Being digital to being vulnerable: does digital transformation allure a data breach?

Santhosh Srinivas and Huigang Liang
The University of Memphis, Memphis, Tennessee, USA

Received 26 August 2022
Revised 8 October 2022
Accepted 8 October 2022

Abstract

Purpose – While every firm is striving to embrace digital transformation (DT) to form new differentiating business capabilities, there are dark sides to such initiatives, and it is essential to acknowledge, identify and address them. The purpose of this paper is to identify and emperically demonstrate the impact of such darksides of DT. While a firm's DT effort may have many dark sides, the authors identify data breaches as the most critical one and focus on proving their impact since it can inflict significant damage to the firm.

Design/methodology/approach – Through the lens of paradox theory, the authors argue that the DT efforts of a firm will lead to increased risk and severity of data breaches. The authors developed a one-of-a-kind longitudinal data set by combining data from multiple sources, including 3604 brands over a 10-year period, and employed a DT performance scorecard to evaluate a firm's DT effort across four key digital selling touchpoints: site, mobile, digital marketing and social media.

Findings – The findings of this study show that a firm's DT efforts pertaining to its mobile and digital marketing platforms significantly increase the likelihood and severity of a data breach event indicating that these two channels are most vulnerable and need heightened attention from firms. Furthermore, the findings suggest that the negative repercussions of some DT initiatives may be minimized as the firm becomes more innovative. The findings can help firms re-strategize their DT efforts by promoting security and also encouraging a balanced communication strategy.

Originality/value – This research is one of the first to identify, recognize and empirically illustrate the downsides of a DT effort that is otherwise thought to provide only benefits.

Keywords Digital transformation, Digital IQ, Data breach

Paper type Research paper

> There are downsides to everything; there are unintended consequences to everything, Steve Jobs, 2003.

Introduction

Almost every firm in recent time has had to face the challenge of digital transformation (DT), and DT has become essential to survive today's turbulent business environment. A firm's DT effort reflects its commitment to delivering high-quality services internally and externally. Firms that are slow or fail to adopt new technologies and are not able to implement DT successfully will be left behind, losing the edge to competitors. Although there are numerous definitions of DT, the most holistic definition with business as a focal point is from Fitzgerald, Kruschwitz, Bonnet, and Welch (2014), and they define DT as "The use of new digital technologies (social media, mobile,

The authors would like to thank Dr. Cheng Yi for her helpful comments.

Journal of Electronic Business & Digital Economics
Vol. 1 No. 1/2, 2022
pp. 111-137
Emerald Publishing Limited
e-ISSN: 2754-4222
p-ISSN: 2754-4214
DOI 10.1108/JEBDE-08-2022-0026

analytics or embedded devices) to enable major business improvements (such as enhancing customer experience, streamlining operations or creating new business models)". According to IDC, a top market research firm, 65% of global GDP will be digitized and almost $6.8 trillion will be expended on DT investments by 2022 (IDC, 2020), to attain digitization that helps them offer an enhanced experience and automation-backed solutions.

Against this backdrop, every firm is actively attempting to make DT a critical component of their business plan to run effectively; 87% of senior business executives feel that digitalization/DT is a corporate priority (Wiles, 2019) and is a critical component of any firm's long-term aim. Organizations across sectors are speeding up DT for long-term growth and profitability (Gartner, 2020b), and DT is thought to help managers exploit and explore businesses' resources, which is necessary for organizational agility (Lee, Sambamurthy, Lim, & Wei, 2015). It also allows for increased production, cost savings and innovation (Hess, Matt, Benlian, & Wiesböck, 2016).

Although DT provides undeniable advantages and helps firms to become more technologically and strategically powerful, it comes at a cost. According to Grover and Kohli (2013), a firm's digital endeavors using micro-applications might "show its hand" to rivals eroding its competitiveness and leading it to lose its advantage, or generating an unforeseen effect. In the quest to become digitally capable, firms may lose their competitive advantage if they divulge too much information via IoT. Vial (2019) has coherently aggregated and highlighted the trends in DT research efforts to date, stating that organizations use digital technologies to alter the value creation paths they have historically relied on to remain competitive and that these changes result in both positive and *unintended consequences* for organizations.

While DT efforts may include digitization and digitalization to maximize efficiency and improve business processes, DT efforts also include adapting/implementing new products that affect the external audience as well as dealing with operational and organizational structure changes that affect internal actors such as employees (Clohessy, Acton, & Morgan, 2017). While new technologies have an influence on internal actors via digital processes like inventory monitoring, project management systems, supply chain management systems and internal communication channels, firms' usage of new commodities, technology and digital platforms influences external actors.

DT activities that affect external actors, particularly customers, are of strategic significance and may potentially have a greater influence on business performance. We term this customer-centric DT (CCDT). CCDT merits special attention since it has a direct impact on customer experiences and, as a result, the firm's income. The primary goal of any DT effort is to engage digital consumers at all touchpoints in the customer service lifecycle (Solis & Littleton, 2014); hence, it is critical to investigate DT activities at all touchpoints where businesses interact with digital customers. The CCDT initiatives have an influence on the touchpoints where businesses encounter digital clients to supply services and/or interact. These tools often include a company's website, an app (stand-alone or mobile), and a communication strategy (digital marketing & social media).

The digital touchpoints are critical in driving the firm's technology and communication strategy and are required for the firm's existence. Consider the site performance of a firm. As the initial point of contact, the website shows the firm's commitment to a client, guaranteeing that the consumer may view/search/buy at the lowest feasible search cost (Galletta, Henry, McCoy, & Polak, 2006). It also plays a vital part in developing a trusted connection between clients and consumers. Another critical mode of operations for firms in the last decade is going mobile. A mobile platform allows customers to get the same service from anywhere. A mobile channel is critical in today's business environment since more than half of internet traffic buying occurs from mobile devices (Clement, 2021), and is expected to exceed 432 billion US dollars in the US by 2022 (Coppola, 2021). While the firm's website and mobile

platform are vital in providing services and serving as a bridge between internal and external players, the firm's ability to communicate is as important in its survival strategy. DT's digital marketing immediately engages customers, enabling more effective advertising, a shorter communication bridge and simpler inquiries. The topic on digital transmission would be incomplete without including social media strategy since the effectiveness with which a firm presents itself on social media platforms is a crucial aspect of DT. In an era in which consumers follow a brand on social media to stay abreast of new products and services, successful social media use may present a positive image of the business in the eyes of customers, therefore enhancing firm performance.

A DT effort may have unintended consequences in the form of excessive information dissemination leading to a loss of competitive advantage in the market (digital marketing and social media), revealing vital system and security information on social channels, making an existing system vulnerable in the course of a DT effort, etc. This accidental over-distribution of confidential information combined with vulnerable systems may have a direct impact on the firm's security by either encouraging hackers to attack or assisting them in breaching the firm's digital resources.

In today's digital world, data breaches are one of the most significant challenges that a company confronts. Whether a firm loses customer or client data, it is certain to harm the firm's reputation and financial performance. Organizations have deliberately allocated resources to prevent and respond to data breaches. A 2020 report from the privacy rights clearinghouse (PRC, 2020) states that 300,562,519 individuals were affected, and the average ransomware payout was greater than $233,000 per event in Q4 of 2020. Data breaches affect the world so much that President Joe Biden signed an executive order on May 12, 2021, after several recent cyber-attacks. For instance, Colonial Pipeline, one of the biggest pipeline operators in the US was a victim of a cyber-breach attack in May 2021, affecting gas delivery across the nation and warranted an all-of-government response (Sanger, Krauss, & Perlroth, 2021). Such occurrences are so regular that they have become the new "normal"; hence, we must examine the reasons of a possible data breach from a vantage point from which we would normally be ignorant.

A recent report sheds light on the lifecycle of a hacking incident and states "hackers may want to use a social engineering path and swindle a corporate login and a password from an employee. For this reason, they will research a firm's structure, email addresses, and operational facts. Based on this information, the attacker will be able to impersonate a corporate IT specialist and request employee credentials via a fake email." A malicious actor has only limited avenues to begin scavenging for any clues or information that can aid him/her find a flaw in the system. The most prominent and easily accessible channels to gather information are the firm's site, social media, mobile, and marketing efforts all of which form CCDT. Thus, while CCDT boosts customer experience by enabling effective customer interactions, search channels, and information exchange, it might also make firms more vulnerable to data breaches.

Are firms paying the price for DT in unanticipated ways? Will a badly designed website or mobile application resulting from the DT initiative invite hackers to locate a backdoor into the organization's system? Will increasing a firm's digital marketing activities entice hackers to initiate hacking? These considerations inspired us to investigate if a firm's CCDT initiatives influence the likelihood and severity of data breaches. This study's research question is: Can CCDT result in a data breach, and if so, would a greater level of CCDT result in a more severe data breach? In this research, we adopt a paradoxical stance to emphasize the dark side of CCDT and examine its implications on firms' susceptibility to security breaches.

While there is no existing metric for CCDT, any impact on all digital touchpoints in the customer lifecycle, such as social media, analytics, cloud, mobile application and the Internet

of Things (IoT), comprise the main elements of DT (Sebastian *et al.*, 2020)Sebastian *et al.*, 2020, and a scorecard that includes the performance score of all these elements would reflect CCDT. The digital IQ (DIQ) index from Gartner is an example of a digital scorecard designed to quantify the CCDT efforts of firms across all touchpoints. DIQ evaluates the digital activities of consumer brands and serves as a trusted metric for over 14,000 businesses in over 100 countries (Gartner, 2020a). In this study, DIQ is used as a proxy for CCDT, and further information regarding DIQ is presented in the Methodology section.

The rest of the paper is organized as follows. We first review existing work on DT and data breaches. We then discuss our research model and hypotheses. Following that, we describe data collection, measurement and analytical approaches in the Methodology section. After reporting the results, we conclude with a discussion on the research and practical implications.

Literature review

Digital transformation

There is a multitude of work on DT, and several attempts have been made to find the influence of DT on modern-day industry and society. Existing research on the operationalization of DT reveals that DT is mirrored in those aspects of technology that influence how firms supply services and connect with clients. A recent review (Vial, 2019) of DT research shows that the composition of most digital technologies fits the SMACIT (Sebastian *et al.*, 2020) acronym, including social (Li, Su, Zhang, & Mao, 2018; Oestreicher-Singer & Zalmanson, 2013), mobile (Hanelt *et al.*, 2015; Pousttchi, Tilson, Lyytinen, & Hufenbach, 2015), analytics (Dürr, Wagner, Weitzel, & Beimborn, 2017), cloud (Clohessy *et al.*, 2017; Du, Pan, & Huang, 2016) and the IoT (Petrikina *et al.*, 2017; Richter, Vodanovich, Steinhüser, & Hannola, 2017). We believe that these factors determine the key dimensions of DT and have an impact on all touch points where the firm interacts with digital clients. Vial (2019) emphasizes the trends in DT research and advocates for greater study to better understand the unintended consequences of DT. While existing research on DT is diverse and focuses on all aspects of an organization, such as identifying the need for DT, antecedents of DT and the impact of DT on an organization, we are particularly interested in studies that have acknowledged and/or identified undesirable outcomes from a DT effort. The research examines 19 current studies on "unintended consequences" and groups the existing work into three categories: *define, design and determine*.

While *define* studies focus on the conceptualization of DT (Fitzgerald *et al.*, 2014; Hess *et al.*, 2016; Horlacher, Klarner, & Hess, 2016; Westerman, Calméjane, Bonnet, Ferraris, & McAfee, 2011), studies in the *design* stream guide users with framework management (Benjamin & Levinson, 1993; Gimpel *et al.*, 2018; Küng, 2017; Muehlburger, Rueckel, & Koch, 2019; Sarvari, Ustundag, Cevikcan, Kaya, & Cebi, 2018; Schallmo, Williams, & Boardman, 2020; Sehlin, Truedsson, & Cronemyr, 2019), ROI (Carcary, Doherty, & Conway, 2016; Parviainen, Tihinen, Kääriäinen, & Teppola, 2017; Zinder & Yunatova, 2016), implementation challenges (Henriette, Feki, & Boughzala, 2016) and execution strategy (Chanias & Hess, 2016; Chanias, Myers, & Hess, 2019; Hansen & Sia, 2015; Matt, Hess, & Benlian, 2015; Schallmo *et al.*, 2020; Sebastian *et al.*, 2020).

Determine studies on the other hand, appear to hold the most significant proportion of work on DT, trying to determine the importance and impact of DT across various domains (manufacturing, banking, retail, etc.), specific departments (human resources, customer relationship) and specific roles (CEO/CDO). We are highlighting studies that are aligned with the SMACIT attributes to assert the relevance and impact of DT along the SMACIT facet, vis-à-vis, social (Berman, 2012), analytics (Gastaldi & Corso, 2012; Piccinini, Gregory, & Kolbe, 2015), internet technologies (Berman, 2012; Liu, Li, & Yang, 2012; Piccinini *et al.*, 2015;

Rothmann & Koch, 2014), digitization (Belk, 2013; Gastaldi & Corso, 2012; Liu *et al.*, 2012; Rothmann & Koch, 2014), innovation (Nambisan, Wright, & Feldman, 2019; Prem, 2015), customer relationship (Berman, 2012; Piccinini *et al.*, 2015), marketing (Berman, 2012; Piccinini *et al.*, 2015) and brand promotion (Melović, Jocović, Dabić, Vulić, & Dudic, 2020). While DT has been extensively examined in these three streams, *determine* phase studies fail to highlight the dark side of DT except for a few who acknowledge the undesired outcomes. No existing study has put effort to reveal and examine the ill effects of DT, as the prominent focus seems to be only on the positive impact of DT on a firm.

Data breaches

A data breach is the intentional or unintentional release of secure or private/confidential information to an untrusted environment. Other terms for this phenomenon include unintentional information disclosure, data leak, information leakage and data spill (Goode, Hoehle, Venkatesh, & Brown, 2017; Cheng, Liu, & Yao, 2017). The number of data breach incidents in businesses has increased from 785 incidents in 2015 to 1108 incidents in 2020, with a total of 300,562,519 records exposed (ITRC, 2021a). Data breaches are becoming more frequent and causing more serious damage to firms. For example, it is estimated that every 11 seconds a business will fall victim to a cyber-threat by 2021 (Morgan, 2019), and firms are paying an average of $3.86 million per incident (IBM, 2020). An assessment (See Table 1) of data breach incidents from The Identity Theft Resource Center (ITRC, 2021b), a nonprofit organization, tracking security breaches since 2005 reveals that an astounding 720.41 million records have been exposed so far.

We conducted an in-depth analysis of the current research on data breach occurrences. The majority of research appears to focus on determining the source and impact of data breaches under the premise that only "faulty" actions may result in a data breach. Following a comprehensive study of current research, we divided them into two primary categories: impact and causality.

Impact studies tried to see the impact of data breach events on firms, vis-à-vis, abnormal stock volatility (Tweneboah-Koduah, Atsu, & Prasad, 2020), abnormal returns (Ali, Lai, Hassan, & Shad, 2021; Cavusoglu, Mishra, & Raghunathan, 2004; Garg, Curtis, & Halper, 2003), stock price fluctuations (Schatz & Bashroush, 2016), market value erosion (Acquisti, Friedman, & Telang, 2006; Cavusoglu *et al.*, 2004; Goel & Shawky, 2009), penalty (Liu, Han, Wang, & Zhou, 2018), reputation (Gwebu, Wang, & Wang, 2018; Kannan, Rees, & Sridhar, 2007; Sinanaj, Muntermann, & Cziesla, 2015; Syed, 2019), shareholder value (Gatzlaff & McCullough, 2010) to name a few. The objective of *causal* studies seems to determine the factors that may contribute to a data breach, such as lack of security measures (Manworren, Letwat, & Daily, 2016; Romanosky, 2016), corporate governance, and social responsibility (Lending, Minnick, & Schorno, 2018), miscellaneous error and insider misuse (Cheng *et al.*, 2017), human/software incompetence (Cheng *et al.*, 2017), theft (Wikina, 2014), hacker prestige (Mello, 2018), human vulnerabilities (Hong & Linden, 2012) and in the likes of these.

Data breaches impacted a variety of industries and businesses, making it to be "the new normal" causing financial harm along with privacy concerns for employees and customers (Culnan & Williams, 2009). However, existing research that aimed to find causes for the breach has all assumed a "fault" perspective, implying that data breaches occur because of firms' "wrong" or "faulty" moves. No study has tried to see if a "right" move caused a breach event. A "right" move, in this context, is a DT effort by the firm, which is often perceived to provide only immense advantages, but paradoxically results in data leaks. We feel this intriguing occurrence may be better understood via the lens of paradox theory, as will be detailed in the next section.

Table 1.
Summary of ITRC breach data from 2010 to 2020

Breach category	Breach type: Electronic Sum[#]	Electronic Count[##]	Not recorded Sum[#]	Not recorded Count[##]	Paper data Sum[#]	Paper data Count[##]	Total Sum[#]	Total Count[##]
Banking/credit/financial	100,761,933	191	11,988,114	388	–	5	112,750,047	584
Business	21,616,192	1,207	276,216,619	2,458	91,211	23	297,924,022	3,688
Educational	3,620,339	157	8,183,061	523	–	–	11,803,400	680
Government/military	4,055,430	167	81,470,278	478	15,125	12	85,540,833	657
Medical/healthcare	49,263,229	895	162,656,660	1,919	472,112	167	212,392,001	2,981
Grand total	179,317,123	2,617	540,514,732	5,766	578,448	207	720,410,303	8,590

Note(s): #Number of records breached
##Sum of records breached

Theoretical foundation

The process of designing and aiding a business that disseminates information effectively via DT creates an unintended consequence of the same information being exploited, creating, what we term as "Digital Transformation Paradox" (DTP). A DTP is a quagmire event where firms put efforts into digitization and digitalization which in turn augments vulnerabilities in the system, creating a need for more DT. Consider a firm that integrates new technology to enable more sophisticated interactions such as a chatbot. While the chatbot introduction was a technological augmentation, it brings with it an additional channel for a data breach, like what happened to Delta airlines (Stupp, 2019). This tension in turn demands another addition to the existing site's design/security, thereby creating a DTP. While the cyclical events may sound "normal" for a business, what we wish to highlight is the fact that firms need to be aware of the paradoxical events that a DT causes and re-strategize every move of theirs.

A firm's preoccupation with a single goal (DT) leads to organizational simplicity and may bring security/information obliviousness and threaten success. Elsass (1993) notes that the same practices that lead organizations in becoming successful often simultaneously push them to a downfall. Can the best practices followed over and over again via DT lead to downfall? We seek to unveil the unintended consequence of DT through a paradoxical lens. Paradox theory has guided organizational theory for decades and has enabled researchers and practitioners to solve a variety of conundrums. Lewis (2000) defines paradox as "contradictory yet interrelated elements – elements that seem logical in isolation but absurd and irrational when appearing simultaneously". The unintended consequence of DT and data breaches may appear logical in isolation but is perplexing when appearing simultaneously. The paradox perspective has the potential to address interwoven organizational challenges (Lewis & Smith, 2014) and can aid a firm to accept and reconcile the tension that it generates via unintended consequences (abundant information leading to data breaches).

Paradox theory has been thus far applied to solve *puzzles* between dual concepts such as innovation and change (Bledow, Frese, Anderson, Erez, & Farr, 2009), cooperation and competition (Raza-Ullah, Bengtsson, & Kock, 2014), social and business (Smith, Gonin, & Besharov, 2013), stability and change (Audia, Locke, & Smith, 2000; Farjoun, 2010), exploration and exploitation (Andriopoulos & Lewis, 2009; Raisch & Birkinshaw, 2008), growth and corruption (Forde, 2013), learning and performance (Van Der Vegt & Bunderson, 2005) and some individual firm tensions such as technological innovation (Jarvenpaa & Wernick, 2011), people management (Zhang, Waldman, Han, & Li, 2015), product innovation (Atuahene-Gima, 2005; Jay, 2013; Tse, 2013), leadership (Schad, Lewis, Raisch, & Smith, 2016), ambidexterity (Raisch & Birkinshaw, 2008; Raisch, Birkinshaw, Probst, & Tushman, 2009) and corporate attribute such as management (Lewis & Smith, 2014). We believe that a paradoxical lens helps to understand the entanglement that a DT's dark side brings. To the best of our knowledge, a paradoxical view of the DT efforts of a firm is a novel attempt and has not been thought of before.

Research model and hypotheses

Our study objective is two-fold. First, we test if the CCDT efforts of the firm affect the risk of a data breach in terms of the likelihood of happening. Second, we see if it impacts the severity of a breach event (once it happens). Every firm that has been a victim of a data breach and regulatory guidelines suggest one of the measures of severity of the breach is the "number of records" breached (Federal Trade Commission 2019). The number of records breached often indicates the number of people affected and the damages relatively. Hence, we choose the number of records as measure of severity.

We now propose a research model (Figure 1). Considering that CCDT, as measured by DIQ, encompasses four dimensions (social media, site and commerce, mobile and digital

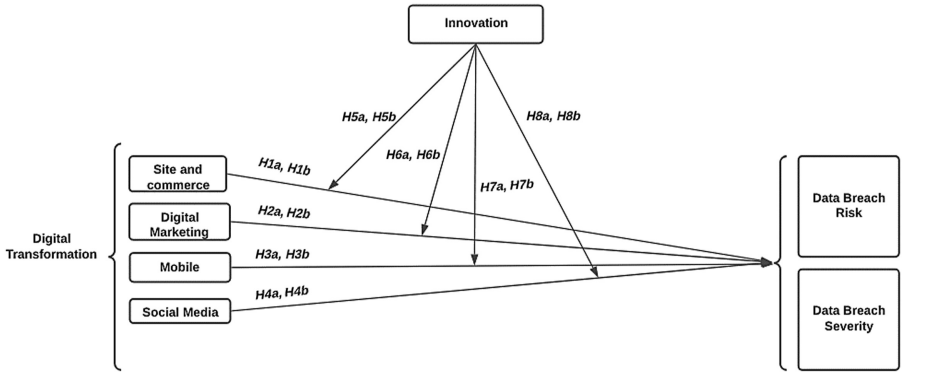

Figure 1.
Research model

marketing), we believe each dimension affects data breach likelihood and severity. While there is no existing theory to justify the four dimensions of Digit IQ, they represent a solid industry standard to benchmark digital competence of firms and carry a lot of practical relevance. Therefore, we believe it is worth proposing a separate hypothesis for each DIQ dimension. Furthermore, we believe that these effects are moderated by the innovativeness of the firm. We control for firm variables such as Revenue, Goodwill and Acquisitions since we believe that having a good financial performance always comes with a sacrifice and that the firm performance indicators impact the likelihood and severity of a breach event.

Firms in the race to increase website traffic and conversion rate inevitably focus on functions, aesthetics and other user experiences. The increased alignment toward the aesthetics may not be paid off given that 92% of all visits to a website do not end with product purchases (Episerver, 2017). DT involves the integration and augmentation of various site technologies which in turn create more vulnerability that could be exploited by hackers. Any firm that has not made adequate efforts to secure the site or to prevent the hack is likely to be breached. Further technological integration and improvement increases not only the risk of vulnerabilities but also the avenues to reach more digitized data (depending on the type of vulnerabilities and channels that it impacts). Hence in an event of a breach, hackers have more avenues to reach the digitized data thereby affecting the severity of a breach event.

For instance, in March 2017, Equifax was initially hacked via a consumer complaint web portal losing hundreds of millions of customer records. Attackers used a widely known vulnerability that should have been patched in their site. Consider another example, in May 2019, a security flaw in First American's website led to a data breach that exposed nearly 885 million records which included personally identifiable information (KrebsOnSecurity, 2019). The company admitted the reason for the breach was a "design defect". A 2019 security report found that 47% of all hacked websites contained at least one backdoor, and a whopping 12 million websites are currently hacked or infected (Martens, 2021) with an average of 30,000 websites being hacked every day (Sophos, 2012). Thus, if firms only focus on the functional aspects and overlook the security of the website, the more efforts firms put into digitizing their websites, the more likely they are to be hacked and the more serious the consequences will be once a data breach occurs. With that, we develop the following hypotheses.

H1a. A firm's DT on site and commerce increases the likelihood of a data breach event.

H1b. A firm's DT on site and commerce increases the severity of its data breach.

Digital marketing is a firm's effort to promote its product or services on a digital platform and is believed to bring enormous benefits such as brand and relationship equity (Rust, Lemon, & Narayandas, 2005), firm value (McAlister, Sonnier, & Shively, 2012) and sales (Kumar, Bezawada, Rishika, Janakiraman, & Kannan, 2016). In a digital marketing effort, data forms a crucial part because firms can then utilize this data to customize and target users. Users seem to support this customization effort, 61% of Americans said that they rather receive personalized offers than restrict firms from accessing their data (Koetsier, 2018). Many of the vulnerabilities that threaten a data breach originate from marketing-related technologies used by marketers to build a digital relationship (Greenlow, 2019) increasing the likelihood of breach event, and hence firms need to focus on security while executing a digital marketing strategy, failing which will ensure security and privacy issues (Sinansoft, 2018; Tellefsen, 2020). Givens (2020) asserts that not only do marketers rely on customer data to personalize their marketing, but they also pull from more sources than ever. The average data sources used in digital marketing went from 8 to 10 in 2020 and are expected to grow to 12 in 2021, suggesting that in an event of a breach, digital marketing can affect the amount of information leaked.

Privacy and data breach concerns emanating from digital marketing have been on everyone's focus for quite some time, and studies have called for more research to empirically test the cost of digital marketing on a firm (Ashworth & Free, 2006). We hypothesize that a digital effort in marketing as part of DT impacts both the probability and severity of a data breach occurrence.

H2a. A firm's DT in digital marketing increases the likelihood of a data breach event.

H2b. A firm's DT in digital marketing increases the severity of its data breach.

There are about 5.19 billion mobile users as of 2020, and while the mobile platform is becoming increasingly popular, so are the vulnerabilities. While chasing revenues, firms are increasingly compromising on security, leading to numerous data breaches. According to Verizon's 2021 report, one in every three organizations were victims of data breaches involving mobile devices (Constantin, 2019), and one of the reasons believed to cause this is that firms are not meeting bare minimum mobile security standards. The report indicates that 'Almost half of the respondents admitted that their organizations sacrificed mobile security to get the job done faster and nearly half of those that cut corners experienced a mobile-related security compromise'. Along with compromised security, fake and malicious apps are also on surge in recent times augmenting data breach incidents. A 2019 McAfee mobile threat report shows that nearly 65,000 fake apps were detected (McAfee, 2019), while an average of 10000+ harmful apps were blocked by Symantec each in 2018 (Symantec, 2019).

In this race to go mobile, firms may be compromising on the security aspect because as of 2019 more than half of the web traffic is on mobile (Clement, 2021) and firms are investing billions of dollars to keep the mobile platform at the top of the selling strategy. On January 15, 2020, Walgreens was notified of an error within its mobile app. It was determined that an internal application error caused personal information viewable by other customers (O'Donnell, 2020). Such incidents flag the fact that firms are increasingly placing less importance on security and more on creating their presence on the mobile platform. While mobile channels increase vulnerabilities, they also enable more channels for hackers to ultimately get access to larger data stockpiles. We propose that firms' DT efforts on mobile platform affects the data breach likelihood and severity.

H3a. A firm's DT on mobile increases the likelihood of a data breach event.

H3b. A firm's DT on mobile increases the severity of its data breach.

There are about 3.6 billion social media users and are expected to grow to about 4.4 by 2025. Firms are placing heightened priority on social media in recent times because 57% of customers are following a brand to keep up to date with new products and services, and as much as 47% will stay up to date by following the company news (Marketingcharts, 2020). Social media facilitates the rapid dissemination of information and allows the accelerated spread and coalescence of interpretive frameworks that make sense of that information (Berthon, Pitt, Plangger, & Shapiro, 2012). Social media marketing aids customer communications on a firm's website or through its social media presence (Chaffey, 2011). While it is unknown if a data breach of a firm had anything to do with social media usage, it can be assumed that the amount of information that is available on social media can have a profound effect on data breach possibility and severity, either because of abundant information availability or the increased possibility of social engineering via social media connections. While more research is needed to see how social media security incidents lead to a data breach, a study finds that 22% of social media users have fallen victim to a security-related incident (Samani & Davis, 2019).

The magnitude of presence on social media seems to be a strong influencer of the likelihood and severity of a data breach because it allows a malicious actor to impersonate and reach an insider to gain unauthorized access. Social media probably do not exacerbate technological vulnerabilities, but they can facilitate social engineering that may lead to unauthorized access to the whole system. The extent of data loss (severity) may be determined by the level of system access or system-related information that has been compromised due to social media. A recent incident took place on LinkedIn where attackers were impersonated to steal users' login credentials. LinkedIn an open letter (Lynch, 2021) warned with a statement that said: "LinkedIn connection requests from individuals impersonating employees from your organization want to build trust using the LinkedIn connection and then eventually collect more sensitive information about you and your organization and/or have you click a link that will download malware onto your computer". We hypothesize that social media might have a role in the probability and severity of data breaches, leading to the following hypothesis.

H4a. A firm's DT on social media increases the likelihood of a data breach event.

H4b. A firm's DT on social media increases the severity of its data breach.

Innovation plays an important role in how firms handle communications, digital strategy or security. Numerous studies have found that innovation impacts firms' very survival (Christensen, Suarez, & Utterback, 1998), this is because innovation makes firms more agile and proactive to changes and tensions in the business. It is also seen that innovation drives organizational renewal by exploiting and exploring its competencies (Danneels, 2002) and aids firms to adapt to changes in markets, technology and competition (Dougherty & Hardy, 1996) and hence an innovative firm will naturally handle the strategies in technology and communication better than the less innovative firm's (Christensen *et al.*, 1998).

Thus, one can argue that highly innovative companies are less likely to reveal sensitive information to the outside world because of their mindset on a competitive and secure digital strategy. Innovative firms understand the importance of the informational assets they possess. They spend tremendous resources on creating innovations, and the last thing they want is their hard-earned intellectual property to be stolen due to careless information spillover. Therefore, they would make every effort to safeguard information assets. Their innate information security awareness will be reflected in their DT efforts. Compared with less innovative peers, innovative firms may spend more effort in censoring information before it can be published on the website, used in digital marketing, released on mobile platforms or disseminated on social media. Based on this logic, we propose that innovation

moderates the relationship between each domain of a firm's DT (site and commerce, digital marketing, mobile and social) and the likelihood of getting a data breach so that the relationship is weaker when innovativeness is high. We propose the same moderation for the severity of the breach too.

H5a, H6a, H7a and H8a. The innovativeness of a firm negatively moderates the relationship between each domain of a firm's DT (site and commerce, digital marketing, mobile and social) and the likelihood of getting a data breach, so the relationship is weaker when innovativeness is high.

H5b, H6b, H7b and H8b. The innovativeness of a firm negatively moderates the relationship between each domain of a firm's DT (site and commerce, digital marketing, mobile and social) and the severity of a data breach so the relationship is weaker when innovativeness is high.

Methodology

Data sources

We use secondary archival data to test the hypotheses. Table 2 provides an overview of the measures of variables and the data sources. Following recommendations from prior research (Cram, Karan, & Stuart, 2009), we integrated multiple sources of data to measure independent and dependent variables. We first collected the list of publicly disclosed data breaches from three reliable sources: Privacy Rights Clearing House (PRC), Identity Theft Resource Center (ITRC) and Verizon DBIR. All three data breach sources comprised various types of hacks that

Variable	Measure/Definition	Source
Digital IQ	A firm's digital transformation effort. It is measured by four indexes: site and commerce, digital marketing, mobile and social	Digital IQ Index from Gartner
Firm Innovativeness	Number of citations received for the patent that a firm holds	Patentsview.org
Data Breach Risk	Security incident in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an individual unauthorized to do so	Privacy Rights Clearing House (PRC), ID Theft Center, and Verizon DBIR
Data Breach Severity	The number of records that were exposed during a specific data breach	Privacy Rights Clearing House (PRC), ID Theft Center and Verizon DBIR
Revenue	Cash and cash equivalents refer to the line item on the balance sheet that reports the value of a company's assets that are cash or can be converted into cash immediately	Compustat
Good Will	Goodwill is the value assigned to the name of a business, client relationship, employee morale and other related factors assumed to increase the earnings potential of the business	Compustat
Acquisitions	An acquisition cost also referred to as the cost of acquisition, is the total cost that a company recognizes on its books for property or equipment after adjusting for discounts, incentives, closing costs, and other necessary expenditures, but before sales taxes	Compustat

Table 2.
Summary of measures for all variables in the model

were classified as either online hacks (hacks to the server, website, database, etc.) or offline hacks (Hard drive stolen, paper hack, etc.). We evaluated data breaches that were only digital (online). We obtained the list of patents filed and associated data from Patentsview.org to measure the innovativeness of a firm. The digital IQ scorecard data were retrieved from Gartner (Gartner, 2021b) to measure CCDT. The data for control variables were obtained from the Compustat database. All of the data from different sources are matched based on firm ID and year to form panel data. Our final data cover 3604 brands over a 10-year timespan (2011-2020).

Measures

CCDT: A scorecard that quantifies the CCDT efforts should measure an organization's ability to use and profit from technological solutions (Ricard, 2020). Several companies survey senior executives and rate the firm's CCDT on several dimensions. The most notable ones are from Gartner (Gartner, 2021a) and PWC (PricewaterhouseCoopers, 2021). We use Gartner's DIQ scorecard as a surrogate for the CCDT efforts of a firm. The data contains a quantified DIQ score for four dimensions: site and commerce, mobile, social and digital marketing, for firms in a variety of industries such as retail, financial, FMCG, hospitality, auto, industrial and fashion and several others. Gartner's Digital IQ index ranks brands on their overall digitization efforts, with Genius as the highest designation. It is a definitive benchmark for online competence which measures more than 1,250 data points across four dimensions of digital, diagnosing their digital strengths. Each point represents the firm's performance on chosen dimension in the respective domain. A brief description (L2 ThinkTank, 2014) of all four dimensions is as follows.

(1) *Site and commerce*: This dimension has been ranked on the Effectiveness of brand site embedding technology, load time, analytics, video integration, visitor action prompts, speed, search and navigation, aesthetics, messaging and visuals of a site the likes of these attributes.

(2) *Digital marketing*: Digital marketing dimension has been rated on performance points such as search, blog, display, SEO/SEM, traffic, email marketing efforts, web authority, sentiment and brand buzz.

(3) *Mobile:* Mobile dimension includes factors like compatibility, mobile android applications and iOS Ranked rated on availability, popularity and functionality. Marketing on smartphones and tablets, smartphone features (compatibility, UI/UX optimization and responsiveness) and mobile (includes SEO/SEM and localization).

(4) *Social media*: Social media dimension has brand presence, community size, content and engagement on Facebook (likes, annual growth, custom tabs, apps,

Variable	Observations	Mean	Std. Dev	Min	Max
diq_site	10,635.00	14.80	6.30	–	34.50
diq_mobile	10,635.00	8.20	4.90	–	25.30
diq_marketing	10,635.00	13.30	5.40	–	38.90
diq_social	10,635.00	6.90	4.30	–	28.00
NumofRecords	9,705.00	51,504.00	2,265,985.00	–	150,000,000.00
PatCite	10,635.00	10.50	181.10	–	8,776.00
lggw	10,635.00	0.60	2.00	–	11.90
log_rev	10,635.00	1.10	2.90	–	13.20
lgacq	10,614.00	1.20	0.80	0.60	10.50

Note(s): Lggw = Log of Goodwill
Log_rev = Log of Revenue
Lgacq = Log of Acquisitions

Table 3.
Descriptive summary of dependent and independent variables

responsiveness and engagement), YouTube (Search visibility, channel experience, video news and the virality of content), Twitter (followers, Growth, frequency), Instagram (presence, community size and engagement), emerging social media (Pinterest, Google, Tumblr and Vine).

Data breach: We collected data breach information for all firms in the digital IQ data (from the previous step) from the following three sources: IDtheftcenter.org, a non-profit organization established to empower and guide consumers, victims, businesses and the government to minimize risk and mitigate the impact of identity compromise and crime (ITRC, 2021b), Privacy Rights Clearinghouse, a non-profit organization that offers consumer information and advocacy programs. Its mission is to engage, educate and empower individuals to protect their privacy (PRC, 2020), and Verizon's Data Breach Investigations Report (Verizon, 2021) provides an annual analysis of security incidents and data breaches categorized by sector. These sources have been used for quantifying data breaches in numerous studies (Alliance, 2015; Boos, Givens, & Larry, 2015; Downing & Geller, 2012; Seymour & Tully, 2018).

Innovation: Past literature has widely used the number of patents filed by a company as a proxy for measuring innovation (Acs, Anselin, & Varga, 2002; Arora & Gambardella, 1994; Griliches, 1998). Although there are other ways to measure innovativeness such as scientific publications, patent information and R&D expenditure, our study required timestamps as the crux of innovation data and as our study required long time series, we chose patents as a proxy for innovation (Dodgson & Hinze, 2000). In addition, the purpose of our research is to examine the link between "innovativeness" and the predicted association, irrespective of the "kind" of innovativeness. Hence, patent data were considered apt for this scenario. In the patent data, we use the citations received by the focal firm from other patent applications as the main data because the length of the patent citation period can dramatically change the picture of the innovativeness measure and they can also indicate the radicalness of innovation (Katila, 2000).

Control variables: Firm variables Revenue, Goodwill and Acquisition score were collected from Compustat.

Method

A descriptive summary of dependent and independent variables (IVs) is available in Table 3. The Total Revenue, Acquisitions and Goodwill scores were transformed into logarithms.

Our study is two-fold. We test the effects of IVs on the risk (likelihood) of a data breach (risk model) and the severity of a data breach when it happens (severity model). We employed two classes of nonlinear estimators, the binary outcome model, and the count-data model. In this binary model (Risk), a dummy variable indicated if a firm has had a breach event or not (1 = Yes, 0 = No). In the count data model, the dependent variable is the number of records breached when a breach event occurred.

The risk model is a firm-specific logit regression (xtlogit) in which we show the probability that a firm gets breached, and the severity model is a negative binomial model (xtnbreg) because the numbers of breached records are over-dispersed (Cameron and Trivedi, 1998). We use Stata to carry out the analysis. The general model is expressed as

$$y_{it} = \alpha_i + \mathbf{x}'_{it}\beta + \varepsilon_{it}$$

where y_{it} denotes a data breach event for a firm i in year t, $\mathbf{x}_{it}$ matrix of predictors, α_i is the unobserved random or fixed effect specific to the i-th subject, and ε_{it} is independent noise.

When we consider the logit firm-specific model with which we show the probability that a firm will get breached. The binary model specifies that

$$\Pr\left(y = 1 | x, \beta, \alpha\right) = \Lambda\left(\alpha + x^{'}\beta\right)$$

where α_i may be a fixed effect (FE) or random effect (RE) and $\Lambda(z) = e^z (1+e^z)$.

We could specify either FE or RE while performing logistic regression. Although the majority of studies use FE models (either because of its default or because the Hausman test suggests so), a preferred model of statistics should be chosen based on the sampling frame. Is the sampling frame fixed to a particular sample? Or is it from a large population sampled at random? The answer to these questions should aid the choice (Bell & Jones, 2015). A recent study assesses the choice decision and highlights the importance of RE over the FE model. It asserts RE may be a better choice for most studies (Bell, Fairbrother, & Jones, 2019), and that the Hausman test is generally misleading. In our study, the brands are very diverse and come from a variety of sectors. DT is usually in various shapes and magnitudes across firms. The DIQ dimensions vary over time dynamically; hence, the RE is appropriate for the logistic regression.

Our regression models also control for several firm-level characteristics that could impact the likelihood of a breach or the severity when it happens. We control for revenue and goodwill as it is believed that hackers target profitable and reputable firms and these firms are always the bigger target. for number of acquistions by a firm as it is believed that companies that go through mergers and acquisitions are at increased possibility of a security breach, as highlighted in Verizon's 2011 Business Breach Research Report (Verizon, 2021) that documented 761 major IT breaches, about 20% of which involved companies going through a merger or an acquisition (Lohrke, Frownfelter-Lohrke, & Ketchen, 2016).

In the analytic model, we regress data breaches on Digital IQ in the same year because Digital IQ is calculated based on the firm's DT performance of the previous year. Hence, a DIQ score of one year would not reflect the DIQ efforts of the same year and would be for the previous year. This temporal separation helps to mitigate the concern for reverse causation.

The variance of the records breached was bigger than the mean, indicating overdispersion, suggesting Poisson regression is not suitable. The Pearson goodness-of-fit test results confirm that the distribution of the number of records breached significantly differs for a Poisson distribution ($p < 0.01$). Hence, we performed a negative binomial regression to test the effect of DIQ on the number of records breached. We applied the Huber/White/sandwich VCE estimator to calculate robust errors for the regression coefficients.

Results

Risk model

Main effects: The results for the risk model (likelihood of a breach event) are reported in Table 4. Column 5 reports the results with *diq_site, diq_mobile, diq_marketing and diq_social* as a measure of DT, and *Patcite* as a measure of innovation. The coefficients on diq_mobile (H3a) ($\beta = 0.082$, $p < 0.01$) and diq_marketing (H2a) ($\beta = 0.035$, $p < 0.05$) are significantly positive. This suggests that firms with more mobile channels and digital marketing activities are more likely to have a data breach.

The coefficient on variables *diq_site* and *diq_social* (H1a and H4a) is not statistically significant, indicating that an increase in these variables may not increase the likelihood of a breach event for the respective firm. It appears that the firm's website and social media may not be the first target of hackers as they focus on more vulnerable mobile and digital marketing platforms. This could also be because the site and social media are relatively more mature and older technologies, and firms may have been using reliable systems with less vulnerability. Using the logit coefficients from the results the logistic regression equation is as below.

$$log(p/1-p) = -5.52 + 0.002^{*}PatCite + 0.082^{*}diq\_mobile + 0.035 * diq\_marketing$$

Interaction effects: We run two sets of tests for interaction effects. We first run the full model with all four interactions included (Column 5). To see if each of the main variables interacts with innovation individually, we re-run the analysis with only one interaction at a time (Columns 1 through 4 in Table 4). Supporting H5a, innovation moderates the DIQ site score with a negative coefficient, indicating a firm with increased innovativeness is likely to secure its website. Innovative firms seem to manage security and the amount of information revealed on their site, causing a decreased likelihood of a breach. We also tested each interaction separately as shown in Columns 1–4. The results in Column 1 confirm our main findings that DIQ site and innovation do have significant interaction. Although DIQ mobile seems to interact with innovation, its significance disappears in the full model (Column 5). This disappearance of significance might be because "Mobile" technology as a concept was a consequence of firms trying to be innovative over the last decade and hence all firms that use mobile as part of their services are all at the same innovation level. In other words, mobile probably does not construe innovation anymore. Therefore, H7a is partially supported. Since the interactions between DIQ marketing/social and innovation are not significant either in the full model or in the separate models, H6a and H8a are not supported.

Severity model

Main effects: The results for the severity model are reported in Table 5. Similar to the logistic model results, the coefficients on diq_mobile ($\beta = 0.074$, $p < 0.001$) and diq_marketing ($\beta = 0.056$, $p < 0.01$) are positive, indicating that diq_mobile and diq_marketing significantly affect the severity (along with likelihood) of a data breach. For a one-unit change in the diq_mobile and diq_marketing scores, the rate for the number of records breached is expected to increase with a factor of 1.079 ($e^{0.074}$) and 1.057 ($e^{0.056}$), respectively, given the other predictors in the model are held constant.

Because mobile and marketing channels hold a significant amount of information as compared to site and social channels, these two channels make large amounts of information available that could be exploited. Firms are increasingly collecting exponentially more customer data in digital marketing to offer customization and mobile is increasingly popular than a traditional site, the amount of information available in these two channels will augment the number of records breached in case of a security breach event. In contrast, firms' site and social media do not seem to affect the severity of the breach event.

Interaction effects: We wished to see if the main variables of DT affect the severity of breach when innovation interacts individually, we run both a full model and separate analysis with only one interaction at a time, and the results are shown in Table 5. The main effects appear the same as in all the models. Interestingly when introduced individually, innovation seems to moderate the relationship between digital marketing and the severity of the breach ($\beta = -0.0003$, $p < 0.05$), meaning that a more innovative firm will manage its digital marketing better in case of a data breach. These firms reveal less information as compared to less innovative firms. Table 6 summarizes the results of all hypothesis testing.

Discussion

In this study, we examined the relationship between DT and data breach possibility along with the severity of a data breach. We proposed that DT will affect a data breach's likelihood and severity. We also proposed that innovation will moderate the relationship between DT and data breaches. We utilized the DIQ scorecard as a proxy to measure DT and patent info to measure innovation. Our results indicate that a firm's marketing and mobile performance in a DT effort can increase the likelihood of a breach event as well as increase the severity of the

Table 4.
Panel logistic regression results (risk model)

	(1)	(2)	(3)	(4)	(5)
diq_site	1.76E−02 (1.32)	1.55E−02 (1.17)	1.46E−02 (1.1)	1.51E−02 (1.15)	2.75E−03 (1.30)
diq_mobile	7.91E−02**** (5.6)	8.25E−02**** (5.8)	7.87E−02**** (5.59)	7.91E−02**** (5.63)	8.18E−02**** (5.71)
diq_marketing	3.90E−02*** (2.52)	3.93E−02** (2.54)	4.08E−02*** (2.63)	3.96E−02** (2.57)	3.71E−02** (2.38)
diq_social	−1.57E−02 (−0.85)	−1.49E−02 (−0.82)	−1.68E−02 (−0.92)	−1.39E−02 (−0.77)	−1.33E−02 (−0.73)
PatCite	2.74E−03*** (3.2)	2.39E−03 (2.68)	1.25E−03 (0.99)	1.49E−03 (1.33)	2.75E−03 (1.46)
PatCite*diq_site	−8.79E−05*** (−2.89)				−7.76E−05** (−2.00)
PatCite*diq_mobile		−1.37E−04* (−1.87)			−9.32E−05 (−0.98)
PatCite*diq_marketing			−2.83E−05 (−0.59)		6.20E−05 (0.95)
PatCite*social				−1.21E−04 (−1.01)	−5.35E−05 (−0.65)
log_rev	2.46E−01**** (7.1)	2.52E−01**** (7.43)	2.54E−01**** (7.53)	2.56E−01**** (7.67)	2.49E−01**** (7.2)
lggw	−8.33E−02* (−1.74)	−8.76E−02* (−1.87)	−9.69E−02* (−2.09)	−9.92E−02* (−2.15)	−8.35E−02* (−1.74)
lgacq	6.58E−02 (1.02)	6.54E−02 (1.02)	7.49E−02 (1.17)	7.13E−02 (1.12)	6.08E−02 (0.94)

Note(s): ****, ***, ** and * Indicate significance at the 0.001, 0.01, 0.05 and 0.10 levels (two−tailed), respectively
Controlled for revenue, goodwill and acquisitions
Table 4 presents the results of panel logit regressions that examine the relation between DT and breach likelihood
Z values (in parentheses) are reported below the coefficient estimates and are based on robust standard error

Model	(1)	(2)	(3) Negative binomial	(4)	(5)
Dependent Variable	Num of records breached	Num of records breached	Num of records breached	Num of records breached	Num of records breached
diq_site	1.74E−02 (0.96)	1.62E−02 (0.9)	1.34E−02 (0.75)	1.45E−02 (0.81)	1.46E−02 (0.82)
diq_mobile	7.34E−02***** (3.56)	7.82E−02***** (3.79)	7.85E−02***** (3.79)	7.60E−02***** (3.7)	7.85E−02***** (3.82)
diq_marketing	5.52E−02**** (2.68)	5.20E−02** (2.52)	5.16E−02** (2.52)	5.60E−02**** (2.71)	5.26E−02** (2.57)
diq_social	−3.61E−03 (−0.14)	−4.94E−03 (−0.2)	−6.28E−03 (−0.25)	−4.87E−03 (−0.19)	−2.27E−03 (−0.09)
PatCite	5.98E−03 (1.05)	2.85E−03 (1.18)	−7.84E−04 (−0.33)	5.83E−03** (2.13)	1.44E−03 (1.36)
PatCite*diq_site	−2.79E−04 (−0.94)	−1.53E−04 (−1.11)			
PatCite*diq_mobile	1.90E−04 (0.78)		4.46E−05 (0.29)		
PatCite*diq_marketing	−1.73E−04 (−0.96)			−3.10E−04** (−2.00)	
PatCite*social	−3.97E−05 (−0.28)				−2.72E−04 (−1.43)
lgacq	2.82E−01***** (4.98)	2.71E−01***** (4.83)	2.68E−01***** (4.74)	2.72E−01***** (4.84)	2.72E−01***** (4.85)

Note(s): *****, ****, ** and * Indicate significance at the 0.001, 0.01, 0.05 and 0.10 levels (two-tailed), respectively
Controlled for acquisitions
Table 5 presents the results of negative binomial regression that examine the relation between DT and the number of records breached
Z values (in parentheses) are reported below the coefficient estimates and are based on robust standard error

Table 5.
Negative binomial model results (severity model)

breach (measured as the number of records breached) suggesting that firms should focus more on security in a mobile and marketing DT efforts. We further employ different models to see various interactions of innovation with DT dimensions and find interesting results. Innovative firms' mobile and marketing channels behave differently when interacting individually attenuating the effect.

Firms that seem to score high on mobile appear to focus more on creating their presence on mobile platforms and in a race to that goal they seem to ignore the security aspect that may arise on mobile platforms. Firms that score high on digital marketing seem to collect user data abundantly and not do enough to secure them, these firms seem to use digital technologies that are vulnerable to hacking and hence an increased likelihood of breach when they perform well on digital marketing. Recalling Given's report, which highlights marketers' increased use of data sources (Givens, 2020), firms collecting data as part of digital marketing must ensure its safety, failing which will result in a data breach, and the findings of this study are reassuring enough of the alarming situation in digital marketing.

Managerial implications

Managerially, the study intended to help firms carefully chisel their DT efforts to mitigate the risk of data breaches by taking preventive measures while formulating digital strategies. Our results indicate that examining DT from the perspective of the potential risk of a data breach could increase long-term DT success. Despite the enthusiasm, DT is still in its infancy for many firms, especially small- and medium-sized firms. When executing a digital marketing/mobile transformation, some firms have relied excessively on insecure digital platforms and technology, offering hackers the opportunity to gain access. This research demonstrates that the expected advantages of these DT initiatives may paradoxically increase the likelihood and severity of data breaches. In light of this study's conclusions, managers must regularly analyze their DT and make the necessary modifications to handle evolving opportunities and risks.

Theoretical implications

By studying the dark side of DT and empirically studying the effects of DT on data breach risk and severity we contribute to the existing and unchartered territories of DT. We introduce a new dimension in a DT called "Customer-centric digital transformation" to help channel the efforts in DT strategy. This new dimension of DT will aid researchers to focus particularly on CCDT and hopefully develop a deepened and holistic understanding of the consequences of DT.

We also contribute to the paradox theory by demonstrating its applicability in the context of DT. Past security studies have explored the cause and effect of a data breach mostly from a

Table 6. Summary of hypothesis testing results

Hypothesis	Supported (Y/N) Risk model	Severity model
H1 (DT site and commerce)	N	N
H2 (DT digital marketing)	*Y*	*Y*
H3 (DT mobile)	*Y*	*Y*
H4 (DT social media)	N	N
PatCite*social	N	N
PatCite*diq_site	*Y*	N
PatCite*diq_mobile	*Y**	N
PatCite*diq_marketing	N	*Y**

Note(s): * significant in the model with only one interaction

fault perspective, but no study intended to see if a so-called "right" move allured a data breach event or affect its severity. Prior studies on DT had mostly focused on the advantages of DT for a firm and its beneficial effects on its profitability and other financial outcomes; hence, the DT effort of an organization leading to a data breach was unknown so far. Our study integrates and extends the existing literature on DT and the information security literature by highlighting the dark side of DT. We institute a contradictory school of thought by drawing from paradox theory and elucidating the dark side of DT. By highlighting the potential risk of getting breached due to higher digital presence, we draw researchers' attention to the holistic evaluation of DT by considering not only the bright side but also the dark side.

Limitations and future research

We identify several limitations of our work, which might be addressed by future researchers to provide more robust and generalizable findings. First, we were unable to gather data on the company's IT expenditures and monitor their impact. The volume of IT investment could influence the frequency of data breaches, as firms allocate funds to ensure the security of their data and information systems. Second, the quantification of DIQ is restricted to retail, hotel, telecom, FMCG, financial services and pharmaceutical sectors. The findings would be more generalizable if additional industries were included. Third, just four domains are included in DIQ to symbolize customer-centric DT. However, other areas of DT, including cloud computing and the IoT, may also lead to a surge in data breaches. This study's data did not contain these aspects of DT, and we recommend that future studies utilize a more thorough scorecard to quantify DT. Fourth, we used the number of patent citations to measure firm innovation, which may not capture the entire innovativeness of the firm. Other measures such as number of patent applications, R&D inputs and number of R&D personnel could be included to provide a more comprehensive measure. Finally, our sample firms self-selected themselves to obtain DIQ ratings from Gartner, making self-selection bias a concern. In addition, the rigor of our findings could have been strengthened by more robustness checks.

Conclusion

In an era where firms are competing though increasing digitization, it is uncommon for them to realize that the very efforts that are enabling new avenues for profits and modes to connect with the customer are creating new channels/modes/situations for a malicious actor to breach the firm's resources and cause a significant adverse impact. In a managerial sense, the research aids firms in fine-tuning their DT efforts to limit the danger of data breaches by using preventative measures when developing digital plans. Our findings challenge the widely held belief that DT always produces positive results. It is alarming since DT seems to influence both the likelihood and severity of a security breach. Firms must prioritize not just digitizing, but also securing and managing the transparency of their information with extreme care. Firms need a specialized plan to guarantee that information that might be exploited by hackers is not accessible over the internet. In addition, firms must find a balance between the functional aspects of multiple channels such as the website, mobile, and social media and data security. We recommend that businesses put a higher premium on safeguarding the platforms they use to digitize to prevent hacking, and also provide sufficient training to ensure that employees do not fall victim to social engineering and divulge sensitive information on digital platforms. Overall, our study illuminates the darker side of DT, and we anticipate that future research will reveal more aspects of the darker side, including particular initiatives in various channels to assist firms in managing digital transformation.

References

Acquisti, A., Friedman, A., & Telang, R. (2006). Is there a cost to privacy breaches? An event study. in *ICIS 2006 Proceedings* (Vol. 94).

Acs, Z. J., Anselin, L., & Varga, A. (2002). Patents and innovation counts as measures of regional production of new knowledge. *Research Policy*, *31*, 1069–1085.

Ali, S. E. A., Lai, F.-W., Hassan, R., & Shad, M. K. (2021). The long-run impact of information security breach announcements on investors' confidence: The context of efficient market hypothesis. *Sustainability*, *13*, 1066.

Alliance, S .C. (2015). The true cost of data breaches in the payments industry. Technical report, March 2015. *29*, 47.

Andriopoulos, C., & Lewis, M. W. (2009). Exploitation-exploration tensions and organizational ambidexterity: Managing paradoxes of innovation. *Organization Science*, *20*, 696–717.

Arora, A., & Gambardella, A. (1994). The changing technology of technological change: General and abstract knowledge and the division of innovative labour. *Research Policy*, *23*, 523–532.

Ashworth, L., & Free, C. (2006). Marketing dataveillance and digital privacy: Using theories of justice to understand consumers' online privacy concerns. *Journal of Business Ethics*, *67*, 107–123.

Atuahene-Gima, K. (2005). Resolving the capability–rigidity paradox in new product innovation. *Journal of Marketing*, *69*, 61–83.

Audia, P. G., Locke, E. A., & Smith, K. G. (2000). The paradox of success: An archival and a laboratory study of strategic persistence following radical environmental change. *Academy of Management Journal*, *43*, 837–853.

Belk, R. W. (2013). Extended self in a digital world. *Journal of Consumer Research*, *40*, 477–500.

Bell, A., Fairbrother, M., & Jones, K. (2019). Fixed and random effects models: Making an informed choice. *Quality & Quantity*, *53*, 1051–1074.

Bell, A., & Jones, K. (2015). Explaining fixed effects: random effects modeling of time-series crosssectional and panel data. *Political Science Research and Methods*, 133–153.

Benjamin, R. I., & Levinson, E. (1993). A framework for managing IT-enabled change. *Sloan Management Review*, *34*, 23–33.

Berman, S. J. (2012). Digital transformation: opportunities to create new business models. *Strategy and Leadership*, *20*(2), 16–24.

Berthon, P. R., Pitt, L. F., Plangger, K., & Shapiro, D. (2012). Marketing meets Web 2.0, social media, and creative consumers: Implications for international marketing strategy. *Business Horizons*, *55*, 261–271.

Bledow, R., Frese, M., Anderson, N., Erez, M., & Farr, J. (2009). A dialectic perspective on innovation: Conflicting demands, multiple pathways, and ambidexterity. *Industrial and Organizational Psychology*, *2*, 305–337.

Boos, E. S., Givens, C., & Larry, N. (2015). Damages theories in data breach litigation. *Sedona Conference Journal*. HeinOnline, 125.

Cameron, A. C., & Trivedi, P .K. (1998). *Regression analysis of count data, econometric society monographs No. 30*. Cambridge: Cambridge University Press.

Carcary, M., Doherty, E., & Conway, G. (2016). A dynamic capability approach to digital transformation: A focus on key foundational themes. *The European Conference on Information Systems Management* (Vol. 20). Academic Conferences International.

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers. *International Journal of Electronic Commerce*, *9*, 70–104.

Chaffey, D. (2011). *E-Business en e-commerce: Een managementperspectief*. London: Pearson Education.

Chanias, S., & Hess, T. (2016). Understanding digital transformation strategy formation: Insights from Europe's automotive industry. In *PACIS 2016 Proceedings* (pp. 296).

Chanias, S., Myers, M. D., & Hess, T. (2019). Digital transformation strategy making in pre-digital organizations: The case of a financial services provider. *The Journal of Strategic Information Systems*, *28*, 17–33.

Cheng, L., Liu, F., & Yao, D. (2017). Enterprise data breach: Causes, challenges, prevention, and future directions. *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, *7*, e1211.

Christensen, C.M., Suarez, F.F., & Utterback, J. M. (1998). Strategies for survival in fast-changing industries. *Management Science*, *44*, S207–S220.

Clement, J. (2021). Mobile percentage of website traffic 2020. available from: https://www.statista.com/statistics/277125/share-of-website-traffic-coming-from-mobile-devices/#:~:text=Mobile%20accounts%20for%20approximately%20half (accessed 1 June 2021).

Clohessy, T., Acton, T., & Morgan, L. (2017). The impact of cloud-based digital transformation on IT service providers: Evidence from focus groups. *International Journal of Cloud Applications and Computing (IJCAC)*, *7*, 1–19.

Constantin, L. (2019). One in three organizations suffered data breaches due to mobile devices. available from: https://www.csoonline.com/article/3353560/one-in-three-organizations-suffered-data-breaches-due-to-mobile-devices.html (accessed 1 June 2021).

Coppola, D. (2021). Topic: Mobile commerce in the United States. available from: https://www.statista.com/topics/1185/mobile-commerce/#dossierSummary (accessed 31 May 2021).

Cram, D. P., Karan, V., & Stuart, I. (2009). Three threats to validity of choice-based and matched-sample studies in accounting research. *Contemporary Accounting Research*, *26*, 477–516.

Culnan, M. J., & Williams, C. C. (2009). How ethics can enhance organizational privacy: lessons from the choicepoint and TJX data breaches. *Mis Quarterly*, *33*(4), 673–687.

Danneels, E. (2002). The dynamics of product innovation and firm competences. *Strategic Management Journal*, *23*, 1095–1121.

Dodgson, M., & Hinze, S. (2000). Indicators used to measure the innovation process: Defects and possible remedies. *Research Evaluation*, *9*, 101–114.

Dougherty, D., & Hardy, C. (1996). Sustained product innovation in large, mature organizations: Overcoming innovation-to-organization problems. *Academy of Management Journal*, *39*, 1120–1153.

Downing, C. O. Jr, & Geller, E. S. (2012). A goal-setting and feedback intervention to increase ID-checking behavior: An assessment of social validity and behavioral impact. *Journal of Organizational Behavior Management*, *32*, 297–306.

Du, W. D., Pan, S. L., & Huang, J. (2016). How a latecomer company used IT to redeploy slack resources. *MIS Quarterly Executive*, *15*(3), 195–213.

Dürr, S., Wagner, H.-T., Weitzel, T., & Beimborn, D. (2017). Navigating digital innovation-the complementary effect of organizational and knowledge recombination. In *Proceedings of the 13th international conference on Wirtschaftsinformatik*.

Elsass, P. M. (1993). The paradox of success: Too much of a good thing?. *The Academy of Management Perspectives*, *7*, 84.

Episerver (2017). Study: 92 percent of consumers visiting a retailer's website for the first time aren't there to buy. available from: https://www.prnewswire.com/news-releases/study-92-percent-of-consumers-visiting-a-retailers-website-for-the-first-time-arent-there-to-buy-300390086.html (accessed 1 June 2021).

Farjoun, M. (2010). Beyond dualism: Stability and change as a duality. *Academy of Management Review*, *35*, 202–225.

Fitzgerald, M., Kruschwitz, N., Bonnet, D., & Welch, M. (2014). Embracing digital technology: A new strategic imperative. *MIT Sloan Management Review*, *55*, 1.

Forde, B. (2013). Double paradox: rapid growth and rising corruption in China. *The China Journal*, *70*, 256, doi: 10.1086/671288.

Galletta, D. F., Henry, R. M., McCoy, S., & Polak, P. (2006). When the wait isn't so bad: The interacting effects of website delay, familiarity, and breadth. *Information Systems Research*, *17*(1), 20–37.

Garg, A., Curtis, J., & Halper, H. (2003). Quantifying the financial impact of IT security breaches. *Information Management and Computer Security*, *11*(2), 74–83.

Gartner. (2020a). Gartner digital IQ Index. available from: https://www.gartner.com/en/marketing/research/luxury-2021 (accessed 31 May 2021).

Gartner. (2020b). The IT roadmap for digital business transformation. available from: https://www.gartner.com/en/publications/the-it-roadmap-for-digital-business-transformation (accessed 31 May 2021).

Gartner. (2021a). Gartner digital IQ Index benchmarks digital performance relative to peers. available from: http://www.gartner.com/en/marketing/research/digital-iq (accessed 1 June 2021).

Gartner. (2021b). Gartner: Fueling the future of business. available from: https://www.gartner.com/en (accessed 1 June 2021).

Gastaldi, L., & Corso, M. (2012). Smart healthcare digitalization: Using ICT to effectively balance exploration and exploitation within hospitals. *International Journal of Engineering Business Management*, *4*, 4–9.

Gatzlaff, K. M., & McCullough, K. A. (2010). The effect of data breaches on shareholder wealth. *Risk Management and Insurance Review*, *13*, 61–83.

Gimpel, H., Hosseini, S., Huber, R. X. R., Probst, L., Röglinger, M., & Faisst, U. (2018). Structuring digital transformation: A framework of action fields and its application at ZEISS. *Journal of Information Technology Theory and Application*, *19*, 3.

Givens, H. (2020). Marketers need to Be data security pros, too | The 360 blog. available from: https://www.salesforce.com/blog/optimize-data-protect-customer-information (accessed 31 May 2021).

Goel, S., & Shawky, H. A. (2009). Estimating the market impact of security breach announcements on firm values. *Information and Management*, *46*, 404–410.

Goode, S., Hoehle, H., Venkatesh, V., & Brown, S. A. (2017). User compensation as a data breach recovery action: An investigation of the Sony PlayStation network breach. *MIS Quarterly*, *41*(3), 703–727.

Greenlow, M. (2019). Customer data security is a marketing problem, too. available from: https://www.thedrum.com/opinion/2019/04/19/customer-data-security-marketing-problem-too (accessed 1 June 2021).

Griliches, Z. (1998). Patent statistics as economic indicators: a survey. In *R&D and productivity: the econometric evidence* (pp. 287–343). University of Chicago Press.

Grover, V., & Kohli, R. (2013). Revealing your hand: caveats in implementing digital business strategy. *Mis Quarterly*, *37*(2), 655–662.

Gwebu, K. L., Wang, J., & Wang, L. (2018). The role of corporate reputation and crisis response strategies in data breach management. *Journal of Management Information Systems*, *35*, 683–714.

Hanelt, A., Nastjuk, I., Krüp, H., Eisel, M., Ebermann, C., Brauer, B., & Kolbe, L. M. (2015). Disruption on the way? The role of mobile applications for electric vehicle diffusion. In *Wirtschaftsinformatik Proceedings 2015* (pp. 69).

Hansen, R., & Sia, S. K. (2015). Hummel's digital transformation toward omnichannel retailing: Key lessons learned. *MIS Quarterly Executive*, *14*(2), 51–66.

Henriette, E., Feki, M., & Boughzala, I. (2016). Digital transformation challenges. In *MICS Proceedings 2016. Mediterranean Conference on information systems* (pp. 33). AIS.

Hess, T., Matt, C., Benlian, A., & Wiesböck, F. (2016). Options for formulating a digital transformation strategy. *MIS Quarterly Executive*, *15*(2), 123–139.

Hong, J., & Linden, G. (2012). Protecting against data breaches; living with mistakes. *Communications of the ACM*, *55*, 10–11.

Horlacher, A., Klarner, P., & Hess, T. (2016). Crossing boundaries: Organization design parameters surrounding CDOs and their digital transformation activities. In *AMCIS 2016: surfing the IT innovation wave - 22nd Americas conference on information systems*.

IBM. (2020). Cost of a data breach report 2020 | IBM. available from: https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/ (accessed 1 June 2021).

IDC. (2020). IDC reveals 2021 worldwide digital transformation predictions; 65% of global GDP digitalized by 2022, driving over $6.8 trillion of direct DX investments from 2020 to 2023. available from: https://www.idc.com/getdoc.jsp?containerId=prUS46967420#:~:text=The%20economy%20remains%20on%20course,investments%20from%202020%20to%202023 (accessed 31 May 2021).

imdb.com (2003). Steve jobs - IMDb. available from: https://www.imdb.com/name/nm0423418/bio (accessed 1 June 2021).

ITRC. (2021a). Identity Theft resource Center®'s 2020 annual data breach report reveals 19 percent decrease in breaches. available from: https://www.idtheftcenter.org/identity-theft-resource-centers-2020-annual-data-breach-report-reveals-19-percent-decrease-in-breaches/ (accessed 1 June 2021).

ITRC. (2021b). About us. available from: https://www.idtheftcenter.org/about-us/ (accessed 1 June 2021).

Jarvenpaa, S. L., & Wernick, A. (2011). Paradoxical tensions in open innovation networks. *European Journal of Innovation Management*, *14*(4), 521–548.

Jay, J. (2013). Navigating paradox as a mechanism of change and innovation in hybrid organizations. *Academy of Management Journal*, *56*, 137–159.

Kannan, K., Rees, J., & Sridhar, S. (2007). Market reactions to information security breach announcements: An empirical analysis. *International Journal of Electronic Commerce*, *12*, 69–91.

Katila, R. (2000). Using patent data to measure innovation performance. *International Journal of Business Performance Management*, *2*, 180–193.

Koetsier, J. (2018). 61% of Americans will share personal data for personalized marketing communications. available from: https://www.inc.com/john-koetsier/61-of-consumers-will-share-personal-data-for-personalized-marketing-communications.html (accessed 1 June 2021).

KrebsOnSecurity. (2019). First American financial corp. Leaked hundreds of millions of title insurance records — krebs on security. available from: https://krebsonsecurity.com/2019/05/first-american-financial-corp-leaked-hundreds-of-millions-of-title-insurance-records/ (accessed 1 June 2021).

Küng, L. (2017). Digital transformation. The organisational challenge–creating a roadmap for change. *Journalism Report V. Innovation and Transition*, 171–180. available from: http://www.lucykung.com/wp-content/uploads/2018/03/Digital_Transformation_organisational_challenge.pdf.

Kumar, A., Bezawada, R., Rishika, R., Janakiraman, R., & Kannan, P. (2016). From social to sale: The effects of firm-generated content in social media on customer behavior. *Journal of Marketing*, *80*, 7–25.

Lee, O. -K., Sambamurthy, V., Lim, K. H., & Wei, K. K. (2015). How does IT ambidexterity impact organizational agility?. *Information Systems Research*, *26*, 398–417.

Lending, C., Minnick, K., & Schorno, P. J. (2018). Corporate governance, social responsibility, and data breaches. *Financial Review*, *53*, 413–455.

Lewis, M. W. (2000). Exploring paradox: Toward a more comprehensive guide. *Academy of Management Review*, *25*, 760–776.

Lewis, M. W., & Smith, W. K. (2014). Paradox as a metatheoretical perspective: Sharpening the focus and widening the scope. *The Journal of Applied Behavioral Science*, *50*, 127–149.

Li, L., Su, F., Zhang, W., & Mao, J. Y. (2018). Digital transformation by sme entrepreneurs: A capability perspective. *Information Systems Journal*, *28*, 1129–1157.

Liu, D., Li, S., & Yang, T. (2012). Competitive business model in audio-book industry: A case of China. *JSW*, *7*, 33–40.

Liu, L., Han, M., Wang, Y., & Zhou, Y. (2018). Understanding data breach: A visualization aspect. *International Conference on Wireless Algorithms, Systems, and Applications* (pp. 883–892). Springer.

Lohrke, F. T., Frownfelter-Lohrke, C., & Ketchen, D. J. Jr (2016). The role of information technology systems in the performance of mergers and acquisitions. *Business Horizons*, *59*, 7–12.

L2 ThinkTank (2014). Digital IQ Index sportswear 2014. available from: https://www.rankingthebrands.com/PDF/Digital%20IQ%20Index%20Sportswear%202014,%20L2%20ThinkTank.pdf (accessed 1 June 2021).

Lynch, A. (2021). Scam warning: Employees contacted on LinkedIn by fraudulent users. available from: https://www.linkedin.com/pulse/scam-warning-employees-contacted-linkedin-fraudulent-users-lynch/ (accessed 1 June 2021).

Manworren, N., Letwat, J., & Daily, O. (2016). Why you should care about the Target data breach. *Business Horizons*, *59*, 257–266.

Marketingcharts. (2020). Why do people follow brands on social media?. available from: https://www.marketingcharts.com/digital/social-media-113405 (accessed 1 June 2021).

Martens, M. (2021). How do websites get hacked?, sucuri blog. available from: https://blog.sucuri.net/2021/03/how-do-websites-get-hacked.html (accessed 1 June 2021).

Matt, C., Hess, T., & Benlian, A. (2015). Digital transformation strategies. *Business and Information Systems Engineering*, *57*(5), 339–343.

McAfee (2019). McAfee mobile threat report Q1. available from: https://www.mcafee.com/enterprise/en-us/assets/reports/rp-mobile-threat-report-2019.pdf (accessed 31 May 2021).

McAlister, L., Sonnier, G., & Shively, T. (2012). The relationship between online chatter and firm value. *Marketing Letters*, *23*, 1–12.

Mello, S. (2018). Data breaches in higher education institutions. *Honors Theses and Capstones*.

Melović, B., Jocović, M., Dabić, M., Vulić, T. B., & Dudic, B. (2020). The impact of digital transformation and digital marketing on the brand promotion, positioning and electronic business in Montenegro. *Technology in Society*, *63*, 101425.

Morgan, S. (2019). Global ransomware damage costs predicted to reach $20 billion (USD) by 2021. available from: https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-20-billion-usd-by-2021/ (accessed 1 June 2021).

Muehlburger, M., Rueckel, D., & Koch, S. (2019). A framework of factors enabling digital transformation. In *Proceedings of the Americas conference on information systems* (pp. 1–10).

Nambisan, S., Wright, M., & Feldman, M. (2019). The digital transformation of innovation and entrepreneurship: Progress, challenges and key themes. *Research Policy*, *48*, 103773.

Oestreicher-Singer, G., & Zalmanson, L. (2013). Content or community? A digital business strategy for content providers in the social age. *MIS Quarterly*, 591–616.

O'Donnell, L. (2020). Walgreens mobile app leaks prescription data. available from: https://threatpost.com/walgreens-mobile-app-prescription-data/153361/ (accessed 1 June 2021).

Parviainen, P., Tihinen, M., Kääriäinen, J., & Teppola, S. (2017). Tackling the digitalization challenge: How to benefit from digitalization in practice. *International Journal of Information Systems and Project Management*, *5*, 63–77.

Petrikina, J., Krieger, M., Schirmer, I., Stoeckler, N., Saxe, S., & Baldauf, U. (2017). Improving the readiness for change-Addressing information concerns of internal stakeholders in the smartPORT Hamburg. In *AMCIS 2017 proceedings* (pp. 1–10).

Piccinini, E., Gregory, R. W., & Kolbe, L. M. (2015). Changes in the producer-consumer relationship-towards digital transformation. *Changes*, *3*, 1634–1648.

Pousttchi, K., Tilson, D., Lyytinen, K., & Hufenbach, Y. (2015). Introduction to the special issue on mobile commerce: mobile commerce research yesterday, today, tomorrow—what remains to be done?. *International Journal of Electronic Commerce*, *19*(4), 1–20, Taylor & Francis.

PRC. (2020). Data breaches | Privacy rights clearinghouse. available from: https://privacyrights.org/data-breaches (accessed 1 June 2021).

Prem, E. (2015). A digital transformation business model for innovation. ISPIM Innovation Symposium. *The International Society for Professional Innovation Management (ISPIM)*, *1*(11), available from: https://www.proquest.com/openview/aafe571adc2facc4b7653ec460ab5e6d/1?pq-origsite5gscholar&cbl52040562.

PricewaterhouseCoopers (2021). 2020 PwC global digital IQ. Buckle up. Uncertainty is back. available from: http://www.pwc.com/us/en/library/digital-iq.html (accessed 1 Jun 2021).

Raisch, S., & Birkinshaw, J. (2008). Organizational ambidexterity: Antecedents, outcomes, and moderators. *Journal of Management*, *34*, 375–409.

Raisch, S., Birkinshaw, J., Probst, G., & Tushman, M. L. (2009). Organizational ambidexterity: Balancing exploitation and exploration for sustained performance. *Organization Science*, *20*, 685–695.

Raza-Ullah, T., Bengtsson, M., & Kock, S. (2014). The coopetition paradox and tension in coopetition at multiple levels. *Industrial Marketing Management*, *43*, 189–198.

Ricard, S. (2020). Improve your company's digital IQ for digital transformation success. available from: https://www.cmswire.com/learning-development/improve-your-companys-digital-iq-for-digital-transformation-success/ (accessed 1 June 2021).

Richter, A., Vodanovich, S., Steinhüser, M., & Hannola, L. (2017). IT on the shop floor-challenges of the digitalization of manufacturing companies. In *Bled eConference* (pp. 483–500).

Romanosky, S. (2016). Examining the costs and causes of cyber incidents. *Journal of Cybersecurity*, *2*, 121–135.

Rothmann, W., & Koch, J. (2014). Creativity in strategic lock-ins: The newspaper industry and the digital revolution. *Technological Forecasting and Social Change*, *83*, 66–83.

Rust, R. T., Lemon, K. N. and Narayandas, D. (2005), *Customer equity management*, Pearson/ Prentice-Hall, Upper Saddle River, NJ.

Samani, R., & Davis, G. (2019). McAfee mobile threat report mobile malware continues to increase in complexity and scope. available from: https://www.mcafee.com/enterprise/en-us/assets/reports/rp-mobile-threat-report-2019.pdf (accessed 1 June 2021).

Sanger, D. E., Krauss, C., & Perlroth, N. (2021). Cyberattack forces a shutdown of a top U.S. Pipeline. The New York times. available from: https://www.nytimes.com/2021/05/08/us/politics/cyberattack-colonial-pipeline.html (accessed 31 May 2021).

Sarvari, P. A., Ustundag, A., Cevikcan, E., Kaya, I. and Cebi, S. (2018), *Technology Roadmap for Industry 4.0. Industry 4.0: Managing the Digital Transformation*, Springer, Cham.

Schad, J., Lewis, M. W., Raisch, S., & Smith, W. K. (2016). Paradox research in management science: Looking back to move forward. *Academy of Management Annals*, *10*, 5–64.

Schallmo, D., Williams, C. A., & Boardman, L. (2020). Digital transformation of business models—best practice, enablers, and roadmap. *Digital Disruptive Innovation*, *21*(8), 119–138. doi: 10.1142/S136391961740014X.

Schatz, D., & Bashroush, R. (2016). The impact of repeated data breach events on organisations' market value. *Information & Computer Security*, *24*(1), 73–92.

Sebastian, I. M., Moloney, K. G., Ross, J. W., Fonstad, N. O., Beath, C., & Mocker, M. (2020). How big old companies navigate digital transformation. *Strategic Information Management*, 133–150.

Sehlin, D., Truedsson, M., & Cronemyr, P. (2019). A conceptual cooperative model designed for processes, digitalisation and innovation. *International Journal of Quality and Service Sciences*, *11*(4), 504–522.

Seymour, J., & Tully, P. (2018). Generative models for spear phishing posts on social media. *arXiv Preprint*, arXiv:1802.05196.

Sinanaj, G., Muntermann, J., & Cziesla, T. (2015). *How data breaches ruin firm reputation on social media!-insights from a sentiment-based event study*, 902–916. Wirtschaftsinformatik.

Sinansoft (2018). Advantages and disadvantages of Digital Marketing - SinanSoft Blog- software development company in glendale. available from: https://sinansoft.com/blog/advantages-and-disadvantages-of-digital-marketing (accessed 31 May 2021).

Smith, W. K., Gonin, M., & Besharov, M. L. (2013). Managing social-business tensions: a review and research agenda for social enterprise. *Business Ethics Quarterly*, *23*(3), 407–442. doi: 10.5840/beq201323327.

Solis, B., & Littleton, A. (2014). The 2014 state of digital transformation. *Altimeter Group*, *1*(3), 1–33.

Sophos (2012). Security threat report 2012. available from: https://www.sophos.com/medialibrary/PDFs/other/SophosSecurityThreatReport2012.ashx (accessed 1 June 2021).

Stupp, C. (2019). Delta sues chatbot provider over 2017 breach. *Wall Street Journal*. available from: https://www.wsj.com/articles/delta-sues-chatbot-provider-over-2017-breach-11565947801 (accessed 1 June 2021).

Syed, R. (2019). Enterprise reputation threats on social media: A case of data breach framing. *The Journal of Strategic Information Systems*, *28*, 257–274.

Symantec (2019). Broadcom inc. | Connecting everything. available from: https://docs.broadcom.com/doc/istr-24-2019-en (accessed 1 June 2021).

Tellefsen, M. (2020). The pros and cons of digital marketing | *ABA Banking Journal*. available from: https://bankingjournal.aba.com/2020/01/the-pros-and-cons-of-digital-marketing (accessed 31 May 2021).

Tse, T. (2013). Paradox resolution: A means to achieve strategic innovation. *European Management Journal*, *31*, 682–696.

Tweneboah-Koduah, S., Atsu, F., & Prasad, R. (2020). Reaction of stock volatility to data breach: an event study. *Journal of Cyber Security and Mobility*, *9*(3), 1–19. doi: 10.13052/jcsm2245-1439.931.

Van Der Vegt, G. S., & Bunderson, J. S. (2005). Learning and performance in multidisciplinary teams: The importance of collective team identification. *Academy of Management Journal*, *48*, 532–547.

Verizon (2021). 2021 DBIR master's guide. available from: https://www.verizon.com/business/resources/reports/dbir/2021/masters-guide/ (accessed 1 June 2021).

Vial, G. (2019). Understanding digital transformation: A review and a research agenda. *The Journal of Strategic Information Systems*, *28*, 118–144.

Westerman, G., Calméjane, C., Bonnet, D., Ferraris, P., & McAfee, A. (2011). Digital transformation: A roadmap for billion-dollar organizations. *MIT Center for Digital Business and Capgemini Consulting*, *1*, 1–68.

Wikina, S. B. (2014). What caused the breach? An examination of use of information technology and health data breaches. *Perspectives in Health Information Management*, *11*, 1–16.

Wiles, J. (2019). Speed up your digital business transformation. available from: https://www.gartner.com/smarterwithgartner/speed-up-your-digital-business-transformation/#:~:text=Eighty%2Dseven%20percent%20of%20senior,revenue%20streams%20in%20new%20ways (accessed 31 May 2021).

Zhang, Y., Waldman, D. A., Han, Y. -L., & Li, X. -B. (2015). Paradoxical leader behaviors in people management: Antecedents and consequences. *Academy of Management Journal*, *58*, 538–566.

Zinder, E., & Yunatova, I. (2016). Synergy for digital transformation: person's multiple roles and subject domains integration. *International Conference on Digital Transformation and Global Society* (pp. 155–168). Springer.

Corresponding author
Huigang Liang can be contacted at: huigang.liang@gmail.com