17th International Conference on Enterprise Systems, Accounting, Logistics and Management
(17th ICESALM 2023)
July 19-21, 2023, Corfu, Greece

Examining Information Security Challenges through a Diversity Lens: A Literature Study

Eli Hustad and Erlend Christiansen Skaar

University of Agder
Department of Information Systems
Kristiansand, Norway

eli.hustad@uia.no, erlecs18@student.uia.no

Abstract:
This study is based on an extensive review of the literature on information systems security. The review focused on topics such as security behavior, security culture, security policies, and compliance. Using a synthesis of 20 selected research studies, we present our findings in a narrative format to provide a rich understanding of the subject. Our results suggest that the field of information systems security is still in its early stages of development. The ever-evolving technological landscape has made security attacks increasingly sophisticated, posing significant challenges for organizations. Our analysis reveals that security behavior, organizational culture, and context are diverse and complex, requiring a nuanced approach to designing security policies that can achieve compliance. This nuanced approach should consider factors such as leadership, trust-building, awareness, and security behavior. Finally, we provide suggestions for future research in this field.

Keywords: *information systems, information security, security behaviour, security compliance, security policy, diversity*

1. Introduction

The importance of information security has garnered significant attention within modern organizations. With a persistent focus on the development of digital solutions and new technologies, novel methods, tools, and techniques for cybercrime continue to emerge (Bendovschi, 2015). Consequently, the imperative for security expertise and the implementation of robust security routines has become increasingly apparent (Cram et al., 2017). Organizations must carefully consider a range of external and internal security threats when formulating their security policies to effectively protect against unauthorized access to their systems (Alassaf & Alkhalifah, 2021; Ali et al., 2021). Of particular significance is the cultivation of awareness and adherence to security routines and best practices among employees, as research indicates that the most significant security threats often arise from within the organization, with security incidents predominantly caused by employees themselves (Hustad et al., 2020). Consequently, there has been a growing interest in recent years to comprehensively understand and identify effective security routines that can adeptly manage the complexities and comprehensiveness of the evolving threat landscape (Xu & Guo, 2019).

The current study is grounded in a comprehensive literature review, which endeavors to provide an overview of key research articles published within the past decade on the topic of information security, specifically as it pertains to information systems. The review specifically focuses on political guidelines, security behavior, and cultural factors that may significantly impact information security.

The following research question has guided our research study:

In the field of information systems research, how are key topics pertaining to information systems security prioritized and addressed in the existing literature?

2. Methodology

A literature review is a scholarly process that provides a comprehensive overview of existing knowledge in a particular field by identifying, collecting, and synthesizing prior research studies. It also involves recommending future research directions. In this study, we followed the systematic literature review procedure and practical guidelines developed by Kitchenham (2004).

Moreover, we utilized the narrative literature approach, as proposed by Paré et al. (2015), to present our study's findings. A narrative literature review offers more flexibility in sourcing a wider range of literature, including conceptual articles, literature reviews, and empirical case studies. Our aim was to synthesize existing research and provide a fresh perspective on the findings derived from our analysis, as recommended by Schryen et al. (2015). This approach facilitated the collation of the literature results and enabled us to identify potential avenues for future research on information systems security topics.

The literature review process in this study comprised three distinct steps, conducted in adherence to established academic protocols. Firstly, an extensive search was conducted to identify existing literature reviews that were relevant to the field of study. Next, a comprehensive protocol was developed, specifying pertinent search phrases, and establishing inclusion and exclusion criteria for the selection of studies to be included in the review. During the second step, a meticulous review was conducted, with a focus on empirical studies, although a few literature studies were included to provide a broader overview. The selection of relevant studies was done with careful consideration, and their quality was critically evaluated. Additionally, related topics and patterns identified from the studies were integrated into the review. Finally, the findings of the literature review were synthesized and summarized in a written report, adhering to academic conventions for presenting research outcomes.

The research studies included in our literature review were published during the last decade, specifically from 2012 to 2022. Additionally, we performed a backward search to ensure that important studies from the last decade were not overlooked.

To identify pertinent research studies, we employed search phrases that were relevant to the themes of information security in information systems, encompassing cultural and policy challenges (as outlined in Table 1). Our search was conducted in the Scopus database, utilizing the "title" and "keywords" fields, with a focus on literature pertaining to specific topics. Inclusion criteria for studies in our review were limited to empirical research studies published in research articles, conference papers, or book chapters. Studies that focused on computer science topics related to cryptography, network security, access control, and other technical solutions or algorithms specifically related to security threats were excluded from our analysis.

Table 1. Overview of research strings

Search phrases in combination (KEYWORDS or TITLE)	“Information systems security” AND “Culture” OR “Policies” OR “Security Behavior” Limited to 2012-2022 “Information systems security” AND “Challenges” Limited to 2012-2022
Inclusion criteria	Peer-reviewed, empirical studies, English language, research articles, conference papers, book sections Topics: Information systems and information security, socio-technical issues, culture and security culture, compliance, policies and guidelines for information securities, supporting technologies
Exclusion criteria	Books, conference reviews Topics: Specific programming languages and code, algorithm development and pure technological focus (e.g., in computer science topics related to cryptography, network security, access control, and other technical solutions or algorithms)

The initial search yielded a total of 331 publications. After removing duplicates and publications that did not meet accepted quality standards, the remaining pool was reduced to 225 publications. Subsequently, the abstracts of these papers were thoroughly reviewed to identify relevant studies for the research question at hand. Inclusion and exclusion criteria were applied to ensure that studies aligned with the topics of interest. This process resulted in a final set of 27 publications. The content of these selected publications underwent a comprehensive examination, guided by the inclusion and exclusion criteria. Additionally, the quality of the research studies, particularly the research methods employed, was meticulously assessed.

As a result of this rigorous selection process, a final body of 20 publications was identified for in-depth analysis, comprising 17 empirical studies and three literature reviews/conceptual studies (Table 2). The empirical studies included in this final set were characterized by robust methodologies and substantial data, making them suitable for detailed analysis. The literature reviews and conceptual studies, on the other hand, were used to provide an overview of the field. Notably, the relatively limited number of empirical studies published in reputable journals suggests that the research area of information security in relation to information systems is still in its early stages of development. Additionally, there appears to be a dominance of conference papers in this field, indicating that it is still a relatively immature research area.

Table 2. List of selected publications

#	**Reference**
1	Alassaf, M., & Alkhalifah, A. (2021). Exploring the Influence of Direct and Indirect Factors on Information Security Policy Compliance: A Systematic Literature Review. *IEEE Access, 9*, 162687-162705.
2	Ali, R. F., Dominic, P., Ali, S. E. A., Rehman, M., & Sohail, A. (2021). Information security behavior and information security policy compliance: A systematic literature review for identifying the transformation process from noncompliance to compliance. *Applied Sciences*, 11(8), 3383.
3	Bendovschi, A. (2015). Cyber-Attacks – Trends, Patterns and Security Countermeasures. *Procedia Economics and Finance, 28*, 24-31.
4	Choi, M., & Song, J. (2016). Leadership of Information Security Managers on the Effectiveness of Information Systems Security Through Mediate of Organizational Culture. Paper presented at the *Advanced Multimedia and Ubiquitous Engineering Conference*, Singapore.
5	Connolly, L., & Lang, M. (2012). Data protection and employee behavior: the role of information systems security culture. Paper presented at the *IADIS WWW/Internet 2012 Conference*.
6	Cram, W. A., Proudfoot, J. G., & D'Arcy, J. (2017). Organizational information security policies: a review and research framework. *European Journal of Information Systems, 26*(6), 605-641.
7	Ismail, O. (2022). Designing Information Security Culture Artifacts to Improve Security Behavior: An Evaluation in SMEs. Paper presented at *The Transdisciplinary Reach of Design Scienc Research*, Cham.
8	Lin, C., & Luo, X. (2021). Toward a unified view of dynamic information security behaviors: insights from organizational culture and sensemaking. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems, 52*(1), 65-90.
9	Lopes, I., & Oliveira, P. (2015). Implementation of Information Systems Security Policies: A Survey in Small and Medium Sized Enterprises. *New Contributions in Information Systems and Technologies: 1, 353*, 459.
10	Niemimaa, E. (2016). Crafting an Information Security Policy: Insights from an Ethnographic Study. In *ICIS proceedings*.
11	Offor, P., & Tejay, G. (2014). Information systems security training in organizations: Andragogical perspective. In *AMCIS proceedings*.

12	Pahnila, S., Karjalainen, M., & Siponen, M. (2013). Information Security Behavior: Towards Multi-Stage Models. *PACIS 2013 Proceedings*, Paper 102.
13	Shahri, A. B., Ismail, Z., & Rahim, N. Z. A. (2013). Constructing Conceptual Model for Security Culture in Health Information Systems Security Effectiveness. *Advances in Information Systems and Technologies*, 213-220.
14	Siponen, M., Adam Mahmood, M., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information & Management, 51*(2), 217-224.
15	Subramanian, V., Seker, R., Ramaswamy, S., & Lenin, R. B. (2012). PCIEF: a policy conflict identification and evaluation framework. *International Journal of Information and Computer Security, 5*(1), 48-67.
16	Tilahun, A., & Tibebe, T. (2017). Influence of national culture on employees' intention to violate information systems security policies: A national culture and rational choice theory perspective. In *Proceedings of the 25th European Conference on Information Systems (ECIS 2017)* 2493-2503.
17	Wall, J., & Iyer, L. (2012). The dark side of leadership in information systems security: A model of the effect of manager transgressions on employee security behaviors. In *AMCIS 2012 Proceedings*, Paper 12.
18	Xu, Z., & Guo, K. (2019). It ain't my business: a coping perspective on employee effortful security behavior. *Journal of Enterprise Information Management, 32*(5), 824-842.
19	Zheng, D., & Walter, Z. D. (2020). Moral Hazard in Compliance: The Impact of Moral Intensity and Competing Values. In *AMCIS proceedings*.
20	Stewart, H. (2022). A systematic framework to explore the determinants of information security policy development and outcomes. *Information & Computer Security, 30*(4), 490-516.

3. Findings

Drawing on the conducted analysis, the outcomes gathered from the analysis of pertinent research studies were categorized into two overarching domains of information security in the field of information systems research: (1) Security behavior, and (2) Security policies and countermeasures. While various factors significantly influence security behavior, organizational culture, security culture, and leadership emerged as predominant ones. The selected papers shed light on the critical topic of security compliance and non-compliance in connection with both security behavior and security policies. The second category accentuates vital countermeasures that can aid organizations in managing information security challenges.

3.1 Security behaviour

Many selected articles center on diverse facets of security behavior and the strategies organizations can employ to ensure compliance or prevent non-compliance among their employees.

In a recent study conducted by Ismail (2022), the findings of the design science research demonstrate a robust correlation between Information Systems (IS) security culture and user behaviors. Specifically, a positive security culture fosters the development of security behaviors. The concepts of organizational culture are congruent with those of security culture, which includes security awareness, ownership, and compliance. By leveraging security culture artifacts, organizations can positively impact security behavior and compliance. Additionally, by providing management support, conducting risk assessments, designing security policies, facilitating education, and training, and interpreting organizational behavior (e.g., job satisfaction and personality traits), customized policies and training materials can be created. This approach leads to increased employee awareness of information security, ultimately resulting in better security practices and reduced security incidents.

Choi & Song (2016) conducted a study that focused on examining the significance of leadership in enhancing the effectiveness of information security managers, mediated by the organizational culture. They found that the shared values, beliefs, and norms that exist within an organization play a crucial role in transforming leadership style and behavior into concrete security outcomes. Similarly, Connolly & Lang (2012) explored the impact of the security culture on employee behavior concerning data protection. Their research showed that a positive security culture, characterized by robust security awareness, norms, and practices, leads to more compliant and secure employee behavior, while a weak security culture may result in negligent or non-compliant behavior. Additionally, leadership commitment, management support, and effective communication play an essential role in shaping the information security culture.

Shahri et al. (2013) developed a conceptual model to identify the factors that influence security culture in health information systems (HIS). Their research identified security communication and security training and education as crucial for enhancing the effectiveness of the security culture in HIS. Leadership commitment, employee awareness, and training and education were identified as significant elements of the security culture, supported by various IS security studies (e.g., Choi & Song, 2016; Wall & Iyer, 2012).

The study conducted by Wall & Iyer (2012) explores the adverse effects of managerial transgressions on employee security behaviors within the context of IS security. The authors propose a theoretical framework that elucidates how unethical conduct by managers can impact employees' security-related behaviors. The findings of this study reveal that when employees observe their managers engaging in transgressive behaviors, such as violating security policies or engaging in unethical practices, it can result in a reduction in employees' adherence to security protocols and an increase in their involvement in risky security behaviors. The study identifies two types of IS security deviance, intentional policy non-compliance and unintentional neglect of proactive security behaviors. Additionally, the research underscores the significance of effective leadership and highlights the need for managers to model ethical behavior as a means of fostering a culture of information security within organizations.

Xu & Guo (2019) find that employee procrastination of security tasks and psychological detachment from security issues are key antecedents of effortful security behavior. These are influenced by perceived externalities of security risk and business task prioritization. Employees use problem-focused (preventive measures, seeking information) and emotion-focused (ignoring or avoiding threats) coping strategies to manage security risks, which are influenced by their perception of security significance, self-efficacy, and organizational context. The study highlights the need for organizations to understand employees' coping mechanisms and provide support and resources to promote effective security behaviors.

In another study of Lin & Luo (2021), they found that a positive organizational culture and effective sensemaking processes can foster a proactive and vigilant approach towards information security, leading to better security behaviors in organizations. Furthermore, the authors propose that before adopting an approach to information security control, organizations should evaluate their cultures. An organization may have various subcultures coexisting within its boundaries. Thus, a uniform information security approach may not be suitable. Instead, multiple approaches that fit each subculture can be implemented to foster effective security behaviors.

Ali et al. (2021) developed a model to explain how organizations can transition from non-compliance to compliance with IS security policies, based on a thorough literature review. The authors identified seven categories of factors that influence compliance behavior, such as national culture and intrinsic/extrinsic motivations. Intrinsic motivation, characterized by positive behavior without external rewards, was found to be the most effective form of motivation. Improving intrinsic motivation can reduce the likelihood of IS security breaches. Protection motivation, which is the desire to protect organizational values, and extrinsic incentives for external rewards, also influence security compliance.

The authors also identified factors leading to non-compliance, including security-related stress/neutralization, value conflicts, and deterrence. Employees may avoid complying with security policies due to the stress or tension it may cause. The literature review found that employees view IS security policies as external and stressful to follow, leading them to adopt non-compliant behavior and tactics to avoid punishment.

Pahnila et al.(2013) propose a multi-stage model for understanding IS security behavior that includes factors such as awareness, knowledge, and perception of security threats. It is crucial to consider the level of employees' knowledge when designing security measures. Compliance with security policies can be influenced by employees' knowledge of security issues. The researchers assessed employees' knowledge of IS security by asking a few questions related to their organization's security policy. The results revealed significant differences between the low and high knowledge groups. Thus, distinct levels of knowledge can be viewed as different stages of employees' compliance with IS security policy.

In a study conducted by Zheng & Walter (2020), they explored the impact of moral intensity and competing values on moral hazard in compliance. Their model incorporated threat appraisal, coping with appraisal, and cost-consequence misalignment, focusing on compliance costs for employees and consequences of non-compliance for organizations. Results indicated that proximity and social consensus were significant factors in the relationship between employees and organizations, and coping appraisal had a greater impact on compliance intention than threat appraisal. The study highlights the importance of employee proximity and organization type in compliance and suggests that reducing the moral hazard of compliance can be achieved by improving the relationship between employees and organizations.

3.2 Information Systems Security Policies (ISSP) and Countermeasures

Several of the selected papers, discuss and suggest countermeasures to tackle a variety of information security issues (Alassaf & Alkhalifah, 2021; Bendovschi, 2015; Choi & Song, 2016) and security policy compliance is influenced by a combination of direct and indirect factors, and organizations should consider implementing effective awareness and training programs, enforcement mechanisms, and fostering a positive organizational culture and leadership to promote compliance with information security policies. Trust-building measures can also be considered to enhance compliance behavior (Alassaf & Alkhalifah, 2021).

Numerous studies have explored information security concerns and offered potential solutions, as evidenced by the selected articles (e.g., Alassaf & Alkhalifah, 2021; Bendovschi, 2015; Choi & Song, 2016). In order to achieve compliance with security policies, organizations must account for both direct and indirect influences. Effective awareness and training programs, along with strict enforcement measures and the cultivation of a positive organizational culture and leadership, can promote policy compliance. Additionally, trust-building measures may prove beneficial in encouraging compliant behavior (Alassaf & Alkhalifah, 2021).

Bendovschi's (2015) article delves into a range of security countermeasures that can be utilized to alleviate the negative effects of cyber-attacks. These countermeasures include technical measures such as firewalls, intrusion detection systems, and encryption, in addition to organizational measures such as employee training, incident response plans, and risk management strategies. The research emphasizes the significance of a multi-faceted approach to cybersecurity that encompasses technical, organizational, and human factors. The article also identifies several obstacles and limitations in addressing cyber-attacks, such as the swift pace of technological advancements, the constantly evolving nature of cyber threats, the absence of international coordination in cybersecurity endeavors, and the human factor as a frail link in security.

Offer & Tejay's (2014) research examines the development of effective information security education programs, aimed at promoting compliance with security policies in organizations. In their study, they utilize Adult Learning Theory, a framework that emphasizes a learner-centric approach. By adopting this approach, the authors suggest that training programs should be designed to incorporate critical elements such as motivation, reinforcement, retention, and transference of knowledge, throughout the entire IS security training process.

The authors contend that adult learners are a diverse group, with unique characteristics and learning needs that should be taken into account when designing IS security education programs. As such, the education provided should be tailored to address the specific problems and tasks that employees are expected to handle, to effectively promote compliance with security policies.

In a research investigation carried out by Siponen et al.(2014), it was demonstrated that an employee's self-efficacy in relation to potential information security threats, their attitude toward adhering to information security policies, and their normative beliefs exerted a highly significant and positive influence on their intention to comply with information security policies and procedures. Furthermore, it was revealed that the intention to comply with these policies had a substantial and positive impact on actual compliance with them. Conversely, the provision of rewards for complying with security policies, and an employee's response efficacy, did not manifest a significant effect on compliance with these policies.

Subramanian et al.(2012) conducted a study that underscores the need to consider the diversity of domains when designing and managing security policies. In the modern business landscape, it is common for enterprises to have a presence in multiple geographical locations. Such organizations often operate in project-based work environments that are in a constant state of evolution. In order to ensure the security of these operations, it is necessary to develop specific security policies that are tailored to the unique requirements of each location, while also maintaining existing policies. This process entails taking into consideration not only technical factors but also socio-political and legal requirements that can vary between regions. These complex and varied considerations can significantly impact the design of effective security policies.

To address these challenges, the authors propose a Policy Conflict Identification and Evaluation Framework (PCIEF), which presents a systematic approach for identifying policy conflicts and assessing their severity and potential impact on information security within an organization. The study highlights the importance of addressing policy conflicts in organizations to enhance the effectiveness of information security policies, by maintaining and modifying policies as required.

Lopes & Oliveira (2015) identified critical success factors for implementing a security policy in SMEs. The study revealed significant differences between SMEs with and without a security culture, leading to a division of the sample into two clusters. User training was found to be the most important factor in both clusters. For SMEs with a security document, the document's clarity and concision and monitoring compliance were critical. For SMEs without a policy, executive board willingness to implement an ISS policy, engagement in implementation, and attention to technology acquisition were crucial. The authors stress that implementing an ISS policy is a dynamic process that requires ongoing evaluation, planning, and adjustment. They also acknowledge that SMEs present a diverse range of sizes and cultures, necessitating the identification of inhibiting factors and the development of an ISS policy model that accounts for this diversity.

In (2017), Tilahun & Tibebe conducted a pilot study with 230 responses examining the impact of national culture on employees' intentions to violate ISS policies. To achieve this, the authors developed and tested an empirical ISS compliance model, which was based on rational choice theory and national culture constructs related to security. The research was conducted in both Ethiopia and the US, and Hofstede's national culture dimensions were utilized. The study's objective was to investigate how national culture affects employees' compliance with ISS policies and to understand the moderating effect of cultural dimensions on ISS countermeasures such as formal sanctions, moral beliefs, shame, and perceived benefits. The authors' findings revealed that cultural dimensions significantly influence employees' intentions to violate their company's ISSP. As a result, ISS managers should be aware of how cultural dimensions impact employees' ISS behavior and consider this factor when designing and implementing ISS policies or strategies.

Stewart (2022) developed a framework with six crucial constructs for successful ISSP development and implementation. Especially, employee awareness and training are crucial for preserving the security of sensitive data and reducing human errors and negligence. It is also essential to remove misperceptions about information security and increase employees' perceptions of its relevance.

Moreover, involving external partners and stakeholders, investing in information security and organizational commitment, increasing security and cyber threat intelligence, and establishing a security culture, were considered critical. Investing in ISSPs offers benefits that outweigh costs, as ISSPs can enhance compliance and yield financial benefits. Stewart's framework provides a practical guide for companies to improve their information security policies and protect sensitive data.

4. Discussion

Drawing upon the analysis of our literature review, a novel perspective arises, namely diversity. Our examination reveals that security behavior manifests in varied ways across diverse organizations. Therefore, devising a uniform security policy capable of accommodating the needs of all organizations presents a formidable challenge.

Through our analysis, we have identified several diversity dimensions in the various studies. For instance, the level of knowledge, awareness, and perception of security threats among employees varied greatly, with some possessing high levels of knowledge while others demonstrated a low level of awareness (Lopes & Oliveira, 2015; Pahnila et al., 2013). These findings formed the basis for the development of a multi-stage model aimed at understanding information system (IS) security behavior and compliance with IS security policies, as proposed by Pahnila et al. (2013).

In addition, several studies discussed different management styles, including those presented by Choi & Song (2016), Shahri et al. (2013), and Wall & Iyer (2012). It was noted that organizational context, organizational and national culture also played significant roles in influencing security behavior and compliance, as shown in the works of Xu & Guo (2019), Lin & Luo (2021), and Ali et al.(2021). Furthermore, due to the diverse nature of adult learners, training and education programs must be tailored to meet the unique needs of organizations' employees, as emphasized in the research conducted by Offor & Tejay (2014).

Moreover, we found that various business domains, technical, socio-political, and legal requirements, which differ across regions and geographical locations, as well as the constantly changing nature of project organizations, as noted by Subramanian et al. (2012), can lead to conflicts in security policies that require customization and modifications to ensure compliance.

Drawing upon the findings of these studies, it has become evident that individuals exhibit varying degrees of awareness and understanding with respect to security threats. This underscores the need for customized security policies and behaviors, as a one-size-fits-all approach may not prove effective. To this end, organizations must account for the diversity of their workforce in terms of attitudes, knowledge, skills, and professional backgrounds. Such a holistic approach will require customized training and education programs to ensure compliance with security policies.

The inclusion of a diverse workforce can facilitate innovative approaches to security, leading to more effective solutions to security challenges. As such, involving employees in the establishment of a security culture and appropriate ISS policy will be vital for organizations to stay ahead of constantly evolving security landscapes and emerging threats.

By acknowledging diversity in security behavior and compliance with security policies, organizations could implement the following measures:

Firstly, organizations should provide regular training and education to all employees on security best practices and the underlying rationale for these practices. This will ensure that everyone is aware of security risks and how to mitigate them.

Secondly, open communication and feedback mechanisms should be encouraged from employees on security policies and behaviors. This will enable organizations to identify areas where policies may not be effective or may need to be adapted to different employee groups.

Thirdly, security policies and behaviors should be flexible and adapted to different roles, responsibilities, and needs within the organization. This approach ensures that everyone is capable of complying with policies and can contribute to security efforts.

Lastly, organizations should create a culture of inclusivity and encourage employees to take ownership of security within the organization. These measures may collectively promote the diversification of security approaches, ultimately improving overall organizational security.

5. Future research

Cram et al. (2017) put forth an inclusive framework for recommending future research endeavors on organizational information security policies and their impact on security practices. Their paper was aiming to propose future research avenues. The authors suggest various areas for future inquiry, such as the development of more effective security policies that account for employees' perceptions of legitimacy, fairness, and justice. They also advocate that managers consider a broader range of employee-centric factors while customizing security policies. Additionally, they propose the significance of identifying factors that may diminish the positive correlation between security policy compliance and organizational security performance, which may result in security incidents. Lastly, the authors recommend exploring how organizations modify security policies following a data breach.

Furthermore, based on the findings from this literature review, we propose the following avenues for further research:

The significance of human factors in information security behavior is a crucial area of research. To gain a comprehensive understanding, future studies should focus on cognitive and behavioral factors influencing security decision-making and ways to design interventions that promote secure behavior (e.g., Zheng & Walter, 2020).

User training and awareness programs have been found to be effective in promoting secure behavior (e.g., Lopes & Oliveira, 2015). Future research could examine the effectiveness of different types of awareness and training programs and enforcement mechanisms, as well as investigate the dynamics of organizational culture and leadership and the role of trust in compliance behavior. Additionally, studies could explore the interactions between direct and indirect factors and contextual factors that may influence compliance behavior (e.g., Alassaf & Alkhalifah, 2021). Longitudinal studies could provide more robust evidence on the temporal dynamics of compliance behavior and help establish causal relationships. Understanding these complex dynamics could aid in the development of effective strategies to promote compliance behavior among employees.

Organizational culture and security policy are critical factors influencing information security behavior. Future research should explore the relationship between these factors and employee behavior, and ways to design effective policies and security cultures to promote secure behavior (e.g., Ismail, 2022).

Design of technology and systems can also have an impact on information security behavior. Future research should focus on designing secure systems that are user-friendly, universal, and accessible to a wide range of users (e.g., Li et al., 2021).

Threat intelligence and response play a crucial role in mitigating security incidents. Research should explore ways to improve these capabilities to better protect organizations and individuals from security threats (e.g., Bendovschi, 2015; Stewart, 2022).

Overall, future research should aim to better comprehend the complex interplay between technology, human behavior, and organizational factors in information security. Effective interventions to promote secure behavior should also be explored in depth to ensure that organizations can better protect themselves and their stakeholders from potential security breaches.

References

Alassaf, M., & Alkhalifah, A. (2021). Exploring the Influence of Direct and Indirect Factors on Information Security Policy Compliance: A Systematic Literature Review. *IEEE Access, 9*, 162687-162705. doi:10.1109/ACCESS.2021.3132574

Ali, R. F., Dominic, P., Ali, S. E. A., Rehman, M., & Sohail, A. (2021). Information security behavior and information security policy compliance: A systematic literature review for identifying the transformation process from noncompliance to compliance. *Applied Sciences, 11*(8), 3383.

Bendovschi, A. (2015). Cyber-Attacks – Trends, Patterns and Security Countermeasures. *Procedia Economics and Finance, 28*, 24-31. doi:https://doi.org/10.1016/S2212-5671(15)01077-1

Choi, M., & Song, J. (2016). Leadership of Information Security Managers on the Effectiveness of Information Systems Security Through Mediate of Organizational Culture. *Advanced Multimedia and Ubiquitous Engineering: FutureTech & MUE*, 649-654.

Connolly, L., & Lang, M. (2012). *Data protection and employee behaviour: the role of information systems security culture.* Paper presented at the IADIS WWW/Internet 2012 Conference.

Cram, W. A., Proudfoot, J. G., & D'Arcy, J. (2017). Organizational information security policies: a review and research framework. *European Journal of Information Systems, 26*(6), 605-641. doi:10.1057/s41303-017-0059-9

Hustad, E., Bekkevik, F. M., Holm, O. R., & Vassilakopoulou, P. (2020). Employee Information Security Practices: A Framework and Research Agenda. *International Journal of E-Services and Mobile Applications (IJESMA), 12*(2), 1-14.

Ismail, O. (2022, 2022//). *Designing Information Security Culture Artifacts to Improve Security Behavior: An Evaluation in SMEs.* Paper presented at the The Transdisciplinary Reach of Design Science Research, Cham.

Kitchenham, B. (2004). Procedures for performing systematic reviews. *Keele, UK, Keele University, 33*(2004), 1-26.

Li, H., Yoo, S., & Kettinger, W. J. (2021). The Roles of IT Strategies and Security Investments in Reducing Organizational Security Breaches. *Journal of*

Management Information Systems, 38(1), 222-245. doi:10.1080/07421222.2021.1870390

Lin, C., & Luo, X. (2021). Toward a unified view of dynamic information security behaviors: insights from organizational culture and sensemaking. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems, 52*(1), 65-90.

Lopes, I., & Oliveira, P. (2015). Implementation of Information Systems Security Policies: A Survey in Small and Medium Sized Enterprises. *New Contributions in Information Systems and Technologies: Volume 1, 353*, 459.

Offor, P., & Tejay, G. (2014). Information systems security training in organizations: Andragogical perspective. *AMCIS Proceedings*, Paper 23.

Pahnila, S., Karjalainen, M., & Siponen, M. (2013). Information Security Behavior: Towards Multi-Stage Models. *PACIS 2013 Proceedings*, Paper 102.

Paré, G., Trudel, M.-C., Jaana, M., & Kitsiou, S. (2015). Synthesizing information systems knowledge: A typology of literature reviews. *Information & Management, 52*(2), 183-199.

Schryen, G., Wagner, G., & Benlian, A. (2015). *Theory of knowledge for literature reviews: an epistemological model, taxonomy and empirical analysis of IS literature.* Paper presented at the 36th International Conference on Information Systems (ICIS) 2015, Fort Worth, TX.

Shahri, A. B., Ismail, Z., & Rahim, N. Z. A. (2013). Constructing Conceptual Model for Security Culture in Health Information Systems Security Effectiveness. *Advances in Information Systems and Technologies*, 213-220.

Siponen, M., Adam Mahmood, M., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information & Management, 51*(2), 217-224. doi:https://doi.org/10.1016/j.im.2013.08.006

Stewart, H. (2022). A systematic framework to explore the determinants of information security policy development and outcomes. *Information & Computer Security, 30*(4), 490-516. doi:10.1108/ICS-06-2021-0076

Subramanian, V., Seker, R., Ramaswamy, S., & Lenin, R. B. (2012). PCIEF: a policy conflict identification and evaluation framework. *International Journal of Information and Computer Security, 5*(1), 48-67.

Tilahun, A., & Tibebe, T. (2017). Influence of national culture on employees' intention to violate information systems security policies: A national culture and rational choice theory perspective. *Proceedings of the 25th European Conference on Information Systems (ECIS 2017)* 2493-2503.

Wall, J., & Iyer, L. (2012). The dark side of leadership in information systems security: A model of the effect of manager transgressions on employee security behaviors. *AMCIS 2012 Proceedings*, Paper 12.

Xu, Z., & Guo, K. (2019). It ain't my business: a coping perspective on employee effortful security behavior. *Journal of Enterprise Information Management, 32*(5), 824-842. doi:10.1108/JEIM-10-2018-0229

Zheng, D., & Walter, Z. D. (2020). Moral Hazard in Compliance: The Impact of Moral Intensity and Competing Values. *AMCIS 2020 Proceedings*, Paper 37.