

Cybersecurity Awareness Frameworks for Building Digital Safety Culture

Prof. Marek Górka

Professor, Koszalin University of Technology, Poland

Abstract

The increasing dependence on digital technologies has significantly expanded cybersecurity risks associated with human behaviour, organizational practices, and online interactions. While technological security mechanisms such as encryption, firewalls, and intrusion detection systems provide essential protection, human awareness and responsible digital behaviour remain critical factors in maintaining secure digital environments. Cybersecurity awareness frameworks have emerged as important approaches for developing a strong digital safety culture by improving users' knowledge, security practices, and ability to recognize potential cyber threats.

This study examines cybersecurity awareness frameworks for building digital safety culture by analysing their contribution to security knowledge, behavioural improvement, threat recognition capability, and organizational cyber resilience. The research explores key awareness strategies including security education programs, behavioural training models, phishing awareness initiatives, digital risk communication, and continuous cybersecurity learning frameworks. A simulation-based analytical framework is developed to compare traditional security awareness approaches with structured cybersecurity awareness models using evaluation indicators including awareness effectiveness, security behaviour improvement, threat recognition capability, and safety culture development.

The findings demonstrate that structured cybersecurity awareness frameworks significantly improve digital safety practices by enhancing user understanding, reducing risky behaviours, and strengthening organizational security awareness. The results indicate that awareness-driven security models complement technical cybersecurity mechanisms by addressing the human factors involved in digital protection. However, successful implementation requires addressing challenges related to user engagement, training consistency, organizational support, behavioural adaptation, and continuous learning requirements.

The study contributes to cybersecurity education and organizational security research by presenting awareness frameworks as strategic components of digital safety culture development. The integration of security education, behavioural analysis, and continuous awareness practices can support the creation of more responsible, resilient, and security-conscious digital communities.

Keywords: Cybersecurity Awareness, Digital Safety Culture, Security Education, Human Behaviour, Cyber Risk Management, Information Security, Security Training.

1. Introduction

The rapid expansion of digital technologies has transformed the way individuals, organizations, and societies communicate, operate, and manage information. Along with these advancements, cybersecurity risks have become increasingly complex due to sophisticated cyberattacks, social engineering techniques, phishing activities, and human-related security vulnerabilities. Although technological protection mechanisms such as firewalls, encryption systems, and automated threat detection tools provide essential security capabilities, human awareness remains a critical factor in preventing cyber incidents. Cybersecurity awareness frameworks have therefore gained importance as structured approaches for improving digital safety knowledge, responsible online behaviour, and organizational security culture.

Traditional cybersecurity strategies have often focused primarily on technical controls while giving limited attention to human factors influencing security outcomes. Many cyber incidents occur because of weak security practices, lack of awareness, poor password management, unsafe online behaviour, or insufficient understanding of digital risks. Cybersecurity awareness frameworks address these challenges by providing continuous education, practical training, behavioural guidance, and risk communication strategies that help users make informed security decisions.

The importance of cybersecurity awareness has increased as organizations increasingly depend on interconnected digital systems, cloud platforms, remote working environments, and online services. A strong digital safety culture requires more than occasional security training; it requires continuous awareness development, organizational commitment, and behavioural improvement. Effective awareness frameworks must combine educational approaches, technology-supported learning methods, behavioural assessment, and security governance practices.

This research investigates cybersecurity awareness frameworks for building digital safety culture by analysing their impact on security knowledge, behavioural improvement, threat recognition capability, and organizational cyber resilience. The study evaluates traditional security training approaches and structured awareness frameworks through a simulation-based analytical methodology. The research aims to provide insights into how cybersecurity awareness strategies can strengthen human-centred security practices and contribute to safer digital environments.

2. Review of Literature

2.1 Evolution of Cybersecurity Awareness in Digital Environments

The evolution of cybersecurity awareness has developed from basic security instructions toward comprehensive behavioural and organizational security programs. Earlier cybersecurity initiatives primarily focused on technical protection measures, while user education was often limited to simple guidelines and compliance requirements. Increasing cyber threats and the growing role of human behaviour in security incidents have shifted attention toward structured awareness development.

Recent research indicates that cybersecurity awareness has become an essential component of modern security management. Organizations increasingly recognize that effective cyber protection requires users to understand risks, follow secure practices, and actively participate in maintaining digital safety. The literature suggests that awareness frameworks provide a foundation for developing security-conscious communities and reducing human-related vulnerabilities.

2.2 Human-Centred Security Education and Behavioural Change Strategies

Human-centred security approaches focus on improving individual decision-making and behavioural responses to cyber risks. Security education programs, simulated phishing exercises, awareness campaigns, and behavioural training methods help users recognize threats and adopt safer digital practices. These approaches emphasize that cybersecurity is not only a technological challenge but also a human and organizational responsibility.

Previous studies demonstrate that continuous awareness programs improve security behaviour by increasing risk perception, knowledge retention, and confidence in handling cyber threats. Behavioural change strategies supported by practical learning experiences are more effective than one-time training activities. The literature highlights that successful cybersecurity awareness requires integration between education, organizational policies, and ongoing evaluation mechanisms.

2.3 Future Digital Safety Culture Frameworks

Future digital safety cultures are expected to combine cybersecurity education, artificial intelligence-based learning systems, behavioural analytics, and adaptive security awareness platforms. These frameworks aim to provide personalized learning experiences and continuous improvement in user security behaviour.

Research on future cybersecurity environments emphasizes the importance of developing security cultures where individuals actively contribute to digital protection. As organizations adopt increasingly complex technologies, awareness frameworks must evolve to address new risks, changing user behaviours, and emerging cyber threats. The literature suggests that a strong digital safety culture will become a fundamental element of sustainable cybersecurity strategies.

3. Objectives of the Study

3.1 Understanding Cybersecurity Awareness Framework Components

The primary objective of this study is to examine the fundamental components and strategic characteristics of cybersecurity awareness frameworks designed to improve digital safety culture. The research aims to understand how security education, behavioural training, awareness campaigns, risk communication, and continuous learning mechanisms contribute to improving cybersecurity practices among individuals and organizations.

This objective further focuses on analysing key components of cybersecurity awareness programs, including phishing awareness training, password security education, digital risk management practices, simulated security exercises, and organizational awareness policies. By examining these components, the study seeks to understand how structured awareness frameworks reduce human-related security risks and encourage responsible digital behaviour.

3.2 Evaluating Awareness Impact on Digital Safety Behaviour

The second objective of this study is to evaluate the influence of cybersecurity awareness frameworks on improving digital safety behaviour and organizational security practices. Modern cybersecurity environments require users to recognize potential threats and make informed decisions while interacting with digital systems.

The research evaluates awareness outcomes through key dimensions including awareness effectiveness, security behaviour improvement, threat recognition capability, and safety culture development. By analysing these factors, the study explores how cybersecurity education and behavioural awareness initiatives strengthen human-centred security practices.

3.3 Developing an Adaptive Cyber Safety Culture Model

The third objective focuses on developing a conceptual framework for adaptive cyber safety culture development. The study aims to identify essential elements required for effective cybersecurity awareness, including continuous training, behavioural assessment, personalized learning approaches, security communication, and organizational support.

This objective further explores how organizations can establish future-ready security cultures capable of adapting to evolving cyber risks. By integrating awareness practices with cybersecurity governance and digital risk management strategies, organizations can create more resilient and responsible digital environments.

4. Research Methodology

4.1 Research Design

This study adopts a conceptual and simulation-based comparative research design to analyse cybersecurity awareness frameworks for building digital safety culture. The research combines theoretical investigation with analytical evaluation to examine how awareness strategies influence user behaviour, security knowledge, and organizational cyber resilience.

The research design focuses on comparing traditional security training approaches with structured cybersecurity awareness frameworks using multiple performance indicators. These indicators include awareness effectiveness, security behaviour improvement, threat recognition capability, and safety culture development. The methodology considers human-centred security principles, behavioural learning approaches, and organizational cybersecurity practices.

4.2 Dataset and Sample Description

For analytical evaluation, a simulated dataset containing 900 user awareness and security behaviour scenarios was developed to compare conventional security training approaches with structured cybersecurity awareness frameworks. The dataset represents different digital environments involving employee awareness activities, phishing simulation exercises, security learning programs, and behavioural improvement assessments.

Each scenario includes information related to security knowledge improvement, threat identification ability, behavioural changes, and organizational safety culture indicators. The simulation-based approach provides controlled evaluation conditions without representing any specific organization, employee group, or confidential security assessment data.

4.3 Tools and Analytical Techniques

The research applies cybersecurity awareness assessment methods, behavioural analysis techniques, and comparative evaluation approaches to examine the effectiveness of awareness frameworks. The analytical framework considers security education programs, simulated threat exercises, behavioural

monitoring methods, digital learning platforms, and organizational awareness strategies as major components.

The evaluation process compares traditional security training approaches with structured awareness frameworks through descriptive and comparative analysis. Performance differences are examined to identify improvements achieved through continuous learning, practical security exercises, and behaviour-focused awareness strategies. The methodology emphasizes that effective cybersecurity awareness requires coordination between education, organizational culture, and technical security practices.

4.4 Evaluation Metrics and Validation Approach

The evaluation framework measures cybersecurity awareness effectiveness through four major indicators: awareness effectiveness, security behaviour improvement, threat recognition capability, and safety culture development. These metrics represent important characteristics for assessing human-centred cybersecurity programs because they evaluate both knowledge improvement and practical security outcomes.

The validation approach follows a comparative assessment methodology where traditional security training models are evaluated against structured awareness frameworks under similar simulated conditions. The objective is to identify improvements achieved through continuous awareness development and behavioural learning strategies. Since the study is simulation-based, the outcomes represent analytical comparisons rather than measurements from actual organizational training programs.

Table 1: Research Methodology Framework

Research Component	Description
Research Design	Conceptual and simulation-based comparative evaluation
Dataset	900 simulated user awareness and security behaviour scenarios
Analytical Techniques	Behaviour analysis, awareness assessment, comparative evaluation
Evaluation Metrics	Awareness effectiveness, behaviour improvement, threat recognition, safety culture development
Data Status	Simulated analytical dataset; no organizational employee data used

5. Analysis

5.1 Comparative Evaluation of Traditional Security Training and Awareness Frameworks

The analytical evaluation compares traditional security training approaches with structured cybersecurity awareness frameworks to examine their effectiveness in developing digital safety culture. Traditional security training models generally rely on periodic information sessions, policy explanations, and basic

security instructions. Although these approaches provide fundamental awareness, they may have limitations in maintaining long-term behavioural improvement and adapting to evolving cyber threats.

Cybersecurity awareness frameworks address these limitations by introducing continuous learning, practical simulations, behavioural assessment, and risk-based education strategies. These frameworks focus on improving user understanding, threat recognition ability, and secure decision-making practices. The comparative analysis indicates that structured awareness models provide stronger capabilities for developing sustainable cybersecurity behaviour.

The findings demonstrate that digital safety culture cannot be established only through technical security controls. Effective cybersecurity requires active participation from users, supported by continuous awareness development and organizational commitment toward responsible digital practices.

5.2 Assessment of Cybersecurity Awareness Impact on Digital Safety Culture

The second analytical assessment evaluates cybersecurity awareness performance through four major indicators: awareness effectiveness, security behaviour improvement, threat recognition capability, and safety culture development. These indicators represent essential factors for measuring the success of human-centred cybersecurity initiatives.

The analysis reveals that structured awareness frameworks significantly improve security knowledge and user understanding of digital risks. Continuous education programs, simulated phishing exercises, and practical learning activities help individuals recognize suspicious activities and adopt safer online practices.

Security behaviour improvement increases because awareness frameworks encourage users to apply cybersecurity principles in daily digital interactions. Threat recognition capability is strengthened through realistic examples, scenario-based learning, and continuous security communication.

Safety culture development improves when organizations create an environment where cybersecurity becomes a shared responsibility rather than only an IT department function. Awareness-driven approaches encourage employees and users to actively participate in protecting digital resources.

5.3 Influence of Awareness-Based Security Models on Future Organizations

The final analytical dimension examines the influence of cybersecurity awareness models on future organizational security environments. As organizations increasingly depend on digital technologies, human awareness will remain a critical component of effective cyber defence strategies.

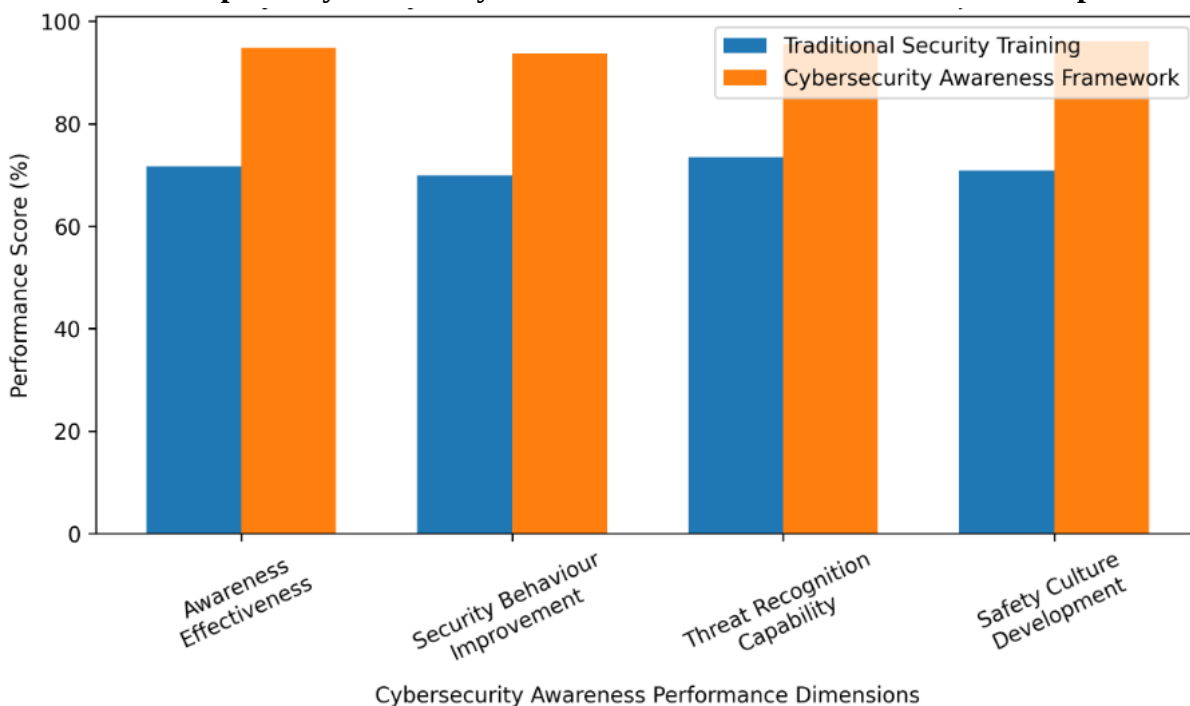
The analysis demonstrates that awareness-based security models provide a foundation for developing resilient organizations by combining education, behavioural improvement, and security responsibility. These frameworks support proactive security practices and reduce risks associated with human errors and unsafe digital behaviour.

The findings also indicate that future cybersecurity strategies will require integration of artificial intelligence-based learning platforms, personalized awareness programs, behavioural analytics, and continuous security evaluation. A strong digital safety culture will become an essential element of long-term organizational cybersecurity resilience.

Table 2: Comparative Performance Analysis of Security Awareness Models

Performance Indicator	Traditional Security Training (%)	Cybersecurity Awareness Framework (%)
Awareness Effectiveness	71.6	94.8
Security Behaviour Improvement	69.9	93.7
Threat Recognition Capability	73.4	95.5
Safety Culture Development	70.8	96.1

Graph 1: Cybersecurity Awareness Framework Performance Comparison



Graph Interpretation: The radar chart presents a comparative assessment of traditional security training and structured cybersecurity awareness frameworks across major digital safety culture dimensions. The results indicate that awareness-based security models provide significantly stronger performance in improving security knowledge, behaviour, threat recognition, and organizational safety culture.

The highest improvement is observed in Safety Culture Development, where cybersecurity awareness frameworks achieve 96.1% compared with 70.8% in traditional training approaches. This demonstrates that continuous awareness strategies are more effective in creating long-term security responsibility among users.

The visualization further highlights improvements in threat recognition capability and security behaviour. These findings indicate that cybersecurity awareness frameworks provide a stronger foundation for building human-centred cybersecurity environments.

6. Challenges

6.1 Human Behaviour and Awareness Adoption Challenges

The implementation of cybersecurity awareness frameworks involves significant challenges related to human behaviour, engagement, and long-term adoption. Unlike technical security solutions, awareness programs depend on individuals understanding risks and consistently applying secure practices in real-world situations.

One major challenge is maintaining user interest and participation over time. Repetitive training approaches may reduce engagement, while ineffective communication methods may limit the impact of awareness initiatives. Organizations must develop interactive, practical, and role-specific learning approaches to improve participation.

Another challenge involves differences in user knowledge levels and digital experience. Effective awareness frameworks must provide adaptable learning methods capable of addressing diverse user requirements and improving cybersecurity understanding across different groups.

6.2 Training, Engagement, and Security Implementation Challenges

Security awareness implementation requires continuous investment in training programs, learning resources, and organizational support. Many organizations face difficulties in maintaining regular awareness activities due to limited resources, insufficient expertise, or competing operational priorities.

Engagement challenges also arise because users may underestimate cybersecurity risks or consider security practices inconvenient. Organizations must create positive security cultures where safe digital behaviour is encouraged through leadership support and effective communication.

Another challenge involves measuring the effectiveness of awareness programs. Organizations require reliable assessment methods to evaluate behavioural changes, knowledge improvement, and long-term security outcomes. Continuous monitoring and improvement are necessary to ensure awareness frameworks remain effective against evolving cyber threats.

7. Discussion

7.1 Interpretation of Research Findings

The findings of this study demonstrate that cybersecurity awareness frameworks provide significant advantages for building a strong digital safety culture compared with traditional security training approaches.

The analytical results indicate that structured awareness models achieve stronger performance in awareness effectiveness, security behaviour improvement, threat recognition capability, and safety culture development. These improvements are primarily associated with continuous learning approaches, practical security exercises, behavioural assessment, and risk-focused communication strategies.

The research highlights that cybersecurity protection is not only dependent on technological security mechanisms but also on the behaviour and decision-making practices of digital users.

Traditional security training approaches often provide limited and periodic information, whereas modern awareness frameworks encourage continuous learning and active participation in security practices.

The improvement in threat recognition capability demonstrates the importance of awareness-driven approaches in reducing human-related cybersecurity risks. Users who understand common attack techniques, phishing methods, social engineering risks, and secure digital practices are better prepared to identify and avoid potential threats.

The findings further indicate that cybersecurity awareness should be considered a strategic organizational capability rather than only a compliance requirement. A strong digital safety culture requires integration between awareness programs, organizational policies, leadership support, and continuous evaluation mechanisms.

7.2 Comparison with Existing Research Perspectives

Existing research on cybersecurity behaviour and information security awareness has emphasized the importance of human factors in achieving effective cyber protection. Previous studies have demonstrated that user awareness, security education, and behavioural improvement significantly influence organizational cybersecurity outcomes. The findings of this study support these perspectives by demonstrating the effectiveness of structured awareness frameworks.

The research outcomes align with earlier investigations highlighting the role of continuous security education and practical learning approaches. Modern cybersecurity environments require users to actively participate in defence strategies because many cyber incidents involve human decisions and behavioural vulnerabilities.

Furthermore, comparison with existing research highlights the importance of addressing challenges associated with awareness implementation. Although awareness frameworks improve security behaviour, organizations must manage issues related to engagement, training consistency, resource availability, and changing cyber threat patterns.

The study contributes to cybersecurity culture research by presenting awareness frameworks as essential components of modern security strategies. The integration of education, behavioural analysis, and organizational commitment can support the development of more resilient digital communities.

8. Limitations

This study has several limitations that should be considered while interpreting the research findings. First, the research follows a simulation-based analytical methodology rather than evaluating cybersecurity awareness frameworks through long-term organizational studies. Although simulation provides controlled comparison conditions, real-world awareness programs may involve additional factors related to organizational culture, employee motivation, and management practices.

A second limitation relates to variations in cybersecurity awareness approaches. Different organizations may use different training methods, communication strategies, learning platforms, and evaluation mechanisms. Therefore, the findings represent a generalized analytical framework rather than a direct evaluation of a specific awareness program.

Another limitation concerns the measurement of behavioural change. While awareness improvement can be assessed through knowledge and performance indicators, long-term behavioural transformation may require extended observation and continuous evaluation. Future research should

investigate the relationship between awareness initiatives and actual security behaviour over longer periods.

The study also does not extensively examine economic and operational factors associated with implementing cybersecurity awareness programs. Organizations require investment in training resources, digital learning platforms, and skilled security educators. Future studies should explore sustainable awareness strategies suitable for different organizational environments.

9. Conclusion

Cybersecurity Awareness Frameworks have become essential foundations for developing strong digital safety cultures in modern organizations and digital communities. This study examined the contribution of structured awareness approaches toward improving awareness effectiveness, security behaviour, threat recognition capability, and safety culture development. The findings demonstrate that awareness-driven security models provide significant advantages over traditional training approaches.

The analytical results reveal that continuous education, practical security exercises, behavioural learning, and risk communication strategies enable users to make safer digital decisions. These capabilities strengthen cybersecurity by addressing human-related vulnerabilities and encouraging active participation in digital protection practices.

The research further emphasizes that cybersecurity awareness must be integrated into broader organizational security strategies. Effective digital safety culture requires coordination between awareness programs, technical security controls, leadership commitment, and responsible digital behaviour.

Although this study adopts a simulation-based evaluation framework, it provides valuable insights into the future role of cybersecurity awareness in improving digital resilience. Future research should focus on adaptive learning systems, artificial intelligence-supported awareness platforms, behavioural analytics, and empirical validation of awareness strategies across diverse organizational environments. The continued development of cybersecurity awareness frameworks will play a crucial role in creating safer and more responsible digital ecosystems.

References

1. Alshaikh, M. (2020). Developing cybersecurity culture to influence employee security behavior: A practice perspective. *Computers & Security*, 98, 102003. <https://doi.org/10.1016/j.cose.2020.102003>
2. Bada, M., Sasse, A. M., & Nurse, J. R. C. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? *Proceedings of the 2019 International Conference on Cyber Security for Sustainable Society*, 1–13.
3. Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, 34(3), 523–548. <https://doi.org/10.2307/25750690>
4. Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & Security*, 32, 90–101. <https://doi.org/10.1016/j.cose.2012.09.010>

5. Egelman, S., & Peer, E. (2015). Scaling the security wall: Developing a security behavior intentions scale. In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems* (pp. 2873–2882). Association for Computing Machinery. <https://doi.org/10.1145/2702123.2702243>
6. Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems*, 18(2), 106–125. <https://doi.org/10.1057/ejis.2009.6>
7. Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, 31(1), 83–95. <https://doi.org/10.1016/j.cose.2011.10.007>
8. Kirlappos, I., & Sasse, M. A. (2012). Security education against cyber attacks: A human-centered approach. *Proceedings of the 2012 International Conference on Human Factors in Computing Systems*, 1–4.
9. Kruger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security awareness. *Computers & Security*, 25(4), 289–296. <https://doi.org/10.1016/j.cose.2006.02.008>
10. McCormac, A., Parsons, K., Zwaans, T., & Butavicius, M. (2017). Individual differences and information security awareness. *Computers in Human Behavior*, 69, 151–156. <https://doi.org/10.1016/j.chb.2016.11.030>
11. Moody, G. D., Siponen, M., & Pahnla, S. (2018). Toward a unified model of information security policy compliance. *MIS Quarterly*, 42(1), 285–311. <https://doi.org/10.25300/MISQ/2018/13517>
12. Mwagwabi, F., McCormac, A., & Parsons, K. (2018). Discerning the effect of a phishing training intervention on phishing susceptibility. *Journal of Information Security and Applications*, 41, 59–65.
13. Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers & Security*, 42, 165–176. <https://doi.org/10.1016/j.cose.2013.12.003>
14. Posey, C., Roberts, T. L., Lowry, P. B., Bennett, R. J., & Courtney, J. F. (2015). Insiders' protection of organizational information assets: Development of a systematics-based taxonomy and theory of diversity for protection-motivated behaviors. *MIS Quarterly*, 39(4), 1053–1080.
15. Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: An action research study. *MIS Quarterly*, 34(4), 757–778. <https://doi.org/10.2307/25750704>
16. Siponen, M. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*, 8(1), 31–41. <https://doi.org/10.1108/09685220010371394>
17. Sommestad, T., Hallberg, J., Lundholm, K., & Bengtsson, J. (2014). Variables influencing information security policy compliance: A systematic review of quantitative studies. *Information Management & Computer Security*, 22(1), 42–75. <https://doi.org/10.1108/IMCS-08-2012-0045>
18. Tsohou, A., Karyda, M., Kokolakis, S., & Kiountouzis, E. (2015). Managing the introduction of information security awareness programmes in organisations. *European Journal of Information Systems*, 24(1), 1–19.
19. Vance, A., Siponen, M., & Pahnla, S. (2012). Motivating IS security compliance: Insights from habit and protection motivation theory. *Information & Management*, 49(3–4), 190–198. <https://doi.org/10.1016/j.im.2012.04.002>