Information & Computer Security

Understanding information security awareness: evidence from the public healthcare sector

Martina Neri
University Centre for Logistics Systems, University of Pisa, Pisa, Italy

Elisabetta Benevento, Alessandro Stefanini and Davide Aloini
Department of Energy, Systems, Territory and Construction Engineering, University of Pisa, Pisa, Italy

Federico Niccolini
Department of Political Sciences, University of Pisa, Pisa, Italy

Annalaura Carducci and Ileana Federigi
Department of Biology, University of Pisa, Pisa, Italy, and

Gianluca Dini
Department of Information Engineering, University of Pisa, Pisa, Italy

Received 24 April 2024
Revised 30 May 2024
Accepted 9 July 2024

Abstract

Purpose – Information security awareness (ISA) mainly refers to those aspects that need to be addressed to effectively respond to information security challenges. This research used focus groups to empirically investigate the main ISA dimensions that emerge from the Italian public health-care sector. This study aims to identify the most critical dimension of ISA and to evaluate the diffusion and maturity of information security policies (ISPs) of health-care infrastructure and training programs.

Design/methodology/approach – This research adopted a qualitative research design and focus groups as a research methodology. Data analysis was conducted using the NVIVO 14 software package and followed the principles of thematic analysis.

Findings – The focus group results highlighted that health-care personnel find it difficult to comply with the main ISA dimensions, a situation that leads to risky behaviors. Password management, data storage and transfer and instant messaging applications emerged as the most critical of the main ISA dimensions in the context of this research. It also transpired that ISPs are not all-encompassing as they mainly focus on privacy problems but neglect security concerns. Finally, training programs are not fully implemented in the investigated context, thus undermining their positive enhancing role for ISA.

This work is supported by the University of Pisa under the "PRA – Progetti di Ricerca di Ateneo (Institutional Research Grant) – Project no. PRA_2022_87 'Valutazione della consapevolezza e della preparazione alla cybersecurity nel settore sanitario'" (Assessing cybersecurity awareness and preparedness in health care).

Information & Computer Security
Emerald Publishing Limited
2056-4961
DOI 10.1108/ICS-04-2024-0094

Originality/value – The public health-care sector emerged as a critical yet still under-investigated context. The need for an in-depth investigation of organizational sciences approaches to overcoming information security challenges is also recommended in several prior research studies.

Keywords Information security awareness, Health-care sector, Focus group

Paper type Research paper

1. Introduction

According to the World Economic Forum (2022), "human error is responsible for 95% of cybersecurity incidents" (p. 52). This has led to the widely acknowledged idea that the adoption of only technological solutions is insufficient to manage cyber threats and incidents (Furnell and Clarke, 2012; Neri *et al.*, 2024; Wiley *et al.*, 2020). As humans are seen as the weakest link in information security (Van Niekerk and Von Solms, 2010), the interplay between organizational sciences and cybersecurity is attracting increased interest from researchers and practitioners (Dalal *et al.*, 2022).

Information security awareness (ISA) is a major driver that needs to be addressed by organizations as the first step to overcome cyber challenges. ISA has been defined in several ways. Bulgurcu *et al.* (2010) define ISA as "an employee's general knowledge about information security and his cognizance of the ISP of his organization" (p. 2), referring respectively to "an employee's overall knowledge and understanding of potential information-security-related issues" (p. 2) and of ISPs' requirements. This is consistent with the ideas of Parsons *et al.* (2017), who conceive ISA as:

> The extent to which an organization's employees understand the importance and implications of information security and the extent to which they behave under the organization's information security policies and procedures (p. 41).

In line with this brief overview, the two main ISA aspects are the understanding of information security risks and the user's alignment with the organization's ISPs (Rohan *et al.*, 2023).

Several dimensions of ISA have been identified over the years, including password management, internet and e-mail use, mobile device security, information handling, and incident reports (McCormac *et al.*, 2017; Kruger and Kearney, 2006; Parsons *et al.*, 2017; Rohan *et al.*, 2023). In addition, a significant body of research highlights the importance of training in influencing employees' overall ISA level (Hwang *et al.*, 2021; Parsons *et al.*, 2014). Training programs and ISP provision are important institutional antecedents in shaping ISA (Haeussinger and Kranz, 2013). According to this perspective, Khando *et al.* (2021) depict training as a factor significantly and positively involved in ISA development in both private and public organizations. Researchers also focus on understanding which training characteristics could enhance ISA (Shaw *et al.*, 2009; Zwilling *et al.*, 2022).

Cybersecurity assumes a particularly relevant role in the health-care sector. According to the International Business Machines Corporation (IBM) (2023), "the healthcare industry reported the most expensive data breaches, at an average cost of USD 10.93 million" (p. 1). Italy, the context of this research, is no exception to the growing number of cyberattacks and related incidents. Indeed, according to the latest Italian Association for Information Security (CLUSIT) report (2023), health-care is a major sector affected and impacted by cyber-criminals, and it "remains a convenient target both for economically motivated cyberattacks and for causing damage to society basic services" (p. 26). In addition, cyberattacks have struck players across the board in the health system, with a major concentration on public hospitals (Jalali and Kaiser, 2018), which lag in protecting their data (Kruse *et al.*, 2017).

Despite the acknowledged need to address cyberattacks via a holistic approach (Pollini *et al.*, 2022), human-based and organizational variables regarding information security in the health-care context appear under-researched (Jalali *et al.*, 2019).

Insert in this context, this research focuses on empirically investigating the ISA main dimensions in the public health-care sector. Specifically, this research has a twofold objective: to identify the most critical areas of ISA and to explore ISP and information security training in the investigated context.

The study used four focus groups comprising medical and administrative staff from two public health-care organizations in an Italian region. Results show that it is critical for participants to comply with many of the ISA main dimensions, with noncompliance resulting in risky behaviors. These results need to be seen alongside those relating to ISPs, which currently mainly focus on privacy issues. In addition, training programs are not fully implemented in the investigated context, thus undermining their positive enhancing role for ISA.

2. Research methodology

This research used a qualitative investigation based on focus group analysis (Morgan *et al.*, 1998) which "involves engaging a small number of people in an informal group discussion (or discussions), 'focused' around a particular topic or set of issues" (Wilkinson, 2004, p. 177). Focus groups are deemed appropriate in the context of this research as they provide an emphasis on a specific topic that needs to be explored in depth (Bell *et al.*, 2018). Focus groups also ensure that participants both question and explain to each other, resulting in an interaction that provides valuable data on the extent of agreement and disagreement (Freeman, 2006; Morgan, 1996; Morgan and Krueger, 1993).

Based on insights from prior research, the conventional recommendation for achieving data saturation in qualitative studies has been three to six focus groups (Morgan *et al.*, 1998; Krueger, 1994). Our research thus used four focus groups involving administrative and medical staff (e.g. doctors and nurses). This appeared sufficient for both theoretical and data saturation (Onwuegbuzie and Collins, 2007; Sandelowski, 2008; Strauss and Corbin, 1990).

The focus groups ranged from 7 to 10 participants to ensure consistency with the suggested number of participants (Morgan *et al.*, 1998; Krueger, 1994; Freeman, 2006). In addition, Guest *et al.* (2017) suggested that more than 80% themes saturation could be reached with a small sample and with a total of focus groups that ranges from two to three. Accordingly, Hennink and Kaiser (2022) performed a review on sample size saturation in qualitative studies and the results:

> Demonstrate saturation can be achieved in a narrow range of interviews (9–17) or focus group discussions (4–8), particularly in studies with relatively homogenous study populations and narrowly defined objectives (p. 9).

Each focus group session lasted about 90 min. This timing is consistent with previous research, which suggests focus groups range from 1 to 2 h (Freeman, 2006; Morgan, 1996). The focus groups were held online via Google Meets. Gathering data via online platforms has frequently been established as a viable way of conducting research, especially after the mandatory social distancing rules caused by COVID-19. Lobe *et al.* (2020) suggested that the digital society has increased people's familiarity with several methods of online communication and interaction, which enhance online data research collection and participation. Data collection took approximately three months, starting from June 2023.

Before starting each focus group session, one researcher explained the overall research objectives. Participants were ensured of the anonymity of data treatment. One researcher took the role of a moderator and another one that of the assistant moderator, thus establishing

the moderation team (Krueger, 1994). The moderator was formally responsible for facilitating and promoting the discussion, following the interview layout, and explaining focus group material. The assistant moderator managed call participation (e.g. ensuring that all attendees had access to the link to the virtual classroom) and took notes. Data analysis was conducted using the NVIVO 14 software package and followed the principles of thematic analysis in accordance with Braun and Clarke's (2006) prescriptions. Each focus group transcription was analyzed by two independent researchers. This allowed for a wider perspective on the analysis, reduced the intrinsic subjectivity of qualitative research methods and enhanced inter-rater reliability (Bryman and Bell, 2015). Interviews were conducted in Italian and transcribed *verbatim*. Quotes from the interviews presented in the results section were translated into English.

3. Results and discussion

3.1 Information security awareness main dimensions

Starting with the investigation of main ISA dimensions, several emerged as critical and posing challenges in the execution of daily job activities. These attitudes are related to both individual (e.g. cyber skills) and organizational (e.g. procedures) dimensions.

Findings revealed that password management was the most challenging issue. In all focus groups, it emerged that the password management procedure (e.g. different passwords for each account to be updated periodically) was overcomplicated, given the large number of passwords to be managed. Participants therefore admitted to engaging in risky behaviors. However, some differences emerged between the administrative and medical staff. The latter repeatedly admitted to performing improper behaviors to speed up work practices. As an example:

> In the medical area, we deal with so many people. Having to change passwords all the time is such a time-consuming process that we end up using other colleagues' passwords to get work done. We know this is a major issue (FG4).

In general, the time issue emerged as a decisive factor. Indeed, health-care services delivered on time were often prioritized over secure behaviors. In addition, the medical staff claimed that the current ISPs did not meet their operational needs. However, greater attention to password management emerged from the administrative staff that regularly observed password management policies. Many participants trace unattended procedures back to distraction. As an example:

> Everyone knows not to share our passwords with other people, however, I then get up and leave my PC unattended with my password in. This certainly is a shortcoming that happens daily yet unintentionally (FG3).

However, even the administrative staff underlined that existing procedures were not suitable for their work needs. As an example:

> We need rules that could simplify passwords choice and reduce their number. Because of work passwords, those needed in private life, and all kinds of passwords, I often find myself in situations where devising a password for the accounting software takes me even a week. What I wanted to point out is that in organizations like ours, the inability to log in because of a password affects the management of emergencies we experience daily (FG1).

To summarize, password management requires both proper training and procedures with simplified technologies that align with daily activities.

Another significant issue is related to data management, i.e. communication and storage. Overall, issues related to how the organization exchanges information with internal and

external parties emerged in all focus groups, although more specifically in the medical staff sector. One participant underlined that:

> [e]veryone asks us for emails to get medical results faster or to get copies. We know what the practice is (e.g., encrypted emails) but the implication is that it appears as if the operator did not want to help the patient. As a result, it happens that, in the rush or under time pressure, mistakes are made. A mistake can also be transmitted to the wrong person. The risk is out there (FG4).

In this regard, it also emerged that the lack of procedures is a contributing factor to these concerns:

> We don't have a secure computer system to send reports to patients. If technically there was an option where encrypted passwords could be created then we could securely email the reports, avoiding so many errors (FG4).

In all four focus groups, many issues related to data storage, such as cloud repositories, then surfaced. Participants perceived both data transfer and storage as insecure. However, the need to use these for operational purposes emphasized the need to change the tools provided. For example:

> Ideally, we would balance the need we have to use these tools and the need to still make them as secure as possible. It is clear that there is a danger, but it is equally clear that there is a need (FG1).

Instant messaging applications also emerged as a critical factor. As a result of the COVID-19 pandemic, new communication habits have been established between patients and medical staff, especially doctors, and with these new potentially risky behaviors arose. For example, one participant stated: *I now reserve the latter part of the day for prescribing medications or medical certificates. Requests often happen* via *text or chat, unsafe tools (FG2).*

In general, massive use of instant messaging applications emerged among the medical staff. This approach was not appropriately matched with sufficient knowledge levels about proper usage procedures, thus leading to information security and privacy risks. In addition, the use of personal and non-business devices also increased. For example: *Medical images (e.g. ulcers) are transferred, even to private cell phones, because we cannot always provide corporate devices (FG2).*

To summarize, it appears that many main dimensions of ISA appear critical to deal with. This is especially true while dealing with daily activities and operational needs, with a resulting increase in risky behaviors. These results should be linked to those of training and ISP, which are depicted in the following section. Table 1 summarizes ISA themes and the corresponding main issues reported by participants.

3.2 Training and information security policy

Findings showed that the lack of training for both administrative and medical staff is another relevant issue that compromised the ISA dimensions. Specifically, medical staff reported:

> There is a lot of ignorance in our field. Unless someone is an administrative employee. Otherwise, medical staff learns from the field, but no one pays attention to the subject (FG2).

The administrative staff consequently had limited knowledge of information security. However, they exhibited a prevailing cautious attitude:

> I tend to be more cautious, before opening an email I wait, I ask, I have it checked, maybe exactly because I have no training or knowledge on the subject, I take such a particularly suspicious and cautious attitude (FG1).

It emerged that participants did not feel sufficiently trained, although they were willing to attend training sessions. Participants from all focus groups were fully aware of the ways in which

Table 1. ISA themes and related main issues summary

ISA themes	Main issues
Password management	• Over complicated procedures that do not consider operational needs • Distractions while working can cause risky behavior
Data management	• Lack of secure data-sharing systems • Lack of defined procedures on how to share data • Patients' needs to have clinical results increase the use of insecure systems for both data sharing and storage
Mobile devices usage	• Use of personal devices to perform work-related activities • Use of instant messaging applications to meet patients' requests

Source: Authors' own work

information security is a key driver of today's business activities, and they wished for both cultural and operational improvements, as "*[w]e handle a lot of data, so the importance of this topic is real heartfelt. […] I think enhancing the culture of cybersecurity is critical and important (FG4).*

Administrative staff called for more pragmatic training that can support them in daily work operations. For example:

> I experience passive training that focuses on the law. However, I do not remember active training with some examples. If there was training with more practical examples, showing what should be done if the system is breached it would be better (FG3).

The medical staff discussion was more diversified. Those more familiar with the topic called for more specific training programs. For example:

> We know data security well, especially on what data we handle and that we should not risk sending out sensitive data. But a specific training in the cybersecurity area is not sensitized enough (FG4).

Those who were less educated on information technology (IT) matters expressed a need for real computer literacy regarding both the IT tools they use daily and the related information security practices. As an example:

> I really need to be cyber literate, acknowledging my profound ignorance on the subject, but also my great desire to increase my literacy, precisely because cyber tools are being used dangerously (FG2).

Participants' response concerning the willingness to invest some of their work time in training activities was affirmative. However, some difficulties emerged regarding time availability. Medical staff highlighted that:

> I think the awareness of the importance of the topic is present. The real problem is finding time in work rhythms that are not usual at the moment. Anything that is not the clinical profession is seen as bureaucracy. This has created a rejection regardless. What then happens is that only those who have a sensitivity and a predisposition for IT pay attention to such issues (FG2).

For the administrative staff, an additional need was to make sure that procedures are established and then followed by everyone. A participant reported that:

> [w]e are very sensitive, so it is far from a waste of time for us, as long as it does not hinder. We need to find tools and ways that are followed by everyone. This is because if I do it but the colleague sitting next to me does not then what is the point? (FG3).

Overall, training programs appeared to be mostly focused on privacy concerns. Indeed, *information security and so cybersecurity occupy a small part of these courses, which are mainly about privacy (FG3).* A medical staff participant added: *I have covered the topic not in a dedicated way, but only within other courses, such as those on data treatment (FG4).*

The training is "incidental" to other training courses. This suggested that privacy risks are prioritized by top management. A consequence of such training gaps is the consistent use of "spread the word" systems in the exchange of knowledge among colleagues. Indeed, *we move forward in our activities also thanks to spread the word, a scheme by which theoretical concepts are frequently transformed (FG1).*

When discussing ISPs, administrative staff reported:

> I have outdated information, but to my knowledge, there is no cybersecurity policy, there is a privacy policy of which cybersecurity is one of many aspects covered. There is no published policy that you can find anywhere (FG3).

This was confirmed in several statements from medical staff, including that:

> [w]e certainly have a framework for privacy and how to handle sensitive data. I believe that we have to work on it, doing specific insights on cybersecurity. I don't feel ready. I wouldn't know how to deal with it (FG2).

It emerged that some guidelines related to software usage (e.g. password management for the specific software) did exist. This practice led to a fragmentation of the information possessed by staff, thus creating uneven levels of awareness and behavior. As reported by administrative staff: *There is no homogeneity in policy behavior among the various entities that manage all the applications (FG3).*

This mechanism drove staff to find alternative solutions. Individual training spontaneously generated a homemade policy. In a few cases, staff assumed the responsibility for informing themselves. Conversely, the majority of participants (both medical and administrative staff) reported lacking specific security skills, thus relying on IT assistance as a regular procedure. As reported:

> If I have any doubts I ask (name of a colleague) or I make a ticket to ask for support. What happens after that I don't know. I remain cautious instead of taking action (FG1).

Some participants supported the idea of the need for a structural intervention by management to establish ISPs. However, this perspective was still far from being realized. For example:

> Awareness should be brought to the highest management level. As much as all the institutional positions and the necessary profiles are established, such as the DPO, etc., it still seems that they are not able to create that awareness, which helps in paying attention (FG3).

From the analysis of the past comments, the important role assumed, either directly or indirectly, by management and leadership was very clear. Senior managers should collaborate with technical experts (e.g. data protection officer) to develop an ISP to be shared in the work environment.

Many participants expressed a desire to have a more comprehensive policy, and to be properly informed about it. As an example: *A vademecum would be useful and helpful (FG1).*

The training and ISP topics allowed room for consideration about the absence of appropriate procedures and training, especially in handling cyber incidents. Awareness of their skill limitations, yet the simultaneous willingness to improve by learning through well-defined reporting and handling procedures, emerged frequently. In this regard, one participant stated:

> Doing some training and making explicit the rules on how to check a suspicious email, would be particularly useful. The same thing should be done for reporting incidents. It would be appropriate in my opinion, but also talking with some colleagues, to establish more structured and predefined

> procedures, making it mandatory to report such incidents. The goal would be to be able to increase user awareness of the issues and give them clear guidelines on how to behave (FG1).

A need for training programs and procedures emerged as fundamental, considering that participants reported often being exposed to cyberattacks (e.g. phishing) that challenge them daily. In addition to countless work-related communications, they also claimed to receive a large number of emails with malicious content in their corporate inboxes. An administrative staff participant claimed that *[s]ome (phishing) emails are easily recognizable, while others are done quite well and many colleagues, mainly because they were overworked, failed to perceive the danger (FG1).*

As participants reported their experiences, they appeared reasonably aware of both the risks associated with their behaviors and the lack of the necessary tools to mitigate those risks. Those who experienced this either directly or indirectly reported that they flagged the most recognizable e-mails as spam and contacted the IT department for any other concerns. As reported by one medical staff participant:

> If you saw unusual e-mails with strange content, the advice was to ignore and delete them. This is the simple and diffuse instruction that we all follow. Coming to a reporting culture or to the existence of special procedures to follow at least personally, I'm not aware of that (FG2).

Overall results suggested that participants would be able to recognize and therefore reduce cyber incidents deriving from phishing when equipped with elementary phishing detection techniques combined with a balanced workload and a limited stress level. Conversely, work overloads, high levels of stress (which have been depicted as standard conditions by medical staff) and sophisticated phishing techniques resulted in a combination that often led to errors and cyber incidents. Administrative staff expressed a deep concern about risky behaviors and the knowledge needed to recognize a cyberattack. These concerns were also confirmed by medical staff: *Honestly, I couldn't tell if the emails included the real one or the fake one (FG2).*

The above discussion reinforced both observations and concerns that most cyberattacks exploit human vulnerabilities. Table 2 summarizes the main issues that emerged concerning training, ISPs and cyber-incidents.

4. Conclusions

This study investigated ISA's main dimensions, as well as ISP and training in the Italian public health-care sector through a qualitative study based on focus groups.

Among the ISA's main dimensions, password management, data storage and transfer and instant messaging applications emerged as the most critical in the research context. Although there was a relatively widespread perception of information security risks, both medical and administrative staff tended to embrace risky behaviors to facilitate their work-related activities. For example, sending medical reports via instant messaging applications seemed to be an established practice to accommodate patient needs and speed up daily activities.

Concerning information security training, health-care organizations did not provide specific courses to their staff. However, focus groups showed a consistent need for training, especially for the medical staff that exhibited a lower literacy level. According to these results, the positive and enhancing role of training (Hwang *et al.*, 2021; Parsons *et al.*, 2014) emerged as severely undermined for both medical and administrative staff. Although both staffs contingents expressed the need to be fully trained and informed about appropriate procedures, top management was seen to be more focused on privacy-related matters and rules – an understandable behavior given the general data protection regulation-sanctioning regime. As many participants relied on a sort of homemade policy, this approach compromised the overall level of ISA in the organizations which, as prior research suggested, is closely related to employees' understanding of and alignment with ISP (Parsons *et al.*, 2017).

Table 2. Training, ISPs and cyber-incident themes and main issues' summary

Themes	Main issues
Training	• Limited knowledge and learning from the field • Insufficient training with respect to operational needs • Training focused on privacy regulations • Limited time available to be dedicated to training • Need for cultural improvement conveyed by the board
ISPs	• Policies focused on privacy and sensitive data handling • Update on policies that are based on how to use new softwares • Employee demands for ISPs to increase awareness about information security
Cyber-incidents	• Lack of incident handling procedures • Lack of cyber-incident mitigation tools • High workloads may lead to cyber-incidents • Phishing e-mails reported by employees as the main cyberattack method experienced

Source: Authors' own work

This research has some limitations that open the way for future research. The qualitative approach is a limitation due to its intrinsic subjectivity. However, the main research prescriptions to reduce subjectivity were followed. In addition, the focus group interpretation was performed by two different researchers, thus allowing an interactive interpretation process, and enhancing inter-rater reliability (Bryman and Bell, 2015). Future research could adopt a quantitative research design to address the ISA dimensions. This may allow for a reduction in subjectivity and could numerically estimate the relevance of ISA dimensions and their relationships. Additional research may include the evaluation of the impact of different forms of training on ISA, e.g. training courses or simulations.

As this research focused on an Italian regional government, the results are context-dependent and limited in their generalizability. Future research could extend the focus and perform cross-country comparisons (both European and non-European). This would allow future research to take into consideration the relevant role of economic, cultural, and legal implications in ISA development.

References

Bell, E., Bryman, A. and Harley, B. (2018), *Business Research Methods*, 5th ed., Oxford University Press, Oxford.

Braun, V. and Clarke, V. (2006), "Using thematic analysis in psychology", *Qualitative Research in Psychology*, Vol. 3 No. 2, pp. 77-101. doi: 10.1191/1478088706qp063oa.

Bryman, A. and Bell, E. (2015), *Business Research Methods*, University Press, Oxford.

Bulgurcu, B., Cavusoglu, H. and Benbasat, I. (2010), "Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness", *MIS Quarterly*, Vol. 34 No. 3, pp. 523-548.

Dalal, R., Howard, D., Bennett, R., Posey, C., Zaccaro, S. and Brummel, B. (2022), "Organizational science and cybersecurity: abundant opportunities for research at the interface", *Journal of Business and Psychology*, Vol. 37 No. 1, pp. 1-29, doi: 10.1007/s10869-021-09732-9.

Freeman, T. (2006), "Best practice' in focus group research: making sense of different views", *Journal of Advanced Nursing*, Vol. 56 No. 5, pp. 491-497, doi: 10.1111/j.1365-2648.2006.04043.x.

Furnell, S. and Clarke, N. (2012), "Power to the people? The evolving recognition of human aspects of security", *Computers and Security*, Vol. 31 No. 8, pp. 983-988, doi: 10.1016/j.cose.2012.08.004.

Guest, G., Namey, E. and McKenna, K. (2017), "How many focus groups are enough? Building an evidence base for nonprobability sample sizes", *Field Methods*, Vol. 29 No. 1, pp. 3-22, doi: 10.1177/1525822X16639015.

Haeussinger, F. and Kranz, J. (2013), "Understanding the antecedents of information security awareness–an empirical study", *19th Americas Conference on Information Systems, AMCIS 2013 - Hyperconnected World: Anything, Anywhere, Anytime*, Vol. 5, pp. 3762-3770.

Hennink, M. and Kaiser, B.N. (2022), "Sample sizes for saturation in qualitative research: a systematic review of empirical tests", *Social Science and Medicine*, Vol. 292, p. 114523, doi: 10.1016/j.socscimed.2021.114523.

Hwang, I., Wakefield, R., Kim, S. and Kim, T. (2021), "Security awareness: the first step in information security compliance behavior", *Journal of Computer Information Systems*, Vol. 61 No. 4, pp. 345-356, doi: 10.1080/08874417.2019.1650676.

International Business Machines Corporation (IBM) (2023), "The costs of data breach report", available at: www.ibm.com/downloads/cas/E3G5JMBP

Jalali, M.S. and Kaiser, J.P. (2018), "Cybersecurity in hospitals: a systematic, organizational perspective", *Journal of Medical Internet Research*, Vol. 20 No. 5, p. e10059, doi: 10.2196/10059.

Jalali, M.S., Razak, S., Gordon, W., Perakslis, E. and Madnick, S. (2019), "Health care and cybersecurity: bibliometric analysis of the literature", *Journal of Medical Internet Research*, Vol. 21 No. 2, p. e12644, doi: 10.2196/12644.

Khando, K., Gao, S., Islam, S.M. and Salman, A. (2021), "Enhancing employees information security awareness in private and public organisations: a systematic literature review", *Computers and Security*, Vol. 106, p. 102267, doi: 10.1016/j.cose.2021.102267.

Krueger, R.A. (1994), *Focus Groups: A Practical Guide for Applied Research*, 2nd ed., Sage, Thousand Oaks, CA.

Kruger, H.A. and Kearney, W.D. (2006), "A prototype for assessing information security awareness", *Computers and Security*, Vol. 25 No. 4, pp. 289-296, doi: 10.1016/j.cose.2006.02.008.

Kruse, C.S., Frederick, B., Jacobson, T. and Monticone, D.K. (2017), "Cybersecurity in healthcare: a systematic review of modern threats and trends", *Technology and Health Care*, Vol. 25 No. 1, pp. 1-10, doi: 10.3233/THC-161263.

Lobe, B., Morgan, D. and Hoffman, K.A. (2020), "Qualitative data collection in an era of social distancing", *International Journal of Qualitative Methods*, Vol. 19, p. 1609406920937875, doi: 10.1177/1609406920937875.

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M. and Pattinson, M. (2017), "Individual differences and information security awareness", *Computers in Human Behavior*, Vol. 69, pp. 151-156, doi: 10.1016/j.chb.2016.11.065.

Morgan, D. (1996), "Focus groups", *Annual Review of Sociology*, Vol. 22 No. 1, pp. 129-152, doi: 10.1146/annurev.soc.22.1.129.

Morgan, D.L. and Krueger, R.A. (1993), "When to use focus groups and why", in Morgan, D.L. (Ed.), *Successful Focus Groups: Advancing the State of the Art*, Sage Publications, Newsbury Park, CA, pp. 3-9, doi: 10.4135/9781483349008.n1.

Morgan, D.L., Krueger, R.A. and King, J.A. (1998), *The Focus Group Guidebook*, Sage, Thousand Oaks, California.

Neri, M., Niccolini, F. and Martino, L. (2024), "Organizational cybersecurity readiness in the ICT sector: a quanti-qualitative assessment", *Information and Computer Security*, Vol. 32 No. 1, pp. 38-52, doi: 10.1108/ICS-05-2023-0084.

Onwuegbuzie, A.J. and Collins, K.M. (2007), "A typology of mixed methods sampling designs in social science research", *The Qualitative Report*, Vol. 12 No. 2, pp. 281-316, doi: 10.46743/2160-3715/2007.1638.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M. and Jerram, C. (2014), "Determining employee awareness using the human aspects of information security questionnaire (HAIS-Q)", *Computers and Security*, Vol. 42, pp. 165-176, doi: 10.1016/j.cose.2013.12.003.

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A. and Zwaans, T. (2017), "The human aspects of information security questionnaire (HAIS-Q): two further validation studies", *Computers and Security*, Vol. 66, pp. 40-51.

Pollini, A., Callari, T.C., Tedeschi, A., Ruscio, D., Save, L., Chiarugi, F. and Guerri, D. (2022), "Leveraging human factors in cybersecurity: an integrated methodological approach", *Cognition, Technology and Work*, Vol. 24 No. 2, pp. 371-390, doi: 10.1007/s10111-021-00683-y.

Rohan, R., Pal, D., Hautamäki, J., Funilkul, S., Chutimaskul, W. and Thapliyal, H. (2023), "A systematic literature review of cybersecurity scales assessing information security awareness", *Heliyon*, Vol. 9 No. 3, p. e14234, doi: 10.1016/j.heliyon.2023.e14234.

Sandelowski, M. (2008), "Theoretical saturation", in Given, L.M. (Ed.), *The Sage Encyclopedia of Qualitative Methods*, Vol. 1 Sage, Thousand Oaks, CA, pp. 875-876.

Shaw, R.S., Chen, C.C., Harris, A.L. and Huang, H.-J. (2009), "The impact of information richness on information security awareness training effectiveness", *Computers and Education*, Vol. 52 No. 1, pp. 92-100, doi: 10.1016/j.compedu.2008.06.011.

Strauss, A. and Corbin, J. (1990), *Basics of Qualitative Research: Grounded Theory Procedures and Techniques*, Sage, Newbury Park, CA.

Van Niekerk, J.F. and Von Solms, R. (2010), "Information security culture: a management perspective", *Computers and Security*, Vol. 29 No. 4, pp. 476-486, doi: 10.1016/j.cose.2009.10.005.

Wiley, A., McCormac, A. and Calic, D. (2020), "More than the individual: examining the relationship between culture and information security awareness", *Computers and Security*, Vol. 88, p. 101640, doi: 10.1016/j.cose.2019.101640.

Wilkinson, S. (2004), "Focus group research", in Silverman, D. (Ed.), *Qualitative Research: Theory, Method, and Practice*, Sage, Thousand Oaks, CA, pp. 177-199.

World Economic Forum (2022), "The global risks report", available at: www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F. and Basim, H.N. (2022), "Cyber security awareness, knowledge and behavior: a comparative study", *Journal of Computer Information Systems*, Vol. 62 No. 1, pp. 82-97, doi: 10.1080/08874417.2020.1712269.

Further reading

Associazione italiana per la Sicurezza Informatica (2023), "Rapporto Clusit 2023 Sulla Sicurezza ICT in Italia", available at: https://clusit.it/wp-content/uploads/download/Rapporto_Clusit_aggiornamento_10-2023_web.pdf

Siponen, M., Mahmood, M. and Pahnila, S. (2013), "Employees' adherence to information security policies: an exploratory field study", *Information and Management*, Vol. 51 No. 2, pp. 217-224, doi: 10.1016/j.im.2013.08.006.

Corresponding author

Martina Neri can be contacted at: martina.neri@phd.unipi.it