elements of the correlation matrix in Table V) should be greater than the absolute value of inter-construct correlations (off-diagonal elements). All constructs met this criterion, suggesting that the items share more variance with their respective constructs than with other constructs. Table V also provides an overview of the average, standard deviations and correlations of the constructs.

4. Results
This paper estimated the structural model (SEM) with the EQS 6.1 software package using maximum likelihood estimation techniques to test the model (SEM–ML). The fit of the model is satisfactory ($\chi^2(17) = 29.982$, $p = 0.183$; RMSEA = 0.053; CFI = 0.99; IFI = 0.99; GFI = 0.98), suggesting that the nomological network of relations fits the data and the validity of the measurement scales. Figure 1 shows the standardized path coefficients with their respective significant levels (Table VI).

$H1$ was supported (0.33, $p < 0.01$), indicating that information security knowledge sharing is related to the information security performance in SMEs. This is the strongest factor in the proposed model. This indicates that the information security knowledge sharing is a critical factor to the performance of information security in industrial SMEs.

$H2$ was supported (0.19, $p < 0.05$), indicating that security education is related to the performance of information security in SMEs, although it is the weakest relation of the model.

$H3$ was supported (0.29, $p < 0.01$). This result shows that security visibility in the firm is an important factor for the performance of information security in SMEs.

Implications of these results are discussed in the next section.

**Table V.** Descriptive statistics and discriminant validity

<table>
<thead>
<tr>
<th>Construct</th>
<th>Av.</th>
<th>SD</th>
<th>(1)</th>
<th>(2)</th>
<th>(3)</th>
<th>(4)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Information security knowledge sharing</td>
<td>2.85</td>
<td>1.11</td>
<td>0.81</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Security education</td>
<td>3.05</td>
<td>1.39</td>
<td>0.58</td>
<td>0.84</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Security visibility</td>
<td>2.61</td>
<td>1.62</td>
<td>0.47</td>
<td>0.70</td>
<td>0.77</td>
<td></td>
</tr>
<tr>
<td>4. Information security effectiveness</td>
<td>2.42</td>
<td>1.47</td>
<td>0.33</td>
<td>0.56</td>
<td>0.71</td>
<td>0.72</td>
</tr>
</tbody>
</table>

Notes: Av., average score of all items includes in the construct. Diagonal values in italic represent the square root of the AVE.

**Figure 1.** Empirical results
5. Discussion
This paper investigates the effects of information security organizational practices (information security knowledge sharing, information security education and information security visibility) on the performance of information security management in industrial SMEs.

The first finding shows that the security education is weakly related to the extent of performance of information security. A possible explanation to this can be the set of companies, SMEs and the sector of the sample, industrial. In Spain, the majority of this type of company subcontracts training in information security, which can be seen by employees as a non-important and complementary task. In any case, the results are consistent with previous research such as Siponen et al. (2010) and Hwang et al. (2017).

Regarding the information security knowledge sharing, results suggested that it is positively associated with the performance of information security of SMEs. This finding supports recent research such as Flores et al. (2014) and Tatu et al. (2018) which found that information security knowledge sharing is adequate tool to improve information security in organizations.

With regard to the information security visibility, its effect on the performance of information security management of SMEs is analyzed. The results show a positive relation between these two constructs. This finding confirms novel previous research (Hwang et al., 2017). Thus, performance of information security in industrial SMEs emerges from information security knowledge sharing and information security visibility, rather than from education.

6. Conclusions, limitations and future research
The competitiveness of SMEs depends on their ability to secure management of their main asset, information, and, because of this, they need to have adequate security organizational practices beyond just technological resources.

Thus, this study extends the analysis of information security in SMEs beyond traditional theories and examines concrete organizational practices such as information security knowledge sharing, information education and information security visibility, by analyzing the effects of these three organizational practices on the performance of information security in industrial SMEs.

This paper provides several implications to the academics. First, this paper extends the theoretical development and empirical evidence on information security initiatives at firm level by focusing on knowledge sharing, education and visibility. Prior information security research has focused more on the technological dimension of IT security practices. This paper focuses on the organizational dimension of information security practices.

Second, this paper focuses on SMEs. Previous studies in the literature tend to focus in large businesses, with very few and recent studies analyzing concrete organizational security practices use in SMEs. In addition, this work goes beyond the usual case studies as it is based on a large sample of SMEs.

Third, we extend previous works by analyzing how security organizational practices affect the performance of information security. Our results suggest that an improved performance of information security in the industrial SMEs requires innovative practices to foster knowledge sharing among employees. Besides, in line with previous works, the positive relation between the information security visibility and the performance of

<table>
<thead>
<tr>
<th>Hypothesis</th>
<th>Path coefficient</th>
<th>p-value</th>
<th>Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>H1</td>
<td>0.33</td>
<td>&lt; 0.01</td>
<td>Support</td>
</tr>
<tr>
<td>H2</td>
<td>0.19</td>
<td>&lt; 0.05</td>
<td>Support</td>
</tr>
<tr>
<td>H3</td>
<td>0.29</td>
<td>&lt; 0.01</td>
<td>Support</td>
</tr>
</tbody>
</table>

Table VI. Summary of hypotheses test
information security management is showed. This finding contributes to the security management field by offering an explanation of the performance of information security within a particular sector. Moreover, the findings significantly contribute to the literature by considering organizational aspects of information security that should be taken into account by both academic and practitioners.

Fourth, in the line of previous works (e.g. Benitez et al., 2018), this paper contributes to IS literature on IT business value by theorizing and demonstrating how investment in organizational information security practices improves its performance, which, in turn, helps companies to create business value from IT.

With respect to the practical implications for the industry: this work relates information security to organizational variables that are comprehensible for managers and can serve as an example to show how information security can be more than technology and how the security of information is associated with organizational practices that positively affect the information security and value generation. The work specifically shows that an appropriate improvement of the personnel knowledge sharing is needed to improve the information security in the industrial SMEs. Making them aware of the importance of information security and its relation with the business processes is also needed, since these factors brake the development of information security in the companies.

With respect to the practical implications for the policymakers: government programs and grants to help companies improve information security focus on supporting companies in the purchase of hardware and software technology solutions, without paying attention to organizational issues. However, this work highlights the importance of the organizational factors regarding information security performance, which should be taken into account when designing plans and information security aids. In particular, the work shows that directing aids and designing plans that improve shared knowledge on information security and the issues that give visibility to the subject of information security will allow companies to improve their information security performance.

To conclude, while the contributions of the present study are significant, we would acknowledge that this study has some limitations, which could be addressed in future research. First, the sample used was from Spain. This means that the findings could be extrapolated to other countries, since economic and technological development in Spain is similar to other OECD member countries. However, in future research, a sampling frame that combines firms from different countries could be used in order to provide a more international perspective on the subject. Second, the sample consisted of SMEs. As SMEs are characterized by having less technological resources than their higher-level counterparts (large firms), this may influence the extent of sophistication in the security practices use. Therefore, in future works, the segment of large companies is worth special analysis. Third, the key informant method was used for data collection. This method, while having its advantages, also suffers from the limitation that the data reflect the opinions of one person. Future studies could consider research designs that allow data collection from multiple respondents within an organization. Fourth, it takes a static, cross-sectional picture. A longitudinal study could enrich the findings. Related to the foregoing, as future research lines, it would be interesting to replicate this work in other sectors, like service companies. These suggestions should be taken into account in future studies to increase the validity of our findings.

References


Further reading


Appendix

| Information security knowledge sharing | ISKS1 | In our company, employees frequently share their experiences about information security |
| Security education | SE1 | Our organization provides employees with appropriate security education before giving them authorized access to the corporate network |
| Security visibility | SV1 | In our organization, information security activities are advertised widely |
| Information security effectiveness | ISE1 | The information security program achieves most of its goals |

Note: 1–5: five-point Likert-type scales

Table AI. Measures

Corresponding author
Daniel Pérez-González can be contacted at: daniel.perez@unican.es

For instructions on how to order reprints of this article, please visit our website: www.emeraldgrouppublishing.com/licensing/reprints.htm
Or contact us for further details: permissions@emeraldinsight.com
Online social network security awareness: mass interpersonal persuasion using a Facebook app

Ehinome Ikhalia, Alan Serrano, David Bell and Panos Louvieris
Department of Computer Science, Brunel University London, Uxbridge, UK

Abstract

Purpose – Online social network (OSN) users have a high propensity to malware threats due to the trust and persuasive factors that underpin OSN models. The escalation of social engineering malware encourages a growing demand for end-user security awareness measures. The purpose of this paper is to take the theoretical cybersecurity awareness model TTAT-MIP and test its feasibility via a Facebook app, namely social network criminal (SNC).

Design/methodology/approach – The research employs a mixed-methods approach to evaluate the SNC app. A system usability scale measures the usability of SNC. Paired samples t-tests were administered to 40 participants to measure security awareness – before and after the intervention. Finally, 20 semi-structured interviews were deployed to obtain qualitative data about the usefulness of the App itself.

Findings – Results validate the effectiveness of OSN apps utilising a TTAT-MIP model – specifically the mass interpersonal persuasion (MIP) attributes. Using TTAT-MIP as a guidance, practitioners can develop security awareness systems that better leverage the intra-relationship model of OSNs.

Research limitations/implications – The primary limitation of this study is the experimental settings. Although the results testing the TTAT-MIP Facebook app are promising, these were set under experimental conditions.

Practical implications – SNC enable persuasive security behaviour amongst employees and avoid potential malware threats. SNC support consistent security awareness practices by the regular identification of new threats which may inspire the creation of new security awareness videos.

Originality/value – Many security systems are cumbersome, inconsistent and non-specific. The outcome of this research provides organisations and security practitioners with a framework for designing and developing proactive and tailored security awareness systems.

Keywords Malware, Online social networks, Social engineering, Mass interpersonal persuasion, SUS, Threat avoidance theory

Paper type Research paper

1. Introduction

Although social engineering may have different meanings, in the context of cybersecurity and therefore in the context of this paper, social engineering is defined as a malicious user’s cunning manipulation of the human propensity to be trustful, helpful, lazy and fearful (Gupta et al., 2017; Luo et al., 2011; Rößling and Müller, 2009). The key objective of the malicious user also known as “an attacker” is to illegally obtain information that allows unauthorised access to one or more systems.

Social engineering is an approach increasingly adopted by attackers as it is often easier to gain illegal access to systems when compared to technology-enabled strategies. For example, it is easier and cheaper to mislead a staff member of an organisation into giving away their password than carrying out a brute-force attack to acquire it (Gupta et al., 2017). Social engineering usually starts with collecting contextual information on potential targets. This activity is typically obtained using a “dumpster diving” technique: gathering information through company phone books, memos, company policy manuals, organisational charts and phone calls. The advent of online social networks (OSNs), however, has introduced new opportunities for attackers to execute their illegal/malicious actions (Ferreira et al., 2015). Attackers are now exploiting OSNs...
such as Facebook to collect preliminary background information on potential victims and to explore both human and technology-based social engineering. Such exploitation is for the purpose of deploying malicious software (commonly referred as malware) designed to steal sensitive data from the systems of unsuspecting OSN users (Nelms et al., 2016). The characteristics of OSNs combined with users’ behaviour make them a particular target of social engineering attacks (Difley and Kearns, 2011; Faghani and Saidi, 2009; Hanna et al., 2011; Lin and Lu, 2011; Yan et al., 2007).

Fogg (2008) offered insights as to why online social platforms lead to the evolution and change in user behaviour at scale. Fogg (2008) defined this phenomenon as Mass Interpersonal Persuasion (MIP). MIP suggests that OSN users tend to get involved in trends that then engage their “friends” and “friends” of “friends”. It is a unique success determinant of OSNs and it is the biggest factor that influences users of OSNs to perform certain behaviours at such a scale. MIP includes six components: persuasive experience, automated structure, social distribution, rapid cycle, huge social graph and measured impact.

It is clear that the characteristics of OSNs support the psychological aspects of social engineering. For example, social engineering thrives on trust-based relationships and the forgery of relationships between an attacker and potential victims to manipulate them to perform illegal actions (Yang et al., 2016). Similarly, OSNs grows on relationships built between users, and frequently this characteristic has been abused for malicious intentions. An attacker can clone the profile of a legitimate OSN user’s connection and then attempt to forge a relationship with the potential target and gradually build trust. Such trust-based relationships can be used to persuade a potential victim into downloading malware on their computing devices. The Zeus virus is an example of such attacks. Kaspersky (2015) reported a Trojan horse malware – Zeus, initially discovered in 2007, had re-emerged and attacked Facebook users in 2014. The Zeus malware was able to capture bank accounts and steal private information such as social security numbers using fake Facebook “fan pages” and compromised OSN accounts (Riccardi et al., 2013).

The escalation of social engineering malware threats has increased the growing demand for end-user security awareness covering associated risks and effective mitigation measures (Parsons et al., 2014). There is a research that argues that security awareness systems are efficient measures to mitigate social engineering malware attacks (Aloul, 2012; Arachchilage and Love, 2014; Oluwasegun and Ihnin, 2013; Thomson and Solms, 1998). Despite this, there are indications that OSN are still vulnerable to social engineering attacks. The authors of this paper argue that most existing systems do not consider the nature and characteristics of the technology platform through which malware attacks occur. OSN platforms present multi-vectors for sophisticated malware attacks which make user detection and avoidance a herculean task.

In this paper, we introduce a web-based Facebook animated video application, “Social network criminal” (SNC) that has been designed and developed based on a theoretical model previously proposed and statistically tested, namely TTAT-MIP (Ikhalia and Serrano, 2016). The motivation for developing SNC is to practically validate the TTAT-MIP model and to create security awareness that improves the threat avoidance behaviour of OSN users. The rest of the paper is structured as follows. The theoretical model from which this application is based is presented in Section 2. Section 3 describes the working functionality of SNC, linking it with the theoretical model. Section 4 describes the methodology adopted to validate the Facebook application, whilst Section 5 presents the data collection, analysis and results of the studies undertaken. Section 6 presents the overall discussion and Section 7 concludes the paper with areas for further research.

2. Rationale: the theoretical model TTAT-MIP
The Facebook application used in this paper has been designed and developed based on an extended version of the technology threat avoidance theory (TTAT) using MIP approach,
namely TTAT-MIP (see Figure 1). For the TTAT-MIP model, a survey questionnaire was used to modify the TTAT adding MIP. We analysed 285 samples by structural equation modelling (SEM) approach, particularly covariance-based SEM.

This paper aims to practically operationalise the TTAT-MIP model using a Facebook app (a.k.a. SNC). The intention is to add knowledge to the quantitative evaluation presented in Ikhalia and Serrano (2016) by using qualitative methods during the validation of the Facebook app. In order to understand the rationale of the model, a brief description is presented in the following paragraph. Detailed information about the creation of this model together with its quantitative validation can be found in Ikhalia and Serrano (2016) and Ikhalia (2017).

The malware threat avoidance behaviour of OSN users is determined by their motivation to avoid the threat (avoidance motivation) which is affected by perceived threat. Perceived threat can be defined as "the degree to which a user views that a malware threat can be dangerous". Threat perception is developed by perceived susceptibility and perceived severity. Perceived susceptibility is defined as the subjective belief that a user will be negatively affected by malware threat. Meanwhile, perceived severity is the degree to which a user perceives that the negative consequences of a threat will be severe:

**H1a.** Perceived susceptibility of being attacked by malware through OSNs positively affects perceived threat.

**H1b.** Perceived severity of being attacked by malware through OSNs positively affects perceived threat.

Avoidance motivation is defined as the degree to which computer users are motivated to avoid malware threats using safeguarding measures:

**H2.** Perceived threat of malware attacks through OSNs positively affects avoidance motivation.

![Figure 1. The TTAT-MIP model](image_url)
The effectiveness of a safeguard is defined as the subjective assessment of a safeguarding measure on how effective it can be applied to avoid the malware threat:


Safeguard effectiveness negatively moderates the relationship between perceived threat and avoidance motivation:

H3a. Perceived threat and safeguard effectiveness have a positive interaction effect on avoidance motivation.

Safeguard cost is defined as the physical and cognitive efforts – such as money, time, comprehension and inconvenience needed to make use of a safeguard measure:

H4. Safeguard cost negatively affects avoidance motivation.

Self-efficacy is defined as the confidence in applying a safeguarding measure to avoid a malware threat:

H5. Self-efficacy positively affects avoidance motivation.

To empirically measure MIP, we intend to focus on the success determinants of MIP which are: persuasive experience, social distribution and a large social graph:

H6. MIP positively affects avoidance motivation.

Furthermore, we argue that MIP positively moderates the relationship between safeguard effectiveness and avoidance motivation:

H6a. MIP and safeguard effectiveness have a positive interaction effect on avoidance motivation.

Finally, avoidance motivation has a positive effect on the threat avoidance behaviour of OSN users:

H7. Avoidance motivation has a positive effect on avoidance behaviour of using the safeguard.

Findings suggest that OSN users develop a threat perception when they perceive the negative consequences of a malware attack would be severe. To motivate OSN users to avoid malware, they need to be convinced that the threats exist and are avoidable. Furthermore, when tackled with a threat, users are motivated to avoid the threat if they perceive the effectiveness of the safeguarding measure (safeguard effectiveness), the convenience of using it (safeguard cost), their self-confidence in using it (self-efficacy) and the MIP of the safeguard (Liang and Xue, 2010; Ikhalia and Serrano, 2016). Results show that when social network users decide to use a safeguarding measure to avoid a malware threat, they are positively influenced by the mass interpersonal persuasion of the safeguarding measure (MIP). These findings suggest that to help OSN users to be aware of the threats posed by social networks environments and avoid them; interested parties should include techniques of persuasion from users’ interpersonal connections. The following section describes in detail how the TTAT-MIP model is operationalised through the Facebook app.

3. Working functionality of social network criminal

SNC uses real-life cases of social network malware attacks to teach users how to detect and avoid social network threats. These cases are dramatically scripted and deployed through short video animation clips. The choice of using video animation for presenting information was based on evidence from the literature which shows the broad adoption of videos as a significant factor for influencing user engagement on OSN settings (Cheng et al., 2008;
Dunlop et al., 2016; Kaplan and Haenlein, 2010). In addition, videos receive less criticism by users, thus, allowing them to focus on the message being delivered (Rosenkrans, 2009; Soika et al., 2010). Next, there is a description of the main functionality of the app (Figure 2).

After the app has been installed, access is possible via a web link or by searching Facebook (you can access a view of the app here www.socialnetworkcriminal.com/). A main page then presents the user with a number of options (see Figure 3). Functionality is available to enable connection to friends (via invites and competition) as well a video viewing with subsequent quiz questions.

3.1 Play video
This feature allows users to observe scripted animation videos based on previous cases of social network malware attacks and the different measures needed to avoid such attacks.
We inform the user about the “threat” and its severity (perceive thread in the TTAT-MIP model in Figure 1) as well as the safeguard measures to avoid them. Figure 4 is a screenshot of an example of a video in SNC.

3.2 Quiz
This feature is also used to increase the level of the perceived threat, as depicted in the TTAT-MIP model. After a user completes a video, a pop-up quiz with a 60 s countdown timer is automatically displayed to the user to test their information retention. There are three questions on the pop-up which are strictly related to the video content. The quiz was designed to make it impossible for users to provide accurate answers without sufficient engagement. A correct answer to a question gives the user “5 points”. When a user gets through the quiz feature, the points gained by the user are automatically computed towards their security ranks. For example, with “200 points” a user becomes a “1-star security general” on SNC. Figure 5 is an example of such quizzes.

3.3 My security team
This feature allows users to send invitations to be part of their security team to their Facebook friends. This feature enhances the persuasiveness of SNC by allowing teammates to observe their security rankings and possibly stir up competition amongst teammates. As TTAT-MIP suggests, OSN users are motivated to avoid malware threats when persuaded by their friends, in this case the persuasion is made through competitiveness. By allowing
them to build a network of security teammates, SNC exemplifies the MIP construct within TTAP-MIP. Figure 6 shows an example of how users can motivate their networks.

3.4 Invite friends
Similar to other Facebook applications, this marketing feature allows SNC users to notify their friends of the existence of the app. Users can inform their friends multiple times at
various intervals. Based on TTAT-MIP, users are more likely to use SNC when persuaded by their friends. As such, the “Invite Friend” feature allows interpersonal persuasion to occur and consequently a change in threat avoidance behaviour. An example of how friends can be invited to participate on SCN is shown in Figure 7.

3.5 Earn points
This feature allows users to earn extra points when they click on a link within the APP that leads to a blog article or news report about malware threats. Through this feature, enthusiastic users that are keen on going further in learning about malware threats can easily do so. The concept of “Earning Points” is a psychological persuasion factor that motivates users for their knowledge about the existence of a threat. It relates strongly with the MIP construct of TTAT-MIP, as it allows security teammates on SNC to observe the progress of their security awareness which tends to persuade members with low-security points to learn more and attain higher points. Figure 8 shows how this can be undertaken.

4. Evaluation methodology
The research employs mixed methods (quantitative and qualitative) to evaluate the SNC app: surveys, lab experiments and semi-structured interviews. The methods were used as follows:

- Systems Usability Scale (SUC) to measure the usability of SNC (usefulness and user satisfaction);
- paired samples *t*-test administered to 40 participants to measure the improvement of their security awareness, before and after intervention; and
- semi-structured interviews to 20 participants to obtain qualitative data about the usefulness of the app.
4.1 System usability scale (SUS)

The first method measures the usability of SNC (usefulness and user satisfaction) and was carried out using an SUS survey questionnaire. SUS has been empirically validated by Bangor et al. (2008) as a useful technique within the usability community for efficiently and quickly collecting user’s subjective assessment of a system’s usability. A closed questionnaire design was used to assist participants in understanding the questions clearly through alternatives provided and also to provide a basis for comparison. Likert scales of 1–5 were used in this study as they are known to be effective (Gliem and Gliem, 2003). Each value of the scale...
denotes a score for the items of each respondent. “5” denotes a score for “strongly agree” and “1” for “strongly disagree”. “3” was used to denote a “neutral” or “undecided” score. Coolican (2004) stated that Likert scales provide higher degrees of reliability and validity while ensuring that participants provide accurate answers due to its highly structured measures. The results of SUS are provided in Section 5.1. Details about SUS questionnaire design are presented in Appendix 1.

4.2 Paired samples t-test
Previous studies have reported on the security behaviour of individuals using laboratory experiments. Egelman et al. (2008) carried out a laboratory experiment that required participants to purchase products from eBay and then they were sent fake malicious “eBay” e-mails. Dhamija et al. (2006) embarked on a laboratory experiment with 22 participants to investigate the reasons why people are vulnerable to phishing attacks.

In the laboratory experiment phase of SNC, the participants were required to undertake an online test to access their risk assessment abilities concerning malware threats on OSNs. Subsequently, they were allowed to engage with SNC by using its security awareness tools (videos animation clips). The participants were required to complete a second online test and their scores were statistically analysed and compared with the initial scores using a paired samples t-test technique.

4.3 Semi-structured interviews
A hybrid thematic analysis approach (inductive and deductive) was used to extrapolate insights from the data gathered from semi-structured interviews – allowing participants to provide verbal feedback about their opinion on receiving security awareness through SNC (Turner, 2010). Semi-structured interviews are widely employed for conducting qualitative research. Semi-structured interviews are particularly suited to this task as they allow the researcher/interviewer to ask follow-up questions in order to gain further information or clarity about a topic of interest. For example, during the interviews in the second study, users were asked to briefly describe their opinion about SNC. Some participants used phrases such as “I found it persuasive or interesting”. Consequently, the interviewer probed them on what they meant by “persuasive” or “interesting”. Hove and Anda (2005) argued that investigations related to issues in software development are usually qualitative and relevant measures are gathered through semi-structured interviews. They argued that semi-structured interviews involve high costs and quality which are often relative to how the interviews are conducted.

4.4 Participants
The study was carried out with 40 participants from a random sample of students in a top UK University. In total, 40 participants voluntarily took part in the paired samples t-test experiments and usability studies, respectively, while 20 of them agreed to provide verbal feedback on their experience with SNC. They were invited to a computer laboratory at the University. Most of the participants were aged from 18 to 25, with a gender split of 67.5 per cent male and 32.5 per cent female. They spent an average of 8 h daily on OSNs (SD: 3.163) and an average of seven years online social networking experience (SD: 1.754). A summary of the study demographics is presented in Table I.

4.5 Study procedure
Each participant was briefed on the nature of the experiment, its phases and signed a consent form required by the ethics committee of the University. The researcher informed
them that the purpose of the experiment was to test their awareness about malware threats on OSNs through a Facebook video animation app – SNC.

The pre- and post-tests were carried out using a Microsoft Windows desktop computer and participants were presented with ten scenarios of OSN malware threats (uploaded on surveymonkey.com). The OSN scenarios were designed based on previously reported incidents of OSN malware attacks (Faghani and Saidi, 2009; Gao et al., 2010, 2011). The participants gave their assessment of ten scenarios each before and after they used SNC. On the pre-test phase, legitimate OSN scenarios were randomly included with five malicious scenarios to avoid selection bias. After completing the assessment of the scenarios on the pre-test phase, they were given 15 min to use SNC and engage with the videos. After that, they were asked to complete a survey containing the SUS items designed to measure their subjective satisfaction of SNC. A post-test followed the SUS assessment and the participants were shown ten more OSN activity scenarios to evaluate. The pre- and post-tests scores of each participant were recorded to observe whether or not their OSN security behaviour improved. Finally, the participants gave verbal feedback when asked to express their opinion about receiving security awareness through SNC.

5. Results

5.1 System usability scale results

SPSS software package (IBM SPSS Statistics 20) was used for the data analysis of the SUS. The Cronbach’s $\alpha$ value to measure the internal consistency of how closely related the set of items are as a group (Gliem and Gliem, 2003) was calculated. Previous research argues that a given $\alpha$ greater than 0.70 is statistically adequate (Gliem and Gliem, 2003). The Cronbach’s $\alpha$ was found to be 0.711, which suggests adequate statistical reliability. In general, the average SUS score for the participants was significantly high scoring 82.9 out of 100 (Brooke et al., 1996). The score was obtained using the same standard procedures recommended in the literature (see Appendix 2 for more details on the SUS score from each participant and the mean and standard deviations).

SUS was created to assess a single study within a scale of 0–100 where higher scores indicate better usability (Bangor et al., 2008). Therefore, a score of 82.9 reflects a relatively high score. To complement this information, the score obtained of 82.9 can be compared to the mean SUS score of a study undertaken by Bangor et al. (2008). In this research, 2,324 surveys have been completed over the course of 206 studies resulting in a mean SUS score for all surveys of 70.14 ($s = 21.71$) with a median of 75 and a range from 0 to 100. In this context, it can be said that the SUS score of SNC (82.9) is above the median and thus it can be considered as a high score. In addition to this, the SUS score was re-affirmed as the participants mentioned that they find SNC intuitive and easy to use during the interviews (see Section 5.4 for more details).

<table>
<thead>
<tr>
<th>Measure</th>
<th>Item</th>
<th>Frequency</th>
<th>%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gender</td>
<td>Male</td>
<td>27</td>
<td>67.5</td>
</tr>
<tr>
<td></td>
<td>Female</td>
<td>13</td>
<td>32.5</td>
</tr>
<tr>
<td>Age</td>
<td>18–24</td>
<td>36</td>
<td>90</td>
</tr>
<tr>
<td></td>
<td>25–34</td>
<td>4</td>
<td>10</td>
</tr>
<tr>
<td>Social networks</td>
<td>Facebook</td>
<td>28</td>
<td>70</td>
</tr>
<tr>
<td></td>
<td>Twitter</td>
<td>9</td>
<td>22.5</td>
</tr>
<tr>
<td></td>
<td>LinkedIn</td>
<td>8</td>
<td>20</td>
</tr>
<tr>
<td></td>
<td>Instagram</td>
<td>17</td>
<td>42.5</td>
</tr>
<tr>
<td></td>
<td>SnapChat</td>
<td>13</td>
<td>32.5</td>
</tr>
</tbody>
</table>

Table I. Main study sample demographics
5.2 Paired samples t-test results: testing user’s awareness
The paired samples t-test compares the mean difference of the values to 0. It depends on the mean difference, the variability of the differences and the number of data (Rietveld and van Hout, 2017). The purpose of this study was to detect if there was a difference between the mean test scores of the participants before and after they used SNC. Using a 95% confidence interval, the procedure for conducting the paired sample t-test involves the following steps.

To calculate the sample means:
\[ \bar{d} = \frac{d_1 + d_2 + \cdots + d_n}{n} \]

To calculate the sample standard deviation:
\[ \hat{s} = \sqrt{\frac{(d_1 - \bar{d})^2 + (d_2 - \bar{d})^2 + \cdots + (d_n - \bar{d})^2}{n-1}} \]

To calculate the test statistic:
\[ t = \frac{\bar{d} - 0}{\hat{s} / \sqrt{n}} \]

where \( D \) is the differences between two paired samples; \( d_i \) the \( i \)th observation in \( D \); \( n \) the sample size; \( \bar{d} \) the sample mean of the differences; \( \hat{s} \) the sample standard deviation of the differences; \( T \) the critical value of the t-distribution with \((n-1)\) degrees of freedom; \( t \) the t-statistic (t-test statistic) for a paired sample t-test; and \( p \) the p-value (probability value) for the t-statistic (Pallant, 2016):

- **H1.** Using SNC can significantly improve the security behaviour of social network users.
- **H0.** Using SNC does not significantly improve the security behaviour of social network users.

The findings show that the participants average mean test scores were significantly improved after using SNC. This is evidenced by the p-value (\( p = 0.001 \)). The participants mean test score was significantly different before and after using SNC as evidenced by the mean and standard deviations, respectively. The mean and standard deviations before test \((M = 30.88, \text{SD} = 5.823)\) and after test \((M = 48.83, \text{SD} = 6.664)\). \( t = 15.959, \text{df} = 39, n = 40, p < 0.05, 95\% \text{ CI for mean difference of 17.950.} \)

5.2.1 The validity of the paired samples t-tests. A normality test was conducted to assess the validity of the results. For the paired samples t-test to be valid, the differences between the paired values should be approximately normally distributed. A Kolmogorov–Smirnov test was conducted to compare the study sample with a reference probability distribution (one-sample K–S test), and the results show a non-significant result (\( p = 0.200 \)). To pass the normality test a non-significant result is required (i.e. \( p > 0.05 \)), this implies that the earlier results are statistically valid and did not occur by chance (Sheng and Magnien, 2007). The diagrams in Figures 9 and 10 show the histogram of differences in marks and a reasonable probability (QQ) plot, respectively.

5.3 Semi-structured interviews
Semi-structured interviews allowed participants to express their viewpoints about the SNC app. In total, 20 participants provided verbal feedback on their perception of SNC app. The participants were asked an initial open-ended question to elicit their thoughts about SNC
Figure 9. Difference in pre- and post-scores

Figure 10. Normal probability QQ plot of the difference scores

ITP 32.5

1288
which were recorded. Subsequently, some participants were told to clarify what they meant with particular words or phrases (e.g. “what do you mean by ‘interesting’?”). The nature of open-mindedness of this approach allowed the participants to provide a reflective view of their experience with the app. According to Creswell (2012), data gathered using this qualitative approach are often burdensome to code and analyse; however, it limits researcher bias within the study.

5.3.1 Semi-structured interviews: steps for data analysis. A hybrid of inductive and deductive thematic analysis approach was employed to analyse the qualitative data (Fereday and Muir-Cochrane, 2006). The choice of using a hybrid approach is motivated by the quest to avoid research bias by allowing the opportunity to identify potential new factors that may have influenced SNC other than the factors inherent within TTAT-MIP. The following process was followed to conduct the analysis.

- Step 1 – familiarisation with the data: after transcribing the data, it was carefully read and re-read.
- Step 2 – initial code generation: features of the data were coded systematically and based on the theoretical model – TTAT-MIP.
- Step 3 – searching for themes: initial codes were collated into initial representative themes as seen in Figure 11.
- Step 4 – reviewing themes: themes were reviewed, and their interrelationships were accessed. Thereafter, strongly related themes were combined to represent a single theme as seen in Figure 12.

5.4 Semi-structured interviews results
In total, 20 participants gave verbal feedback on their viewpoints about SNC and their responses supported the results of the paired samples t-tests and the SUS study. For confidentiality, the identification of the participants is made through numbering: Participant 1, Participant 2, etc.

The participants acknowledged that SNC raised their awareness about malware threats in an engaging manner. They appraised the story-telling technique used by SNC and found it relatable and easy to understand. They mentioned that they feel persuaded to apply the knowledge gained to avoid OSN malware threats in the future. Furthermore, the results suggest SNC had an interpersonal persuasive effect on the participants. Most of the participants expressed their willingness to share the SNC experience with their OSN friends. Overall, the key findings from the thematic analysis suggest that SNC demonstrates the following seven key themes: threat awareness; relatable; persuasive; interpersonal persuasion; engaging; easy to use; and useful safeguard measures. These are discussed in more detailed next.

5.4.1 Threat awareness. All the participants acknowledged that the SNC app increased their awareness about malware threats on OSNs. Nevertheless, it was somewhat of a surprise to find out that most of the study participants were unaware of malware threats on OSNs. Such threats are commonly distributed through malware links. Supporting statements from Participant 6 are:

I don’t think many people are educated when they click on the link that it could lead to something else.

It’s scary that they can get your details “like with rose in the videos” just by clicking on a link. That’s worrying, erm, is there no software that can stop these?

Previous studies argue that malware threat awareness has not received adequate attention. Most organisations predominantly focus on refining the capabilities of their firewalls and
anti-malware software which are solely unable to circumvent malware threats (Ferreira et al., 2015; Shaw et al., 2009; Stephanou and Dagada, 2014; Workman, 2007). More often, the consequence of unawareness leads to exploitation of the biggest weakness in the cybersecurity landscape – the social engineering of humans. The videos on SNC demonstrate the proficiency to make users aware of provoking their thought processes. Supporting statements from Participant 5 are:

The videos are good; they kinda scare you into thinking, to be more aware, and I did learn the actual signs of threat.

Motivating OSN users to think about malware threats increases consciousness of every single interaction they make online. Additionally, threat awareness has a significant theoretical foundation. Ikhalia et al. (2017) argued that a key construct of TTAT-MIP which influences threat avoidance motivation is perceived threat. Perceived severity strongly affects perceived threat. The result of the semi-structured interviews validates

Figure 11. Initial thematic map, showing nine main themes
this construct because most of the participants admitted their vulnerability having identified the dangers of carelessly downloading software through malicious links on OSNs. Participant 4 comments:

Erm, basically, from what I just saw, it showed me the insights into how you can easily be manipulated, like getting a virus, cause if I saw something like what the person in the video saw, I would have downloaded it.

The findings suggest a need to stress the immense dangers of OSN malware threats may have a significant influence on the depth of users’ security awareness. In other contexts, however, this finding may not apply; for example, it is a public debate that smoking addicts simply do not quit smoking because of its associated health hazards. Other predisposing factors could influence their decision to quit smoking.

In the context of OSN malware threats, users need more than mere warnings such as “be careful of what you click”; they need to be informed on the short- and long-term negative consequences of clicking a malware link. By intensifying security awareness on the psycho-socio and economic severity of OSN malware threats, users’ threat avoidance capabilities could reach unprecedented depths.

5.4.2 Relatability. Relatability describes the quality or state of being relatable. Unpredictably, some participants acknowledged this quality after watching the videos on SNC. For example, Participant 3 commented:

It iterated things I already have an idea about.
A key noteworthy point in the above statement is “iterated”. We argue that iterating an already known concept makes it relatively easy for OSN users to retain their security awareness and consequently their security behaviour. According to Ikhalia and Serrano (2015), one of the limitations of existing security awareness systems is the lack of contextual knowledge. Contextualised awareness implies that information on threat avoidance needs to be delivered to users relative to the technology setting through which they are being exploited. In the case of SNC, we employed a story-telling technique to accomplish this task. As earlier mentioned, SNC adopted previous cases of OSN malware attacks and presented them to users in the form of animation videos. Such a technique was positively appraised by most participants as it made the security awareness information somewhat relatable to their on-going OSN experience. Supporting statements from Participant 1 are:

I think it's very useful, the real-life cases idea was very good.

The little story really helps.

From the participants’ statements, it is fairly suggestive to attribute the perceived helpfulness of the SNC app to story-telling previous real-life cases of OSN malware threats. By adopting a story-telling technique, this study avoided disseminating security awareness information in an abstract manner. The value of relatability could be drawn from its ability to stimulate the interest of OSN users. According to social marketing theory, a good strategy to get an audience interested in a product or service is by using recognisable and easily understandable media entities such as images/videos about the idea intended to be sold (Hutter et al., 2013; Lin and Lu, 2011). As a result, a pleasant setting is created for the promotion of the idea/product/service. The relatable quality of SNC is a useful tactic as everyday events (real-life cases of OSN malware threats) are used to attach emotions to the security awareness videos.

5.4.3 Persuasive. Persuasion describes the extent to which SNC influenced the participants to change their security behaviour. The study identified sub-themes such as: application of the knowledge; intention to reuse; curiosity developed; and extra cautious. All these sub-themes provide substantial evidence to support a fundamental construct within TTAT-MIP: avoidance behaviour. Further explanation of each of these sub-themes is found next.

Application of the knowledge. The findings show that the study participants are willing to apply the knowledge gained from SNC app to avoid OSN malware threats in the future. Supporting statements from Participant 2 are:

I guess I will always keep the knowledge I gained to use in the future when opening certain pages on Facebook.

Now that I have received the knowledge, I would definitely pass it down to other people and make them aware, people that are less tech savvy than me.

Intention to reuse. The majority of the participants acknowledged their intention to use SNC in gaining more awareness about OSN malware threats. For example, Participant 8 comments:

I wouldn’t mind watching another one again.

I would actually and I am not joking I would go home and use this right now.

Curiosity developed. The findings also show that the SNC app stirred the curious instincts of the participants into seeking further information about cybersecurity. Supporting statements from Participant 7 are:

It kept me wanting to listen and to find out more about cybersecurity.

Can you get hacked if you are using the app?
Extra cautious. The participants admitted that through SNC, they learnt the need to be extra careful when carrying out their online social networking activities. Supporting statements from Participant 10 are:

It taught me a lot to be extra cautious about opening certain things.

If I saw something like what the person in the video saw, I would have downloaded it. But now that I know, that if you go into a third-party website and they want you to download something, you just shouldn’t unless you actually check it out first, otherwise you will get a virus.

The sub-themes provide evidence that SNC was able to persuade the participants into making verbal declarations to reuse the app, apply the knowledge acquired, seek further knowledge within cybersecurity and become extra cautious while on OSNs. Based on the underlying theoretical model (TTAP-MIP), there is substantial evidence that OSN users’ avoidance motivation could influence their actual avoidance behaviour. In the context of this study, avoidance behaviour depicts whether OSN users would develop the intention to seek awareness using SNC and regularly update their knowledge as well. Nonetheless, the persuasive nature of SNC is found to be well-matched with the TTAT-MIP model.

5.4.4 Interpersonal persuasion. Almost every participant in this study showed a tendency to share their security awareness experience using SNC with their friends. Interpersonal persuasion defines how willing the participants are to invite their OSN friends to use SNC for security awareness. The current study expected SNC would stimulate interpersonal persuasion as the SNC theoretical model TTAT-MIP suggests. Supporting statements from Participant 12 are:

I will be happy to share this information to help my friends out and fight this cause, yeah.

I definitely will invite my friends to use this.

I might invite my friends to watch the videos, although I expected more details.

Interpersonal persuasion that occurs within an OSN with millions of interconnected users is referred as MIP (Fogg, 2008). One of the significant values that interpersonal persuasion brings to SNC is its propensity to aid the viral distribution of security awareness videos from one OSN user to his/her connections. Although the success of MIP hinges on three key components (persuasive experience, social distribution and rapid cycle), social influence theory is a fundamental persuasion theory which supports this phenomenon.

According to Venkatesh and Brown (2001), social influence states that an individual in a social network is influenced by the behaviour of members of the network to conform to community behaviour patterns. While the goal of MIP aligns with social influence theory, they both have different practical applications. MIP is a phenomenon unique to OSN environments driven by digital technology, and social influence theory is not specific to any technology context.

Interpersonal persuasion brings tremendous benefits to SNC because many OSN users are more inclined to use products/services recommended by their friends. Supporting statements from Participant 13 are:

I would trust a close friend more if they invite me to use this than a distant friend.

No matter how well a security awareness app is designed, many OSN users may not use it unless recommended by a trusted friend. This research considers interpersonal persuasion a vital attribute of SNC. Therefore, SNC has been developed with technological features to facilitate interpersonal persuasion at scale.

With hindsight, SNC has the features for users to observe the level of their friends’ security awareness; it then becomes relatively seamless for OSN users to estimate the potential
vulnerability of their friends which may stimulate a revolutionary security culture shift. In this context, Participant 15 comments:

It’s a persuasive technique, I like the “Dr and Patient form”. I would definitely tell my friends about it, they are more careless than me.

The statement above is suggestive that the persuasive technique used to make OSN users aware of malware threats could be the driving force behind their motivation to share such experience by inviting their friends. Without a persuasive experience created through story-telling of previous malware threats, it could have been somewhat unrealistic to stimulate interpersonal persuasion.

5.4.5 Engaging. The findings show that the participants perceived SNC as engaging. Engagement in this context implies how well the security awareness videos captured the attention of participants. Also, engagement in this context means that the participants learnt about OSN malware threats in a humorous manner. Supporting statements from Participant 16 are:

I thought they were very informative, but in an interesting way.

It was engaging; I was really listening and didn’t find it boring so it was good.

Erm the animation was quite funny as well so it kept me wanting to listen.

From the participants’ responses, it is evident that the manner in which security awareness was conveyed to OSN users through SNC attracted their attention substantially. In the systematic literature review conducted by Ikhalia and Serrano (2015), one of the factors identified for designing effective security awareness for OSN users is end-user engagement.

5.4.6 Ease-of-use. There is substantial evidence to support the ease-of-use of SNC. In the context of this study, ease-of-use describes the degree at which SNC can be seamlessly used. As previously mentioned, the functionalities within SNC include video play, pause, like share, comments and volume controls. In addition, it involves the feature for an automated pop-up quiz, teammate’s collation and friend invitation. Supporting statements from Participant 17 are:

I mean it sheds light on things that people need to know and it’s simplified. It doesn’t talk too much jargon.

The SNC videos were carefully scripted to avoid the use of technical jargons often associated with the typical cybersecurity setting. We ensured that considerable efforts were invested in simplifying the security awareness information to make it appealing to all classes of users regardless of their computing background. Supporting statements from Participant 18 are:

The message was put across very clearly.

I thought it was quite well like the way it was laid out.

Additionally, the participants positively appraised the short time constraints of SNC’s security awareness videos. They mentioned how straightforward the videos were organised without being boring. Supporting statements from Participant 19 are:

It was quite straightforward; I could understand what was going on.

The videos were quite short, and it has the information in two minutes or so, it’s a good amount of time and won’t bore a person and make them click next.

It was well organised, and I think that the information that was set through it would help someone that needed it.
In line with the fundamental theoretical model TTAT-MIP, ease-of-use is found to support a key independent construct – safeguard costs. Safeguard costs are the time and effort needed to use a safety measure to avoid a malware threat on OSNs.

5.4.7 Useful safeguard measures. The findings also show that the participants perceived the safeguard measures of SNC as useful. Safeguard measures describe the steps taken to avoid a malware threat. Supporting statements from Participant 20 are:

So for me I just kind of need to be aware and what I need to do in terms of steps taken to make sure I am protecting myself correctly.

But now that I know, that if you go into a third party website and they want you to download something, you just shouldn’t unless you actually check it out first.

Similarly, the construct – safeguard effectiveness included in TTAT-MIP – provides support for this finding. Arguably, OSN users are inclined to consider the perceived effectiveness of a safeguard measure before using it.

6. Discussion of the results

The results of the experimental design provide evidence supporting SNC as having a significant effect on users’ threat avoidance behaviour. The SUS score showed a significantly high usability level of 82.9 which suggests that the SNC app is not only effective at improving users’ behaviour, OSN users found the system useful as well. According to results from a thematic analysis of participant feedback, SNC was found to be persuasive, interpersonal persuasive, engaging, easy to use, relatable, informative and generally useful.

Reflecting on the TTAT-MIP factors that influence the threat avoidance motivation of OSN users, safeguard cost relates to the “ease of use” element and perceived threat relates to the informative element identified from the results of the semi-structured interview. SNC is seen to be informative due to the relatively good level of awareness it provided participants’ during the experimental validation.

Interpersonal persuasion was an essential element identified. Users mentioned how SNC enhanced their persuasion to invite their OSN connections, particularly the vulnerable ones to improve their threat avoidance skills. The interpersonal persuasive element can be linked to MIP which essentially postulates the effect of social influence on the behaviour of users connected within a social network. Overall, the findings from the interviews provided significant support for the initial empirical validation of TTAT-MIP from the SUS study and paired sample t-test, respectively. This means that the TTAT-MIP model was tested both theoretically through SEM, and practically through SCN adding further credibility to TTAT-MIP.

7. Conclusion and further work

OSNs are designed to improve social relationships amongst users. These users share different kinds of information such as lifestyles, careers, interests, activities and other significant information. Today, users of these platforms share most of their private information with the platform owners as well as third-party applications. This model of information sharing and trust poses a considerable risk to user privacy and security.

The structure of OSNs is helping malicious users to carry out their activities without the possibility of detection. Baskerville and Rowe (2012) argued that as functionality increases in IT systems, security threats facing users increase proportionately. There is a need, therefore, for a more proactive measure to undercut these threats facing users of OSNs. Such measures should involve effective security awareness for end-users pointing out all the threat-based activities to the user and their possible implications.

The research identified that the success of a system for OSN security awareness must consider factors such as: persuasion, interpersonal persuasion, relatability and ease-of-use.
Additionally, such a system should also be overtly useful and engaging while making OSN users aware of the specific threats and avoidance measures to ensure that their digital assets and identities are kept secure. From the participants' statements, it is reasonably suggestive to attribute the perceived helpfulness of SNC app to story-telling previous real-life cases of OSN malware threats. By adopting a story-telling technique, the research avoided abstractly delivering security awareness messages.

Persuasion describes the extent to which the SNC app influenced the participants to change their security behaviour. The study identified sub-themes such as: apply the knowledge, intention to reuse, curiosity developed and extra caution, all providing substantial evidence to support a fundamental construct within TTAT-MIP – avoidance behaviour.

The evaluation of the SNC in this study has potential implications for the design and implementation of security awareness for individuals and employees working in various organisations. When employees attend security awareness sessions and understand the concept, they will precisely get to know about web safety and online threats. Employee awareness can avoid potential risks which may have arisen in the past due to the lack of knowledge. The IT group can identify the current and potential security concerns. During security awareness training, the IT group can simulate malware attack incidents based on relatable events as suggested from the practical evaluation of SNC, which could compel employees to think before performing any online activity and keep them a step ahead of malware attackers.

Security awareness is not only for lower and middle management, but it is also considered for senior management staff. Constructing a security awareness programme using TTAT-MIP supports security awareness interaction and persuasive knowledge sharing between lower and senior management. This approach would improve commitment from management towards a proactive and highly persuasive security culture.

Future research may involve exploring a field experiment or applied research to investigate the impact of SNC in real-world settings without any form of control. Research efforts should be invested to study the scalability and adaptability of SNC in other social network platforms. The outcome of such research may contribute significantly to the field of behavioural science which may effectively elucidate the degree to which people avoid malware threats when influenced by their online connections.

References


Further reading

Appendix 1. SUS questionnaire items

<table>
<thead>
<tr>
<th>Item</th>
<th>Strongly Disagree</th>
<th>Strongly Agree</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. I think that I would like to use this Facebook animated video application frequently.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. I found this Facebook animated video application unnecessarily complex.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. I thought this Facebook animated video application was easy to use.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. I think that I would need assistance to be able to use this Facebook animated video application.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5. I found the various functions in this Facebook animated video application were well integrated.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6. I thought there was too much inconsistency in this Facebook animated video application.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7. I would imagine that most people would learn to use this Facebook animated video application very quickly.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8. I found this Facebook animated video application very cumbersome/awkward to use.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9. I felt very confident using this Facebook animated video application.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10. I needed to learn a lot of things before I could get going with this Facebook animated video application.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Appendix 2. Average score for each SUS question

<table>
<thead>
<tr>
<th>Question</th>
<th>Mean score</th>
<th>SD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Q1</td>
<td>3.90</td>
<td>0.852</td>
</tr>
<tr>
<td>Q2</td>
<td>4.7</td>
<td>0.470</td>
</tr>
<tr>
<td>Q3</td>
<td>4.10</td>
<td>0.641</td>
</tr>
<tr>
<td>Q4</td>
<td>4.7</td>
<td>0.470</td>
</tr>
<tr>
<td>Q5</td>
<td>3.90</td>
<td>0.718</td>
</tr>
<tr>
<td>Q6</td>
<td>4.7</td>
<td>0.470</td>
</tr>
<tr>
<td>Q7</td>
<td>3.75</td>
<td>1.164</td>
</tr>
<tr>
<td>Q8</td>
<td>3.90</td>
<td>0.718</td>
</tr>
<tr>
<td>Q9</td>
<td>4.55</td>
<td>0.605</td>
</tr>
<tr>
<td>Q10</td>
<td>4.55</td>
<td>0.686</td>
</tr>
</tbody>
</table>

Table AI. Summary of the average score for each SUS question

Corresponding author
David Bell can be contacted at: david.bell@brunel.ac.uk

For instructions on how to order reprints of this article, please visit our website: www.emeraldgrouppublishing.com/licensing/reprints.htm
Or contact us for further details: permissions@emeraldinsight.com
The effect of cybercrime on open innovation policies in technology firms

Vanessa Ratten

Department of Entrepreneurship, Innovation and Marketing,
La Trobe Business School, La Trobe University, Melbourne, Australia

Abstract

Purpose – Open innovation is important for technology firms as they can use freely available resources to source creative and innovative ideas. Despite the usefulness of open innovation for technological advancements, few studies have focused on the role of cybercrime in affecting an organization’s strategic direction. The purpose of this paper is to examine the effect of open innovation on cybercrime in technology firms.

Design/methodology/approach – Semi-structured in-depth interviews were conducted on technology firms to understand the role of open innovation in terms of technology scouting, horizontal collaboration and vertical collaboration on cybercrime activity.

Findings – The study found that there is a dilemma most technology firms face in having an open innovation strategy and how to manage cybercrime. This means that a coopetition strategy is utilized that helps to not only balance the need to have open innovation but also protect intellectual property.

Research limitations/implications – The study has implications for emerging technology innovations that not only need to have cyber security but also harness the use of Big Data.

Practical implications – Managers of technology firms need to encourage open innovation as a strategy but manage cybercrime that comes from sharing too much information in an online context.

Originality/value – This paper is one of the first to link open innovation strategy to cybercrime activity in technology firms. Thus, it contributes to the literature on open innovation and cyber theft and security.

Keywords Collaboration, Coopetition, Technology collaboration, Innovation strategy, Open innovation, Business innovation, Cybercrime, Technology scouting

Paper type Research paper

Introduction

The increased trend to share information via the internet has not only created opportunities for organizations but also increased the threat of cybercrime (Choo, 2011). Whilst organizations need to utilize innovation in order to compete in the global marketplace, they should also be cognizant of the risks associated with sharing information (Broadhead, 2018). Open innovation is a trend that has gained prominence in recent years particularly amongst technology firms due to the ability to share information with competitors (Amrollahi and Rowlands, 2017; Randhawa et al., 2016; Spender et al., 2017). In this paper, Chesbrough’s (2003, p. xxiv) definition of open innovation is adopted, which states it is “a paradigm that assumes that firms can and should use external ideas as well as internal ideas, and internal and external paths to market, as firms look to advance their technology.”

Whilst there has been an increased interest in open innovation in technology firms, the negative publicity from the use of Facebook information to understand voting behavior in the US elections has brought to life the quandrum about how to share information but at the same time be respectful of privacy issues. In addition, websites like Wikipedia have become more prevalent and these are premised on the idea of open innovation but this has resulted in some incorrect and false information being posted on their websites. Thus, whilst Wikipedia encourages the posting of information, there is a secondary issue of what happens when the information is the result of cybercrime. This has occurred with restaurants like Kentucky Fried Chicken and Subway taking to court franchisees who posted illegally information about recipes. Therefore, particularly for technology firms that
pride themselves of being innovative, a question arises of how to regulate and be mindful of information that was the result of cybercrime whilst at the same time fostering an environment for open innovation (Gillespie, 2015; Robertson et al., 2017).

Organizations need to balance opening up their resource repositories to new ideas in order to generate innovation with the need to safeguard their intellectual property because of cyber threats and security concerns (Klimburg, 2011). Cybercrime is one of the fastest growing types of crime that influences organizations technology policies (Joffee, 2010; Katos and Bednar, 2008).

Cyber security involves ensuring that information in an online context is safe and secure (Hunton, 2011). Technology organizations who share information via an open innovation strategy are concerned about the theft of intellectual property (Lazzarotti et al., 2015). This has influenced organizations strategy to include issues surrounding cybercrime such as security strategies that ensure the sharing of online information is safe (Katos and Bednar, 2008). Open innovation is important for organizations as it facilitates the sharing of knowledge, which is important for innovation. Randhawa et al. (2016) stated that the process of open innovation for organizations involves “opening up their boundaries to seamlessly collaborate and exchange knowledge with external stakeholders to leverage complementary assets and capabilities.”

Broadhead (2018, p. 1181) utilized the Europol definition of cybercrime by referring to it as “any crime that can only be committed using computers, computer networks or other forms of information communication technology.” Another definition of cybercrime by Gordon and Ford (2006, p. 4) is that includes criminal offences that occur in an online forum and include copyright infringement, content misappropriation, fraud, unauthorized access and cyberstalking. This definition is adopted in this paper as it focuses on the illegal taking of information in an online format that relates to the current trend toward open innovation in terms of making information freely available.

Early views about the role of innovation on organizational strategy viewed it as a closed process that occurred in a sequential way. This view changed with the recognition that an open approach to innovation enables the more flexible and fluid sharing of knowledge. Spender et al. (2017) suggested that the adoption of an open innovation strategy is necessary for organizations due to the need to search for new ideas. This is supported by Chesbrough and Appleyard (2007) who proposed the concept of open strategy as a way of understanding how businesses can create value from having an open approach to value creation. By being inclusive and flexible with the sharing of information, it can help businesses capture more value (Bogers et al., 2017). This is important as more businesses utilize collaborative models to deploy their strategies. To do this an open strategy requires a different form of governance system that facilitates the sharing of knowledge (Du et al., 2016; Fisher and Fang, 2017; Lauritzen, 2017). Chesbrough (2011) has further linked the concept of open strategy to open service innovation that requires collaboration with customers and suppliers in the innovation process.

In order to advance the process of innovation more organizations are utilizing open innovation as it enables inflows and outflows of knowledge that can enable better value creation for organizations (Laursen and Salter, 2006). Chesbrough (2003) viewed open innovation as being different to previous conceptualizations of innovation due to the acknowledgment that external and internal ideas are needed for innovation. Open service innovation is important in the international marketplace that is time dependent on new innovations (Massa et al., 2017). Innovation ecosystems are part of this process as they facilitate partnering with other network entities to co-create value (Eckhardt et al., 2018). To do this, businesses need to transition from traditional to open business models that enable a different method to collecting and disseminating knowledge. Randhawa et al. (2016) suggested that the dynamic capabilities perspective can be used in open innovation to
reconfigure resources. This is important in markets with environmental turbulence that require the use of relational capabilities.

Part of the open innovation process particularly for technology firms means utilizing knowledge for entrepreneurial business ventures. Knowledge-based entrepreneurship is important for open innovation as it promotes the development of new knowledge practices. Spender *et al.* (2017, p. 20) defined knowledge-based entrepreneurship as “the ability to discern or avail of an opportunity and act to fulfill an innovative knowledge practice or product.” Chaston and Scott (2012) in a study of firms in Peru found that there is more emphasis on double loop learning with firms involved in open innovation because of knowledge and entrepreneurial potential. To access the effect of open innovation, it is important to evaluate the efficiency and effectiveness of ideas.

This paper investigates the role of cybercrime in influencing an originations open innovation strategy. Open innovation is discussed in the literature review in terms of its effect on coöpetition, horizontal technology collaboration, vertical technology collaboration and technology scouting. In-depth interviews of technology firms are utilized to see how their innovation strategy is focusing on open innovation and its affect on firm performance. As there is still debate about the role of open innovation in technology firms, the results of this paper help to shed light on the coöpetition paradox in which firms not only need to collaborate but also compete in the global marketplace. The next section discusses the literature review for this study. This is followed by the methodology, the findings are then presented and implications for managers stated. Finally, the limitations and research suggestions are addressed.

**Literature review**

A firm’s innovation strategy is influenced by its ability to scout for new knowledge. Wang *et al.* (2015, p. 223) defined technology scouting as “a firm’s innovation resource scanning and acquisition process: it implies both searching for technology acquisition channels and supporting the process of innovation efforts.” Technology scouting involves assessing appropriate capabilities and technology in other firms and industry settings. This is important in the technology industry as there are new and emerging innovations changing the business environment. When firms scout for technology, they are trying to discover new opportunities that provide a competitive advantage (Tether, 2002). Sometimes it is too costly for a firm to develop technology internally so they look for alternative sources. This helps a firm develop innovation resources that can use information and knowledge obtained from external sources (Wang *et al.*, 2015).

Firms need to be open to outside innovation due to the ability to access and utilize external knowledge (Enkel *et al.*, 2009). This is especially important in technology firms that need networks to build innovation. Firms need to collaborate and exchange knowledge in order to increase their knowledge base. There are some risks firms have with open innovation but this can be minimized with the right kinds of collaboration. Enkel *et al.* (2009) suggested that there are three core processes in open innovation: outside-in, inside-out and coupled. The outside-in process refers to the notion that knowledge can be created outside a firm but the innovation in a firm (Enkel *et al.*, 2009). This has led to firms becoming more engaged in networks and communities as a way to integrate knowledge into their firms. This helps increase the sources of knowledge that can enrich potential innovations. The inside-out process means a firm takes ideas to the market rather than relying on internal support. This enables other firms to support the ideas by transferring knowledge and providing feedback. The coupled process means partnering with another firm to help with the innovation. Increasingly, this coupled approach has been referred to as co-creation as it enables firms to work together on innovations. This provides joint capabilities that help an innovation be successful.
There has been a shift toward the use of open innovation as a way to source ideas and for collaboration (Kim and Lui, 2015). The concept of openness refers to knowledge flows that facilitate innovation practices. More openness between firms can encourage access to external knowledge, which affects innovativeness. Openness can enable the creation of new ideas and stimulate knowledge acquisition (Knudsen and Mortensen, 2011). More firms are focusing on open innovation for their success and as a way to foster collaboration. Despite the benefits associated with open innovation, there are few empirical studies examining the role of different types of technology collaboration in fostering firm performance due to the difficulties in measuring the concept (Knudsen and Mortensen, 2011).

The environmental context affects the relationship between open innovation and performance in both positive and negative ways (Cruz-Gonzalez et al., 2015). This is due to external knowledge acquisition not only impacting innovation within a firm but also meaning that potential intellectual property might be misappropriated. Open innovation enables a firm to redefine the boundary between itself and the environment in order to encourage the acquisition and dissemination of knowledge (Laursen and Salter, 2006). In the more connected world, it is important for firms to gain access to knowledge from a variety of sources that influence innovation. Chesbrough (2003) discussed how the open search for knowledge enables the acquisition of new ideas. These ideas play a key role in identifying knowledge and information important for a firm’s innovation activities. By being open to new ideas a firm an increase their knowledge base and identify appropriate sources of information. This helps a firm to improve its knowledge management processes and look for new opportunities in the marketplace (Huizingh, 2011).

More firms are accessing informal knowledge sources that lead to collective learning within a firm. The information gained from open sources comes from customers, competitors, industry associations, suppliers and universities (Cruz-Gonzalez et al., 2015). These many different sources of information provide a firm with complementary sources of knowledge that can be used for innovation. Openness can have negative connotations due to it being costly to source the right information in a timely manner. This is evident in Knudsen and Mortensen (2011) finding that openness can have a negative effect as it leads to slower projects. This means it is important for firms to have multiple sources of external knowledge and the appropriate management practices (Laursen and Salter, 2006).

Firms whilst scanning for appropriate partners need to be cognizant of the type of information they require. Laursen and Salter (2006) suggested that more external knowledge sources lead to a more open search strategy. This is due to the chance of acquiring the right knowledge being associated with integrating knowledge from appropriate sources. Chang et al. (2012, p. 448) defined openness capability as “a firm’s ability to search for diversified sources of creative ideas from external, distant and wider orientations, rather than from internal, local and narrow ones.” The implementation of open innovation needs to be integrated into a firm as there may be the “not invented here” syndrome. Therefore, for open innovation to be effective there needs to be the appropriate managerial attitudes within a firm. This is due to it being hard to integrate ideas into a firm when the source is external.

The process of open innovation involves integrating knowledge via shared communication mechanisms with competitors, which is referred to as coopetition. Coopetition is defined generally as “the simultaneous pursuit of cooperation and competition between firms” (Raza-Ullah et al., 2014, p. 189). This means that coopetition is a paradox but is increasingly common in technology firms who must compete but need to collaborate. Therefore, coopetition enables a firm to have a larger value net by decreasing opportunism whilst pursuing innovation (Bouncken and Fredrich, 2016). Coopetition acknowledges that often firms particularly those in knowledge intensive industries can leverage valuable
knowledge through collaboration with competitors. This is due to there being similar motivations for the need to access knowledge that is essential for innovation (Bouncken and Kraus, 2013).

Coopetition incorporates opposing forces of competition and collaboration but when combined can lead to potential gain for the firms involved (Fernandez et al., 2014). Part of the process for coopetition involves inlearning, which refers to how a firm leverages absorbed knowledge (Bouncken and Kraus, 2013). Thus, inlearning stems from the coopetition in which use of external knowledge is internalized and combined with existing knowledge sources. Inlearning incorporates relationship building into the way firms transform implicit knowledge into explicit knowledge (Bouncken and Fredrich, 2016).

The willingness to use open innovation will positively affect firm performance as it is part of an innovation strategy. Sisodiya et al. (2013) found a positive impact of open innovation on firm performance. Therefore, the openness of a firm's external search for knowledge is linked to the ability to access breadth and depth of knowledge. Breadth refers to the number of external sources a firm can rely on in terms of innovation (Laursen and Salter, 2006). This means that having more search channels will enable greater access to multiple sources of information (Cruz-Gonzalez et al., 2015). Depth refers to how a firm uses its knowledge in terms of finding the most appropriate ways to innovate and give meaning to the objectives of the firm's strategy (Laursen and Salter, 2006). Therefore, depth means the extent that a firm accesses information in a meaningful way from external sources. Both breadth and depth have been related to as exploratory and exploitative learning (Cruz-Gonzalez et al., 2015). This means that a firm's innovation strategy in terms of its breadth and depth will affect its overall performance.

Horizontal technology collaboration refers to collaboration with external competitors and partners in order to acquire technology-related knowledge (Wang et al., 2015). This form of collaboration involves accessing knowledge from firms in usually the same industry level in order to influence innovation. These types of collaboration are important due to the short product life cycles of many technological innovations. For many technology firms, improving access to innovation through collaboration is the key source of performance. Collaboration is a major way technology firm's gain access to innovation that helps them develop new products and services (Alexiev et al., 2016). A growing source of information utilized for collaboration is open innovation, but less is known about the effects on a firm's innovation strategy. Collaboration is often an innovation strategy by technology firms but there is a lack of understanding about how firms utilize technology scouting in order to facilitate performance.

Vertical technology collaboration involves collaboration with customers in order to gather feedback and help about market developments (Wang et al., 2015). Utilizing customer ideas in innovation helps firms develop better products and services. The use of customers in collaboration helps a firm to innovate with novel technologies (Von Hippel, 2005). This enables firms to access information and knowledge about technology from first-hand users. This experience means customers can contribute their own ideas about how a firm should innovate. Often customers are users and innovators so with vertical collaboration firms can tap into this expertise. Customers can help firm's source new or improved products and services in a more cost efficient manner (Wang et al., 2015). This helps a firm to test out ideas and see if customers will be receptive to the technology innovation.

Technology firms are more likely to cooperate with competitors because of the high level of interdependence (Gnyawali and Park, 2009). Often technology firms need to access each other's resources to develop integrative products and services. This is becoming more important as collaboration with competitors enables the acquisition and creation of new knowledge depositories. Firms utilize their competitor's technological knowledge to pursue collaborative ventures that are innovative (Wang et al., 2015). The collaboration with
competitors can lead to increased performance for all firms involved through the creation of new businesses. Collaboration enables the leveraging of competitors technological capabilities and know-how that is needed for innovation. Increasingly, horizontal technology collaboration is viewed as a competitive advantage for the firms involved as it leads to increased performance (Parida et al., 2012).

Communication needs to identify the knowledge and assimilate it within the firm context (Cohen and Levinthal, 1990). Moreover, the external knowledge needs to be linked to prior firm competences in order to apply it effectively. Collaboration can be both a process and an output between two or more firms (Crossan and Apaydin, 2010). Alexiev et al. (2016, p. 975) referred to interorganizational collaboration as “a feature of the innovation process related to the extent to which other organizations-firms or institutions-take an important part in the innovation process.” Collaboration occurs at different stages of the innovation value chain depending on the type of innovation (Hansen and Birkinshaw, 2007). Collaboration is a strategic decision that involves coordinating innovation activities and managing relationships (Alexiev et al., 2016). In this paper, a firm's innovation strategy will determine whether vertical collaboration is utilized. The next section will discuss the methodology utilized to analyze the role of cybercrime on an organization's open innovation strategy.

Method

Data collection

An exploratory qualitative research approach was adopted in this study. In qualitative research, there are no minimum number of participants needed as it depends on the type and nature of the study (Yin, 2013). Purposeful sampling enables an in-depth understanding about the topic under investigation (Patton, 2002). An open-ended question design structure was undertaken to enable probing of interesting information (Kalaftoglu and Mendoza, 2017). This enabled a semi-structured design process to provide rich insights.

A purposeful sampling approach to collecting the data was utilized (Lincoln and Guba, 1985). To select participants, the technology industry was chosen as it is influenced by open innovation and cybercrime. The informants were selected from the technology industry as they were deemed to be the most knowledgeable about the subject (Corley and Gioia, 2004). In addition, participants were asked if they knew others in the technology industry who might also provide useful information. The study included 16 participants and 2 cases were excluded as the managers moved to another city and could no longer be contacted. To be included in the study, the managers needed to be present in the interviews and have knowledge about their innovation business processes. The participants were all senior-level managers who had decision-making power in their organizations. However, they had differences in terms of innovation and cybercrime experiences and innovation behavior. This enabled better insights into how the nature of cybercrime is changing technology organizations' innovation strategies.

Preliminary interviews were conducted with the participants to understand their thoughts about the effect cybercrime have on open innovation strategies. An interview protocol was developed then adjusted based on the preliminary interviews. The interview protocol was organized around understanding the concept and process of open innovation, innovation strategy and technology collaboration. The data collection instrument was an interview protocol based on issues addressed in the literature review. The interview protocol focused on the main issues and themes under investigation in this study. Open-ended questions were utilized in order to have some flexibility in terms of asking follow-up questions. This enabled some changes depending on responses to the questions in terms of additional areas of enquiry. The sequence of the questions mostly followed the format given in the interview protocol. A total of 16 information technology professionals in Australia...
were asked about how open innovation influences cybercrime. The definition of open innovation used in the interviews was “firms using external and internal ideas to advance their technology.” The questions of interest to this study included: how does a strategy of open innovation influence cybercrime at your business? What cybercrime issues are associated with the sharing of information and knowledge? What are the key suggestions you have about dealing with cybercrime coming from an open innovation environment? And finally what mechanisms would you suggest information technology businesses adopt for managing open innovation? To provide more information about the environmental context influencing open innovation, archival data were also collected such as newspaper articles, website information, books and various other documents relating to cybercrime. This enabled more information to be obtained about the process of open innovation and enabled the triangulation of the data sources (Yin, 2003).

As stated in Table I, the interviewees were all in the information technology sector and had different lengths of experience. Thus, they have specific knowledge about cybercrime. The respondents in the sample had varied academic qualifications with most having studied information technology at university or via a post graduate diploma. The interviews were conducted in English via phone, e-mail and in-person. Most interviews went for at least 20 min and were transcribed.

Analysis

The transcripts were analyzed for main themes using a thematic analysis approach. This enabled an analysis of the outputs and topics emerging from the interviews. The themes were analyzed in terms of patterns and convergence in responses. Areas of divergence were also analyzed to help understand different points of view. The study utilized an interactive approach to take into account data from not only interviews but also continuous dialogue. Notes were taken during the interview to highlight key points and interesting findings. The data were analyzed manually by categorizing then recategorising quotes based on emerging themes. This enabled relevant patterns to emerge that enabled an understanding about the role of open innovation for cybercrime.

To preserve anonymity of the participants we utilized codes. The data were coded with the aim of identifying relationships and links to the existing literature (Strauss and Corbin, 1998). This involved the data being examined in stages to see emerging themes that were becoming evident until a point of data saturation was reached. The data were read and

<table>
<thead>
<tr>
<th>Case</th>
<th>Line of business</th>
<th>Position</th>
<th>Years worked in industry</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Services</td>
<td>Managing director</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>Retail</td>
<td>Employee</td>
<td>20</td>
</tr>
<tr>
<td>3</td>
<td>Services</td>
<td>Employee</td>
<td>2</td>
</tr>
<tr>
<td>4</td>
<td>Government</td>
<td>Director</td>
<td>20</td>
</tr>
<tr>
<td>5</td>
<td>Services</td>
<td>Managing director</td>
<td>3</td>
</tr>
<tr>
<td>6</td>
<td>Services</td>
<td>Director</td>
<td>2</td>
</tr>
<tr>
<td>7</td>
<td>Retail</td>
<td>Director</td>
<td>4</td>
</tr>
<tr>
<td>8</td>
<td>Government</td>
<td>Employee</td>
<td>3</td>
</tr>
<tr>
<td>9</td>
<td>Services</td>
<td>Owner</td>
<td>10</td>
</tr>
<tr>
<td>10</td>
<td>Services</td>
<td>Director</td>
<td>2</td>
</tr>
<tr>
<td>11</td>
<td>Services</td>
<td>Director</td>
<td>3</td>
</tr>
<tr>
<td>12</td>
<td>Government</td>
<td>Employee</td>
<td>3</td>
</tr>
<tr>
<td>13</td>
<td>Retail</td>
<td>Owner</td>
<td>5</td>
</tr>
<tr>
<td>14</td>
<td>Retail</td>
<td>Managing director</td>
<td>2</td>
</tr>
<tr>
<td>15</td>
<td>Services</td>
<td>Employee</td>
<td>10</td>
</tr>
<tr>
<td>16</td>
<td>Services</td>
<td>Employee</td>
<td>2</td>
</tr>
</tbody>
</table>

Table I. Sample profile

The effect of cybercrime
re-read to understand its meaning (Gioia et al., 2013). The data were coded based on themes that helped to identify the main connections. The data analysis involved comparing information with the previous interviews in an ongoing process. The analysis involved going back to the interviewees to clarify and amend the responses (Guba and Lincoln, 1994). This enabled a process of amplification so that novel insights were highlighted then clarified for meaning amongst the participants. In addition, it enabled the data collected to be corroborated to ascertain the main themes.

Following the approach used by Werthes et al. (2018), each of the participants was compared to see the changes in response and attitude. This enables an examination of the patterns among the participants of the study to be analyzed (Eisenhardt and Graebner, 2007). In addition, the study followed Yin’s (2009) quality measures for qualitative research that include internal validity, external validity and reliability. Thus, two other researchers examined the data to see if they derived the same themes. These external researchers came to the same conclusion about the themes and corroborated the findings.

Research findings

Subsequently, the study analyses the effect of cybercrime on open innovation policies in technology firms. A process logic approach is followed to understand the role of innovation strategy and technology scouting for open innovation policies. In addition, the effect of horizontal and vertical forms of technology collaboration on open innovation strategy is discussed. Throughout the analysis, illustrative quotes from the managers of the technology firms are provided. The data indicate that all participants are interested in the way open innovation is used as a business strategy. Over time each of the managers from the technology firms has adopted a way to cope with the threat of cybercrime. The findings reveal that all participants are changing their innovation strategy based on the environmental context. The analysis suggests that technology collaboration is a way of reducing risk of cybercrime as increased usage of partnerships can deter the risk of inappropriate stealing of data and information.

There was a range in the background profile of the respondents, which is illustrative of the different amounts of time people spend in the information technology industry. The years worked in the industry ranged from 1 to 20 years, which is also linked to the age of the respondents. Some of the interviewees might also have seen the years worked in the industry as related to the current position as Managing Director rather than the overall number of years spent in the Information and Communications Technology industry. This is reflected in these quotes: “I have worked specifically in the IT industry for 2 years as a Service Manager for a large technology company. But I have (had) a range of other roles that are linked in some way to my current position but would not necessarily classified as information technology” (Interviewee 6) and “I am an employee of this firm so one of the top employees in terms of sales. Here I have worked in the industry for 2 years. Before that I was in technology but in a different industry” (Interviewee 16). This broad range of experiences is helpful to understand the different points of view that individuals have about the effect of cybercrime and innovation on the industry. In addition, the diversity is good as it takes into account the views of individuals with both a short- and long-term experience of change in the information and communication industry.

The interviewees all were aware of the growing risk of cybercrime and had a variety of opinions about its relevance to open innovation. Most of the interviewees expressed the view that innovation was needed but open forms of innovation created additional risks in terms of potential data theft. This is evident in the following quote:

In the tech industry we need constant innovation to stay ahead of competitors. But some of the innovation requires collaboration. That is what you refer to as open innovation. But it comes at a price.
Open is not always open because people choose what they want to share. Some of the information can be stolen. There is a lot of cybertheft but the information as intentionally shared then it is not stealing but part of the sharing process. (Interviewee 5)

The greatest cyber security concern of most of the interviewees related to data breaches in terms of confidential and private information. This was evident in the discussion in the interviewees that focused on how to balance the sharing of information in the view of open innovation but also protecting important information. As the concept of open innovation seemed to be more an idea rather than practiced by the interviewees it produced some interesting quotes. For example:

Open innovation sounds a wonderful idea. In the online format it makes sense if people are not concerned with money. But our company needs to make a profit. How to do that with open innovation is an issue I think about. (Interviewee 12)

Open innovation is a good idea but we work hard and our ideas are money. So we share some information but not all. Some information has the potential to accidentally share intellectual property that was not deliberately intended. So security wise we need to share but be careful with the content. (Interviewee 2)

The issue of innovation strategy and its impact on cybercrime was discussed in the interviews. This seemed to be an important area of concern for the interviewees who needed to search for knowledge that had specific relevance to their businesses. Interviewees expressed the view that technology firms needed new knowledge for competitive reasons and this was part of the nature of their industry. However, obtaining the right knowledge was hard as evidenced by their collaboration strategy using open innovation. This is expressed in the following quotes:

Our strategy is to have access to more information in the hope that some will be relevant for our business. Being open about what we need and have helps with our innovations. (Interviewee 5)

I try to get others to read widely as a way to see new trends in the marketplace. Business partners are helpful and the strategy of sharing knowledge is useful in the technology industry. (Interviewee 9)

Interviewees discussed the role of technology scouting as a way to support the open innovation process. This means assessing other businesses in terms of information being shared to determine if it was useful for their business. Cybercrime was one of the issues that interviewees thought was a risk and there was efforts to ensure more private ways of sharing information between businesses. This is evident in this quote:

We look to see for change and this is part of our open innovation strategy but we need to ensure some information is only shared through the appropriate channels. Some gets lost. Some gets stolen. It depends on the website, the technology and the information. (Interviewee 10)

The impact of open innovation for business strategy was an issue that influenced the building of cyber security systems. This was important as even though the thought of open innovation means it is accessible to all in reality the technology firms were hesitant to share all types of knowledge. This meant that the firms took different forms of strategy in order to cope with open innovation.

Horizontal and vertical forms of technology collaboration were used by the businesses in pursuit of their open innovation strategy. Horizontal collaboration tended to be the preferred form as it was easier for the firms to connect with each other. The interviewees expressed the view that they understood the business strategy of other firms in the same industry level, which made it easier to collaborate. This enabled the interviewees to discuss how their firm was dealing with cybercrime. For many of the interviewees, horizontal collaboration
enabled sharing of strategies that focused on deterring cybercrime. This is stated in the following quote:

To talk to others in the same industry is part of business. Is industry practice. These talks refer to a range of topics with cybercrime always coming up in conversations. (Interviewee 8)

Vertical technology collaboration occurred in different contexts amongst the interviewees. This tended to reflect the need for open innovation to help customers, suppliers and business partners communicate about new developments in their field. The communication from the interviewees suggested that knowledge was important to improving processes and business systems. This means that part of the open innovation process involved the technology firms sharing information about how cybercrime might harm their business strategy. This is reflected in the following quotes:

Sharing information with them helps improve our processes but we need to keep careful attention on information that slips through. In the past some of our information was lost and had malware viruses attached to them that meant it was insecure. This is part of the cybercrime that happens on an everyday basis in tech firms. (Interviewee 14)

The next section will further discuss the results of the interviews in terms of cybercrime issues influencing technology firms.

Discussion of findings

This study contributes to the literature on open innovation by investigating the role of innovation strategy in preventing cybercrime. Previous research by Alexiev et al. (2016) suggests that an organization’s innovativeness is influenced by how it responds to security threats in its environment. This paper helps to build an understanding about how horizontal and vertical technology collaboration influences the way technology firm’s scout for information that might impact their performance. Amrollahi and Rowlands (2017) suggested that a more open approach to collaboration can result in better performance outcomes. Open innovation was evaluated using three different measures: innovation strategy, horizontal technology collaboration and vertical technology collaboration. This study provides some direction to technology entrepreneurs to develop their open innovation strategy but recognize the potential pitfalls in sharing information. This complements research by Gillespie (2015) who highlights that cybercrime is a disadvantage of increased collaboration but can be combatted through better organizational strategies.

It is important for technology entrepreneurs to demonstrate the benefits of open innovation as a way to enable a co-creation process and as an effective tool to find new opportunities. This confirms research by Elg et al. (2012) who found that co-creation can help firm’s develop better market innovations. Thus, in line with the literature review it was found that the data collected from the technology firms influenced open innovation practices. This supports research by Brown and Mason (2014) who found that the knowledge exploitation is a crucial part of an entrepreneurial ecosystem.

An innovation strategy helps to influence the type of information and knowledge that is scouted for in the environment. The potential for innovativeness increases when firms collaborate and share knowledge about potential future market trends (Tajeddini and Trueman, 2008). Thus, it helps to explain how a firm’s internal and external environment impacts its decision to utilize different types of technology to collaborate. This supports research by Rubin et al. (2015) who suggested that there are different types of knowledge produced by firms that depend on the nature of the knowledge flow. As open innovation is premised on the idea that customers, competitors and stakeholders have valuable insights this links with the notion of coopetition impacting cybercrime in technology firms.

As more technology firms seek to find ways to exploit their knowledge sources, it is helpful to understand the ways they can influence their innovation strategies in order to
increase their overall firm performance (Lazzarotti et al., 2015). The findings of cybercrime being influenced by both horizontal and vertical collaboration corroborate research by Tajeddini (2015) who found that to increase effectiveness and efficiency in firms they need to collaborate and share knowledge in order to enhance their competitiveness. Therefore, the findings of this paper can be useful to managers of small- and medium-sized organizations that are thinking about ways to utilize open innovation but protect themselves from cybercrime. This means that in the competitive marketplace some sharing of information is required in order to contribute to the innovation process but the level and amount of this information shared needs to be carefully considered. Thus, policies need to be in place that deal with potential cybercrime to ensure that confidential and sensitive information is not used in a malicious way. The findings of this research show that there can be open innovation but it needs to be managed in a careful way with other entities that the organization trusts. Therefore, a vetting process needs to be in place to ensure the right type of entities is being included in innovation discussions that have the potential to collaborate or help organizations in the future.

However, as Bader and Enkel (2014) found that a greater level of openness requires more organizational complexity there needs to be some management support on knowledge flows. Organizations can pursue innovative strategies but use the results of this paper to decide how to combat cybercrime when adopting an open innovation strategy. This supports research by Schott and Sedaghat (2014) who found that entrepreneurial social capital helps new entrepreneurs to innovate.

The study shows that the open innovation process of the interviewees was important in moving the direction of discussion to matters about cybercrime. With the exception of two interviewees, most in the study had a formal organizational strategy of participating in open innovation. This strategic direction influenced the willingness of interviewees to share valuable information that might have intellectual property rights associated with its usage. This involved coopetition in the open innovation process as the interviewees indicated that most knowledge shared was intelligence that had the potential to benefit their competitors. Therefore, the study provides a valuable basis based on the theoretical framework of open innovation for further research about the impact of cybercrime. Clausen and Rasmussen (2015) found that there are more social than private benefits of open innovation. The findings from this study are helpful to innovation and technology interest groups involved in cyber security. Governments not only need to provide training on how to deal with cyber security but also encourage technology firms to pursue open innovation. Policy makers should provide support to technology firms involved in open innovation to improve our understanding about how to deal with cybercrime.

Research contributions
The strongest finding from this research relates to the importance of collaboration for innovation whilst being mindful of cybercrime threats. For many technology firms, cybercrime has meant they are reluctant to share information but with changes in the market environment occurring at a rapid pace it is becoming important for them to have partners. As reflected in the discussion section, both horizontal and vertical forms of collaboration help increase innovation repositories in technology firms. However, there is seemingly an acknowledgment amongst managers of these technology firms that open innovation is part of their business strategy. Thus, technology scouting in terms of finding new solutions and different sources of information is a tool for innovation. Many of the technology firm managers seemed to regard cybercrime as an inevitable occurrence in their business.

The results from this study demonstrate that open innovation causes a change in an organizations strategy toward cybercrime. This supports previous findings by...
Lazzarott et al. (2015) who suggested that open innovation requires firms to absorb knowledge. The interviewees in the study were all from the technology industry and had knowledge about innovation processes in their organization. The interviewees suggest that cybercrime is an important issue in technology firms that influences the level of open innovation. As stated by Minshall et al. (2010), open innovation strategies benefit from asymmetric partnerships between firms due to differences in knowledge. To understand how open innovation and cybercrime are related it is important to situate it within the tech industry. As suggested by Spender et al. (2017), more longitudinal studies of open innovation are required due to their complex and evolving nature.

During the open innovation process, there should be more knowledge and information circulated between firms (Verbano et al., 2015). The findings of this study suggest that technology firms have to weight up the advantages of being in an open innovation ecosystem and the potential cybercrime risks that might result. Therefore, this research supports Tajeddini et al. (2015) who found that the performance of firms is increased through collaboration. Past research has found that inter-firm market orientation is an important way to increase overall firm performance (e.g. Elg, 2007, 2008; Tajeddini and Ratten, 2017). This process can be difficult but this study suggests that it is better for organizations to utilize open innovation to share information about preventing cybercrime. As Chesbrough (2006) stated that there are different strategies for firms adopting open innovation. The findings indicate that there are different ways cybercrime is perceived by managers. Therefore, further research should focus on understanding how cybercrime is embedded in the innovation ecosystem environment for technology firms. This should involve focusing on emerging and novel types of open innovation such as cross-sector collaboration partnerships to see the way they deal with cybercrime.

Theoretical implications
From a theoretical perspective, this study relies on open innovation theory and its wider contextualization within innovation strategy to explain the effect of cybercrime. In line with open innovation theory, managers of technology firms can serve as coordinators and instigators of an innovation policy that takes into account risks concerning cybercrime. The application of open innovation theory to cybercrime offers a way to encourage collaboration between technology firms to understand the negative effects of cybercrime. As there is more emphasis on technology firms having an open innovation policy, innovation theory has rarely been applied in the context of cybercrime. Other theories such as innovation strategy have been more prevalent in the literature but open innovation offers a better contemporary direction for the innovation activities of technology firms. The direct consequences of cybercrime have negative effects for technology firms so it is important that managers of these firms foster collaboration but are also aware of the downside effects.

Practical implications and future research suggestions
The findings from this study help managers to focus on the positive benefits of open innovation, which are increasingly needed in the technology industry in order to compete in the global marketplace. Existing practices can be improved by taking safeguards to protect intellectual property when collaborating with other organizations. This can be conducted by having clear policies in place that not only encourage innovation but also highlight the potential cyber security threats. Workshops that disseminate information about new ideas and technology but at the same time have limitations on the amount of data shared would be a way to manage cyber security risks.

Managers should frame their innovation strategies so that they incorporate both horizontal and vertical forms of technology collaboration. This ensures that firms listen to and gain information from a variety of different sources including their
competitors and customers. In the past, most knowledge about potential new innovations came from competitors but now with increased emphasis on user innovation customers can be good sources of knowledge and information. Therefore, managers should provide mechanisms for customers to share their ideas in an online and open forum in order to encourage innovation. In addition, as managers scout their environment for potential trends it would be useful if they discussed these approaches with customers and competitors in the form of co-competitive strategy.

Future studies could advance the findings of this research by addressing some of the limitations due to time and resource scarcity. As this study focused on technology firms in one geographic setting, it would be useful to analyze internationally if there are any cultural differences in the way collaboration and innovation affect cybercrime. In addition, due to the cross-sectional nature of this study, it would be interesting to evaluate changing perceptions toward open innovation over a longer time period. Therefore, longitudinal and process-orientated studies could be conducted to see how technology firm managers are changing the way they deal with open innovation. Understanding the decision making about open innovation could also further help understand how it can be incorporated into a firm’s strategy (Aloini et al., 2015). In addition, this study focused on vertical and horizontal technology collaboration but there may be various other more hybrid forms of collaboration. For example, do firms specifically focus on partners for horizontal or vertical forms of technology collaboration? What type of technology collaboration to prevent cybercrime is preferred? And what is the best form of technology collaboration for open innovation? This would be helpful for managers to understand in more depth the complex and dynamic nature of open innovation.

Conclusion

In conclusion, open innovation is an important way for technology firms to increase their performance as long as they understand the different types of collaboration and have an appropriate innovation strategy to manage cybercrime. Managers of technology firms need to decide when to use horizontal or vertical collaboration as an innovation strategy. Simultaneously, technology firms need to be scouting their environment for trends and changes. Therefore, open innovation and environmental contexts may offer important insights in how to improve firm performance in the competitive marketplace. Future research can further focus on the role of collaboration in technology firm’s innovation strategy and its effect on firm performance.

References


**Further reading**


**Corresponding author**

Vanessa Ratten can be contacted at: v.ratten@latrobe.edu.au

For instructions on how to order reprints of this article, please visit our website: www.emeraldgrouppublishing.com/licensing/reprints.htm
Or contact us for further details: permissions@emeraldinsight.com
Cybersecurity economics – balancing operational security spending

Stale Ekelund
Parsec Software AS, Oslo, Norway, and
Zilia Iskoujina
Coventry University, Coventry, UK

Abstract

Purpose – The purpose of this paper is to demonstrate how to find the optimal investment level in protecting an organisation’s assets.

Design/methodology/approach – This study integrates a case study of an international financial organisation with various methods and theories in security economics and mathematics, such as value-at risk (VaR), Monte Carlo simulation, exponential and Poisson probability distributions. Thereby it combines theory and empirical findings to establish a new approach to determining optimal security investment levels.

Findings – The results indicate that optimal security investment levels can be found through computer simulation with historical incident data to find VaR. By combining various scenarios, the convex graph of the risk cost function has been plotted, where the minimum of the graph represents the optimal invest level for an asset.

Research limitations/implications – The limitations of the research include a modest number of loss observations from one case study, and the use of normal probability distribution. The approach has limitations where there are no historical data available or the data has zero losses. These areas should undergo further research including larger data set of losses and exploring other probability distributions.

Practical implications – The results can be used by leading business practitioners to assist them with decision making on investment to the increased protection of an asset.

Originality/value – The originality of this research is in its new way of combining theories with historical data to create methods to measure theoretical and empirical strength of a control (or set of controls) and translating it to loss probabilities and loss sizes.

Keywords Organization, Cybersecurity

Paper type Research paper

1. Introduction

Cybersecurity economics is an area concerned with whether an organisation is spending enough on securing their assets and whether the security budget is spent on the right things (Anderson and Schneier, 2004). While there has been a significant increase in research on cybersecurity economics (e.g. Jacobs et al., 2016; Buiith, 2015; Choudhry and Wong, 2013; Brecht and Nowey, 2012), the in-depth understanding of the security level, investments in security controls and improvements for new controls need to be examined further.

Brecht and Nowey (2012) have categorised security spending by a proposed model for quantifying security costs that they argued will increase accuracy, objectivity and comparability. Defence costs are what an organisation has chosen to invest to protect their assets. Gordon and Loeb (2006) claimed that the benefits from cybersecurity investments come from cost-savings related to the avoidance of potential incidents; the outcome of the potential losses from incidents; the loss probability and the loss reduction from an investment. A different approach has been presented by Lee et al. (2011) who identified which security investment levels are optimal in terms of balancing costs of protection and risks to an asset. They argued that the security level can be viewed as the strength or effectiveness of the
controls applied to protect an asset (Lee et al., 2011). Therefore, it is vital to understand the marginal strength improvement of the security level, and how it translates to the reduced loss probability when investing in an additional security control. National Institute of Standards and Technology (NIST, 2008) provides a guide for performance measurement for information security, but fundamentally lacks a method for measuring effectiveness of a given security level. Peláez (2010) suggested an approach to measure how much a control decreases the loss probability and link risk to the effectiveness of control. While Peláez (2010) provided guidance on how to measure effectiveness using a quantitative technique, it lacks a clear linkage to determine loss probabilities and marginal improvements for new controls.

The Basel Committee on Banking Supervision (2005) organised by Bank of International Settlements are the regulator of the well-known Basel regulatory framework for financial institutions. This framework includes risk measurement using value-at-risk (VaR) for capital preservation purposes to secure banking operations in difficult times, defining VaR as the sum of expected and unexpected losses. Also, Jacobs et al. (2016) presented an approach to determine future loss probability by using Cyber VaR, a risk quantification method for cyber risks adapted from the framework proposed by World Economic Forum (2015). Cheung and Powell (2012) also examined how to calculate VaR using Monte Carlo simulation methods, where a stochastic process replaces the need to specify the probability distribution. Monte Carlo simulation is used in this study to determine VaR.

As seen, despite an increasing amount of research on cybersecurity economics, the question for cybersecurity practitioners as to how much to invest in protecting an organisation’s information assets remains. Therefore, the research objective of this study is to examine how an organisation can determine how much it is recommended to invest in the protection of a digital information asset. To reach this objective, this paper will address the following three research questions:

RQ1. How can defence costs be determined, and losses calculated?

RQ2. How can the effectiveness of a security control be measured in terms of reduction in future loss probability?

RQ3. How can cybersecurity investment aimed at protecting an asset be optimised?

The paper begins by briefly reviewing the literature on cybersecurity economics in such areas as security costs, loss probability, effectiveness of security controls and investment optimisation. These areas are discussed in order to develop research propositions that will be tested before the findings are presented.

2. Theoretical background

2.1 Costs of the cyber defence effort

Investment in defence costs and security controls are aimed at protecting the assets of an organisation; when this fails, costs related to damages and losses are incurred (Wang et al., 2008). These two cost streams are explored to understand better how to categorise and quantify such costs. For example, Brecht and Nowey (2012) established a model for quantifying cybersecurity costs for increasing accuracy, objectivity and comparability. Their criterion for cost–benefit calculation (Brecht and Nowey, 2012) are as follows: costs for managing information security (in this research referred to as defence cost), costs related to information security measures (in this research referred to as defence cost), costs incurred by information security incidents (in this research referred to as losses) and cost of capital induced by information security risks (considered outside scope of this research). Subsequently, Brecht and Nowey (2012) suggested the information security management system (ISMS)-layers approach to information security cost quantification,
which takes the perspective of information security management. According to ISO (n.d.), ISMS is a risk management process involving people, processes and technology in protecting organisations’ assets. Brecht and Nowey (2012) discussed measurement, determinability (difficulty in security attribution) and information security cost ratio (percentage attributed to security).

The ISMS-layers approach appears adequate in determining information security costs. The security cost ratio, however appealing, is less helpful as one must anticipate substantial variations between organisations. Operational measures are assumed to be direct costs and the other layers to be indirect costs. Therefore, to assess the cost–benefit of an asset’s defence, further investigation on how defence costs can be determined and losses calculated is needed. This will be examined in RQ1. The research question will be tested through the following propositions (Figure 1):

\[ P1a. \] Direct defence costs can be defined as any security cost that is exclusively aimed at protecting one or more, but not all, assets.

\[ P1b. \] Indirect defence costs can be defined as any security cost that is aimed at protecting all assets.

\[ P1c. \] Defence cost can be shared between some or all assets, or between security and non-security budgets.

\[ P1d. \] Cost of damages and losses caused by a cyber-incident can be categorised in short- and long-term losses.

2.2 Determining effectiveness of a security control

The purpose of measuring the effectiveness of security controls is to understand how a set of applied controls translate to a loss probability, and particularly the marginal improvement of adding one to a set of controls is already in operation. Ideally, improvements may be expressed in terms of impact of VaR. NIST (NIST, 2008; Peláez, 2010) provide approaches but fail to link to loss probabilities and marginal improvements for new controls. Pagett and Ng (2010) argue that standards-based IT governance models such as COBIT, NIST and ISO27004 are more focussed on “what” needs to be measured rather than “how”. In response they propose an information security effectiveness framework to address the “how”, with effectiveness measured based on characteristics of a control (Pagett and Ng, 2010).

To measure effectiveness this way seems promising, but the proposal is leaning on what a designated policy prescribes, such as how many computers have antivirus installed. What if the policy is imperfect, but the characteristics otherwise score fully? This may lead an organisation to be lulled into a false sense of security. The method proposed increases understanding on how the effectiveness of a security control can be measured, but it does not link to a loss probability nor to VaR. By contrast, the

---

**Figure 1.** 
Theoretical framework
approach presented by Huang et al. (2008) is more geared towards finding the optimal investment level where a security incident is associated with a probability function $p$ that leads to losses. They further claimed that beyond some point of adding new controls, “the utility of the investment to the firm would actually be smaller than the expected utility from potential security breach” (Huang et al., 2008, p. 11). Moreover, Wang et al. (2008), Lee et al. (2011) and Huang et al. (2008) presented solid mathematical models in deriving the expected value and VaR at a given security level, but the marginal effectiveness of adding a security control in terms of strength or effectiveness score is not covered.

In summary, the research has identified several approaches attempting to express effectiveness of security controls. However, as they lack solid numerical representations, they are not particularly useful for this research. There may, however, be opportunities for syntheses between the approaches. It is therefore necessary to further explore how the effectiveness of a security control is measured and linked to loss probability. Therefore, RQ2 in this paper will address how the effectiveness of a security control can be measured in terms of reduction in future loss probability. This research question will be tested through the following propositions (Figure 1):

$P2a$. The reduction in loss probability is measurable and based on the characteristics of the security control, i.e. the effectiveness.

$P2b$. The reduction measure is impacting VaR.

2.3 Determining optimal security investments

Faced with an opportunity to invest in more protection, it is beneficial to understand how to calculate the benefits from security investments and get guidance on how to find the optimal level to invest. Gordon and Loeb (2006) claim that cost-savings are an outcome of the potential losses from incidents, the loss probability and its reduction from an investment. They propose an approach to determine the optimal level of investment by a loss probability function with an investment level and a vulnerability level. Expected losses are given by the product of threat probability and monetary losses to an asset. The calculation may be conducted without historical attack data, that is, the investment level is the only decision variable. However, the vulnerability level and expected losses still need to be derived somehow. By contrast, Huang et al. (2008) discuss the use of expected utility theory to identify the security investment level that maximises the utility of the investment. The framework presented is similar to the one Gordon and Loeb (2002) used but with different boundary conditions and assumptions. To compute the optimal investment, the probability of a security incident occurring in a given time frame, an investment level, a potential loss and a risk-aversion coefficient must be determined. This approach (Huang et al., 2008) applies classical economic theories to compute an optimal security investment to protect an asset. As an input, historical data to determine the loss probability are needed, as well as a risk-aversion coefficient.

The approaches reviewed are useful contributions in understanding the optimal amount to invest in security. They are not, however, particularly beneficial on their own as they require input variables such as loss probabilities, vulnerability level and risk-aversion coefficients, which are not straightforward to determine. In effect, these approaches must be combined with supplemental methods to deal with the more demanding input variables. Therefore, RQ3 will examine how a cybersecurity investment aimed at protecting an asset can be optimised. This research question will be tested through the following proposition (Figure 1):

$P3a$. The optimal investment level can be expressed as the minimum sum of defence costs and losses to an asset.
2.4 Theoretical framework

The theoretical framework is a model consisting of the factors and their relationships that contribute to a problem and prepares for further discussions and investigation. It helps postulate and test certain relationships in order to improve our understanding (Sekaran, 2003). The theoretical framework in this case has been created from the hypotheses identified above: that the risk cost – the sum of defence costs and losses – has a minimum value that can be identified by adding or subtracting controls; increasing defence cost should supposedly reduce the losses (VaR), but it is also dependant on the effectiveness of the control invested in. The variables used in the framework are therefore one dependant variable, the risk cost, with underpinning independent variables. From the findings and interpretations of the literature review, the dependant variable has been identified as minimum risk cost as the measure of "how much to invest". The dependent variable, key independent variables and their interconnections are illustrated in Figure 1.

3. Research methodology

This research is based on the scientific method, which is a systematic approach towards observing phenomena, drawing conclusions and testing hypothesis (Sekaran, 2003). Building and testing theories from a case study is a strategy that is used as a complementary method; developing theories and propositions from such empirical evidence is one of the best bridges from qualitative evidence to deductive research (Eisenhardt and Graebner, 2007). Kulmala et al. (2006, p. 147) deployed this approach arguing that "a single case study was selected because initial understanding on the studied phenomenon was the target". Shih et al. (2017) based their research on a case study arguing its suitability for investigating contemporary phenomena, which aligns well with the nature of this research. The general problem statement – how much an organisation should invest in protection – induces the need for researching existing knowledge in a set of multi-disciplinary topics. The identification of gaps in existing knowledge generates this study’s research questions, which in turn generates the propositions. To answer each proposition, qualitative or quantitative research is conducted. The propositions are created in alignment to the theoretical framework, as illustrated in Figure 2.

The research questions are addressed using a case study with a mixed method. The qualitative approach serves as an input to a quantitative approach, which in turn will be used to acquire answers to the research questions. The data were collected through interviews and archival records. The case study took place at an anonymised international financial services organisation referred to as “FinCorp Ltd,” a substantial player in the European market and with offices around the world. During the course of six weeks, three leaders from the information security department were interviewed, which in turn relayed many of questions to various subordinates for supporting information and provision of archival data. This department was chosen as it has overall responsibility for the protection of information assets. The interviews were conducted through plenary sessions. The participants were the chief information security officer, the head of security architecture and the head of risk management. To set the stage, the first session was initiated by asking how security investments are justified today. Subsequently, questions were asked and discussed sequentially. The questions were sent a day in advance of the two sessions arranged. The objective of data analysis is to meet the research objective, and therefore the most important aspect of data evaluation is to convert the data collected into a format which will support adequate inference and decision support (Sreejesh et al., 2014). Where appropriate, data are converted into a numerical format appropriate for calculations and simulations.

Computer-based simulation uses mathematical models to determine effects of change and has been used to study risk management in the finance area for some time (Sekaran, 2003).
Particularly when considering VaR, Monte Carlo simulation – an algorithm randomly simulating outcomes based on historical data – is the preferred method for data analysis for two reasons: to take advantage of any historical distribution of risk factors (Choudhry, 2013), and to join a discrete distribution (loss arrivals) with a continuous one (loss sizes) (Navarrete, 2006). The simulation starts with initial values for annual loss occurrence probability, and the loss sizes’ mean and standard deviation from the collected data. Then new arrival and size data are simulated by randomisation and joined to create new 12-months loss scenarios. The approach is illustrated in Figure 3.

4. Data analysis, findings and discussion

4.1 Proposition 1a: direct defence costs can be defined as any security cost that is exclusively aimed at protecting one or more, but not all assets

Direct costs are costs directly associated with security controls protecting an asset; “if the asset is removed, the controls and their associated costs are detachable”, as one interviewee put it. Furthermore, a security control may protect more than one asset (but not all) but still constitute direct costs. FinCorp Ltd has deployed four security controls with the following annual operation costs to (directly) protect $A_1$ (Table I).

When considering the cost of cybersecurity, both defence cost and losses are considered as suggested by Brecht and Nowey (2012). As argued by Gordon and Loeb (2002) and Huang et al. (2008), the level of defence cost is related to the losses. It is therefore beneficial to cover these two cost categories in concept to monitor their interaction. Identifying what represent direct costs of protecting an asset is a matter of

Source: Derived from Sekaran (2003, p. 56)

Figure 2. Research approach
agreeing on what to include in such calculations. Based on the data collected from FinCorp Ltd, this research considers the direct defence cost as operational measures (as per the ISMS-layers approach in Figure 4), and the other categories as indirect costs. In general, the defence costs are represented as an annual cost that include an initial investment cost, an annual operating cost and depreciation expenses due to a limited useful lifetime.

Consider a set of security controls \( \{n_1, n_2, \ldots\} \) protecting an asset \( A_i \in \mathcal{P} \). Each control, denoted node, has a cost, \( c(n) > 0 \). Further, view this set of nodes as forming a risk vector, denoted \( v(A) \). The concept of a risk vector will be formally defined and discussed below, but for now it is sufficient to realise that each node has an individual cost and thus the cost of vector \( v(A) \), denoted \( c(v(A)) \), is the cost of all nodes protecting it.

<table>
<thead>
<tr>
<th>No.</th>
<th>Security control</th>
<th>Estimated annual operation cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>End-user with antivirus</td>
<td>£0</td>
</tr>
<tr>
<td>2</td>
<td>Application firewall</td>
<td>£600,000</td>
</tr>
<tr>
<td>3</td>
<td>Two-factor authentication</td>
<td>£200,000</td>
</tr>
<tr>
<td>4</td>
<td>Fraud detection module</td>
<td>£300,000</td>
</tr>
</tbody>
</table>

Table I. Deployed security controls at FinCorp Ltd
4.2 Proposition 1b: indirect defence costs can be defined as any security cost that is aimed at protecting all assets

Indirect costs are, as expressed during the interviews, "costs that are incurred by all employees with part or full-time responsibility for information security, security policies and guidelines, security awareness and training, and the ISMS". The estimated annual indirect costs of protecting all assets at FinCorp Ltd including protect $A$ are categorised as follows (Table II).

The obtained indirect cost data align well with the cost categories defined by Brecht and Nowey (2012). Let $\Omega$ be the total annual information security cost of an organisation in protecting its portfolio of assets $P = \{A_1, A_2, \ldots, A_k\}$. Also, let $\psi$ be the direct annual defence cost and $\omega$ the indirect annual cost, or expressed more formally:

$$\Omega = \omega + \psi = \omega + c(v(A_1)) + c(v(A_2)) + \cdots + c(v(A_k)).$$

Further assume $\psi = c(v(A_1)) + c(v(A_2)) + \cdots + c(v(A_k))$, where $\psi_1 = c(v(A_1)), \ldots, \psi_k = c(v(A_k))$. In contrast to Brecht and Nowey (2012), $\psi$ is considered to be 100 per cent dedicated to information security according to the definition of a risk vector, see Section 4.5. The formula for indirect costs $\omega$ is exhibited as follows:

Cost of management system $\times 1$
+ Cost of people and process $\times 0.85$
+ Cost of architecture and concepts $\times 0.5$
+ Cost of prerequisites $\times 0.25$

$= \omega.$

<table>
<thead>
<tr>
<th>No.</th>
<th>Security cost category</th>
<th>Estimated annual indirect cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Cost of operating the management system</td>
<td>£1,000,000</td>
</tr>
<tr>
<td>2</td>
<td>Cost of people and processes</td>
<td>£2,000,000</td>
</tr>
<tr>
<td>3</td>
<td>Cost of architecture and concepts</td>
<td>£250,000</td>
</tr>
<tr>
<td>4</td>
<td>Cost of prerequisites</td>
<td>£500,000</td>
</tr>
</tbody>
</table>

Table II. Information security cost categories
The indirect annual cost $\omega_{A_x}$ of protecting $A_x$ is exhibited in the following equation:

$$\begin{align*}
\text{Cost of management system} \times 1 & = £1,000,000 \\
+ \text{Cost of people and process} \times 0.85 & = £2,000,000 \\
+ \text{Cost of architecture and concepts} \times 0.5 & = £250,000 \\
+ \text{Cost of prerequisites} \times 0.25 & = £500,000 \\
= \text{Total indirect costs} & = £3,750,000.
\end{align*}$$

The obtained indirect cost $\omega_{A_x}$ is valid only if asset $A_x$ is the only asset. There are, however, more assets in FinCorp’s possession. It is therefore necessary to investigate how direct and indirect costs are shared (see the next PIc).

4.3 Proposition 1c: defence costs can be shared between some or all assets, or between security and non-security budgets

The case study obtained information on several nodes including all that are used to protect asset $A_x$, that is $n_i \in v(A_x)$. Table V in Section 4.5 displays the nodes and their annual operation costs.

The total number of assets in FinCorp’s possession was not obtained from the case study, but using the asset as a service approach, the case study participants anticipated it to be less than 10. As per the case study, a node $n$ can be protecting several assets. Therefore, the node cost $c(n)$ should be divided between all the assets being protected by that node. This “reuse” of nodes is thus beneficial from a cost standpoint but may not be so from a protection standpoint as a defeated node may cause collateral damage. It is not, however, considered in the scope of this research to explore this potential weakness further.

Let $\overline{m} \geq 1$ be the number of “reuses” a node $k$ has in protecting assets in $P$. The direct annual cost $\psi_i = c(v(A_i))$ for protecting asset $A_i \in P$ is thus:

$$\psi_i = c(v(A_i)) = \sum_{n_i} \frac{c(n_i)}{\overline{m}_i}.$$

(2)

Also, when considering the indirect annual cost $\omega$, the cost may be equally divided between the assets in the portfolio $P$. For an asset $A_i \in P$ the indirect annual cost is:

$$\omega_i = \frac{\omega}{\text{Number of assets in } P}.$$  

(3)

At FinCorp Ltd the direct annual costs of protecting $A_x$ are illustrated in Table I. Applying these to (2), the direct defence cost of $c(v(A_x))$ is obtained:

$$\psi_{A_x} = c(v(A_x)) = \frac{c(n_1)}{\overline{m}_1} + \frac{c(n_2)}{\overline{m}_2} + \frac{c(n_3)}{\overline{m}_3} + \frac{c(n_4)}{\overline{m}_4} =
\frac{0}{1} + \frac{600,000}{4} + \frac{200,000}{1} + \frac{300,000}{1} = £650,000.$$  

(4)

Further assume that FinCorp Ltd has five assets in total, then the indirect cost $\omega_{A_x}$ is obtained through:

$$\omega_{A_x} = \frac{\text{Total indirect costs}}{5} = £750,000.$$  

(5)

In summary, the total annual cost of protecting $A_x$ by applying (2) and (3) is:

$$\Omega_{A_x} = \psi_{A_x} + \omega_{A_x} = £650,000 + £750,000 = £1,400,000.$$
Based on this, an annual level of defence cost has been calculated. For this level of defence, FinCorp Ltd experienced losses of £491,825 over a period of 30 months (see the next P1d).

4.4 Proposition 1d: cost of damages and losses caused by a cyber-incident can be categorised in short and long-term losses

The Information Security Department at FinCorp Ltd may or may not be representative in their response to what is more important: short-term or long-term losses following a security incident. As the department is being measured on short-term data, this was considered most important. Loss observations, caused by 54 incidents, were provided for a period of 30 months. The losses incurred, £491,825 in total, were short-term losses caused by cyber-attacks.

Long-term losses, such as those arising from loss of competitive advantage, missing growth opportunities and loss of customers themselves, were by contrast hard to determine within the time allocated by the study. They are therefore omitted from this research. It is, nevertheless, considered plausible to find persons and even whole departments that value long-term losses above short-term losses. The loss observations that took place in this study are what Jacobs et al. (2016) consider as operational continuity and payments; typical short-term losses affecting daily income and cash flow. These figures can be used for further calculations and simulations to investigate how defence costs and cost of losses are connected, and how future loss probability can be derived.

To study this further, there is a need to construct a function denoted risk cost, which will take both the defence cost and the losses into account.

Risk cost. The asset value of $A_x$ was estimated to £240,000,000. At the defence level $\Omega = £1,400,000$, losses worth £491,825 were incurred, yielding a 12-month average of £196,730. Assume a new node is added aimed at protecting $A_x$ with some cost $c(n) > 0$. One would expect losses to be reduced by an amount $x$. However, adding another similar node with the same cost will reduce the losses by less than $x$, i.e. $x - y_1$. And another similar node will thus reduce the losses by $x - y_2$ where $y_2 < y_1$. This is in alignment with that the marginal improvement on security decreases with higher investments, where at some point “the utility of the investment to the firm would actually be smaller than the expected utility from potential security breach” (Huang et al., 2008, p. 11). This can be generalised through the following function:

$$\text{Risk cost} = \text{defence cost} + \text{losses}. \quad (6)$$

According to the extreme value theorem (Renze and Weisstein, n.d.) the risk cost function will have a maximum and minimum and create a U-shaped graph as illustrated in Figure 5. This is supported by Lee et al. (2011) claiming that the risk cost function is continuous and convex (U-shaped). Inspired by its shape, it is referred to as the U-graph of an asset. By construction, it follows that all assets have a U-graph, i.e. a minimum risk cost exists for all assets. Thus, this graph is suitable to depict if an increased investment in defence is worthwhile.

Since risk is about a future event that may or may not occur, and the example above is referring to incurred losses, there is a need to be a little more specific. Three variants of risk cost can be identified as described in Table III.

VaR calculation for determining future loss. To collect data for the U-graph of $A_\infty$, it is necessary to calculate future losses in terms of expected loss and VaR. It is also necessary to find a way to determine the effectiveness of the security controls and translate them into quantitative values and explore how this will affect the loss probabilities. As suggested by the World Economic Forum (2015), Jacobs et al. (2016), Wang et al. (2008), Lee et al. (2011)
and Huang et al. (2008), VaR can be applied for determining future losses. Based on the data obtained from FinCorp Ltd VaR can be calculated for the online services asset $A_2$ employing a Monte Carlo simulation in R. Initially, it is assumed that no historical data exist. The simulation follows the steps described in Figure 3, and the code for the computation is shown in Figure 6, where each step is followed by a description.

### Figure 5.
U-graph (risk cost function) of an asset

### Table III.
Risk cost variants

<table>
<thead>
<tr>
<th>Risk cost variant</th>
<th>Variables</th>
<th>Formula</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incurred risk cost</td>
<td>Defence cost, mean incurred losses</td>
<td>$IRC = \Omega + L$</td>
<td>The actual risk costs, given $\Omega$</td>
</tr>
<tr>
<td>Expected risk cost</td>
<td>Defence cost, expected losses</td>
<td>$ERC = \Omega + E[L]$</td>
<td>How the expected future risk costs will be, given $\Omega$</td>
</tr>
<tr>
<td>VaR risk cost</td>
<td>Defence cost, VaR</td>
<td>$VRC = \Omega + VaR$</td>
<td>What the maximum future risk costs with a given confidence level will be, given $\Omega$</td>
</tr>
</tbody>
</table>

### Figure 6.
VaR calculations with Monte Carlo simulation

```R
Monte Carlo method - using R

```
Subsequent simulations take advantage of the actual historical distribution for the risk factor rather than assuming a pre-determined normal distribution (see Section 4.6). Many simulations are run, each yielding different results. In the end, the simulation will aggregate to a more realistic result (Choudhry, 2013). By using the mean ($\mu$) and standard deviation ($\sigma$) derived from the loss observations, 5 per cent VaR loss value is obtained: $\text{VaR} = £82,706$ per month. This indicates that there is a 5 per cent probability of losing more than £82,706 in the next month as a result of cyber incidents, or £286,504 over the next 12 months. The expected value of a normal distribution is its mean value (Hildebrand, n.d.), thus:

$$E[L] = \mu = |{-0.0068\%} \cdot £240,000,000| = £16,320 \text{ per month.}$$

Thus, FinCorp Ltd can expect to lose on average £16,320 per month or £195,840 per year, by construction approximately the same as the average losses incurred. Applying these numbers to the risk cost variants yields Table IV.

4.5 Proposition 2a. The reduction in loss probability is measurable and based on the characteristics of a security control, i.e. the effectiveness

One of the key points in this research is to demonstrate how to depict the U-graph for an asset. This will be shown by using $A_\pi$ as an example. Consequently, a method to determine the effectiveness of a node, both alone and in union with a set of existing ones, is needed. As the literature review did not increase our understanding as to how to determine such effectiveness, this research demonstrates a possible approach.

Inspired by the attack-defence process articulated by Jacobs et al. (2016), and paths of attacks (aka attack vectors), a simple framework for visualising and exploring the effectiveness of nodes can be created, referred to as a risk vector. This research assumes the term risk vector for the pathway where incidents leading to malicious exploitation may occur with potential to cause losses. It is correspondingly along this pathway where security controls are applied, and their effect can be measured, e.g. reduction in loss amounts. To illustrate how the malicious exploitation of an asset occurs, consider the cyber kill chain (Lockheed, n.d.) depicted in Figure 7.

Signs of a security incident are considered as either precursors or indicators, where the former is a sign that an incident may occur in the future and the latter is a sign that an incident is ongoing or has already occurred (NIST, 2012). The prime interest is in the precursors and indicators appearing along the vector. A complementary view is the

<table>
<thead>
<tr>
<th>Risk cost variant</th>
<th>Calculation</th>
</tr>
</thead>
<tbody>
<tr>
<td>IRC</td>
<td>£1,400,000+£196,730 = £1,596,730</td>
</tr>
<tr>
<td>ERC</td>
<td>£1,400,000+£195,840 = £1,595,840</td>
</tr>
<tr>
<td>VRC</td>
<td>£1,400,000+£286,504 = £1,686,504</td>
</tr>
</tbody>
</table>

Table IV. Risk cost calculations 1
attack-defence process, describing attack flow and an organisation’s cyber defence capability (Jacobs et al., 2016) as illustrated in Figure 8.

The relation between the two views is shown in Figure 9, offering an illustration of a risk vector.

In a vector \( v = v(A) \), consider a node \( n \in v \) with a strength, \( \rho(n) > 0 \) which is derived from a score, \( s(n) \geq 0 \), according to the control effectiveness scoring scheme discussed below. Thus, \( v(A) \) will have a cumulative cost denoted \( c(v(A)) \) or simply \( c(v) \) if it is clear which asset it pertains to. Likewise, \( v(A) \) will have a cumulative strength denoted \( \rho(v(A)) \) or simply \( \rho(v) \). The strength will be a measure on how much all nodes will reduce the risk of loss to an asset \( A \). The following risk vector \( v(A) \) was observed at FinCorp Ltd (Figure 10 and Table V).

\[
\begin{array}{c}
\text{Non-criminal assessment} \\
\text{Criminal assessment} \\
\text{Abuse} \\
\end{array}
\]

\[
\begin{array}{c}
\text{Prevention from entry} \\
\text{Prevention of abuse} \\
\text{Prevention of abuse} \\
\end{array}
\]

\[
\begin{array}{c}
\text{Breach detection and response} \\
\text{Breach detection and response} \\
\text{Breach detection and response} \\
\end{array}
\]

\[
\begin{array}{c}
\text{Recovery of losses} \\
\text{Recovery of losses} \\
\text{Recovery of losses} \\
\end{array}
\]

Figure 8. Attack-defence process

Source: Jacobs et al. (2016, p. 150)

Figure 9. Relation between the cyber kill chain (Lockheed, n.d.) and the attack-defence process (Jacobs et al., 2016, p. 150)

Figure 10. Risk vector \( v(A) \) at FinCorp

Note: The nodes identified in Table V

<table>
<thead>
<tr>
<th>Node</th>
<th>Security control</th>
<th>Estimated annual operation cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>( n_1 )</td>
<td>End-user with antivirus</td>
<td>£0</td>
</tr>
<tr>
<td>( n_2 )</td>
<td>Application firewall</td>
<td>£600,000</td>
</tr>
<tr>
<td>( n_3 )</td>
<td>Two-factor authentication</td>
<td>£200,000</td>
</tr>
<tr>
<td>( n_4 )</td>
<td>Fraud detection module</td>
<td>£300,000</td>
</tr>
</tbody>
</table>

Table V. Nodes protecting \( A \)
Through the construct of the risk vector, a framework for measurement and modelling of risk has been established. The literature review did not, however, identify any complete method of measuring a security control’s effectiveness alone or in concert with other controls in protecting an asset, and even less so linking effectiveness to loss probabilities. Nevertheless, Pagett and Ng (2010) argue that the effectiveness is linked to the characteristics of a control. Thus, a purpose-built approach is needed.

**Control effectiveness and strength.** A security control instantiates a mitigation treatment strategy such as deterrence, prevention, detection or recovery, aiming to reduce the likelihood and/or impact of a risk (Straub and Welke, 1998). Peláez (2010) argues that ISO/IEC 27004 provides guidance for measuring the effectiveness, not only of the controls themselves, but also management and implementation processes, commonly referred to as the ISMS. Based on this, consider the nature of the control (type), its mean of functioning (prescription), its susceptibility to being defeated (fallibility) and its ability to adapt to new threats (agility) as characteristics that impact its effectiveness. It is thus possible to assess a control’s effectiveness against its capability in deterrence, prevention, detection and recovery. Assessing these factors may also implicitly measure the effectiveness of the treatment strategy. Table VI illustrates the scoring scheme.

By rating the control against these characteristics, an effectiveness score can be determined. For each characteristic, a score of 4 is strongest and 1 is weakest. A characteristic that is not applicable is scored as 0. That gives a possible scoring range $0 \leq S \leq 16$ for each control, and the sum of effectiveness scores of all controls in the risk vector $v(A)$ is simply:

$$S = S(v(A)) = \sum s_i, S \geq 0, i = 0, 1, 2, \ldots$$  \hspace{1cm} (7)

Applying the scoring scheme to the nodes in $v(A)$ is illustrated in Figure 11, and the selected rating marked with green. The result of applying (9) to these scorings is $S = 9+11 +9+11 = 40$.

Adding a security control to protect an asset reduces the risk of that asset. The key question is how much and how this relates to $S$. To answer this, another heuristic method will be applied assuming that the marginal improvement on security decreases with additional controls (Huang et al., 2008). As an introduction, one can use intuition to depict a reasonable trajectory that resonates with probability, i.e. taking on values in the interval $[0, 1]$.

To depict this trajectory in accordance with the security level as proposed by Lee et al. (2011), and in such a way that it can be linked to probability, consider the exponential probability distribution with a scale parameter $\tau$ (Taboga, 2010):

$$f(x) = e^{-\tau x} \hspace{1cm} x \in [0, \infty),$$  \hspace{1cm} (8)

and particularly the cumulative density function:

$$F(x) = 1-e^{-\tau x} \hspace{1cm} x \in [0, \infty).$$  \hspace{1cm} (9)

<table>
<thead>
<tr>
<th>Score</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Characteristic</strong></td>
<td><strong>Type</strong></td>
<td>Administrative</td>
<td>Administrative/technical</td>
<td>Technical/administrative</td>
</tr>
<tr>
<td></td>
<td><strong>Prescription</strong></td>
<td>Logging</td>
<td>Rules/signature/heuristics</td>
<td>Live threat intelligence</td>
</tr>
<tr>
<td></td>
<td>only/observation</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Fallibility</strong></td>
<td>Likely</td>
<td>Possible</td>
<td>Unlikely</td>
<td>Impossible</td>
</tr>
<tr>
<td><strong>Agility</strong></td>
<td>Reprogramming</td>
<td>Re-configuration</td>
<td>Run-time</td>
<td>Self-learning</td>
</tr>
</tbody>
</table>

Table VI. Control effectiveness scoring scheme
This function will always generate a value in the interval from \([0, 1]\). By substituting \(x\) with the control effectiveness score \(S\), and applying it to (9), the following is achieved:

\[
F(S) = 1 - e^{-\tau S} \quad S \in [0, \infty).
\]  

(10)

By assigning an appropriate initial value to the scale parameter \(\tau\), the control effectiveness score to strength conversion function is finalised. For example, let:

\[
\tau = 0.05.
\]  

(11)

This results in the following trajectory (Figure 12).

This trajectory aligns well with the decreasing marginal effect and should serve the purpose for converting the security control effectiveness score to a strength metric \(\rho\).

<table>
<thead>
<tr>
<th>Score Characteristic</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Administrative</td>
<td>Administrative/technical</td>
<td>Technical/administrative</td>
<td>Technical</td>
</tr>
<tr>
<td>Prescriptive</td>
<td>Logging only/observation</td>
<td>Automation/monitoring</td>
<td>Live threat intelligence</td>
<td>Machine learning</td>
</tr>
<tr>
<td>Fallibility</td>
<td>Likely</td>
<td>Possible</td>
<td>Unlikely</td>
<td>Impossible</td>
</tr>
<tr>
<td>Agility</td>
<td>Reprogramming</td>
<td>No configuration</td>
<td>Run-time</td>
<td>Self-learning</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Score Characteristic</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Administrative</td>
<td>Administrative/technical</td>
<td>Technical/administrative</td>
<td>Technical</td>
</tr>
<tr>
<td>Prescriptive</td>
<td>Logging only/observation</td>
<td>Automation/monitoring</td>
<td>Live threat intelligence</td>
<td>Machine learning</td>
</tr>
<tr>
<td>Fallibility</td>
<td>Likely</td>
<td>Possible</td>
<td>Unlikely</td>
<td>Impossible</td>
</tr>
<tr>
<td>Agility</td>
<td>Reprogramming</td>
<td>No configuration</td>
<td>Run-time</td>
<td>Self-learning</td>
</tr>
</tbody>
</table>

Figure 11. Control scoring of nodes in \(\tau(A_\pi)\).

<table>
<thead>
<tr>
<th>Score Characteristic</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Administrative</td>
<td>Administrative/technical</td>
<td>Technical/administrative</td>
<td>Technical</td>
</tr>
<tr>
<td>Prescriptive</td>
<td>Logging only/observation</td>
<td>Automation/monitoring</td>
<td>Live threat intelligence</td>
<td>Machine learning</td>
</tr>
<tr>
<td>Fallibility</td>
<td>Likely</td>
<td>Possible</td>
<td>Unlikely</td>
<td>Impossible</td>
</tr>
<tr>
<td>Agility</td>
<td>Reprogramming</td>
<td>No configuration</td>
<td>Run-time</td>
<td>Self-learning</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Score Characteristic</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>Administrative</td>
<td>Administrative/technical</td>
<td>Technical/administrative</td>
<td>Technical</td>
</tr>
<tr>
<td>Prescriptive</td>
<td>Logging only/observation</td>
<td>Automation/monitoring</td>
<td>Live threat intelligence</td>
<td>Machine learning</td>
</tr>
<tr>
<td>Fallibility</td>
<td>Likely</td>
<td>Possible</td>
<td>Unlikely</td>
<td>Impossible</td>
</tr>
<tr>
<td>Agility</td>
<td>Reprogramming</td>
<td>No configuration</td>
<td>Run-time</td>
<td>Self-learning</td>
</tr>
</tbody>
</table>

Figure 12. Control effectiveness score
This research thus defines strength of vector $v$ as:

$$F(S) = \rho(v) = 1 - e^{-\gamma} \quad S \in [0, \infty).$$  

(12)

Table VII presents some calculations applying (11) with (12) including the effectiveness scoring of $\rho(A_{\pi})$.

The next step is to establish a link between strength $\rho(v)$ and a desirable risk metric of $\rho(A)$: the probability for a loss occurrence on asset $A$ along risk vector $v(A)$, referred to as loss probability. Marchini (2008) argues that a Poisson distribution is a discrete probability distribution for the counts of events that occur randomly in a given time interval; a counting process. Consider the discrete random variable $X$ representing losses occurring through $v(A)$; the arrival of these occurrences can be viewed as a counting process as each arrival is independent of each other, and thus has a Poisson distribution. If $\lambda$ is the mean number of observed loss occurrences per day, then the probability of observing $x$ events on a given day is determined by the following distribution function (Mikosch, 2009):

$$p(X = x) = \frac{e^{-\lambda} \lambda^x}{x!} \quad x = 0, 1, 2, 3, \ldots$$  

(13)

It follows that the cumulative distribution function is given by:

$$F(X = x) = \sum_{i=0}^{x} e^{-\lambda} \frac{\lambda^i}{i!}$$  

(14)

By the law of large numbers, if one has $N(t)$ events occurring during time $t$, $\lambda$ is determined through (Mikosch, 2009):

$$\lambda = \frac{N(t)}{t}.$$  

(15)

The positive real number $\lambda$ also happens to be equal to the expected value of $X$ and its variance (Mikosch, 2009):

$$\lambda = E[X] = \text{Var}[X].$$  

(16)

FinCorp Ltd endured 54 loss occurrences over a 30-month period, a mean of 1.8 losses per month, i.e.:

$$\lambda_m = 1.8 \quad \text{loss probability, per month},$$  

(17)

<table>
<thead>
<tr>
<th>$S$</th>
<th>$\rho(v)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>10</td>
<td>0.39</td>
</tr>
<tr>
<td>20</td>
<td>0.63</td>
</tr>
<tr>
<td>30</td>
<td>0.78</td>
</tr>
<tr>
<td>40</td>
<td>0.86</td>
</tr>
<tr>
<td>50</td>
<td>0.92</td>
</tr>
<tr>
<td>100</td>
<td>0.99</td>
</tr>
</tbody>
</table>

Table VII. Samples of conversion between effectiveness and strength scores.

Cybersecurity economics
which by (16) is also the expected value going forward. Then, the following cumulative probability function is obtained (Figure 13).

The trajectory of a cumulative Poisson distribution function resembles that of the cumulative exponential probability distribution; this neighboring similarity will be used to approximate a link between the strength and the mean loss probability \( \lambda \). From (17) \( \lambda_m = 1.8 \) for a month was found, thus a one-day (1/30 of a month) time horizon yields:

\[
\lambda_d = 0.06 \quad \text{loss probability, per day.}
\]  

(18)

By design, the closer to 1 the strength \( p(v) \) moves, the closer to 0 the loss probability moves. The following construct articulates exactly this point, where \( \varepsilon \) is some error adjustment factor:

\[
\lambda_d = 1 - p(v) \cdot \varepsilon.
\]  

(19)

Recall from (12) that \( p(v) = 1 - e^{-\tau S} \). As an adjustment factor is already in place, the scale parameter \( \tau \), one can simply combine (12) and (19):

\[
\lambda_d = e^{-\tau S}.
\]  

(20)

If the effectiveness score of a risk vector and the scale parameter \( \tau \) are determined, these produce an estimator for the mean number of loss occurrences. Conversely, once historical data have been collected, the mean \( \lambda_d \) can be easily computed and the scale parameter \( \tau \) assigned an appropriate value. By rearranging (20), the following is obtained:

\[
\tau = -\frac{\ln(\lambda_d)}{S}.
\]  

(21)

This finalises the heuristic model for the relationship between the strength \( p(v) \) and the mean loss probability \( \lambda_d \). For risk cost calculations, an adjustment of the calculations based on the new scale parameter \( \tau \) is needed. Then one must select a new prospective node, and run new calculations to determine the new losses. Consider an expansion of Table VII with the new knowledge obtained from (18) and (21) to derive the new \( \tau \). In addition, the values

![Cumulative Poisson distribution](image-url)
for the scenarios of adding and subtracting up to two nodes are calculated. From Figure 11, an average effectiveness score of $s = 10$ is inferred. The new calculations are derived from the current situation as highlighted in green, i.e. with $\lambda_d = 0.06$.

4.6 Proposition 2b: the reduction measure is impacting VaR
No quantitative data were collected for this proposition, but the discussion below elaborates logically on the knowledge created so far. To obtain the relevant points in the U-graph of $A_\pi$, Monte Carlo simulations must be run to compute the numbers. This is supported by Cheung and Powell (2012) claiming that the stochastic process of the Monte Carlo method replaces the need to specify the probability distribution. This research assumes that adding a node reduces the loss probability, and conversely, subtracting a node increases it (as per Table VIII). Since only the loss probabilities at various levels of protection are known, this must be translated to loss sizes. Recall from (4) that the direct costs of protecting $A_\pi$ come from four nodes. Consider the two-factor authentication and fraud detection module incurring a cost of £200,000 and £300,000, respectively. These nodes will be used for estimating $\Omega_{A_\pi}$ at various levels. The following steps are executed to obtain graph values (Table IX).

The result from the simulation is illustrated in Figure 14, which incidentally shows that the risk reduction impacts VaR and therefore verifies this proposition. An extract of the simulation results is presented in Table AI.

The risk reduction is impacting VaR as demonstrated in the calculations. The immediate interpretation of the U-graph is that FinCorp Ltd does not currently need to invest more in security as the risk cost would increase; there are presently no better investment choices, and the research has thereby also found the financially optimal investment level.

<table>
<thead>
<tr>
<th>$s$</th>
<th>Initial calculation, $\tau = 0.05$</th>
<th>New calculation, $\tau = 0.07$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\rho(v) = 1 - e^{-s \lambda}$</td>
<td>$\lambda_d = 1 - \rho(v)$</td>
<td>$\rho(v) = 1 - e^{-s \lambda}$</td>
</tr>
<tr>
<td>-2 nodes</td>
<td>20</td>
<td>0.63</td>
</tr>
<tr>
<td>-1 node</td>
<td>30</td>
<td>0.78</td>
</tr>
<tr>
<td>Current</td>
<td>40</td>
<td>0.88</td>
</tr>
<tr>
<td>+1 node</td>
<td>50</td>
<td>0.92</td>
</tr>
<tr>
<td>+2 nodes</td>
<td>60</td>
<td>0.99</td>
</tr>
</tbody>
</table>

Table VIII. Adjustment calculations

<table>
<thead>
<tr>
<th>Step</th>
<th>Activity</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Start with the current strength $S = 40$, which gives an annual mean $\lambda^* = \lambda^* 365 = 21.9$ to be used as input to the Monte Carlo simulation together with the mean and standard deviation for the normal distributed VaR calculation, $\mu = -0.0068%$ and $\sigma = 0.0168%$. The simulation will generate 1,000 simulated values for: Annual loss probability $\lambda^*$. 5% VaR loss for as percentage and value. Expected loss $E[L]$ as value.</td>
</tr>
<tr>
<td>2</td>
<td>Compute mean values of $\lambda^<em>$, VaR and $E[L]$. Verify that mean $\lambda^</em>$ is approximately the same as entered in Step 1. For $S = 40$, also verify that the mean VaR £286,504 and $E[L] = £195,840$ (from 0) to ensure the simulation is reliable</td>
</tr>
<tr>
<td>3</td>
<td>Compute the defence cost. For $S = 40$, it is £1,400,000. For the other levels of $S$, use the cost £200,000 for the first node (both adding and subtracting), and £300,000 for the second node. Note: for simplicity, the indirect cost is assumed to be fixed although in reality it will vary somewhat with adding/subtracting controls</td>
</tr>
<tr>
<td>4</td>
<td>Compute VaR risk cost and expected risk cost for $S = 20, 30, 40, 50$ and 60</td>
</tr>
</tbody>
</table>

Table IX. Process for obtaining values for U-graph
4.7 Proposition 3a: the optimal investment level can be expressed as the minimum risk cost (sum of defence costs and losses) to an asset

Previously it was argued that the convex risk cost function exists for all assets and will form a U-graph. It is also shown that the minimum of this function will correspond to the financially optimal defence level for an asset, as demonstrated above. The approach resembles the model developed by Gordon and Loeb (2006) but expands it by using the U-graph as historical data are used to determine loss probability rather than just assuming it. Gordon and Loeb (2002) and Huang et al. (2008) present approaches that identify the budget, but the strength must also be determined. By applying the approach from this research, a control having a cost within budget and a strength that reaps the most benefit can be identified. Combining models like those developed by Gordon and Loeb (2002) and Huang et al. (2008) with approaches described in this research would therefore reinforce each other in order to verify this.

5. Discussion

This research articulates an easily deployable approach to convey an organisation’s risk posture in a continuous manner to top management. Through its scientific basis, it should therefore be considered more reliable as a decision support tool than the prevalent “fear, uncertainty, and doubt (FUD) strategy” (Brecht and Nowey, 2012, p. 2) used to sell...
investments in cybersecurity. This study has employed a combination of qualitative and quantitative techniques to expand the understanding of this topic.

$P1a$–$P1d$ demonstrated how defence costs can be determined and categorised as direct and indirect. Defence costs can also be shared and categorised according to the ISMS-layers approach (Brecht and Nowey, 2012) to prepare for a more realistic cost picture. Cost of damages and losses can be divided into short-term and long-term to prepare for loss calculations. The research has thus shown how cost of damages and losses can be categorised and by knowing both the defence cost and the correlated losses, the risk cost of an asset is determined. The risk cost function will for all assets be convex and form a U-graph. The findings and logical reasoning support existing knowledge. This answers $RQ1$.

The risk vector framework was established to aid in visualising and exploring the effectiveness of security controls. Through the control effectiveness scoring scheme, the characteristics of a security control is quantified a correlated to loss probability for an asset. By applying the collected data to the proposed Monte Carlo simulation, it is demonstrated how the adding (or subtracting) of a security control to the risk vector impacts VaR and will generate a U-graph. The research has shown how the loss probability of an asset can be measured by the characteristics of the security controls protecting it. The findings and logical reasoning are connecting existing knowledge from different areas, creating a synthesis that expands the knowledge obtained from the literature review. This answers $RQ2$.

The use of Monte Carlo simulation to generate U-graphs can be used as a generic method to identify the minimum of the U-graph by adding or subtracting security controls until it is located. As both defence costs and future losses are considered, this minimum will correspond to the financially optimal defence level for an asset. Conclusively, the logical reasoning is connecting existing knowledge from different areas, creating a synthesis that expands the knowledge obtained from existing literature. This answers $RQ3$.

To summarise, this research has demonstrated how to categorise information security costs; direct and indirect defence costs and losses. Direct costs can be identified through their dependency on one or more, but not all, assets. Otherwise, defence cost is regarded as indirect. It is also found that defence costs can be shared. For direct costs, this can be done between assets that are collectively being protected by a control, whereas indirect costs can be evenly distributed between all assets. By knowing both the defence cost and correlated losses, the risk cost of an asset is determined. The risk cost function will for all assets be convex and form a U-graph. The minimum of this function will correspond to the financially optimal defence level for an asset, obtained through calculating VaR for various scenarios. It has further been shown how loss probabilities of an asset can be measured through the controls’ characteristics, linked to a strength score and adjusted by actual data. The risk amendment following the addition or subtraction of new controls in the risk vector is impacting VaR, which is demonstrated in the calculations and the U-graph. Finally, this research has shown that an organisation can balance its operational security spending by using the U-graph, so it supports the business leadership in making informed decisions on whether the defence spending is enough, too much or too little in protecting assets.

6. Conclusion
The research has verified and demonstrated how organisations can determine the optimal investment level in protecting assets, and the case study has been used as a verification of the theories articulated. By means of a multi-disciplinary scientific approach, the paper provides guidance to leading business practitioners to assist them with decision making on cybersecurity. The approach can be integrated with existing risk management practices and strengthen business-case discussions and cybersecurity-related communication with top management. By the adoption of this approach, an organisation can balance its operational security spending.
The limitations of the research include a modest number of loss observations from one case study, and the use of normal probability distribution. These areas should undergo further research including larger data set of losses and exploring other probability distributions. Furthermore, the approach has limitations where there are no historical data available or the data have zero losses. Future research should therefore investigate how to integrate very low probability events with devastating impact.

References


Further reading


### Cybersecurity economics

#### Appendix

<table>
<thead>
<tr>
<th>Run</th>
<th>dt(y)</th>
<th>VaR month</th>
<th>VaR month %</th>
<th>VaR year</th>
<th>VaR year %</th>
<th>$H_L$</th>
<th>No. of simulation runs</th>
<th>Mean VaR year %</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\lambda = 0.24/-2$ node</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>91.42</td>
<td>261,600</td>
<td>-0.109</td>
<td>907,200</td>
<td>-0.378</td>
<td>866,058</td>
<td></td>
<td>89.32</td>
</tr>
<tr>
<td>1</td>
<td>87.42</td>
<td>230,400</td>
<td>-0.096</td>
<td>799,200</td>
<td>-0.333</td>
<td>647,586</td>
<td></td>
<td>238.848</td>
</tr>
<tr>
<td>2</td>
<td>89.42</td>
<td>240,000</td>
<td>-0.055</td>
<td>830,400</td>
<td>-0.346</td>
<td>674,565</td>
<td></td>
<td>-0.0995</td>
</tr>
<tr>
<td>3</td>
<td>91.92</td>
<td>249,600</td>
<td>-0.104</td>
<td>864,000</td>
<td>-0.36</td>
<td>659,558</td>
<td></td>
<td>827.256</td>
</tr>
<tr>
<td>4</td>
<td>83.08</td>
<td>225,600</td>
<td>-0.094</td>
<td>782,400</td>
<td>-0.326</td>
<td>608,581</td>
<td></td>
<td>-0.3447</td>
</tr>
<tr>
<td>5</td>
<td>87.92</td>
<td>222,800</td>
<td>-0.057</td>
<td>806,400</td>
<td>-0.336</td>
<td>645,161</td>
<td></td>
<td>658.380</td>
</tr>
<tr>
<td>6</td>
<td>88</td>
<td>235,200</td>
<td>-0.088</td>
<td>813,600</td>
<td>-0.329</td>
<td>653,118</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>88.25</td>
<td>240,000</td>
<td>-0.1</td>
<td>830,400</td>
<td>-0.346</td>
<td>653,918</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>90.83</td>
<td>249,600</td>
<td>-0.104</td>
<td>864,000</td>
<td>-0.36</td>
<td>670,633</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>89.75</td>
<td>242,400</td>
<td>-0.101</td>
<td>840,000</td>
<td>-0.35</td>
<td>664,841</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>86.08</td>
<td>223,200</td>
<td>-0.093</td>
<td>772,800</td>
<td>-0.322</td>
<td>636,782</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$\lambda = 0.12/-1$ node</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>48.25</td>
<td>141,600</td>
<td>-0.059</td>
<td>489,600</td>
<td>-0.204</td>
<td>331,424</td>
<td></td>
<td>43.74</td>
</tr>
<tr>
<td>1</td>
<td>43.67</td>
<td>129,600</td>
<td>-0.054</td>
<td>448,800</td>
<td>-0.187</td>
<td>322,090</td>
<td></td>
<td>127.296</td>
</tr>
<tr>
<td>2</td>
<td>45.75</td>
<td>132,000</td>
<td>-0.055</td>
<td>458,400</td>
<td>-0.191</td>
<td>323,079</td>
<td></td>
<td>-0.0230</td>
</tr>
<tr>
<td>3</td>
<td>42</td>
<td>124,800</td>
<td>-0.052</td>
<td>432,000</td>
<td>-0.18</td>
<td>314,727</td>
<td></td>
<td>441.192</td>
</tr>
<tr>
<td>4</td>
<td>45.17</td>
<td>129,600</td>
<td>-0.054</td>
<td>448,800</td>
<td>-0.187</td>
<td>323,896</td>
<td></td>
<td>-0.1838</td>
</tr>
<tr>
<td>5</td>
<td>45.42</td>
<td>132,000</td>
<td>-0.055</td>
<td>458,400</td>
<td>-0.191</td>
<td>324,565</td>
<td></td>
<td>324.097</td>
</tr>
<tr>
<td>6</td>
<td>44.17</td>
<td>129,600</td>
<td>-0.054</td>
<td>448,800</td>
<td>-0.187</td>
<td>345,787</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>43.5</td>
<td>124,800</td>
<td>-0.052</td>
<td>432,000</td>
<td>-0.18</td>
<td>342,080</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>45.75</td>
<td>129,600</td>
<td>-0.054</td>
<td>448,800</td>
<td>-0.187</td>
<td>344,152</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>49.83</td>
<td>120,000</td>
<td>-0.05</td>
<td>415,200</td>
<td>-0.173</td>
<td>308,502</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>43.67</td>
<td>122,400</td>
<td>-0.051</td>
<td>424,800</td>
<td>-0.177</td>
<td>314,700</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$\lambda = 0.06/current$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>22.67</td>
<td>72,000</td>
<td>-0.03</td>
<td>249,600</td>
<td>-0.104</td>
<td>156,737</td>
<td></td>
<td>21.87</td>
</tr>
<tr>
<td>1</td>
<td>23</td>
<td>69,600</td>
<td>-0.029</td>
<td>240,000</td>
<td>-0.1</td>
<td>143,268</td>
<td></td>
<td>70.680</td>
</tr>
<tr>
<td>2</td>
<td>21.75</td>
<td>64,800</td>
<td>-0.027</td>
<td>225,600</td>
<td>-0.094</td>
<td>177,715</td>
<td></td>
<td>-0.0295</td>
</tr>
<tr>
<td>3</td>
<td>19.92</td>
<td>64,800</td>
<td>-0.027</td>
<td>225,600</td>
<td>-0.094</td>
<td>157,021</td>
<td></td>
<td>244.464</td>
</tr>
<tr>
<td>4</td>
<td>24.58</td>
<td>76,800</td>
<td>-0.032</td>
<td>266,400</td>
<td>-0.111</td>
<td>171,338</td>
<td></td>
<td>-0.1019</td>
</tr>
<tr>
<td>5</td>
<td>20.75</td>
<td>64,800</td>
<td>-0.027</td>
<td>225,600</td>
<td>-0.094</td>
<td>164,337</td>
<td></td>
<td>163.460</td>
</tr>
<tr>
<td>6</td>
<td>23.33</td>
<td>74,400</td>
<td>-0.031</td>
<td>256,800</td>
<td>-0.107</td>
<td>160,603</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>21.92</td>
<td>72,000</td>
<td>-0.03</td>
<td>249,600</td>
<td>-0.104</td>
<td>153,439</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>18.67</td>
<td>62,400</td>
<td>-0.026</td>
<td>216,000</td>
<td>-0.09</td>
<td>176,444</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>17.75</td>
<td>57,600</td>
<td>-0.024</td>
<td>199,200</td>
<td>-0.083</td>
<td>162,013</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>22.87</td>
<td>76,800</td>
<td>-0.032</td>
<td>266,400</td>
<td>-0.111</td>
<td>168,829</td>
<td></td>
<td></td>
</tr>
<tr>
<td>$\lambda = 0.03/-1$ node</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>12.87</td>
<td>60,000</td>
<td>-0.025</td>
<td>208,800</td>
<td>-0.087</td>
<td>77,173</td>
<td></td>
<td>10.98</td>
</tr>
<tr>
<td>1</td>
<td>10.85</td>
<td>40,800</td>
<td>-0.017</td>
<td>141,600</td>
<td>-0.059</td>
<td>72,171</td>
<td></td>
<td>42.984</td>
</tr>
<tr>
<td>2</td>
<td>10.52</td>
<td>45,600</td>
<td>-0.019</td>
<td>158,400</td>
<td>-0.066</td>
<td>79,716</td>
<td></td>
<td>-0.01791</td>
</tr>
<tr>
<td>3</td>
<td>11.83</td>
<td>50,400</td>
<td>-0.021</td>
<td>175,200</td>
<td>-0.073</td>
<td>67,200</td>
<td></td>
<td>148.992</td>
</tr>
<tr>
<td>4</td>
<td>11.35</td>
<td>43,200</td>
<td>-0.018</td>
<td>148,800</td>
<td>-0.062</td>
<td>79,990</td>
<td></td>
<td>-0.06208</td>
</tr>
<tr>
<td>5</td>
<td>10.33</td>
<td>45,600</td>
<td>-0.019</td>
<td>158,400</td>
<td>-0.066</td>
<td>81,538</td>
<td></td>
<td>80.902</td>
</tr>
<tr>
<td>6</td>
<td>10.93</td>
<td>45,600</td>
<td>-0.019</td>
<td>158,400</td>
<td>-0.066</td>
<td>81,199</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>10.59</td>
<td>40,800</td>
<td>-0.017</td>
<td>141,600</td>
<td>-0.059</td>
<td>84,569</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table AI. Result tables from Monte Carlo simulation

(continued)
### Table AI

<table>
<thead>
<tr>
<th>Run</th>
<th>$\lambda(y)$</th>
<th>VaR month</th>
<th>VaR month %</th>
<th>VaR year</th>
<th>VaR year %</th>
<th>$E[L]$</th>
<th>No. of simulation runs</th>
<th>1,000</th>
</tr>
</thead>
<tbody>
<tr>
<td>8</td>
<td>11.43</td>
<td>45,600</td>
<td>-0.019</td>
<td>158,400</td>
<td>-0.066</td>
<td>74,118</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>11.01</td>
<td>40,800</td>
<td>-0.017</td>
<td>141,800</td>
<td>-0.059</td>
<td>81,237</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>12.16</td>
<td>50,400</td>
<td>-0.021</td>
<td>175,200</td>
<td>-0.073</td>
<td>85,279</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

$\lambda = 0.01/4.2$ nodes

<table>
<thead>
<tr>
<th>Run</th>
<th>$\lambda(y)$</th>
<th>VaR month</th>
<th>VaR month %</th>
<th>VaR year</th>
<th>VaR year %</th>
<th>$E[L]$</th>
<th>Mean $\lambda$</th>
<th>3.59</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>3</td>
<td>14,400</td>
<td>-0.006</td>
<td>50,400</td>
<td>-0.021</td>
<td>26,750</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>3.42</td>
<td>16,800</td>
<td>-0.007</td>
<td>57,600</td>
<td>-0.024</td>
<td>22,156</td>
<td>Mean VaR month</td>
<td>17.400</td>
</tr>
<tr>
<td>2</td>
<td>3.58</td>
<td>16,800</td>
<td>-0.007</td>
<td>57,600</td>
<td>-0.024</td>
<td>27,619</td>
<td>Mean VaR month %</td>
<td>-0.00725</td>
</tr>
<tr>
<td>3</td>
<td>3.33</td>
<td>16,800</td>
<td>-0.007</td>
<td>57,600</td>
<td>-0.024</td>
<td>22,984</td>
<td>Mean VaR year</td>
<td>60.240</td>
</tr>
<tr>
<td>4</td>
<td>3.5</td>
<td>16,800</td>
<td>-0.007</td>
<td>57,600</td>
<td>-0.024</td>
<td>12,457</td>
<td>Mean VaR year %</td>
<td>-0.0251</td>
</tr>
<tr>
<td>5</td>
<td>3.5</td>
<td>16,800</td>
<td>-0.007</td>
<td>57,600</td>
<td>-0.024</td>
<td>31,243</td>
<td>$E[L]$</td>
<td>27.192</td>
</tr>
<tr>
<td>6</td>
<td>3.08</td>
<td>16,800</td>
<td>-0.007</td>
<td>57,600</td>
<td>-0.024</td>
<td>29,150</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>2.38</td>
<td>12,000</td>
<td>-0.005</td>
<td>40,800</td>
<td>-0.017</td>
<td>27,422</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>3.67</td>
<td>19,200</td>
<td>-0.008</td>
<td>67,200</td>
<td>-0.028</td>
<td>23,095</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>4.42</td>
<td>19,200</td>
<td>-0.008</td>
<td>67,200</td>
<td>-0.028</td>
<td>28,769</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>3.33</td>
<td>14,400</td>
<td>-0.006</td>
<td>50,400</td>
<td>-0.021</td>
<td>17,740</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Notes:** 1,000 runs were conducted, and the mean numbers are calculated based on this. For brevity, only the first ten rows are displayed.

---

**Corresponding author**

Zilia Iskoujina can be contacted at: ac2729@coventry.ac.uk

---

For instructions on how to order reprints of this article, please visit our website: www.emeraldgrouppublishing.com/licensing/reprints.htm

Or contact us for further details: permissions@emeraldinsight.com
Preserving over 100 years of management research online

A lifetime investment for your institution, Emerald Backfiles will significantly enhance your library’s offering by providing access to over 125,000 articles from more than 260 journals dating back to 1898.

Visit emeraldinsight.com

Get Backfiles Collections for your library
Recommend Backfiles to your librarian today.
Find out more: emeraldpublishing.com/backfilescollections
Over 160,000 articles from more than 300 journals by end of 2017, Emerald eJournals combine research rigour with practical relevance to showcase the most relevant topics from the leading thinkers within their field.

Visit emeraldinsight.com

Get eJournal Collections for your library

Recommend eJournals to your librarian today.
Find out more: emeraldpublishing.com/eJournalcollections
Information Technology & People

Number 5
Cybercrimes prevention: promising organisational practices
Guest Editors: Mahmood Hussain Shah, Paul Jones and Jyoti Choudrie

1125 Guest editorial
1130 Solutions for counteracting human deception in social engineering attacks
Curtis C. Campbell
1153 Prevention of cybercrimes in smart cities of India: from a citizen’s perspective
Sheshadri Chatterjee, Arpan Kumar Kar, Yogesh K. Dwivedi and Hatice Kizgin
1184 Preventing identity theft: identifying major barriers to knowledge-sharing in online retail organisations
Abdulah Mailo, Nisreen Ameen, Hamid Reza Peikari and Mahmood Shah
1215 Crime and social media
Simplice Asongu, Jacinta Nwachukwu, Stella-Maris Orim and Chris Pyke
1234 Shoplifting in mobile checkout settings: cybercrime in retail stores
John A. Aloysius, Ankur Arora and Viswanath Venkatesh
1262 Organizational practices as antecedents of the information security management performance: an empirical investigation
Daniel Pérez-González, Sara Trigueros Preciado and Pedro Solana-González
1276 Online social network security awareness: mass interpersonal persuasion using a Facebook app
Ehinome Ikhalia, Alan Serrano, David Bell and Panos Louvieris
1301 The effect of cybercrime on open innovation policies in technology firms
Vanessa Ratten
1318 Cybersecurity economics – balancing operational security spending
Stale Ekelund and Zilia Iskoujina


www.emeraldinsight.com/loi/itp