A Systematic Review of Data Vulnerabilities and the Role of Advanced Security Testing Tools in Enhancing Cybersecurity, Compliance, and User Trust

Rohit Singh Raja

rajarohitsingh@gmail.com

Abstract

Introduction: Cybersecurity has become a fundamental necessity in the digital era, where data underpins government functions, business operations, and communication. With the rise of digitalization and global expansion, organizations face increasing risks from ransomware, data breaches, and insider threats. While businesses focus on functionality, security is often overlooked, leading to vulnerabilities. Protecting data is vital to prevent damage of reputation, financial losses, and legal ramifications in this interconnected world.

Objective: To conduct systematic review on the studies involving data vulnerabilities and cybersecurity compliances.

Method: The study utilized a Systematic Literature Review (SLR) approach, integrating both qualitative and quantitative studies to explore information security behaviors (ISB) and policy compliance. It followed five stages: defining objectives, conducting a systematic search, selecting relevant studies, extracting data, and presenting results. Emphasizing theoretical frameworks like PMT and TPB, the research analyzed 514 articles from 2010-2021 to synthesize key factors influencing compliance and behavioral transitions.

Results: The results highlight diverse factors influencing Information Security Policy (ISP) compliance. Intrinsic motivations showed stronger impacts than extrinsic ones, while Protection Motivation Theory (PMT) better explained voluntary compliance. Leadership, organizational culture, and social factors significantly shaped compliance behaviors. Security awareness and training improved compliance, and past behaviors influenced intentions. Systematic reviews identified research gaps, emphasizing the multidimensional nature of ISP compliance across individual, organizational, and situational factors, showcasing varying levels of influence.

Conclusion: The study concludes that advanced security testing tools are essential for identifying and mitigating vulnerabilities, ensuring regulatory compliance, and building customer trust. By prioritizing cybersecurity investments, organizations can reduce risks and enhance information security behavior and policy compliance.

Keywords: Compliance, User Trust, Cybersecurity, Data Vulnerabilities

Introduction

Cybersecurity has emerged from a technical requirement to a fundamental necessity in this digital era where data is the backbone for the functioning of government, business operations, and communication. There is a need to protect information as there is an increase in emerging digitalized operations and cyber threats. As there is global expansion of organizations, they face huge risks from ransomware and data breaches to insider software vulnerabilities and insider threats [1]. In the present digital era to increase their functionality businesses are using cloud-based resources. Consequently, protecting data has become a major concern for governments, businesses, and individuals. The risk of cyberattacks has increased with the growing dependency on the internet. Most of the business priority is functionalization rather than security which can lead to various consequences like jeopardizing the data and damaging the organization's reputation. Hence it is important to identify the vulnerabilities before the hackers can access them at an early stage [1, 2].

Data vulnerabilities

It refers to the defects in the infrastructure, processes, and systems that could be used to exploit the integrity, confidentiality, or availability of data. Numerous factors, including out-of-date software, incorrect setups, human mistakes, and sophisticated cyberattacks, can contribute to these vulnerabilities. The difficulty of finding and fixing vulnerabilities increases when attackers use more sophisticated tactics. The stakes are increasingly high from financial data to personal data which cause reputational damage, financial losses, and legal ramifications [3].

Security testing tools

The most widely used methods to identify these vulnerabilities are assessment of vulnerabilities and penetration tests. By taking these steps, companies may adhere to data regulations and safeguard themselves against possible cyber threats. Assessment of vulnerability is a security process where a specialist uses analysis tools to evaluate a target. The website of the organization can be reviewed for any threats through vulnerability scanning where the specialists scan the target website using vulnerability assessment tools. These tools analyze the vulnerability, assess its seriousness, and suggest countermeasures. Penetration testing, as opposed to vulnerability assessment, entails a tester manually evaluating the website using tools [2, 3].

A website vulnerability is a threat where attackers can exploit the data from unauthorized access. Security can identify these vulnerabilities and can analyze the threats by using tools. The website is scanned by using automated scanning tools for identification of security vulnerabilities. A list of vulnerabilities found, along with information on their effect, severity, and required fixes, is generated by the scan. The program classifies the severity of the security flaws that have been found [4].

Penetration testing is a calculated procedure whereby cybersecurity professionals mimic assaults in a test setting to take advantage of known vulnerabilities on a website. Ethical hackers carry out this more laborious process, using tools and their expertise to find the website's flaws and vulnerabilities before malevolent intruders make use of them. They can simulate several attack types, including brute-force attacks, business logic flaws, and access control flaws, using any tools or methods to accomplish their objective. A report detailing the vulnerabilities and weaknesses found is produced after the testing is finished [3, 4].

Compliance is maintained and achieved in organizations by using advanced security testing tools. These tools produce audits, provide compliance, and adhere to the requirements of the regulator. Organizations can reduce legal and financial risks while protecting sensitive data by including compliance-focused testing in their cybersecurity plans. For any success in digital enterprise trust of the customer is the main cornerstone. Whether in e-commerce, healthcare, or financial services, users entrust organizations with their personal and financial data, expecting it to be handled responsibly and securely. The security testing tools demonstrate transparency and accountability besides preventing breaches. By making significant investments in cybersecurity, businesses show users that their data is respected and safe, which builds enduring loyalty and trust [5, 6].

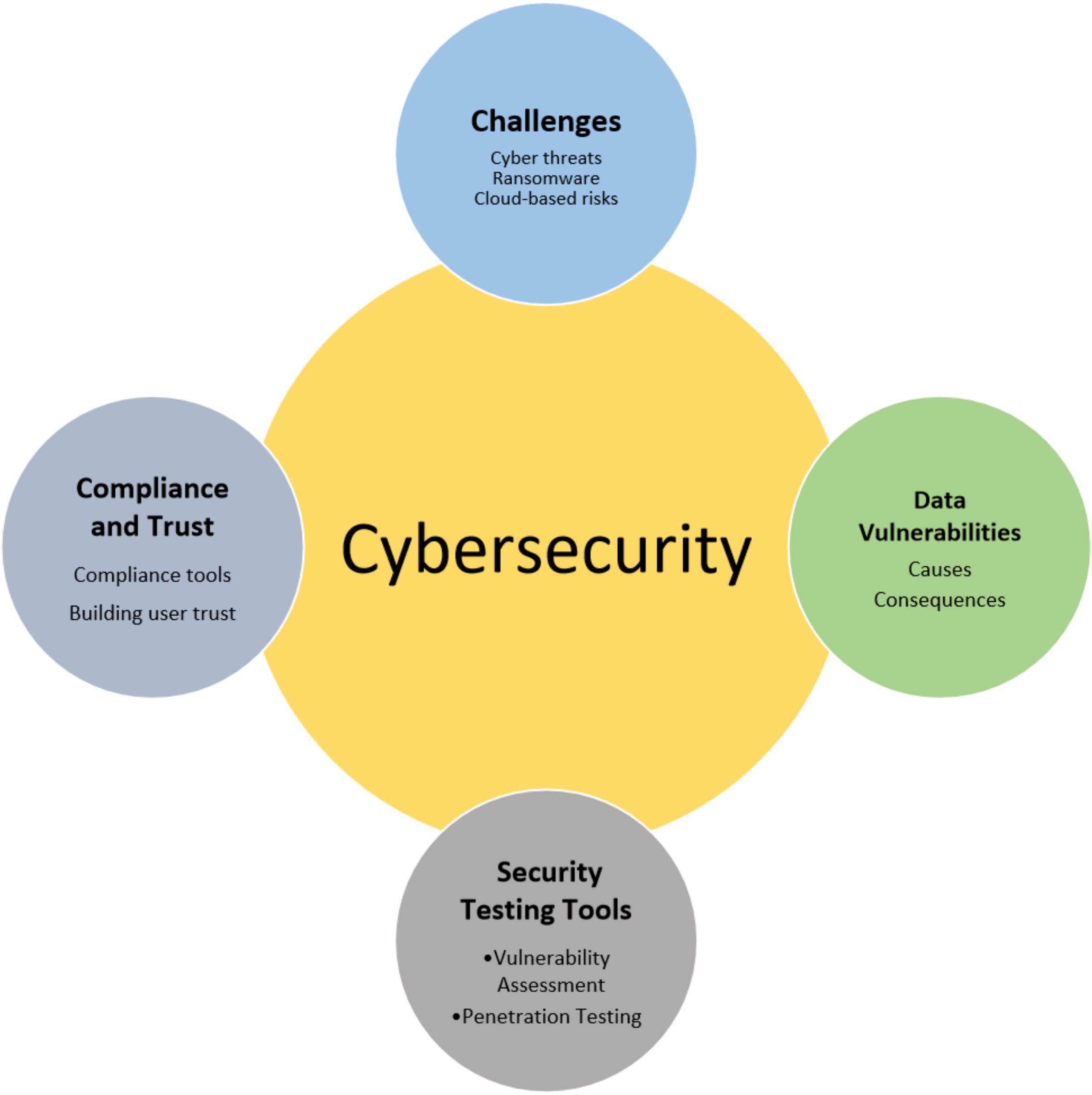

Figure 1: Cybersecurity and its arms

Method

ResearchDesign

This is a Systematic Literature Review (SLR) approach allows for an in-depth investigation of existing studies regarding the information security behavior (ISB) and policy compliance. This study ensures the complete and unbiased inclusion of relevant literature. The grounded theory method provided the theoretical foundation for this SLR.

This study was used five key stages such as defining objectives, conducting a systematic search, selecting relevant studies, extracting and analyzing data, and presenting results. This study reviews the data vulnerabilities and other security testing tools in strengthening the cybersecurity and user compliance.

This research design integrates qualitative and quantitative studies that capture the complex nature of human behavior. This research design considers theoretical frameworks, methods, and results from diverse sectors which ensure a holistic perspective. Moreover, this SLR provides a healthy foundation for developing a behavioral transformation model, which helps as a practical and theoretical contribution to the field.

Literature Search

In order to conduct this study, this research process involved both automated and manual methods that can ensure a thorough and comprehensive rescue of relevant studies. This search strategy used "information security behavior," "policy compliance," "noncompliance behaviors," "security awareness," and "protection motivation theory" these keywords. The study used several online libraries like Scopus, Web of Science, IEEE Xplore, Google Scholar for effective literature search. This research strategy focused on studies which was published from 2010 to 2021 that ensure the significance and suitability of findings. This study used different disciplines including information systems, psychology, and organizational studies. On the other hand, this study was searched around 514 articles. These articles were introduced into reference management software, which was employed to organize and remove duplicates. The abstracts of these paper were then screened for significance based on predefined inclusion and exclusion criteria. Again, studies that aligned with the research objectives continued to a full-text review.

During the search, special attention was assumed to studies using healthy methodologies and theoretical frameworks. For example, studies using Protection Motivation Theory (PMT), Theory of Planned Behavior (TPB), and Deterrence Theory (DT) were prioritized, as these outlines have been commonly applied in information security research. Studies that comprised empirical data and severe methodological approaches were also emphasized.

Inclusion Criteria

- This study focused on Information Security Behavior (ISB) and its connection to policy compliance.This article addressed the compliance or noncompliance behaviors in organizational backgrounds.
- It also provided methodological evidence, including empirical data or theoretical models.
- In addition, peer-reviewed journal articles written in English.
- Studies published from 2010 to 2021.

Exclusion Criteria

- This study was excluded those studies which focused solely on technical solutions or without behavioral components.
- This study addressed non-organizational contexts.
- This study had lacked methodological details or empirical validation.
- Books, theses, or magazine articles.

This study focused on cybersecurity without addressing information security policies (ISP).

Based on these criteria, this study was identified 514 articles were narrowed down to 80 studies. After the final selection, this study included qualitative, quantitative, and mixed-method studies.

By using a PRISMA flow diagram, it outlined each step of the selection procedure, from the initial database search to the final inclusion of studies. Again, the flow diagram also provided transparency about the reasons for excluding studies, such as duplication or irrelevance.

Data Extraction and Evaluation

In the data extraction and evaluation stage, detailed and structured methodologies were employed to synthesize insights from selected studies, focusing on key aspects that influence information security behavior (ISB) and policy compliance. The extraction process meticulously recorded whether each study addressed compliance, noncompliance, or both within organizational settings. The research design of each article was carefully analyzed to identify whether it employed qualitative, quantitative, or mixed-method approaches. Attention was given to the sample size, noting the number of participants or data points analyzed.

Results

Figure 3 shows the number of studies conducted each year from 2010 to 2020. The data shows a fluctuating trend over the decade. In 2010 and 2011, the number of studies was at its lowest, with only 2 studies each year. This increased to 4 studies in 2012, followed by a peak of 5 studies in 2013, which remained consistent until 2015. A slight decline occurred in 2016, with 3 studies, before returning to 5 studies in 2017. The number of studies dropped again to 4 in 2018, then rose to the highest number of 7 in 2019. In 2020, the number of studies reverted to 5. Overall, the data indicates periods of both growth and decline in study numbers, with significant peaks in 2013–2015 and 2019.

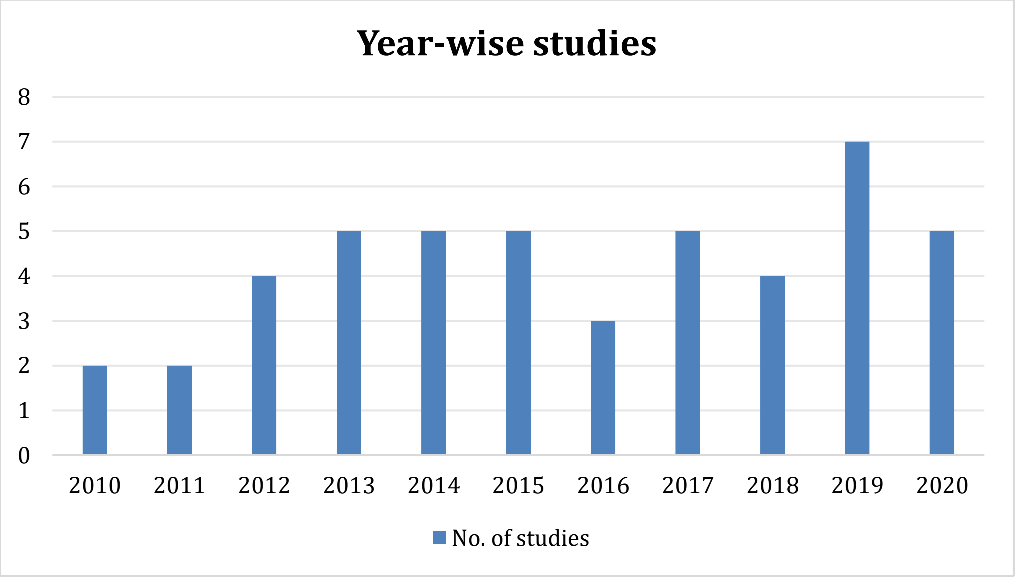

Figure 3: Number of studies with respect to year

Table 1 shows the number of studies conducted each year from 2010 to 2020 and highlights the methodologies employed by these studies. Quantitative research methodology was the most widely used, contributing significantly across multiple years with studies such as [7], [9], [11], [18], [20], and [24], among others. Mixed methodologies were also commonly applied, encompassing studies like [10], [13], [14], [16], and [17], indicating a balanced approach combining qualitative and quantitative elements. Qualitative research methodology, while less frequent, is represented by studies like [25], [32], and [50]. Some studies used specific designs, including pre- and post-test design ([12], [36], [37]), scenario-based design ([22]), and systematic literature review or meta-analysis ([8], [15], [31]). Notably, empirical quantitative studies were also utilized, as evidenced by study [43]. Overall, the diversity in methodologies reflects the varied approaches researchers adopted over the decade to address their research questions effectively.

Table 1: Studies and their methodologies

Research Method	Studies
Quantitative Research Methodology	[7], [9], [11], [18], [20], [21], [24], [33], [34], [35], [36], [39], [40], [43], [48], [49], [51], [52], [53], [55], [56]
Mixed Methodology	[10], [13], [14], [16], [17], [19], [27], [29], [37], [41], [57]

Qualitative Research Methodology	[25], [32], [50]
Pre- and Post-Test Design	[12], [36], [37]
Scenario-Based Design	[22]
Systematic Literature Review or Meta-Analysis	[8], [15], [31]
Empirical Quantitative Study	[43]

Figure 4 shows the total sample size associated with each thematic category identified among the included studies. The theme "Studies on PMB’s (Protective Motivational Behaviors) and ISPC (Information Security Policy Compliance)" had the largest sample size of 3,850 participants, reflecting significant research interest and comprehensive data coverage in this area. The second-largest sample size, 3,377 participants, was associated with "Studies on Management Behaviors and Compliance," highlighting the importance of management practices in influencing compliance behaviors. This is followed by "Studies on Social Behaviors and Compliance," which involved 2,528 participants, underlining the role of social dynamics in compliance behavior. "Studies on Culture/Security Awareness Behaviors and Compliance" had a sample size of 1,614 participants, suggesting moderate research attention to the influence of cultural and security awareness factors. Lastly, "Studies on Intrinsic/Extrinsic Motivations and ISPC" had the smallest sample size, with 1,081 participants, indicating relatively limited data availability on this theme compared to the others. Therefore, the distribution of sample sizes across themes underscores the varying levels of emphasis placed on different aspects of ISPC in the included studies.

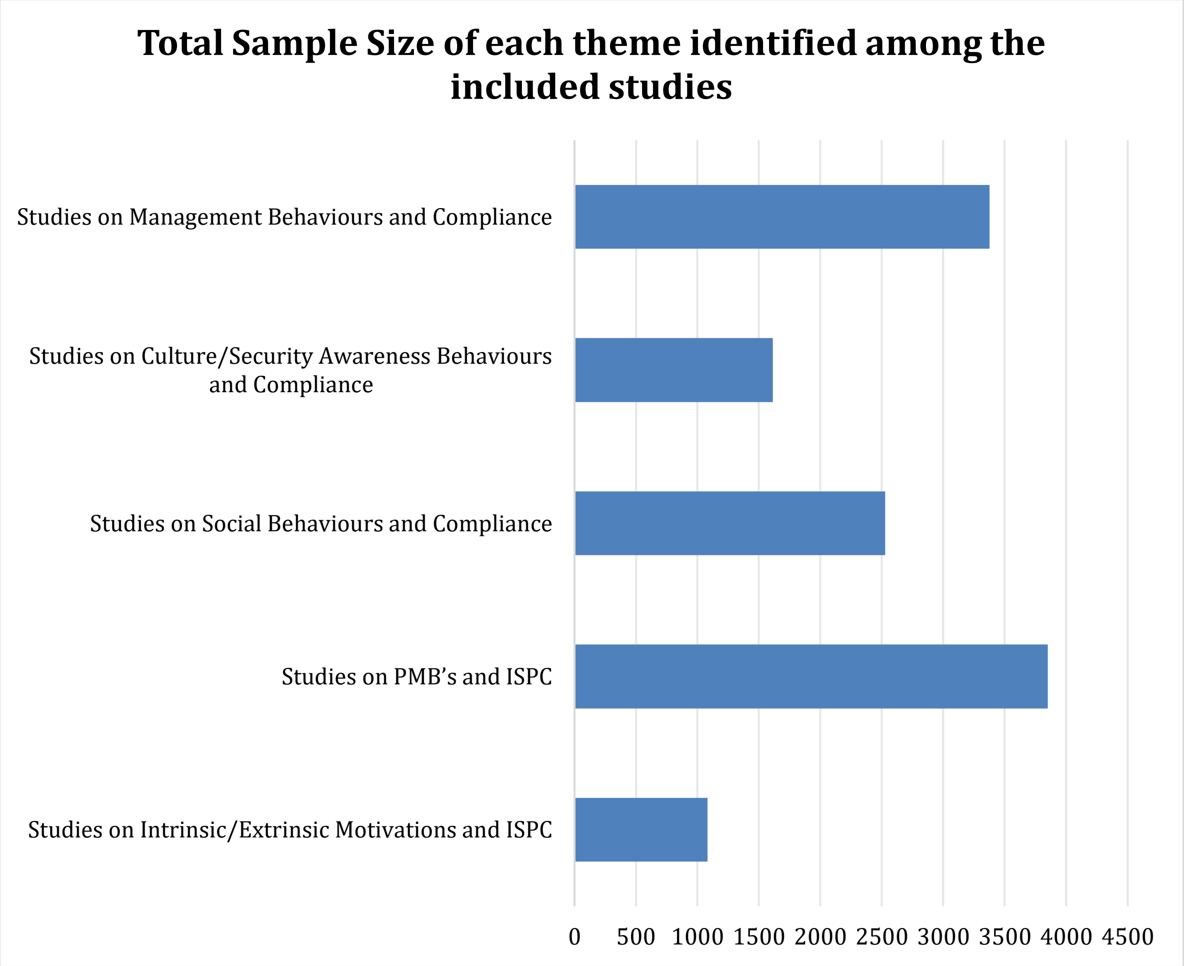

Figure 4: Total Sample Size of each theme identified among the included studies

Table 2 compares the main findings from included studies, revealing diverse factors influencing Information Security Policy (ISP) compliance. A significant insight is that intrinsic motivations have a stronger impact on ISP compliance than extrinsic motivations, as reported in studies [7] and [9]. However, extrinsic factors also play a role in shaping compliant behaviors, though further exploration is needed to better understand intrinsic factors, as suggested by studies [8], [7], and [9].

Protection Motivation Theory (PMT) is highlighted as being more effective in explaining voluntary compliance compared to mandatory compliance ([15], [18], [20], [23]). Additionally, factors such as fear appeal, response efficacy, self-efficacy, and social influence significantly affect compliance behaviors ([10], [11], [14], [16], [17], [19], [18]). Self-efficacy has a consistently positive impact on information security behavior and compliance ([11], [13], [14], [24], [29], [39]).

Leadership, top management support, and organizational culture also emerge as crucial in shaping compliance behaviors ([26], [29], [32], [34], [42], [43]). Similarly, attitudes, intentions, and moral obligations are identified as significant predictors of compliance ([14], [18], [24], [26], [33], [40]), while past behavior and habits are shown to influence compliance intentions ([12], [17], [38]). Employees' performance of multiple security behaviors is influenced by perceived threats, costs, and self-efficacy ([19], [20], [23], [24], [52], [55]). The findings further suggest that situational and social factors, such as bonding and organizational governance, enhance compliance ([29], [53], [54], [57]). Security awareness and training programs are also effective in improving employee compliance behaviors ([11], [29], [34], [35], [39]). Lastly, systematic literature reviews ([8], [15], [31]) have identified key gaps in the current understanding of ISP compliance, underscoring the need for more research to address these issues comprehensively.

Thus, the comparison highlights the multidimensional nature of ISP compliance, encompassing individual, organizational, and situational factors, with varying levels of influence across different studies.

Table 2: Main findings identified from included studies and the studies against each finding

Finding	Studies
Intrinsic motivations have a stronger impact on ISP compliance than extrinsic motivations.	[7], [9]
Extrinsic factors significantly affect compliant behaviors but need further exploration for intrinsic factors.	[8], [7], [9]
Protection Motivation Theory (PMT) explains voluntary compliance better than mandatory compliance.	[15], [18], [20], [23]
Fear appeal, response efficacy, self-efficacy, and social influence significantly affect behavior.	[10], [11], [14], [16], [17], [19], [18]
Self-efficacy positively influences information security behavior and compliance.	[11], [13], [14], [24], [29], [39]
Leadership, top management, and organizational culture play a crucial role in shaping ISP compliance behaviors.	[26], [29], [32], [34], [42], [43]
Attitudes, intentions, and moral obligations are significant predictors of compliant behavior.	[14], [18], [24], [26], [33], [40]

Past behavior and habits significantly influence intentions to comply with ISP.	[12], [17], [38]
Employees perform multiple security behaviors influenced by perceived threats, costs, and self-efficacy.	[19], [20], [23], [24], [52], [55]
Situational and social factors such as bonding and organizational governance improve compliance.	[29], [53], [54], [57]
Security awareness and training enhance employee compliance behaviors.	[11], [29], [34], [35], [39]
Systematic literature reviews identify gaps in understanding and improving ISP compliance.	[8], [15], [31]

Discussion

In comparison to previous networks fifth generation (5G) networks are provided with high speed, connectivity, and reliability. Various sectors have been revolutionized with these advancements and supported the applications that require real-time data processing. However, to operate these infrastructures properly, security issues brought about by the quick deployment and integration of 5G networks must be resolved. A study assessed the security vulnerabilities in 5G networks with penetration testing. It is a way of ethical hacking that simulates network security in situations of cyberattacks. A comparative analysis of penetration testing tools highlights their emphasis on advanced security measures against cyber threats, and their effect on vulnerabilities in 5G networks [6].

As there has been an increase in cyberattacks on financial institutions in recent years there is a need for an advanced system that can predict the attack. Since it gives financial institutions proactive controls to stop an attack by anticipating patterns, such a system must be incorporated into their current detection systems. The software security and designs of new advanced cyber security are enhanced by advanced prediction systems by providing new testing procedures. A study developed a new testing model with the use of a deep neural network that forecasts cyberattacks on financial institutions. Some of the largest cyberattacks on financial institutions throughout the previous three years made up the dataset used to train and test the algorithm. This sheds light on novel trends that could result in cybercrime. The behavioral similarities between these new assaults and the closest known attack or a combination of many existing attacks were also assessed. After that, the forecasting model's performance was assessed in an actual banking setting, yielding a 90.36% forecasting accuracy [7].

To test the website security of organizations several tools have been created for the organizations and cybersecurity. A study examined the importance of automated penetration testing tools for providing affordable and effective security systems for small organizations. Multiple data gatherings were employed in a case study. The data was collected through experiments and interviews. They stated that small organizations can be safeguarded with the use of cost-effective automated testing methods. The penetration tools have determined that there are numerous vulnerabilities in the website, Nessus showed 37 vulnerabilities in the website and ZAP demonstrated that the website is nearly failing with an accumulation of vulnerabilities. First, small businesses may simply protect their cybersecurity without paying for specialist assistance by using automated penetration testing solutions. Second, because each tool contributes differently to cybersecurity, it is advised that automated penetration testing tools be employed in a variety of combinations considering the findings [8].

A novel framework was designed in a study to evaluate the multiple Web Application Vulnerability Scanners (WAVS). Two algorithms are used by the framework to generate combined vulnerabilities: a novel combination and automation algorithms that provide list of detectable vulnerabilities. OWASP ZAP and Arachni capabilities were tested by the framework. They demonstrated that greater accuracy is seen in the outcomes of the proposed framework compared to the results that are obtained using OWASP ZAP and Arachni. According to the study, the Union List performs better than individual scanners, especially in terms of memory and F-measure. As a result, using several vulnerability scanners is advised as a practical way to improve web application vulnerability detection [9].

The discussion on penetration testing and its implementation was done in a study. It also discusses the vulnerabilities and hazards in relation to the web environment and the protective measures that need to be taken. According to the study's findings, integrating analytic tools can yield comprehensive information about web vulnerabilities, and not all web penetration testing solutions have the same qualities [10].

Conclusion

The study has concluded that advanced security testing tools, such as vulnerability assessments and penetration testing, play a crucial role in enhancing cybersecurity by identifying and mitigating data vulnerabilities. These tools not only help organizations comply with regulatory requirements but also build customer trust by demonstrating transparency and accountability. Additionally, addressing intrinsic and extrinsic motivators, situational and organizational factors, and integrating compliance-focused strategies are essential for improving information security behavior and policy compliance in the evolving digital landscape. Investments in cybersecurity are critical for reducing risks and fostering loyalty, especially in industries where customer trust is a cornerstone for success.

References

1. Borky, J. M., & Bradley, T. H. (2018). Protecting Information with Cybersecurity. *Effective Model-Based Systems Engineering*, 345. https://doi.org/10.1007/978-3-319-95669-5_10
2. Rane, Nikhil & Qureshi, Amna. (2024). Comparative Analysis of Automated Scanning and Manual Penetration Testing for Enhanced Cybersecurity. 10.1109/ISDFS60797.2024.10527240.
3. Aslan, Ömer & Aktug, Semih & Ozkan, Merve & Yılmaz, Abdullah & Akin, Erdal. (2023). A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions. Electronics. 12. 1-42. 10.3390/electronics12061333.
4. Zaid, T., & Garai, S. (2024). Emerging Trends in Cybersecurity: A Holistic View on Current Threats, Assessing Solutions, and Pioneering New Frontiers. *Blockchain in Healthcare Today*, *7*, 10.30953/bhty.v7.302. https://doi.org/10.30953/bhty.v7.302
5. Tariq, U., Ahmed, I., Bashir, A. K., & Shaukat, K. (2022). A Critical Cybersecurity Analysis and Future Research Directions for the Internet of Things: A Comprehensive Review. *Sensors*, *23*(8), 4117. https://doi.org/10.3390/s23084117
6. Smith-Haynes, Shari-Ann. (2024). Advanced Penetration Testing for Enhancing 5G Security. 10.48550/arXiv.2407.17269.
7. J.-Y. Son, "Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies," *Inf. Manag.*, vol. 48, pp. 296–302, 2011. [Online]. Available: https://doi.org/10.1016/j.im.2011.07.002

8. K. Padayachee, "Taxonomy of compliant information security behavior," *Comput. Secur.*, vol. 31, pp. 673–680, 2012. [Online]. Available: https://doi.org/10.1016/j.cose.2012.04.004
9. J. Kranz and F. Haeussinger, "Why deterrence is not enough: The role of endogenous motivations on employees' information security behavior," in Proc. Int. Conf. Inf. Syst., Auckland, New Zealand, Dec. 2014, pp. 23–44.
10. M. Warkentin and A. C. Johnston, "Fear appeals and information security behaviors: An empirical study," MIS Q., vol. 34, pp. 549–566, 2010. [Online]. Available: https://doi.org/10.2307/25750693
11. P. Ifinedo, "Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory," *Comput. Secur.*, vol. 31, pp. 83–95, 2012. [Online]. Available: https://doi.org/10.1016/j.cose.2011.10.007.
12. A. Vance, M. Siponen, and S. Pahnila, "Motivating IS security compliance: Insights from habit and protection motivation theory," Inf. Manag., vol. 49, pp. 190–198, 2012. [Online]. Available: https://doi.org/10.1016/j.im.2012.04.002.
13. C. Posey, T. L. Roberts, P. B. Lowry, and R. J. Bennett, "Insiders' protection of organizational information assets: Development of a systematics-based taxonomy and theory of diversity for protection-motivated behaviors," MIS Q., vol. 37, pp. 1189–1210, 2013.
14. S. Boss, D. Galletta, P. B. Lowry, G. D. Moody, and P. Polak, "What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors," *MIS Q.*, vol. 39, pp. 837–864, 2015. [Online]. Available: https://www.jstor.org/stable/26628654.
15. T. Sommestad, J. Hallberg, K. Lundholm, and J. Bengtsson, "Variables influencing information security policy compliance," *Inf. Manag. Comput. Secur.*, vol. 22, pp. 42–75, 2014. [Online]. Available: https://doi.org/10.1108/IMCS-08-2012-0045.
16. M. Warkentin and M. Siponen, "An enhanced fear appeal rhetorical framework: Leveraging threats to the human asset through sanctioning rhetoric," MIS Q., vol. 39, pp. 113–134, 2015.
17. W. Merrill and C. Allen, "Continuance of protective security behavior: A longitudinal study," Decis. Support Syst., vol. 92, pp. 25–35, 2016.
18. A. Burns, C. Posey, T. L. Roberts, and P. B. Lowry, "Examining the relationship of organizational insiders' psychological capital with information security threat and coping appraisals," Comput. Hum. Behav., vol. 68, pp. 190–209, 2017.
19. R. E. Crossler, F. Bélanger, and D. Ormond, "The quest for complete security: An empirical analysis of users' multi-layered protection from security threats," Inf. Syst. Front., vol. 21, pp. 343–357, 2017. [Online]. Available: https://doi.org/10.1007/s10796-017-9756-2

20. .J. M. Blythe and L. Coventry, "Costly but effective: Comparing the factors that influence employee anti-malware behaviors," Comput. Hum. Behav., vol. 87, pp. 87–97, 2018. [Online]. Available: https://doi.org/10.1016/j.chb.2018.05.012

21. V. Hooper and C. Blunt, "Factors influencing the information security behavior of IT employees," Behav. Inf. Technol., vol. 39, pp. 1–13, 2019. [Online]. Available: https://doi.org/10.1080/0144929X.2018.1551132.
22. N. K. Lankton, C. Stivason, and A. Gurung, "Information protection behaviors: Morality and organizational criticality," Inf. Comput. Secur., vol. 27, pp. 468–488, 2019.
23. M. Rajab and A. Eydgahi, "Evaluating the explanatory power of theoretical frameworks on intention to comply with information security policies in higher education," *Comput. Secur.*, vol. 80, pp. 211–223, 2019.

24. S. T. Alanazi, M. Anbar, S. A. Ebad, S. Karuppayah, and H. A. Al-Ani, "Theory-based model and prediction analysis of information security compliance behavior in the Saudi healthcare sector," Symmetry, vol. 12, p. 1544, 2020.
25. S. Alfawaz, K. Nelson, and K. Mohannak, "Information security culture: A behavior compliance conceptual framework," in *Proc. Eighth Australasian Conf. Inf. Security*, Brisbane, Australia, Jan. 2010, pp. 47–55.
26. Q. Hu, T. Dinev, P. Hart, and D. Cooke, "Managing employee compliance with information security policies: The critical role of top management and organizational culture," Decis. Sci., vol. 43, pp. 615–660, 2012.
27. S. Pahnila, M. Karjalainen, and M. T. Siponen, "Information security behavior: Towards multi-stage models," in Proc. Pacific Asia Conf. Inf. Syst., Jeju Island, Korea, Jun. 2013, pp. 102–122.
28. J. D'Arcy and G. Greene, "Security culture and the employment relationship as drivers of employees' security compliance," Inf. Manag. Comput. Secur., vol. 22, pp. 474–489, 2014.
29. N. S. Safa et al., "Information security conscious care behavior formation in organizations," Comput. Secur., vol. 53, pp. 65–78, 2015.
30. F. Bélanger, S. Collignon, K. Enget, and E. Negangard, "Determinants of early conformance with information security policies," *Inf. Manag.*, vol. 54, pp. 887–901, 2017.
31. A. Tsohou and P. Holtkamp, "Are users competent to comply with information security policies? An analysis of professional competence models," *Inf. Technol. People*, vol. 31, pp. 1047–1068, 2018.
32. D. Harnesk and J. Lindström, "Shaping security behavior through discipline and agility: Implications for information security management," Inf. Manag. Comput. Secur., vol. 19, pp. 262–276, 2011.
33. C. Yoon and H. Kim, "Understanding computer security behavioral intention in the workplace: An empirical study of Korean firms," Inf. Technol. People, vol. 26, pp. 401–419, 2013.
34. N. Humaidi and V. Balakrishnan, "Exploratory factor analysis of user's compliance behavior towards health information system's security," J. Health Med. Inform., vol. 4, pp. 2–9, 2013. [Online]. Available: https://doi.org/10.4172/2157-7420.1000121
35. N. Humaidi and V. Balakrishnan, "The moderating effect of working experience on health information system security policies compliance behavior," Malays. J. Comput. Sci., vol. 28, pp. 70–92, 2015. [Online]. Available: https://ejournal.um.edu.my/index.php/MJCS/article/view/6856
36. S. Aurigemma and T. Mattson, "Privilege or procedure: Evaluating the effect of employee status on intent to comply with socially interactive information security threats and controls," Comput. Secur., vol. 66, pp. 218–234, 2017. [Online]. Available: https://doi.org/10.1016/j.cose.2017.02.002
37. J. Han, Y. J. Kim, and H. Kim, "An integrative model of information security policy compliance with psychological contract: Examining a bilateral perspective," Comput. Secur., vol. 66, pp. 52–65, 2017. [Online]. Available: https://doi.org/10.1016/j.cose.2017.01.005

38. H. L. Kim and J. Han, "Do employees in a 'good' company comply better with information security policy? A corporate social responsibility perspective," Inf. Technol. People, vol. 32, pp. 858–875, 2018. [Online]. Available: https://doi.org/10.1108/ITP-01-2018-0011
39. Z. Ahmad, T. S. Ong, T. H. Liew, and M. Norhashim, "Security monitoring and information security assurance behavior among employees: An empirical analysis," Inf. Comput. Secur., vol. 27, pp. 165–188, 2019. [Online]. Available: https://doi.org/10.1108/ICS-06-2019-0070
40. S. Sharma and M. Warkentin, "Do I really belong? Impact of employment status on information security policy compliance," Comput. Secur., vol. 87, p. 101397, 2019. [Online]. Available: https://doi.org/10.1016/j.cose.2019.101397

41. 77.M. Sillic, "Critical impact of organizational and individual inertia in explaining non-compliant security behavior in the shadow IT context," Comput. Secur., vol. 80, pp. 108–119, 2019. [Online]. Available: https://doi.org/10.1016/j.cose.2018.10.015
42. A. Koohang, A. Nowak, J. Paliszkiewicz, and J. H. Nord, "Information security policy compliance: Leadership, trust, role values, and awareness," J. Comput. Inf. Syst., vol. 60, pp. 1–8, 2020. [Online]. Available: https://doi.org/10.1080/08874417.2018.1542638.
43. C. Liu, N. Wang, and H. Liang, "Motivating information security policy compliance: The critical role of supervisor-subordinate guanxi and organizational commitment," *Int. J. Inf. Manag.*, vol. 54, p. 102152, 2020.
44. Qasaimeh, M., Hammour, R. A., Yassein, M. B., Al-Qassas, R. S., Torralbo, J. A. L., & Lizcano, D. (2022). Advanced security testing using a cyber-attack forecasting model: A case study of financial institutions. *Journal of Software: Evolution and Process*. https://doi.org/10.1002/smr.2489
45. Alkhurayyif, Yazeed &Almarshdy, Yazeed. (2024). Adopting Automated Penetration Testing Tools: A Cost-Effective Approach to Enhancing Cybersecurity in Small Organizations. Journal of Information Security and Cybercrimes Research. 7. 51-66. 10.26735/RJJT2453.
46. Abdulghaffar, K., Elmrabit, N., & Yousefi, M. (2023). Enhancing Web Application Security through Automated Penetration Testing with Multiple Vulnerability Scanners. *Computers*, *12*(11), 235. https://doi.org/10.3390/computers12110235
47. Altulaihan, E. A., Alismail, A., &Frikha, M. (2022). A Survey on Web Application Penetration Testing. *Electronics*, *12*(5), 1229. https://doi.org/10.3390/electronics12051229
48. N. I. Jaafar and A. Ajis, "Organizational climate and individual factors effects on information security compliance behavior," Int. J. Bus. Soc. Sci., vol. 4, pp. 1–13, 2013.
49. P. Ifinedo, "Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition," Inf. Manag., vol. 51, pp. 69–79, 2014.
50. C. Posey, T. L. Roberts, P. B. Lowry, and R. T. Hightower, "Bridging the divide: A qualitative comparison of information security thought patterns between information security professionals and ordinary organizational insiders," Inf. Manag., vol. 51, pp. 551–567, 2014.
51. J. S.-C. Hsu, S.-P. Shih, Y. W. Hung, and P. B. Lowry, "The role of extra-role behaviors and social controls in information security policy effectiveness," Inf. Syst. Res., vol. 26, pp. 282–300, 2015.
52. A. Yazdanmehr and J. Wang, "Employees' information security policy compliance: A norm activation perspective," Decis. Support Syst., vol. 92, pp. 36–46, 2016.
53. N. S. Safa, R. Von Solms, and S. Furnell, "Information security policy compliance model in organizations," Comput. Secur., vol. 56, pp. 70–82, 2016.
54. N. S. Safa, C. Maple, T. Watson, and R. Von Solms, "Motivation and opportunity-based model to reduce information security insider threats in organisations," J. Inf. Secur. Appl., vol. 40, pp. 247–257, 2018.
55. .H. Chen and W. Li, "Understanding commitment and apathy in IS security extra-role behavior from a person-organization fit perspective," Behav. Inf. Technol., vol. 38, pp. 454–468, 2019
56. .A.Yazdanmehr, J. Wang, and Z. Yang, "Peers matter: The moderating role of social influence on information security policy compliance," Inf. Syst. J., vol. 30, pp. 787–790, 2020.
57. R. F. Ali, P. Dominic, and K. Ali, "Organizational governance, social bonds and information security policy compliance: A perspective towards oil and gas employees," *Sustainability*, vol. 12, p. 8576, 2020.