RAIS RESEARCH ASSOCIATION for INTERDISCIPLINARY STUDIES
November 21-22, 2024

DOI:10.5281/zenodo.14514698

Emerging Vulnerabilities in Cyberspace: Analyzing Organizational Behaviors and Complexities

Horace C. Mingo

Marymount University, Arlington, United States, hcm67738@marymount.edu

ABSTRACT: The increasing frequency and sophistication of cyberattacks have exposed organizational systems to significant vulnerabilities. However, much of the current research remains focused on technical solutions. This study addresses this gap by examining how organizational behaviors, internal complexities, and leadership dynamics can exacerbate or mitigate cybersecurity risk. This study employs a qualitative content analysis approach to investigate how these factors contribute to cyber vulnerabilities. It uses a hypothetical organizational model to simulate real-world cyber incidents, such as ransomware attacks, phishing, data breaches, and insider threats. These findings demonstrate the critical importance of an integrated approach that addresses technical and organizational challenges in enhancing cybersecurity resilience. By focusing on these often-overlooked aspects, this study provides practical insights for organizational leaders and cybersecurity professionals, offering them actionable strategies for improving their cybersecurity posture. Based on our key findings, these strategies can be implemented immediately to bolster organizational cybersecurity. This review article delineates the research methodologies employed, highlights the key findings, and discusses practical strategies to improve organizational cybersecurity.

KEYWORDS: Cybersecurity vulnerabilities, organizational behavior, leadership, human factors, complex adaptive systems

Introduction

The increasing reliance on digital infrastructure has revolutionized organizational operations and heightened cybersecurity risks. Despite technological advances, such as encryption and intrusion detection systems, businesses globally face persistent cyberattacks, with data breaches and ransomware incidents growing in frequency and cost. Human behavior and organizational structure significantly affect cybersecurity vulnerabilities (Pollini et al. 2022). This study explores often-overlooked organizational behaviors and internal complexities contributing to vulnerabilities, advocating a comprehensive cybersecurity approach.

Ransomware attacks on organizations surged in 2021, with 66% of companies targeted, up from 37% in the previous year, an increase of 78% (Baig, Mekala, and Zeadally 2023, 1). This rise is mainly due to vulnerabilities from remote work and the rapid adoption of digital technology. Manufacturing, telecommunications, business, marketing, transportation, and healthcare sectors are particularly susceptible (Fatim, Mustafa, and Farooq 2021, 21). High-profile ransomware incidents such as the Colonial Pipeline and Kaseya attacks have a severe impact on supply chains and critical services (Ologunde 2023, 2-4).

Recent studies have emphasized the limitations of traditional cybersecurity approaches focused mainly on technological defenses, ignoring human and organizational factors. Human errors cause 95% of security breaches (Nobles 2018, 82). Cybersecurity research often overlooks theoretical and cultural aspects (Rahman et al. 2021, 10). Emotional intelligence is vital for effective cybersecurity leadership, fostering innovative work behavior, and improving responses to complex threats (Burton et al. 2023, 163). Organizations are adopting more holistic strategies that integrate advanced technologies like AI and ML with an understanding of human factors and compliance with international standards (Abrahams et al. 2024, 13). Continuous education and training combined with a balanced approach of technological and human elements is recommended for effective cybersecurity management.

Contemporary cyber threats require an integrated approach that addresses technical vulnerabilities as well as human and organizational factors. This investigation examines the organizational behavior, leadership dynamics, and internal complexities that drive

cybersecurity vulnerabilities. By exploring these dimensions, this study offers insights into enhancing cyber resilience and the efficacy of cybersecurity strategies, which are essential for mitigating successful cyberattacks and establishing robust cybersecurity frameworks across diverse industries.

Problem Statement

Cybersecurity has become crucial for organizations in the digital landscape (Untawale 2021, 963). Organizations' dependence on technology and supply chains has rendered them more susceptible to cybersecurity threats (Boyens et al. 2021, 1). Despite advancements in technical solutions, a significant gap persists in understanding and addressing the organizational behaviors and complexities that contribute to these vulnerabilities (Pollini et al. 2022, 385). This study investigates organizational behaviors that increase cybersecurity vulnerabilities in hypothetical automotive manufacturing organizations.

Purpose of the Study

This study aims to investigate the impact of organizational behaviors and internal complexities on cybersecurity vulnerabilities. It focuses on how leadership, culture, employee behaviors, and communication affect cyber risk exposure and identifies effective mitigation strategies.

Significance of the Study

This study fills a crucial gap in cybersecurity research by examining how organizational behaviors, leadership dynamics, and internal complexities contribute to vulnerabilities. This emphasizes that technical solutions alone are inadequate against sophisticated cyberattacks; the relationship between human behaviors, organizational culture, and technical systems often dictates cybersecurity effectiveness. This study advocates integrating organizational and technological strategies to enhance cybersecurity resilience.

Several alarming trends underscore the importance of the present study. Despite significant investments in cybersecurity infrastructure, human errors account for 95% of security breaches (Nobles 2018, 82). This study examines how leadership, employee training, and interdepartmental communication contribute to cybersecurity risks, with the aim of shifting the focus from purely technological solutions to human and organizational dimensions. The significance of this study lies in providing actionable insights to mitigate breaches from internal vulnerabilities, thereby reducing the financial and operational impacts of cyberattacks.

Research Questions

This study examined the complex relationship between organizational behavior and cybersecurity, emphasizing the need for a holistic approach to cybersecurity risk management.

Main Research Question (RQ0)

RQ0: How do organizational behaviors and internal complexities influence cybersecurity vulnerabilities in a hypothetical organization focused on cybersecurity and what strategies can effectively mitigate these risks? This study investigated the connection between organizational structures and cybersecurity challenges by examining weaknesses and successful risk reduction approaches.

Sub-Questions (RQ1-RQ4)

The following sub-questions address the main research questions.

RQ1: What specific organizational behaviors and cultural aspects contribute to the increased cybersecurity vulnerabilities in organizations? This inquiry examined and evaluated

organizational behavior patterns, cultural norms, and attitudes that could potentially increase or decrease cybersecurity threats.

RQ2: How do internal organizational complexities, such as structure, communication flow, and leadership, impact the management and effectiveness of cybersecurity measures? This inquiry explores how internal organizational frameworks and interactions affect the effectiveness of cybersecurity approaches and methods.

RQ3: How do technological advancements and human elements interact within an organization to influence cybersecurity postures? The emphasis is on examining how technical systems and human elements interact and evaluating how this interplay affects an organization's overall cybersecurity posture.

RQ4: What practical strategies and practices can organizations adopt to mitigate cybersecurity risks, considering technical and behavioral aspects? This inquiry explores and suggests strategic methods that combine technological innovations and organizational cultural changes to bolster cybersecurity measures.

Literature Review

Organizational Behavior and Cybersecurity

Human factors are critical in cybersecurity; however, organizations often emphasize technical solutions to organizational behavior. Employee negligence, poor cybersecurity culture, and inadequate training significantly heighten risk (Aksoy 2023, 52; Triplett 2022, 574). Although 85% of breaches result from human factors, 97% of the security budget is spent on technology (Aksoy 2023, 53). Effective cybersecurity management requires integrating technical and human elements (Aksoy 2023, 53; Pollini et al. 2021, 385). Establishing a security-first culture is vital, with leadership playing a pivotal role (Willie 2023, 183). However, some senior executives still consider cybersecurity as an IT-only issue (Willie 2023, 191). To reduce risks, organizations should prioritize education, awareness, and communication (Triplett 2022, 584) and adopt user-centered strategies that consider individual, organizational, and technological dimensions (Pollini et al. 2021, 377).

Social Engineering and Human Factors

Social engineering attacks effectively exploit human vulnerabilities and bypass technical security measures (Siddiqi, Pak, and Siddiqi 2022, 1). These attacks utilize psychological mechanisms such as emotional manipulation, social influence, and persuasion (Wang, Zhu, and Sun 2021, 11897). They specifically target cognitive biases, behavioral habits, and personality traits (Montañez, Golob, and Xu 2020, 2). Standard methods include phishing and social network manipulation (Maraj and Butler 2022, 187). Organizations must focus on technological defenses and human factors to mitigate these threats, as advanced technologies alone are insufficient (Maraj and Butler 2022, 185). Siddiqi, Pak, and Siddiqi (2022, 11) explored the potential of machine learning-based countermeasures. A comprehensive strategy that integrates technical solutions with an understanding of human psychology and behavior is essential to combat social engineering attacks.

Complex Adaptive Systems (CAS) and Cybersecurity

Complex Adaptive Systems (CAS) theory offers crucial insights into addressing challenges across cybersecurity, disaster management, healthcare, and global health. The CAS highlights the adaptability, learning capabilities, and interconnectedness of system components (Burger, Kennedy, and Crooks 2021, 2-6; Kiviliene and Blaževičienė 2019, 47). This approach allows us to examine the interactions between human and technical elements in cybersecurity, moving beyond technocentric solutions to include sociotechnical factors (Thinyane 2024, 562). Similarly, CAS provides a framework for analyzing the interactions among physical, social, and individual actor systems in disaster studies (Burger, Kennedy, and Crooks 2021, 3-11). In healthcare, CAS theory

introduces new perspectives on nursing leadership and organizational structures (Kiviliene and Blaževičienė 2019, 47-49). Applying a CAS perspective to health systems can enhance policy-making and resilience to transnational health risks (Borghi et al. 2022, 7-8). Overall, the CAS offers a comprehensive method for understanding and managing complex systems across various disciplines.

The Role of Organizational Culture

Organizational culture is pivotal in shaping cybersecurity risk management. Aksoy (2024, 99) argues that a strong cybersecurity culture driven by beliefs, values, and attitudes bolsters resilience against cyber threats. Quader and Janeja (2021, 653-656) highlight the importance of human behavior and organizational culture in understanding and mitigating cyber-attacks, suggesting that proactive strategies can improve security preparedness. Hopcraft et al. (2022, 14) emphasized that incorporating cyber risk into safety culture is vital for maritime organizations to enhance cyber incident readiness. Nifakos et al. (2021, 14) found that human factors and inadequate awareness create cybersecurity vulnerabilities in healthcare, underscoring the need for comprehensive training and risk assessment. These studies underscore the importance of fostering a robust organizational culture to mitigate cybersecurity risks across various sectors.

Constructivism in Cybersecurity and Social Engineering

Social engineering, a significant cybersecurity threat, exploits human vulnerabilities rather than technical flaws (Klimburg-Witjes and Wentland 2021, 1317-1319; Akyesilmen and Alhosban 2024, 343), impacting individual, institutional, and national security (Akyesilmen and Alhosban 2024, 344). The discourse often portrays users as "deficient," shifting blame from institutions to individuals (Klimburg-Witjes and Wentland 2021, 1326). Marketing's use of big data and digital techniques is evolving into social engineering methods, signaling a paradigm shift (Lies 2019, 141). AI in social engineering introduces new risks such as manipulating public consciousness and violating human security (Kolinko, Petryshyn, and Chumak 2024, 11). Mitigation strategies include penetration testing, awareness training (Akyesilmen and Alhosban 2024, 355) and fostering a culture of collective cyber responsibility (Klimburg-Witjes and Wentland 2021, 333).

Technology-Organization-Environment Framework

The Technology-Organization-Environment (TOE) framework explains technological innovation adoption through technological, organizational, and environmental contexts (Alam and Islam 2021, 59-61), evaluates cybersecurity adoption factors such as IT infrastructure, competence, top management support, and perceived benefits (Alam and Islam 2021, 65-72). Regulatory requirements and industry standards influence cybersecurity practices (Bondoc and Malawit 2020, 19). However, the traditional TOE framework may not fully address cybersecurity complexities, leading to an expanded framework that includes cyber catalysts and practice standards (Wallace et al. 2020, 341). The TOE framework has been adapted for technologies such as blockchain, integrating perceived risks and information transparency (Malik et al. 2021, 2-5) and big data technology adoption, emphasizing compatibility and security (Harun et al. 2022, 407). Extending the TOE framework to include cybersecurity-specific factors better addresses evolving cyber threats and complex decision-making processes to protect digital assets (Alam and Islam 2021, 73-75; Harun et al. 2022, 405-407; Wallace et al. 2020, 340-341).

Theory of Planned Behavior

The Theory of Planned Behavior (TPB) has been widely applied to understand user behavior in cybersecurity and technology adoption. Research shows that TPB components, such as attitude and subjective norms, influence users' intentions to adopt clean technologies (Pakravan and MacCarty 2020, 15) and food delivery apps (Belanche, Flavián, and Pérez-Rueda 2020, 3). TPB is recognized as explaining compliance and violation behaviors in cybersecurity (Sulaiman et al. 2022, 9–10).

Studies have also examined how attitudes impact user security strategies, identifying that behavioral, affective, and cognitive elements differentiate user groups (Szűcs, Tick, and Reicher 2024, 134–135). Additionally, perceived security and lifestyle compatibility influence user intentions and word-of-mouth behavior in technology adoption (Belanche, Flavián, and Pérez-Rueda 2020, 3-4). These findings highlight the importance of understanding user attitudes and motivations for promoting desired behaviors across various domains.

Research Methodology

This study employed qualitative content analysis to examine the interplay between organizational behavior and cybersecurity vulnerabilities (Mingo 2024, 75). The data were drawn from the scholarly literature, case studies, and industry reports. The hypothetical organizational model of CyberKirk Inc. was developed to simulate real-world cybersecurity scenarios, including ransomware attacks, insider threats, and phishing campaigns. NVivo software was used to conduct a thematic analysis of the qualitative data and identify patterns and recurring themes related to organizational behavior and cybersecurity risks.

Research Design

A qualitative content analysis was conducted to systematically review scholarly literature, industry reports, and case studies, particularly suitable for examining complex, non-quantifiable aspects of organizational behavior, such as leadership, cultural attitudes toward cybersecurity, and human-technology interactions. Thematic analysis identified recurring patterns and themes related to cybersecurity vulnerabilities stemming from organizational behavior. The research is based on the Technology-Organization-Environment (TOE), Theory of Planned Behavior (TPB), and Complex Adaptive Systems (CAS) theories, offering a multidimensional perspective on the interactions between technological systems, human behavior, and organizational structures.

Data Collection

Data were systematically collected to examine how organizational behaviors contribute to cybersecurity vulnerability. The research utilized three primary sources–scholarly literature, industry reports, and case studies–offering comprehensive insights into theoretical and practical organizational influences on cybersecurity.

Scholarly Literature

Scholarly literature was sourced from peer-reviewed journals in the cybersecurity, organizational behavior, and related fields. The following keywords were used to search academic databases such as Google Scholar, IEEE Xplore, and JSTOR: "cybersecurity vulnerabilities," "organizational behavior," "social engineering," "cyber incident response," and "leadership and cyber risk." A total of 150 articles were reviewed, 45 of which were selected for further analysis based on their relevance to organizational and human factors in cybersecurity.

Industry Reports

Industry reports from cybersecurity firms and consultancy organizations are crucial data sources, offering real-world examples of how organizational structure, employee behavior, and leadership impact cybersecurity defenses. Searches used databases and platforms such as Gartner, McKinsey, and Forrester with keywords such as "cyber incident response" and "leadership and cyber risk." Of the 50 reports reviewed, 20 were chosen for their detailed coverage of organizational vulnerabilities in cybersecurity incidents.

Case Studies

To enhance the literature and reports, detailed case studies of real-world cybersecurity breaches were analyzed. These studies have focused on ransomware attacks, phishing campaigns, and insider threats. Of the 30 reviewed case studies, 10 were chosen for the final analysis, offering qualitative insights into how human factors and internal organizational complexities contributed to cybersecurity failures.

Table 1 summarizes the key components of the hypothetical organizational model used in this research, highlighting how different internal factors contribute to cyber risk.

Table 1: Content Analysis Search Strategy

Source Type	Keywords	Articles Reviewed	Selected Sources
Scholarly Literature	"cybersecurity vulnerabilities," "organizational behavior," "social engineering"	150	45
Industry Reports	"cyber incident response," "leadership and cyber risk"	50	20
Case Studies	"ransomware," "phishing attacks," "insider threat"	30	10

Note: Table 1 shows the search strategy used to collect data for qualitative content analysis, focusing on cybersecurity-related organizational factors.

Hypothetical Organizational Model: CyberKirk Inc.

To simulate real-world organizational behaviors and their impact on cybersecurity, this study developed the CyberKirk Inc. model, a hypothetical organization designed to reflect the typical internal complexities and cybersecurity challenges faced by mid-to-large-sized enterprises. Table 1 lists the critical components of the hypothetical organizational model. Table 2 shows the search strategy used to gather literature and reports for analysis, detailing the research focus areas on organizational behavior and cybersecurity vulnerabilities.

Table 2: Hypothetical Model Components

Component	Description
Organizational Structure	Simulates departments with siloed communication and leadership styles
Employee Behavior	Simulated varying levels of cybersecurity awareness among employees
Leadership Dynamics	Different levels of commitment to cybersecurity practices
Cybersecurity Incidents	Includes ransomware, phishing, insider threats, and data breaches

Note: Table 2 presents the key elements of the CyberKirk Inc. hypothetical model, which simulates the internal organizational complexities contributing to cybersecurity vulnerabilities.

This model incorporates organizational structures simulating various departments (e.g., IT, HR, Finance) with distinct communication channels and hierarchies to mimic siloed behavior and fragmented communication, employee behavior simulating employees with different levels of cybersecurity awareness, adherence to policies, risk perceptions, and leadership dynamics, and a leadership structure that highlights differences in commitment to cybersecurity, creating opportunities for analyzing how leadership influences risk management. This model explored four critical cybersecurity scenarios: ransomware attacks, insider threats, supplier data breaches, and phishing campaigns. These scenarios were chosen based on their

prevalence and relevance in the current cybersecurity landscape, and their dependence on organizational behavior as a critical factor in mitigating or exacerbating risks.

Data Analysis

NVivo qualitative analysis software was used to facilitate thematic coding of the data. The coding process is as follows.

1. Initial Coding: Identifying broad themes such as "organizational culture," "employee behavior," "leadership influence," and "cybersecurity strategies."
2. Axial Coding: Refining these categories to explore their interconnections, such as how leadership commitment affects employee adherence to security protocols or how internal communication influences an organization's ability to respond to cyber threats.
3. Thematic Analysis: Final themes were synthesized to provide insights into overarching research questions. The analysis focused on how each CyberKirk model scenario demonstrated the influence of organizational behavior on cybersecurity outcomes.

Validity and Reliability

Several strategies were employed to ensure the rigor of the research.

- Triangulation: Data were drawn from multiple sources (literature, industry reports, and case studies) to validate the findings from different perspectives.
- Peer Review: Cybersecurity professionals and organizational behavior experts reviewed the initial findings and coding categories to confirm the accuracy and relevance of the identified themes.
- Reflexivity: The researcher remained conscious of potential biases throughout the analysis, particularly regarding interpretations of leadership and organizational culture, by revisiting the coding frameworks and critically reviewing the literature.

Results and Analysis

Organizational Behaviors and Cybersecurity Vulnerabilities

The findings indicate that certain organizational behaviors, such as poor adherence to cybersecurity policies and resistance to change, directly contribute to an increased risk of cyberattacks (Mingo, 2024, 15). Employees often disregard security protocols, believing that they are either unnecessary or too restrictive, thus creating significant vulnerabilities (Ncubukezi 2022, 400). Additionally, the lack of cybersecurity training exacerbates the likelihood of employees falling victim to social engineering attacks, which rely on human error.

Complex Internal Dynamics

Organizations with complex internal structures, characterized by siloed departments and fragmented communication, struggle to implement cohesive cybersecurity strategies. Mtsweni, Gcaza, and Thaba (2018, 2-3) confirmed that internal complexities can delay decision-making and response times during a cyber incident, allowing threats to proliferate. In such environments, leadership often fails to integrate cybersecurity into broader organizational goals, leaving organizations vulnerable to both internal and external threats.

Human-Technology Interface

The interaction between human factors and technological infrastructure creates significant security gaps, particularly when employees are undertrained or unaware of risks. Human factors are a critical weak point in cybersecurity, where the misalignment between human behavior and technological defenses often results in breaches (Hughes-Lartey, Li, Botchey, and Qin 2021, 8). Despite significant investments in technological defenses, organizations continue to experience data breaches owing to human-related vulnerabilities.

Risk Mitigation Strategies

This study emphasizes the pressing necessity for organizations to adopt a comprehensive cybersecurity approach that integrates behavioral and technical measures. Suggestions include regular, scenario-based training to increase awareness and reduce human error; leadership involvement in promoting a cybersecurity culture by emphasizing compliance and allocating adequate resources; and implementing continuous monitoring systems to identify vulnerabilities and respond proactively, highlighting the ongoing nature of cybersecurity.

Discussion

Implications for Organizations

This study demonstrates that organizations must address the technical aspects of cybersecurity and organizational behaviors that contribute to vulnerabilities. Leadership plays a crucial role in shaping an organization's security culture, and a lack of engagement at the leadership level can lead to widespread security lapses. Additionally, cross-departmental collaboration and improved communication are necessary to integrate cybersecurity into all organizational processes.

Policy Recommendations

This study suggests that policymakers should promote regulations that encourage organizations to adopt comprehensive cybersecurity frameworks that address both human and technical factors. These policies should mandate regular employee training, leadership accountability, and the implementation of incident response plans. To address emerging threats, experts recommend enhanced collaboration among stakeholders, regular security awareness training, and investment in AI-powered cybersecurity infrastructure (Guembe et al. 2022, 2-3).

Conclusion and Implications

This study reveals that cybersecurity vulnerabilities are influenced not only by technological factors, but also by organizational behaviors and internal dynamics. Organizations that foster a culture of security awareness, supported by leadership commitment and continuous monitoring, are more resilient to cyberattacks. These findings highlight the need for a holistic cybersecurity approach that integrates technical defenses and organizational reforms to mitigate risks effectively (Mingo 2024, 168-169).

Key Contributions

Organizational culture, particularly poor culture characterized by low awareness, inadequate training, and employee negligence, has been identified as a critical cybersecurity risk factor that increases vulnerability to threats such as social engineering, phishing, and insider attacks. Leadership engagement plays a crucial role in shaping cybersecurity posture, with leaders prioritizing cybersecurity and fostering a shared responsibility culture that enhances resilience, while negligence creates exploitable gaps. Utilizing the lens of complex adaptive systems, the dynamic interplay between human and technological factors in cyberspace and organizations was examined, revealing how minor changes in employee behavior or leadership decisions can significantly impact vulnerabilities. The human-technology interface was highlighted as a critical weakness, where human errors, miscommunication, and insufficient training often undermine technical solutions, emphasizing the need for ongoing employee training and awareness programs.

Implications for Practice

Technological defenses alone are insufficient for organizational cybersecurity, and leadership must promote awareness, establish clear communication, and foster accountability. Scenario-based training programs for all employees should be implemented to improve adherence to security

policies and to raise awareness of social engineering threats. Leaders should integrate cybersecurity at all operational levels and ensure cross-departmental collaboration to address technical and human vulnerabilities. Implementing these steps can significantly enhance an organization's cybersecurity posture against evolving threats. Future research should explore the interplay between organizational behavior, leadership, and technological defenses in cybersecurity risk management.

Future Research

The findings of this study advance our understanding of the organizational behaviors and complexities driving cybersecurity risks and lay the foundation for further exploration in this critical field. As the cyber threat landscape evolves rapidly, our research methodologies and focus areas must be considered. Future research could apply the CyberKirk model to specific industries to explore how unique organizational structures and regulatory environments influence cybersecurity risk. A longitudinal approach could provide deeper insights into how changes in organizational behavior over time affect cybersecurity outcomes. As emerging technologies are integrated into cybersecurity practices, further research is required to explore how these technologies can enhance or mitigate the identified behavioral risks.

References

Abrahams, Temitayo Oluwaseun, Sarah Kuzankah Ewuga, Samuel Onimisi Dawodu, Abimbola Oluwatoyin Adegbite, and Azeez Olanipekun Hassan. 2024. "A Review of Cybersecurity Strategies in Modern Organizations: Examining the Evolution and Effectiveness of Cybersecurity Measures for Data Protection." *Computer Science & IT Research Journal* 5 (1): 1-25.

Aksoy, Cenk. 2024. "Building a cyber security culture for resilient organizations against cyber attacks*." İşletme Ekonomi ve Yönetim Araştırmaları Dergisi* 7(1): 96-110. https://doi.org/10.33416/baybem.1374001.

Akyeşilmen, Nezir, and Amal Alhosban. 2024. "Non-Technical Cyber-Attacks and International Cybersecurity: The Case of Social Engineering." *Gaziantep University Journal of Social Sciences* 23(1): 342-360.

Alam, S. S., and Islam, K. Z. 2021. "Examining adoption of electronic human resource management from the technology organization environment framework perspective." *IEEE Engineering Management Review* 49(4): 59-75.

Baig, Zubair, Sri Harsha Mekala, and Sherali Zeadally. 2023. "Ransomware attacks of the COVID-19 pandemic: Novel strains, victims, and threat actors." *IT Professional* 25(5): 37-44.

Belanche, Daniel, Marta Flavián, and Alfredo Pérez-Rueda. 2020. "Mobile Apps Use and WOM in the Food Delivery Sector: The Role of Planned Behavior, Perceived Security and Customer Lifestyle Compatibility." *Sustainability 12*(10): 4275.

Bondoc, Castro Mayleen Dorcas, and Tumibay Gilbert Malawit. 2020. "Classifying relevant video tutorials for the school's learning management system using support vector machine algorithm." *Global Journal of Engineering and Technology Advances* 2(3): 001-009.

Borghi, Josephine, Sharif Ismail, James Hollway, Rakhyun E. Kim, Joachim Sturmberg, Garrett Brown, Reinhard Mechler et al. 2022. *Viewing the global health system as a complex adaptive system–implications for research and practice.* F1000Research, 11.

Boyens, Jon, Celia Paulsen, Nadya Bartol, Kris Winkler, and James Gimbi. 2021. Key practices in cyber supply chain risk management: Observations from industry (No. NIST Internal or Interagency Report (NISTIR) 8276). National Institute of Standards and Technology.

Burger, Annetta, William G. Kennedy, and Andrew Crooks. 2021. "Organizing Theories for Disasters into a Complex Adaptive System Framework." *Urban Science* 5(3): 61.

Burton, Sharon L., Darrell Norman Burrell, Calvin Nobles, and Laura A. Jones. 2023. "Exploring the Nexus of Cybersecurity Leadership, Human Factors, Emotional Intelligence, Innovative Work Behavior, and Critical Leadership Traits." *Scientific Bulletin* 28 (2): 162-175.

Fatim, Ghulam, Irfan Mustafa, and Hassan Farooq. 2021. "A study of ransomware attacks on windows platform." *i-Manager's Journal on Computer Science* 9(4): 21.

Guembe, Blessing, Ambrose Azeta, Sanjay Misra, Victor Chukwudi Osamor, Luis Fernandez-Sanz, and Vera Pospelova. 2022. "The emerging threat of ai-driven cyber attacks: A review." *Applied Artificial Intelligence* 36(1): 2037254.

Harun, N., Jalil, H., and Zolkepli, M. 2022. "Technological, organizational and environmental factors influencing on user intention toward big data technology adoption in Malaysian educational organization." *Accounting* 8(4): 403-408.

Hopcraft, Rory, Kimberly Tam, Juan Dorje Palbar Misas, Kemedi Moara-Nkwe, and Kevin Jones. 2023. "Developing a maritime cyber safety culture: Improving safety of operations*." Maritime Technology and Research* 5(1): 258750-258750.

Hughes-Lartey, Kwesi, Meng Li, Francis E. Botchey, and Zhen Qin. 2021. "Human factor, a critical weak point in the information security of an organization's Internet of things." *Heliyon* 7(3).

Kiviliene, J., and Blazeviciene, A. 2019. "Review of complex adaptive systems in nursing practice." *Journal of Complexity in Health Sciences* 2(2): 46-50.

Klimburg-Witjes, Nina, and Alexander Wentland. "Hacking Humans? Social Engineering and the Construction of the "Deficient User" in Cybersecurity Discourses." *Science, Technology, & Human Values* 46: 1316-1339.

Kolinko, Maryna, Halyna Petryshyn, and Halyna Chumak. 2024. "Reactualising the problem of social engineering and digital security." *Skhid* 6 (1).

Lies, Jan. 2019. "Marketing Intelligence and Big Data: Digital Marketing Techniques on their Way to Becoming Social Engineering Techniques in Marketing." *Int. J. Interact. Multim. Artif. Intell*. 5: 134-144.

Maraj, Arianit, and William Butler. 2022. "Taxonomy of Social Engineering Attacks: A Survey of Trends and Future Directions." *International Conference on Cyber Warfare and Security* vol. 17, pp. 185-193.

Malik, Saleem, Mehmood Chadhar, Savanid Vatanasakdakul, and Madhu Chetty. 2021. "Factors affecting the organizational adoption of blockchain technology: Extending the technology–organization–environment (TOE) framework in the Australian context." *Sustainability* 13(16): 9404.

Mingo, Horace. C. 2024. "Emerging vulnerabilities in cyberspace: A qualitative content analysis of organizational behaviors and complexities that drive cybersecurity risks." (Unpublished doctoral dissertation). Marymount University.

Montanez Rodriguez, Rosana, Edward Golob, and Shouhuai Xu. 2020. "Human cognition through the lens of social engineering cyberattacks." *Frontiers in Psychology* 11, 1755.

Mtsweni, Jabu, Noluxolo Gcaza, and Mphahlele Thaba. 2018, September. "A unified cybersecurity framework for complex environments." In *Proceedings of the Annual Conference of the South African Institute of Computer Scientists and Information Technologists* (pp. 1-9).

Ncubukezi, Tabisa. 2022. "Human errors: A cybersecurity concern and the weakest link to small businesses." In Proceedings of the 17th International Conference on Information Warfare and Security (pp. 395-403).

Nifakos, Sokratis, Krishna Chandramouli, Charoula Konstantina Nikolaou, Panagiotis Papachristou, Sabine Koch, Emmanouil Panaousis, and Stefano Bonacina. 2021. "Influence of human factors on cyber security within healthcare organisations: A systematic review*." Sensors 21*(15): 5119.

Nobles, Calvin. 2018. "Botching Human Factors in Cybersecurity in Business Organizations." *HOLISTICA – Journal of Business and Public Administration* 9(3): 71-88.

Ologunde, Ezekiel. 2023. "Ransomware". *Social Science Research Network*. doi.org/10.2139/ssrn.4823359.

Pakravan, M.H., and MacCarty, N.A. 2020. "What Motivates Behavior Change? Analyzing User Intentions to Adopt Clean Technologies in Low-Resource Settings Using the Theory of Planned Behavior." Energies.

Pollini, Alessandro, Tiziana C. Callari, Alessandra Tedeschi, Daniele Ruscio, Luca Save, Franco Chiarugi, and Davide Guerri. 2021. "Leveraging human factors in cybersecurity: An integrated methodological approach." *Cognition, Technology and Work* 24(2): 371–390.

Pollini, R., Safitra, H., and Gutzwiller, S. 2022. "Identifying and addressing organizational behaviors that exacerbate cybersecurity risks." *Information Security Review* 14(2): 45–62.

Quader, Faisal, and Vandana P. Janeja. 2021. "Insights into organizational security readiness: Lessons learned from cyber-attack case studies." *Journal of Cybersecurity and Privacy* 1(4): 638-659.

Rahman, Tashfiq, Rohani Rohan, Debajyoti Pal, and Prasert Kanthamanon. 2021. "Human Factors in Cybersecurity: A Scoping Review." *Proceedings of the 12th International Conference on Advances in Information Technology*.

Rohan, M., Islam, S., and Dalal, P. 2023. "Organizational culture and cybersecurity management: Bridging the gap." *Cybersecurity Management Journal* 12(1): 45–64.

Siddiqi, Murtaza Ahmed, Wooguil Pak, and Moquddam A. Siddiqi. 2022. *"*A study on the psychology of social engineering-based cyberattacks and existing countermeasures." *Applied Sciences* (Switzerland) 12(12). https://doi.org/10.3390/APP12126042.

Sulaiman, Noor Suhani, Muhammad Ashraf Fauzi, Walton Wider, Jegatheesan Rajadurai, Suhaidah Hussain, and Siti Aminah Harun. 2022. "Cyber–Information Security Compliance and Violation Behaviour in Organisations: A Systematic Review." *Social Sciences 11*(9): 386.

Szűcs, Kata Rebeka, Andrea Tick, and Regina Zsuzsanna Reicher. 2024. "Applying attitude theory to determine user security approaches." *Serbian Journal of Management 19*(1): 133-148.

Thinyane, Mamello. 2024, June. "Unpacking the Complex Socio-Technical Systems Assemblages in Cybersecurity." In *European Conference on Cyber Warfare and Security* 23(1): 562-571.

Triplett, William, J. 2022. "Addressing Human Factors in Cybersecurity Leadership." *Journal of Cybersecurity and Privacy 2*(3): 573-586.

Untawale, T. 2021. "Importance of cyber security in digital era." *International Journal for Research in Applied Science and Engineering Technology 9*(8): 963-966.

Wallace, Steven, Karen Y. Green, Catherine Johnson, Joseph Cooper, and Collin Gilstrap. 2020. "An extended TOE framework for cybersecurity-adoption decisions." *Communications of the Association for Information Systems* 47(1): 51.

Wang, Zuoguang, Hongsong Zhu, and Limin Sun. 2021. "Social engineering in cybersecurity: Effect mechanisms, human vulnerabilities, and attack methods." *IEEE Access* 9: 11895-11910.

Willie, Michael Mncedisi. 2023. "The Role of Organizational Culture in Cybersecurity: Building a Security-First Culture." *Journal of Research, Innovation and Technologies* 2, 2 (4): 179-198.