Bus Inf Syst Eng 67(2):141–147 (2025)
https://doi.org/10.1007/s12599-025-00933-7

EDITORIAL

# The Damocles Sword of Cyber Attacks

## A Call for Information Systems Security

**Frederik Hering · Oliver Hinz · Jella Pfeiffer · Wil van der Aalst**

Published online: 21 February 2025


### 1 Introduction

Geopolitical tensions, international conflicts, and wars exacerbated an increasing threat to organizations and society. A more connected world, advances in digitalization, and greater dependence on information systems (IS) leveraged part of the conflicts into cyberspace (Sen et al. 2022). The attackers' professionalization increased the threat by recruiting IT experts to carry out sophisticated cyber attacks (Kotsias et al. 2023). The steadily increasing number of cyber attacks and data breaches emphasizes this. Figure 1 shows the increased threat situation. US data breaches increased from 2014 to 2023 by 246 % (Clearinghouse 2023). Furthermore, experts believe the expected financial damage caused by cyber attacks will rise from 9 trillion to over 13 trillion US dollars over the next four years (Statista 2024). These statistics usually neglect indirect or immaterial damage, such as increased stress among cybersecurity employees (Singh et al. 2023), the loss of company market value (Rosati et al. 2017; Schatz and Bashroush 2016), deteriorated customer relationships (Janakiraman et al. 2018), and other side effects. As a result, hacker attacks have become a major concern for organizations (Li and Chen 2022).

At the same time, the complexity of software and the resulting number of attack vectors increases, making it even more challenging for companies to defend themselves against cyber attacks. The number of officially reported software vulnerabilities increased by 268% from 2014 to 2023 (MITRE Corporation 2024). In addition, technological advances, such as artificial intelligence (AI), make it easier for attackers to detect vulnerabilities and carry out impactful attacks (National Cyber Security Centre 2024). The Allianz Risk Barometer identifies cyber attacks as the top threat to businesses in 2025 (Allianz Commercial 2025). Therefore, some security experts believe that "Everybody will be hacked; it is just a matter of when, not if" (Holst 2025). The looming threat of a cyber attack and data breach is akin to the sword of Damocles hanging over organizations. In the story of Damocles, a single strand of horsehair suspends the sword above, serving as a powerful metaphor for the critical role of cybersecurity.

However, what exactly is cybersecurity? Or what do we, as IS researchers, mean by it? The academic community uses the terms cyber, information-, computer- or IT security interchangeably (Dhillon et al. 2021). In a broader sense, cybersecurity deals with the "(...) protection of a person, organization, or country and their computer information against crime or attacks carried out using the Internet" (Cambridge University Press 2024). The traditional security objectives comprise confidentiality, availability, and integrity of personal and organizational assets and information (Von Solms and Van Niekerk 2013). While computer science research is concerned with detecting attacks and vulnerabilities and developing resilient and secure systems, information systems security (ISS) research focuses on the interface between

F. Hering (✉) · O. Hinz
Faculty of Economics and Business Administration, Goethe University Frankfurt, Theodor-W.-Adorno-Platz 4, 60323 Frankfurt am Main, Germany
e-mail: hering@wiwi.uni-frankfurt.de

J. Pfeiffer
Karlsruhe Institute of Technology, Kaiserstraße 93, 76133 Karlsruhe, Germany

W. van der Aalst
Lehrstuhl Für Informatik 9, RWTH Aachen University, Ahornstr. 55, 52056 Aachen, Germany

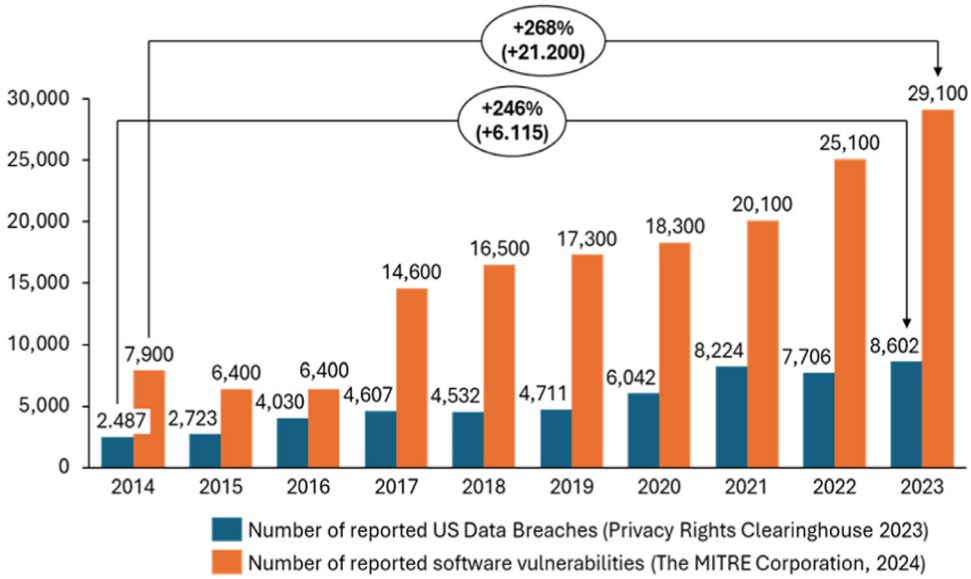


**Fig. 1** Annual number of reported US data breaches (Clearinghouse 2023) and annual number of reported software vulnerabilities (MITRE Corporation 2024)

cybersecurity, information systems, and human behavior (Dhillon et al. 2021). Dhillon et al. (2021) describe ISS as the protection of information handling at the technical, formal, and informal levels. ISS is not solely a technical issue but involves human, organizational, and social dimensions. The socio-technological orientation of BISE positions it as an ideal venue for impactful publications in this dynamic field.

## 2 The State of ISS Research

The focus of ISS research has been constantly evolving. In a first literature review, Baskerville (1993) describes how ISS evolved from simple security checklists in the 1970 s to logical control designs and data flow diagrams in the late 1980 s. The following literature reviews from Dhillon and Backhouse (2001), Siponen (2005), Siponen and Oinas-Kukkonen (2007) describe the development from a purely technical perspective of ISS research to multi-perspective research, which incorporates behavioral, conceptual, and design-oriented aspects. Siponen and Oinas-Kukkonen (2007) emphasize that an overarching approach that includes human behavior is necessary for a successful organizational security strategy. In a recent literature review, Dhillon et al. (2021) describe ISS research as an interconnected socio-technical concept to understand the interplay between technical and social systems (see Fig. 2). This perspective considers how structures (e.g., policy and regulation frameworks), people (e.g., security behavior and security compliance), technology (e.g., IS security attack and threat detection technologies), and tasks (e.g., system design) interact to avoid cyber attacks and shape ISS research.

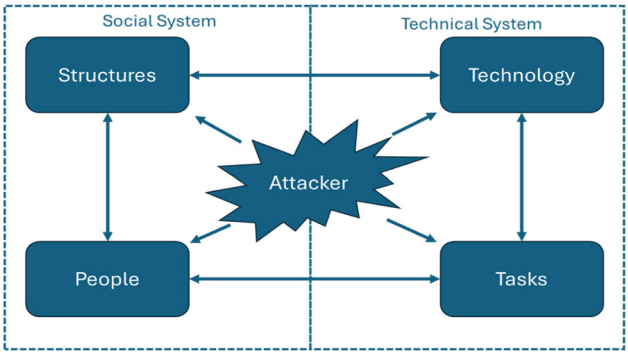


**Fig. 2** Conceptual overview about the central research problems within ISS based on Dhillon et al. (2021)

A central socio-technological problem of ISS research is the duality in secure information systems design (Baskerville 1993; Siponen 2005). Duality refers to the conflict between the functionality and security of information systems (Siponen 2005). Finding the ideal balance between the two conflicting aspects often results in prioritizing the information systems functionality and leads to the consideration of security aspects after the implementation of information systems (Siponen 2005; Karlsson et al. 2017). The duality problem can also explain why users may resist security measures implemented after the initial system design (Siponen 2005; Paananen et al. 2020). In recent research, Paananen et al. (2020) still sees the duality problem as a major issue for secure information system design.

A further research area deals with human security behavior. Central research questions focus on motivating individuals to adopt protective best practices, such as using strong passwords, and on exploring what triggers non-compliant security behavior (Hui et al. 2016; Dhillon et al.

2021). Numerous studies have investigated employee compliance with IS policies, examining various behavioral factors and their impacts (Cram et al. 2019). In a meta-analysis of 95 existing publications, Cram et al. (2019) concluded that employee attitudes, norms, and beliefs are the strongest predictors of compliance. In contrast, factors such as rewards, punishments, and threats were found to have a relatively weak impact on compliance (Cram et al. 2019). More recent studies, such as Cram et al. (2024), criticize the nomothetic approach of behavioral studies. The reliance on cross-sectional data with one-time surveys provides limited insights into how individual behavior changes over time. They are calling for more idiographic research approaches to validate existing theories by examining how individual behavior aligns with theoretical predictions over time (Cram et al. 2024). Another research stream deals with the impact of cyber attacks on human behavior. Phishing attacks are particularly highlighted in ISS research and are well-suited for both experimental and field setups (Wright et al. 2023; Jensen et al. 2022). Publications try to explain why people fall for phishing attacks using various models, such as the cognitive evaluation (Jensen et al. 2022) or the contextual theory (Wright et al. 2023; Jaeger and Eckhardt 2021). Closely linked are studies on security awareness and the resulting increase in phishing susceptibility (Jaeger and Eckhardt 2021; Pienta et al. 2020). Additional publications deal with design science research to create attributes that increase phishing susceptibility (Zahedi et al. 2024; Abbasi et al. 2021). For instance, Abbasi et al. (2021) developed a design artifact to predict users' susceptibility to phishing websites. Employees using the design artifact responded significantly less to phishing threats than control groups, resulting in substantial cost savings for the company. ISS research often overlooks complex attacks and their detection and defense mechanisms through advanced threat protection. This omission is probably due to the fact that simulating such complex attacks in a laboratory setting is quite challenging, and it can be difficult to find appropriate subjects, such as security experts, for behavioral research questions.

In addition to individual safety behavior, research also looks at the organizational perspective. For example, Wang et al. (2023) found a positive relationship between IT innovativeness and data breach risk, especially in complex organizational environments. The research uses organizational learning theory to explain how IT innovation can enhance organizational capabilities and introduce new vulnerabilities (Wang et al. 2023). In another study, Ghahramani et al. (2023) show that the ability of an organization to learn and utilize new knowledge plays a crucial role in improving ISS. They demonstrate that the competitive pressure between companies strengthens the mediating role of adaptability (Ghahramani et al. 2023).

In addition to using new technologies (Wang et al. 2023) and organizational learning (Ghahramani et al. 2023), security investments are another focus of the organizational perspective. A study by Kwon and Johnson (2014) shows that proactive investment in the security of IS reduces the risk of data breaches. Angst et al. (2017) emphasize that focusing solely on technological solutions (increased IT security investments) may not be sufficient to prevent data breaches. They argue that understanding how institutional factors influence IT adoption is crucial for developing effective security strategies (Angst et al. 2017).

Another organizational research stream deals with risk management (Hui et al. 2016). For instance, Chen et al. (2011) focus on the risk of information network failure due to cyber attacks that exploit software vulnerabilities. They provide valuable insights into the optimal level of software diversification within an information network, considering the trade-offs between the benefits of compatibility and the risks of failures (Chen et al. 2011).

The previously presented studies generally investigate how companies deal internally with new technology, security investments, human behavior, and strategies to avoid data breaches. Further research deals with the consequences of a data breach. For example, Hoehle et al. (2022) investigate the impact of post-data breach compensation strategies on customer relationships. They showed that meeting customer expectations regarding compensation was crucial for positive justice perceptions and provided insights to organisations regarding how to effectively respond to data breaches and mitigate their negative consequences (Hoehle et al. 2022). This research demonstrates that effective post-breach compensation strategies are crucial for maintaining customer trust and mitigating the negative impacts of data breaches (Hoehle et al. 2022). Another focus is on how companies can learn from data breaches. Research conducted by Mehrizi et al. (2021) highlights that data breaches often consist of a series of interconnected events. Organizations need to engage in an iterative process that incorporates different learning models. The authors stress the importance of adopting a more holistic and dynamic approach to organizational learning from IS incidents (Mehrizi et al. 2021). Current studies often overlook the context during or immediately after a security incident. These situations present unique opportunities to strengthen an organization's resilience by examining crisis and business continuity management. A crucial question is how organizations can transition from crisis mode back to normal operations as quickly as possible.

Since 2017, additional research investigates the attacker's perspective. This shift stems from an increasing recognition that cyber attacks and data breaches are not random (Hui et al. 2016). The research utilizes design

science methodology to proactively identify threats by analyzing darknet and hacker forums and marketplaces (Chan et al. 2024; Ampel et al. 2024; Li and Chen 2022; Ebrahimi et al. 2020). Instead of focusing on past events (e.g., log file analysis), researchers attempt to anticipate exploits by infiltrating and observing darknet and clearnet hacker forums and marketplaces (Bromiley 2016) to detect attacks as early (de Nobrega et al. 2024; Kotsias et al. 2023). Attackers can also employ new technologies, such as large language models, to make phishing attacks even more difficult to detect. As early as 2010, an MISQ editorial by Mahmood et al. (2010) called for an investigation into the motivations and techniques of attackers. Despite the passage of time, there is still limited literature on this subject. Gaining a deeper understanding of attacker behavior and how they leverage new technologies could enhance proactive security measures.

In terms of methodology, ISS research offers a wide range of possibilities. As previously mentioned, there are experimental studies that focus on human behavior (Jensen et al. 2022; Jaeger and Eckhardt 2021), design science approaches aimed at developing artifacts to enhance ISS in organizations (Zahedi et al. 2024; Abbasi et al. 2021), and long-term studies that investigate employee compliance behavior (Cram et al. 2024). However, there is a lack of empirical data on how companies respond before, during, and shortly after a cyber attack. Siponen and Oinas-Kukkonen (2007) called for more empirical studies in this area. Due to the lack of reliable data, many questions about the costs of cyber attacks remain unanswered. Research neglects indirect costs, such as employee burnout caused by overworked security staff, as well as cascading effects, like the impact of a data breach on suppliers and customers, when analyzing the financial damage to organizations.

Within BISE, the publications of ISS are sparse. Several articles deal solely with privacy or access management (Glöckler et al. 2024; Binzer et al. 2024; Baumann et al. 2019; Mannhardt et al. 2019). Over the last ten years, only four publications within BISE have focused on ISS-related research. These publications deal with human security behavior (Nofer et al. 2014), security risk (Matulevičius et al. 2018), and organizational aspects of ISS (Jiang et al. 2023; Arce 2022), and we present them briefly in the following.

Jiang et al. (2023) propose a comprehensive taxonomy to model the interconnections and dependencies between information technology and operation technology security. Their approach enables cascade modeling for vulnerability assessment and identification of critical components. The paper further suggests power-grid reference models to enhance the reproducibility and applicability of the proposed method.

Arce (2022) observed that cloud providers use security measures (e.g., cryptography) to lock in customers, making switching harder. This strategy can increase profits and cloud providers prioritize lock-in over price leadership, hindering standardization in the cloud industry.

Nofer et al. (2014) distinguish between the impacts of privacy violations and security breaches on consumer trust and behavior. Results support the privacy paradox where people prioritize privacy in theory but prioritize security in practice. This intention-behavior gap persists even after privacy breaches.

The fourth publication from Matulevičius et al. (2018) developed an approach for eliciting and introducing security requirements into business processes using security risk-oriented patterns. These patterns identify security risks and suggest mitigations, reducing the effort required for risk analysis. The authors share their experience in applying the presented approach to derive security requirements for distributed airline turnaround systems. To stimulate more research in this critical area, we provide the following overview of ISS-relevant topics that could be published in BISE.

## 3 ISS Research Agenda

ISS research within the scope of BISE focuses on a socio-technical perspective, considering the interconnection between technological and organizational factors. Possible ISS questions can relate to the interplay between the structures (regulation), people (human behavior), technologies, and tasks conceptualized in Fig. 2. Attackers constantly threaten this dynamic construct and offer a rich playground for IS researchers. Research can focus on how the introduction of new structures (such as the upcoming EU-wide NIS2 regulation) or technologies (like GenAI) affects organizational tasks and human behavior. Reciprocal relationships, such as the regulation of new technologies, can also be the subject of research. In particular, AI technologies such as large language models and GenAI lead to new research questions. These research questions are part of a call for papers in MISQ (MISQ 2024) and underline the topic's importance. Focusing on the BISE departments, Table 1 shows potential research questions from the ISS area that match the departments' editorial statements.

The perspective of organizations and their strategic response to the heightened threat environment offers further opportunities for investigation. How organizations deal with data breaches also provides excellent research potential. While researchers have addressed the communication of data breaches as well as their impact on customer behavior (Janakiraman et al. 2018) and on

**Table 1** BISE department with potential ISS research questions

| BISE department | Research questions |
|---|---|
| Business Process Management | How can we evaluate the security risk associated with business processes? |
| | How can we design secure business processes? |
| Decision Analytics and Data Science | How can we leverage AI and ML to detect cyber attacks proactively? |
| | What are quantitative methods for dealing with the increased threat situation? |
| Digital Business Management and Digital Leadership | How can organizations integrate cybersecurity into their business strategy effectively? |
| | How can organizations balance the need for digital innovation with cybersecurity concerns? |
| Economics of Information Systems | How can organizations value the impact of cyber attacks? |
| | How does cybersecurity affect the economics of digital platforms and marketplaces? |
| Enterprise Modeling and Enterprise Engineering | How can we efficiently model security using information system concepts? |
| | What are reference architectures for secure information systems? |
| Human-Centered Information Systems | What contextual factors influence users' security behaviors? |
| | What influence do new technologies have on the security behavior of users? |
| | How do workplace dynamics influence the security behavior of employees? |
| Information Systems Engineering and Technology | How can we overcome the duality problem of ISS? |
| | How can we develop information systems to protect organizations from cyber attacks? |

companies' reputation (Syed 2019), IS management during or after a cyber attack remains understudied. In addition, the investigation of coping strategies and organizations' cyber resilience can also be part of further research. Other topics within this research area are the impact of innovations and the influence of security on digital business strategies. These topics address BISE's *Digital Business Management and Digital Leadership* department.

Including attacker perspectives in current research and the resulting proactive action of organizations offers potential for investigation. The design, implementation, and evaluation of technical solutions to detect and prevent cyber attacks is an essential research area (Hui et al. 2016). Dhillon et al. (2021) stated that much of the existing research focuses on phishing attacks and that it is important to investigate other types of cyber attacks (e.g., DDoS, Social Engineering, Ransomware) as well. While developing quantitative methods to detect cyber attacks and cyber risks is part of *Decision Analytics and Data Science*, the development of secure information systems, in general, is part of the *Information Systems Engineering and Technology* department. At BISE, however, we are not interested in purely technical solutions but in the interplay between technical solutions, human behavior, structures, and tasks. A better understanding of attack strategies on information systems and attackers' behavior might support countermeasures in a proactive manner.

Another research area is human behavior and human-computer interaction. Cram et al. (2024) advocate an idiographic approach, which focuses on the temporal changes in human behavior. In addition, Dhillon et al. (2021) highlight the context of research studies as an essential factor for developing behavioral theories. Research can investigate contextual theories that examine non-compliant employee behavior and workplace dynamics. Furthermore, researchers can examine the effects of the increasing threat situation on human behavior. On the other side, attackers can use new technologies, like GenAI, to develop even more sophisticated phishing techniques to deceive humans. The *Human-Centered Information Systems* department covers the effects of these technologies on human behavior (defender and attacker) and offers many opportunities for IS researchers.

Submissions focused on *Business Process Management* can explore the security aspects of business processes. Research questions may focus on enhancing the security of existing processes as well as designing new secure business processes. Submissions can explore process mining to discover hidden processes and verify compliance with respect to business rules or process models (Silalahi et al. 2022). This includes anomaly and drift detection. Additionally, it is possible to examine how organizations can automate security-related processes and the socio-technological implications of these changes. Submissions can also address aspects related to the duality problem of ISS (Baskerville 1993).

In the context of the *Economics of Information Systems*, researchers can investigate how to quantify cyber risk and the effects of cybersecurity on digital platforms and marketplaces. This research area also includes topics such as investments in cybersecurity architecture and the economic impact of data breaches. The research themes *market*

*effects of security enhancements* and *security investment studies*, as outlined in a research curation by Kai-Lung et al. (2016), align with the editorial statement of the *Economics of Information Systems* department.

*Enterprise Modeling and Enterprise Engineering* provide a conceptual perspective on ISS. Research questions can relate to the modeling of security aspects into digital twins and their consequences. Authors can address the investigation of reference architectures based on implemented information systems with case studies.

From a methodological perspective, we agree with the argument made by Siponen and Oinas-Kukkonen (2007) for the need to conduct more empirical studies, particularly in the development of new data science and machine learning (ML) methods. This approach can enhance the creation and design of systems for detecting threats, attacks, and incidents. Additionally, empirical data beyond laboratory settings is crucial to understanding the risks and vulnerabilities associated with human behavior. Given the current threat landscape, we believe that organizations need to be more open to research collaboration.

ISS is a vast and dynamic field of research, and the presented research areas provide a rough guide for researchers interested in publishing in BISE. Potential BISE submissions can address the increased threat situation, resulting dynamics, and effects on human behavior and organizations. As IS researchers, we cannot eliminate the threat of cyber attacks, symbolized by the sword of Damocles. However, we can strengthen the holding strand of horsehair by conducting insightful empirical analyses, enriching theory and understanding the behavior of players in this setting.

**Funding** Open Access funding enabled and organized by Projekt DEAL.



## References

Abbasi A, Dobolyi D, Vance A, Zahedi FM (2021) The phishing funnel model: a design artifact to predict user susceptibility to phishing websites. Inf Syst Res 32(2):410–436. https://doi.org/10.1287/isre.2020.0973

Allianz Commercial (2025) Allianz risk barometer. https://commercial.allianz.com/news-and-insights/reports/allianz-risk-barometer.html, accessed 20 Jan 2025

Ampel B, Samtani S, Zhu H (2024) Creating proactive cyber threat intelligence with hacker exploit labels: a deep transfer learning approach. MIS Q 48(1):137–166, https://doi.org/10.25300/MISQ/2023/17316

Angst C, Block E, D'Arcy J, Kelley K (2017) When do IT security investments matter? Accounting for the influence of institutional factors in the context of healthcare data breaches. MIS Q 41(3):893–916, https://doi.org/10.25300/MISQ/2017/41.3.10

Arce D (2022) Security-induced lock-in in the cloud. Bus Inf Syst Eng 64(4):501–513

Baskerville R (1993) Information systems security design methods: implications for information systems development. ACM Comput Surv (CSUR) 25(4):375–414

Baumann A, Haupt J, Gebert F, Lessmann S (2019) The price of privacy: an evaluation of the economic value of collecting clickstream data. Bus Inf Syst Eng 61(4):413–431

Binzer B, Kendziorra J, Witte AK, Winkler TJ (2024) Trust in public and private providers of health apps and usage intentions: a sectoral privacy calculus and control perspective. Bus Inf Syst Eng 66(3):273–297

Bromiley M (2016) Threat intelligence: what it is, and how to use it effectively. SANS Inst InfoSec Reading Room 15:172

Cambridge University Press (2024) The Cambridge Dictionary cybersecurity definition. https://dictionary.cambridge.org/dictionary/english/cybersecurity, accessed 09 Dec 2024

Chan J, He S, Qiao D, Whinston A (2024) Shedding light on the dark: the impact of legal enforcement on darknet transactions. Inf Syst Res 35(1):145–164. https://doi.org/10.1287/isre.2023.1222

Chen PY, Kataria G, Krishnan R (2011) Correlated failures, diversification, and information security risk management. MIS Q 35(2):397–422. https://doi.org/10.2307/23044049

Clearinghouse PR (2023) PRC Data Breach Chronology. https://privacyrights.org/, 01 Dec 2024

Cram W, D'Arcy J, Proudfoot J (2019) Seeing the forest and the trees: a meta-analysis of the antecedents to information security policy compliance. MIS Q 43(2):525–554, https://doi.org/10.25300/MISQ/2019/15117

Cram W, Arcy J, Benlian A (2024) Time will tell: The case for an idiographic approach to behavioral cybersecurity research. MIS Q 48(1):95–136, https://doi.org/10.25300/MISQ/2023/17707

de Nobrega KM, Rutkowski AF, Saunders C (2024) The whole of cyber defense: syncing practice and theory. J Strateg Inf Syst 33(4):101,861, https://doi.org/10.1016/j.jsis.2024.101861

Dhillon G, Backhouse J (2001) Current directions in is security research: towards socioorganizational perspectives. Inf Syst J 11:127–153. https://doi.org/10.1046/j.1365-2575.2001.00099.x

Dhillon G, Smith K, Dissanayaka I (2021) Information systems security research agenda: exploring the gap between research and practice. J Strateg Inf Syst 30(4):101,693

Ebrahimi M Jr, JFN, Chen H, (2020) Semi-supervised cyber threat identification in dark net markets: a transductive and deep learning approach. J Manag Inf Syst 37(3):694–722. https://doi.org/10.1080/07421222.2020.1790186

Ghahramani F, Yazdanmehr A, Chen D, Wang J (2023) Continuous improvement of information security management: an

organisational learning perspective. Europ J Inf Syst 32(6):1011–1032. https://doi.org/10.1080/0960085X.2022.2096491

Glöckler J, Sedlmeir J, Frank M, Fridgen G (2024) A systematic review of identity and access management requirements in enterprises and potential contributions of self-sovereign identity. Bus Inf Syst Eng 66(4):421–440

Hoehle H, Venkatesh V, Brown S, Tepper B, Kude T (2022) Impact of customer compensation strategies on outcomes and the mediating role of justice perceptions: a longitudinal study of target's data breach. MIS Q 46(1):299–340, https://doi.org/10.25300/MISQ/2022/14740

Holst M (2025) Everybody will be hacked, it's just a matter of when, not if. Interview Digi.no. https://riversecurity.eu/interview-digi-no-everybody-will-be-hacked-its-just-a-matter-of-when-not-if/, 02 Jan 2025

Hui KL, Vance A, Zhdanov D (2016) Securing digital assets. MIS Q Res Curations https://www.misqresearchcurations.org/blog/2017/5/10/securing-digital-assets-1, accessed 09 Dec 2024

Jaeger L, Eckhardt A (2021) Eyes wide open: the role of situational information security awareness for security-related behaviour. Inf Syst J 31(3):429–472. https://doi.org/10.1111/isj.12317

Janakiraman R, Lim JH, Rishika R (2018) The effect of a data breach announcement on customer behavior: evidence from a multichannel retailer. J Market 82(2):85–105

Jensen ML, Wright RT, Durcikova A, Karumbaiah S (2022) Improving phishing reporting using security gamification. J Manag Inf Syst 39(3):793–823. https://doi.org/10.1080/07421222.2022.2096551

Jiang Y, Jeusfeld MA, Ding J, Sandahl E (2023) Model-based cybersecurity analysis: extending enterprise modeling to critical infrastructure cybersecurity. Bus Inf Syst Eng 65(6):643–676

Karlsson F, Hedström K, Goldkuhl G (2017) Practice-based discourse analysis of information security policies. Comput Secur 67:267–279. https://doi.org/10.1016/j.cose.2016.12.012

Kotsias J, Ahmad A, Scheepers R (2023) Adopting and integrating cyber-threat intelligence in a commercial organisation. Europ J Inf Syst 32(1):35–51. https://doi.org/10.1080/0960085X.2022.2088414

Kwon J, Johnson M (2014) Proactive versus reactive security investments in the healthcare sector. MIS Q 38(2):451–471, https://doi.org/10.25300/MISQ/2014/38.2.06

Li W, Chen H (2022) Discovering emerging threats in the hacker community: a nonparametric emerging topic detection framework. MIS Q 46(4):2337–2350

Mahmood M, Siponen M, Straub D, Rao R, Santanam R (2010) Moving toward black hat research in information systems security: an editorial introduction to the special issue. MIS Q 34(3):431–433. https://doi.org/10.2307/25750685

Mannhardt F, Koschmider A, Baracaldo N, Weidlich M, Michael J (2019) Privacy-preserving process mining: differential privacy for event logs. Bus Inf Syst Eng 61(5):595–614

Matulevičius R, Norta A, Samarütel S (2018) Security requirements elicitation from airline turnaround processes. Bus Inf Syst Eng 60(1):3–20

Mehrizi MR, Nicolini D, Rodon J (2021) How do organizations learn from information system incidents? a synthesis of the past, present, and future. MIS Q 46(2), https://doi.org/10.25300/MISQ/2022/14305

MISQ (2024) Call for papers: Special issue on AI-IA nexus. https://misq.umn.edu/call-for-papers-ai-ia, accessed 12 Dec 2024

MITRE Corporation (2024) Common vulnerabilities and exposures database. https://www.cve.org/About/Metrics, accessed 09 Dec 2024

National Cyber Security Centre (2024) The near-term impact of AI on the cyber threat. https://www.ncsc.gov.uk/report/impact-of-ai-on-cyber-threat, accessed 18 Jan 2025

Nofer M, Hinz O, Muntermann J, Roßnagel H (2014) The economic impact of privacy violations and security breaches: a laboratory experiment. Bus Inf Syst Eng 6(6):339–348

Paananen H, Lapke M, Siponen M (2020) State of the art in information security policy development. Comput Secur 88(101):608. https://doi.org/10.1016/j.cose.2019.101608

Pienta D, Thatcher J, Johnston A (2020) Protecting a whale in a sea of phish. J Inf Technol 35(3):214–231. https://doi.org/10.1177/0268396220918594

Rosati P, Cummins M, Deeney P, Gogolin F, Van der Werff L, Lynn T (2017) The effect of data breach announcements beyond the stock price: Empirical evidence on market activity. Int Rev Financ Anal 49:146–154

Schatz D, Bashroush R (2016) The impact of repeated data breach events on organisations' market value. Inf Comput Secur 24(1):73–92

Sen R, Heim G, Zhu Q (2022) Artificial intelligence and machine learning in cybersecurity: applications, challenges, and opportunities for mis academics. Commun AIS 51:179–209, https://doi.org/10.17705/1CAIS.05109

Silalahi S, Yuhana UL, Ahmad T, Studiawan H (2022) A survey on process mining for security. In: 2022 international seminar on application for technology of information and communication (isemantic), pp 1–6, https://doi.org/10.1109/iSemantic55962.2022.9920473

Singh T, Johnston AC, D'Arcy J, Harms PD (2023) Stress in the cybersecurity profession: A systematic review of related literature and opportunities for future research. Organ Cybersecur J Pract Process People 3(2):100–126

Siponen MT (2005) An analysis of the traditional IS security approaches: implications for research and practice. Europ J Inf Syst 14(3):303–315

Siponen MT, Oinas-Kukkonen H (2007) A review of information security issues and respective research contributions. SIGMIS Database 38(1):60–80. https://doi.org/10.1145/1216218.1216224

Statista (2024) Cybercrime expected to skyrocket in coming years. https://www.statista.com/chart/28878/expected-cost-of-cybercrime-until-2027/, accessed 09 Dec 2024

Syed R (2019) Enterprise reputation threats on social media: a case of data breach framing. J Strateg Inf Syst 28(3):257–274. https://doi.org/10.1016/j.jsis.2018.12.001

Von Solms R, Van Niekerk J (2013) From information security to cyber security. Comput Secur 38:97–102

Wang Q, Ngai EWT, Pienta D, Thatcher JB (2023) Information technology innovativeness and data-breach risk: a longitudinal study. J Manag Inf Syst 40(4):1139–1170. https://doi.org/10.1080/07421222.2023.2267319

Wright R, Johnson S, Kitchens B (2023) Phishing susceptibility in context: a multilevel information processing perspective on deception detection. MIS Q 47(2):803–832, https://doi.org/10.25300/MISQ/2022/16625

Zahedi FM, Chen Y, Zhao H (2024) Ontology-based intelligent interface personalization for protection against phishing attacks. Inf Syst Res 35(3):1463–1478. https://doi.org/10.1287/isre.2021.0065