https://doi.org/10.52131/jcsit.2026.0801.3252

*i*RASD Journal of Computer Science and Information Technology

Volume 8, Number 1, 2026, Pages 01 - 12

Journal Homepage:
https://journals.internationalrasd.org/index.php/jcsit

Human Factors in Cybersecurity and Privacy: A Systematic Review with Implications for Zimbabwe's Digital Transformation

Elisha Mutize[1], Admire Mthombeni[2], Leonard Chitongo[3]

[1] Lecturer, Management Accounting and Finance Department, Walter Sisulu University, Mthatha Campus, South Africa. Email: emutize@wsu.ac.za
[2] Postdoctoral Research Fellow, Graduate School of Business and Leadership, University of KwaZulu-Natal, South Africa. Email: mthombeniA@ukzn.ac.za
[3] Senior Lecturer Human Geography, Department of Biological and Environmental Sciences, Walter Sisulu University, Mthatha, South Africa. Email: lchitongo@wsu.ac.za

ARTICLE INFO

Article History:
Received: July 11, 2026
Revised: October 07, 2026
Accepted: October 12, 2026
Available Online: November 11, 2026

Keywords:
Cybercrime
Cybersecurity Policy
Digital Economy
Data Privacy
Socio- Technical Systems Theory

ABSTRACT

Across the globe, cybersecurity and privacy have become an important aspect of sustainable digital transformation as governments and organisations rely on digital technologies despite the growing sophistication of cyber threats. The study examined how human factors contribute to the persistence of cyber risks despite having cybersecurity controls being put in place within Zimbabwe's evolving digital landscape. The study was hinged on the Socio-Technical Systems Theory. It employed a qualitative systematic literature review that followed the PRISMA 2020 framework. Literature published between 2015 and 2025 was searched across various academic databases. From 446 records identified, 35 studies met the inclusion criteria and were synthesised using thematic analysis. The review established that cybersecurity awareness, risk perception, organisational culture, system usability and insider-related behaviours are the main human factors limiting the effectiveness of technological security controls. The findings also revealed that persistent cyber risks arise from the interaction between human behaviour, organisational practices and technology instead of just technological shortcomings. The review therefore concludes that sustainable cybersecurity requires integrated human-centred approaches that align technological safeguards with behavioural and organisational interventions. It recommends institutionalising behavioural cyber risk assessment, strengthening organisational security culture, embedding user-centred security design and promoting context-specific research to enhance Zimbabwe's cyber resilience and support secure digital transformation.

© 2026 The Authors, Published by iRASD. This is an Open Access article under the Creative Common Attribution Non-Commercial 4.0

Corresponding Author's Email: emutize@wsu.ac.za

1. Introduction and Background

Digital transformation has been a great force that has changed how government, business, and people interact with each other. The rapid adoption of digital technologies has accelerated economic growth while creating new opportunities for innovation and service delivery. Many governments around the world are increasingly pursuing digital transformation technologies to improve public service efficiency, financial inclusion as well as economic competitiveness. Nevertheless, the rising digitization of economies is associated with elevated cybersecurity threats that endanger critical infrastructure and everyone's privacy and safety. According to the World Economic (2025), cyber espionage, cybercrime and misinformation remain among the most significant global risks confronting

governments and organisations. The reports by the International Telecommunication Union (National Institute of & Technology, 2024) shows that an increase in digital connectivity continues outpacing cybersecurity preparedness in many developing countries. As such, the protection of digital systems requires not only advancement in technology but also some resilient and organisational and human centred cybersecurity strategies.

As a response to cyber threats, entities have made an investment in technical strategies that include firewalls, intrusion detection systems, end point security, encryption, multifactor authentication as well as security information and event management systems. Notwithstanding these huge investments, cyber incidents have become more frequent in both frequency and sophistication. Across the globe, the average cost of a data breach reached US$4.88 million which was the highest ever recorded. This demonstrates that investments in technology alone have not eliminated cyber risks (Ibm, 2024). According to Verizon (2024), most of these cyber incidents have continued to involve human interaction with social engineering, phishing, stolen credentials and human error remaining as the leading causes of organisational security breaches. These findings show that technological controls alone are insufficient when human behaviour still undermines their performance and effectiveness.

The existence of this implementation gap has resulted in a high focus on human factors in cybersecurity research. Human factors in cybersecurity research are regarded as behavioural, psychological, organizational and environmental characteristics that bear influence on how individuals interact with information systems and cybersecurity controls. It includes cybersecurity awareness, risk perception, decision making, compliance with security policies, organizational culture, insider related behaviours as well as system usability. Pollini et al. (2022) highlighted that, rather than viewing technology as the sole determinant of cybersecurity effectiveness, contemporary research increasingly recognises that cybersecurity outcomes emerge from interactions between people, technology and organisational environments. Workers who do not recognise phishing attempts, use the same passwords, bypass the organisational policies for convenience or deal with sensitive information inappropriately, and could sabotage even the best-designed cybersecurity systems. Moreover, malicious insiders continue to exploit legitimate systems, facilitate fraud, intellectual property theft and data breaches and thus, cybersecurity is fundamentally a socio-technical challenge rather than a purely technological one.

Growing empirical evidence reinforces the importance of addressing human behaviour in cybersecurity governance. This is highlighted by Jyoti et al. (2026) who identified social engineering, phishing and identity-based attacks as among the fastest-growing cyber threats affecting organisations in the world. Similarly, the (European Union Agency for, 2024) alluded that building resilient cybersecurity requires continuous user education, secure organisational practices and the development of strong security cultures alongside technological safeguards. In this regard, Bishop et al. (2025) argues that risky online behaviours and limited cybersecurity awareness significantly increases risk exposure to both individuals and organisations. Meanwhile Sutton and Tompson (2025) contends that cultivating a positive cybersecurity culture enhances compliance with security policies thus reduces risky employee behaviour. Studies by these authors indicate that sustainable cybersecurity resilience depends on the integration of behavioural interventions and implementing technical security measures.

The importance of human factors is particularly pronounced in developing countries that are currently undergoing a digital revolution. Across Africa, increased use of mobile banking, digital government services, e-commerce platforms and cloud computing have created new opportunities for economic development while at the same time making people more vulnerable to cybercrime, online fraud and data privacy breaches. Nevertheless, many developing economies continue to face challenges relating to cybersecurity awareness, digital literacy, institutional capacity and organisational preparedness, making them particularly susceptible to cyber threats (Akter et al., 2022). These challenges suggest that strengthening cybersecurity within developing contexts requires greater awareness to behavioural, organisational and institutional factors that manipulate how individuals interact with digital technologies.

Zimbabwe mirrors many of these developments by accelerating digital transformation through the expansion of mobile financial services, electronic commerce, digital government platforms and ICT-enabled service delivery in support of the National Development Strategy 2 (NDS2) and Vision 2030. To reinforce cybersecurity governance and privacy protection, Zimbabwe enacted the Cyber and Data Protection Act (Chapter 12:07), providing a legislative framework for protecting personal information, regulating cybercrime and promoting trust within the digital economy. These policy initiatives demonstrate Zimbabwe's commitment to creating a secure digital environment capable of supporting sustainable socio-economic development. Nevertheless, the increased adoption of digital technologies has also created more opportunities for phishing attacks, online fraud, ransomware, identity theft and other cyber-enabled offences that increasingly take advantage of human vulnerabilities rather than technological weaknesses. As Zimbabwe's digital economy continues to expand, understanding the behavioural factors that contribute to cyber risks becomes essential for supporting organisational resilience and public confidence in digital systems.

Although there is an extensive body of literature on cybersecurity, there are still knowledge gaps to be filled. Previous studies have concentrated on technological aspects of cybersecurity architecture, encryption mechanisms and technical risk mitigation strategies, while they paid less attention on understanding why cyber risks continue to rise. Furthermore, research examining cybersecurity awareness, risk perception, organisational culture, system usability and insider-related risks has often developed in isolation, resulting in a fragmented understanding of how these human factors collectively influence cybersecurity effectiveness. In Zimbabwe this limitation is evident because there is limited evidence that integrates behavioural, organisational and policy-oriented perspectives to explain the persistence of cyber risks in the context of a rapidly evolving digital environment.

Against this background, this study aims to establish the role that human factors play in the perpetuation of cyber risks despite the existence of cybersecurity measures in context of Zimbabwe's digital landscape. The findings further provide empirical evidence needed by policymakers, organisational leaders and cybersecurity professionals seeking to strengthen security culture, improve cybersecurity awareness and enhance organisational resilience in support of Zimbabwe's broader digital transformation agenda.

2. Literature Review

2.1. Theoretical Framework

This study is guided by the Socio-Technical Systems Theory (STS), originally developed by Trist and Bamforth (1951), and subsequently refined by Emery (1959) and Cherns (1976). The theory posits that organisational effectiveness is achieved through the improvement of two separate but related systems; the technical system comprising technologies of infrastructure and work processes, and the social system comprising people, organisational culture, leadership, communication and work practices. The Socio-Technical Systems Theory (STS) puts forward the argument that organisations will attain an optimal performance when the two systems are designed and managed complimentarily. On the other hand, a misalignment between technological solutions, human factors as well as organisational factors reduces system effectiveness thereby increasing organisational vulnerability (Mai & Khalid, 2025).

Socio-Technical Systems Theory is an appropriate framework for examining why cyber-risks continue to exist despite the significant investment in cybersecurity technologies. While organisations are increasingly adopting advanced technical controls such as firewalls, encryption, intrusion detection systems and multi-factor authentication, these technologies ultimately depend on how individuals interact with them and how organisations incorporate cybersecurity into their everyday practices. Human behaviours, organisational culture, leadership commitment and system usability influence whether security controls are followed, ignored or circumvented (Iyer & Raji, 2025). Therefore, cybersecurity cannot be understood solely as a technological issue but rather because of continuous interactions between technological capabilities and the social environment in which they exist.

The theory aligns closely with the aim of this study. This is because it states that individuals' risk perceptions, cybersecurity awareness, organisational culture, system usability and insider-related risks are core factors that influence the effectiveness of cybersecurity and privacy controls within Zimbabwe's changing digital landscape. These factors represent the social dimensions of cybersecurity that interact with existing technological controls to shape organisational resilience.

From a socio-technical perspective, persistent cyber risks are not necessarily an indication of inadequate technologies but often reflect poor alignment between security technologies, user behaviour and organisational practices. As Zimbabwe continues to advance its digital transformation agenda under the National Development Strategy 2 (NDS2) and Vision 2030, STS offers a useful framework for explaining why enhancing cybersecurity requires equal attention to human behaviour, organisational processes and technology design. Therefore, the theory support and complement the study's central argument that sustainable cybersecurity and privacy protection may be achieved through integrated and human centred approaches that aligns technological controls.

2.2. The Human Dimension of Cybersecurity and Privacy

The rapid expansion of digital technologies has transformed cybersecurity and privacy from predominantly technical concerns into multidisciplinary problems. This implies that apart from the technical aspect of digital security, other aspects such as organizational and human factors must be considered. Most organisations are investing heavily in cybersecurity technologies such as firewalls, encryption, intrusion detection systems and multi-factor authentication devices to protect their data and information. However, there is strong empirical evidence that these technological measures might prove to be inadequate if users do not embrace appropriate digital security measures and the organizational aspect of the problem is not addressed (Chat et al., 2023). As a result, modern cybersecurity discourse increasingly acknowledges that understanding how individuals interact with technology and how organizational contexts influence security-related behavior is essential to effectively protecting digital systems.

Cybersecurity refers to the protection of information systems, networks and digital infrastructure against unauthorised access, disruption, modification or destruction while ensuring the confidentiality, integrity and availability of information (Aslan et al., 2023). Its scope has expanded from the technical aspect of safeguarding information systems to include governance, risk management, organisational resilience and human behaviour as integral components of secure digital ecosystems (von Solms & van Niekerk, 2013). Although cybersecurity and privacy are separate concepts, they are complementary aspects where effective cybersecurity will help protect personal information from cyber-attack and effective privacy will promote safe and lawful information handling and sharing. As a result, cybersecurity and privacy offers the basis for building digital trust ecosystems for economic development.

Human factors which encompass the behavioural, cognitive, organisational and environmental characteristics that influence how individuals interact with digital technologies and cybersecurity controls are paramount. Human factors extend beyond individual knowledge to include cybersecurity awareness, risk perception, organisational culture, leadership commitment, system usability and insider behaviour, all of which shape the effectiveness of cybersecurity programmes (Rendahl, 2026). According to Evaline (2026), as organisations become increasingly digitised, employees are expected to make security-conscious decisions when handling information, accessing organisational systems and responding to cyber threats. Nevertheless, numerous studies highlight that humans are often subject to errors, misjudgment, intentional violations of policy, and social engineering resulting in attacks and breaches of systems.

The growing prominence of human factors has shifted cybersecurity research from a technology-centred approach towards a more integrated understanding of cybersecurity as a socio-technical phenomenon. This perspective acknowledges the value of technological controls as emanating from the people who design, implement, manage and use them. For instance, advanced security technologies can be rendered ineffective if employees do not

follow established standards and procedures for convenience, ignore security warnings or lack sufficient awareness to recognise emerging cyber threats. Similarly, poorly designed systems that are difficult to use may inadvertently encourage risky user behaviour, thereby reducing the effectiveness of existing cybersecurity controls (Akampurira et al., 2026). These interactions illustrate that cybersecurity resilience depends on achieving alignment between technological capabilities and human behaviour within organisational contexts.

Although there is an increasing recognition on the importance of human factors, the existing literature remains fragmented. Current research studies on cybersecurity literature continue to examine behavioural issues, organisational dynamics and technological controls independently, with relatively limited synthesis of how these dimensions interact to influence cybersecurity and privacy outcomes. There is a knowledge gap in this area, which is specifically acute in the context of cybersecurity in developing countries like Zimbabwe. Thus, there is a need for a comprehensive synthesis of the literature to develop a more integrated understanding of the human dimensions that contribute to persistent cyber risks despite the presence of technological controls.

2.3. Empirical Perspectives on Human Factors and Persistent Cyber Risks

The increasing complexity of cyber threats has prompted numerous studies which investigate why cyber-risks continue to thrive despite the progress in cybersecurity technologies.

Although organisations have increasingly invested in technical protections such as encryption, firewalls, intrusion detection systems and multi-factor authentication, empirical evidence consistently indicates that human factors remain among the leading contributors to cybersecurity incidents. The Verizon (2024) Data Breach Investigations Report reveals that most data breaches involve a human element, including phishing, misuse of credentials, social engineering and human error. Moreover, the social engineering attacks, according to Faotu et al. (2024) are one of the common cybersecurity threats because they take advantage of the human element, not the software design, which is a critical weakness. The studies have shown that cybersecurity threats cannot be eliminated by only relying on technological innovations without addressing without addressing the human factor issue.

A bigger number of research has made an examination of the behavioural determinants of cybersecurity effectiveness. In this regard, (Tran et al., 2024) emphasises that employees with high levels of cybersecurity awareness demonstrated high level of compliance with organisational security policies were less likely to engage in risky online behaviours. As such, Ifinedo (2014) highlights that information security awareness improves employees' intentions to comply with organisational policies on cybersecurity. However, awarenes on its own is not sufficient in promoting a more secure behaviour. Sachs (2025) highlights that individuals that have adequate cybersecurity knowledge may still engage in unsafe online practices because of behaviour that is habitual, overconfidence and complacency. This suggests that cybersecurity awareness should be improved by continuous behavioural interventions that encourages compliance consistency rather than only relying on knowledge acquisition.

Empirically, research highlights the influence of organisational environments on cybersecurity outcomes beyond individual awareness. According to Temitayo Oluwaseun et al. (2024) organisations that are characterised by a strong cybersecurity culture, a visible leadership commitment and a continuous employee engagement experience higher level of security policy compliance. In the same sentiment, (Pigola et al., 2025) provides that managerial support, effective policy enforcement and organisational accountability significantly reduces an employee’s intention to violate information security policies. On the other hand, organisations with weak security cultures are much less likely to have higher levels of compliance, even with enhanced technological measures in place to control and monitor activity. The findings suggest that organisational culture can be a key mechanism through which cybersecurity behaviours are encouraged or discouraged.

The research has also demonstrated the need to consider the design and usability of technology to promote secure necessary behaviours. Security controls that are perceived as overly complex or disruptive are frequently bypassed by users seeking to improve efficiency or convenience. According to Kwarteng et al. (2020), increased demands for security tend to cause users to adopt countermeasures that inadvertently create opportunities for compromising organizational cybersecurity vulnerabilities. Similarly, Delso-Vicente et al. (2025) argue that security technologies that fail to consider user needs and work practices often undermine compliance, as employees prioritise task completion over strict adherence to security procedures. Both works highlight the socio-technical nature of cybersecurity by emphasizing the need to consider factors that improve the likelihood that users will engage in cybersecurity behaviours.

Insider-related risks have attracted growing empirical attention since the authorised users have got access to organisations' information systems. Waiganjo and Nandjenda (2025) found that insider threats emerge due to a combination of organisational dissatisfaction, lack of security awareness and weak governance mechanisms rather than purely malicious intent. Likewise, Pathirana et al. (2026) argue that insider threats are often preceded by behavioural indicators that organisations fail to identify because cybersecurity programmes traditionally focus more on external attackers than internal vulnerabilities. These studies demonstrate that addressing organisational policies, employee engagement and proactive risk management practices should be considered together with the technical measures for effective control of insider-related risks.

Although empirical evidence has identified the importance of human factors to cybersecurity, there remains a need to understand the key factors that contribute towards recurring cyber threats.

Studies have examined areas of cybersecurity awareness, organizational culture, system usability, risk perception and insider threats as separate constructs hence this resulted in a fragmented understanding of how such variables collectively contribute to the persistence of cyber risks. Some of the empirical evidence has originated from the developed countries, where growth in technology is pronounced, regulatory environments and organisational contexts differ considerably from those found in developing countries (National Institute of & Technology, 2024). Few studies have systematically synthesized the interaction between behavioral tendencies, organizational practices and technology design in the context of Zimbabwe, despite the country's accelerating digital transformation and an evolving cybersecurity regulatory framework. As such, there is need to address this existing knowledge research gap through the consolidation of the existing literature that talks human factors and cybersecurity to establish factors that influence cybersecurity and privacy.

3. Methodology

3.1. Research Design

Researchers used a qualitative systematic literature review as guided by the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA 2020) framework. PRISMA was appropriate in the current study because the research on human factors in cybersecurity and privacy is dispersed across behavioural, organisational, technological and policy domains hence a systematic synthesis necessary to develop an integrated understanding human factors in cybersecurity and privacy (Page et al., 2021). The review was centred on synthesising contemporary evidence while at the same time ensuring transparency, rigour and reproducibility throughout the review process. This is supported by the Socio-Technical Systems Theory (Cherns, 1976; Trist & Bamforth, 1951), which provided analytical lens rather than being part of the reviewed evidence.

3.2. Search Strategy

Databases that included Scopus, Web of Science, IEEE Xplore, ScienceDirect and SpringerLink were explored. The databases index high-quality interdisciplinary literature in cybersecurity, information systems as well as digital governance. To ensure that recent developments in cybersecurity were captured, only studies published between 2025 to 2025 were considered for inclusion in the review. Boolean operators (AND, OR) combined

keywords including human factors, human behaviour, cybersecurity awareness, risk perception, organisational culture, security culture, system usability, insider threat, cybersecurity, privacy, data privacy and data protection. In addition, manual searches of reference lists from eligible studies were also undertaken to identify additional relevant publications that may not have been retrieved through database searches.

3.3. Inclusion and Exclusion Criteria

Studies were eligible for inclusion if they were published in English between 2015 and 2025, available in full text, published in peer-reviewed journals or refereed conference proceedings, and examined the influence of human factors on cybersecurity and privacy within organisational, governmental or national contexts. Empirical systematic reviews and policy-oriented studies were included because they provided evidence relevant to understanding behavioural and organisational determinants of cybersecurity effectiveness. Studies were excluded if they focused exclusively on technical cybersecurity mechanisms without considering behavioural or organisational dimensions; were editorials, opinion papers, book reviews, theses or dissertations; lacked sufficient methodological detail; were unavailable in full text; or were duplicate records. Even though seminal work published prior to 2015, including the Socio-Technical Systems Theory were used to underpin the study, they were not included in the PRISMA review sample. The review exclusively included contemporary studies which were published between 2025-2025.

3.4. Study Selection and Data Analysis

The study followed the PRISMA 2020 stages that included identification, screening, eligibility and inclusion. The database searching identified 428 records, additional 18 records identified using manual reference list searches thus producing 446 records. After the removal of 86 duplicate records, 360 studies remained for title and abstract screening. The screening process excluded 278 records which were not in alignment with the study objective. This left 82 full-text articles for a detailed eligibility assessment. The inclusion and exclusion criteria resulted in the exclusion of 47 studies, mainly because they focused solely on technical cybersecurity controls, lacked methodological rigour and were not sufficiently relevant to human factors in cybersecurity and privacy. As such, there were, 35 studies that met all the eligibility requirements and were included in the final qualitative synthesis.

The study used a structured data extraction matrix to capture and record author(s), the year of publication, the context of study, research methodology, the human factors examined and the principal findings. Thematic synthesis was used to analyse the extracted evidence and identify the recurring patterns, relationships and inconsistencies across the reviewed studies. The Socio-Technical Systems Theory was used as theoretical lens as such the theory was used in interpreting the interactions between technological systems, how human behaviours and organisational practices contribute to persistent cyber risks despite the existence of cybersecurity controls.

3.5. Trustworthiness and Rigour

Methodological rigour was achieved through using the PRISMA 2020 reporting guidelines, conducting a systematic search across multiple academic databases, a transparent application of the predefined inclusion and exclusion criteria as well as using a structured study selection process. Using multiple academic databases led to the reduction of publication bias, while a manual reference searching helped to improve the retrieval of studies which were relevant.

4. Results And Discussion

4.1. Human Factors as Drivers of Persistent Cyber Risks

The systematic literature review demonstrated that human factors stand as one of the causes of the persistent cyber risks despite continuous advances in cybersecurity technologies. The studies reviewed indicated that cybersecurity awareness, risk perception,

organisational culture, system usability and insider-related behaviours are interrelated and have an impact on the effectiveness of cybersecurity. Instead of functioning independently, these factors collectively determine how individuals interact with technological controls and influence organisational resilience against cyber threats.

This finding reinforces growing consensus that cyber incidents are increasingly driven by behavioural and organisational vulnerabilities rather than technological deficiencies alone (European Union Agency for, 2024; Verizon, 2024).

Cybersecurity awareness emerged as one of the most investigated human factors across the reviewed studies. While most studies tried to establish a link between organisational security outcomes and general awareness of employees about cyber threats, the results remained conflicting. On the one hand, the majority of the authors concluded that awareness campaigns contribute to better practices and more compliant behaviour (Khadka & Ullah, 2025). However, studies also revealed that theoretical knowledge does not necessarily translate into safe actions due to overconfidence in technological tools and established work routines as well as technological safeguards (Prabhu, 2025). Thus, continuous training and behavioural change rather than a one-time programme are required to improve the human factor in cybersecurity.

It should also be noted that organisational culture plays a crucial role in cybersecurity outcomes. This was evidenced by the fact that companies that exhibited visible support from leadership, promoted a culture of accountability and incorporated cybersecurity into everyday organisational practices consistently reported higher levels of policy compliance and stronger cybersecurity resiliency (Alshaikh, 2020; Oh et al., 2025). On the other hand, companies with ineffective organisational cultures characterised by limited management support, poor communication and inadequate employee engagement often led to poor implementation of technical controls (Govender & Bussin, 2020). These findings suggest that cybersecurity culture serves as an important mechanism through which allows companies to use technology to enforce secure operational practices.

Another recurring theme is the role of system's usability in cybersecurity behaviours. The reviewed studies indicated that users are more inclined to avoid security controls when systems are perceived as overly complex, time-consuming or irrelevant to their tasks (Sinan et al., 2025). Therefore, cybersecurity technologies that fail to consider user needs may prompt organisations to develop dangerous workarounds, creating new vulnerabilities. Thus, it is evident that cybersecurity processes should not only on technology sophistication but also be convenient for the users and serve their needs.

Corroborating the above, insider-related risks also emerged as an important contributor to contemporary cyber threats. The reviewed studies indicate that insider incidents often result from a combination of inadequate governance, weak organisational cultures, insufficient monitoring and behavioural factors rather than purely malicious intent (Lishchynsky, 2025). These findings underscore the importance of integrating behavioural risk management with technical security measures to strengthen organisational resilience and this aligns with the Socio-Technical Systems Theory, which argues that organisational performance depends on the effective integration of social and technical systems (Trist & Bamforth, 1951). The reviewed evidence therefore highlights that cybersecurity technologies alone cannot eliminate cyber risks if they are implemented without corresponding investments in employee awareness, supportive organisational cultures, effective leadership and user-centred system design. Persistent cyber risks therefore reflect misalignment between technological controls and the human systems responsible for their effective implementation.

5. Advancing Human-Centred Cybersecurity for Zimbabwe's Digital Future

The results have significant implications for Zimbabwe as it seeks to develop its digital government services, electronic commerce and digital financial systems under the National Development Strategy 2 (NDS2) and Vision 2030. Although, Zimbabwe has taken important steps to establish a legal framework for cybersecurity and data protection with the Cyber and Data Protection Act (Chapter 12:07), the reviewed evidence suggests that

legislative and technological interventions alone will be insufficient to achieve sustainable cybersecurity if human factors are not inadequately addressed. Effective cybersecurity requires organisations to adopt complementary approaches that go beyond technology to include organisational and behavioural strategies to promote secure digital practices.

The synthesis also shows that most of the research was conducted in developed countries. There is a need for more research on how human factors, organisational culture and the design of technology can be integrated to enhance cybersecurity and privacy outcomes. This will be important for informing strategies and policies to address crime and insecurity in Zimbabwe as the factors differ from those in the developed countries. Hence, context-specific evidence remains necessary to inform policies and interventions that respond to Zimbabwe's unique digital environment.

From a socio-technical standing, the way to enhance and strengthen cybersecurity in Zimbabwe requires a balanced approach that integrates technological, organisational and human dimensions. Entities should go beyond just complying, promoting user-friendly technologies and mitigating insider threats. Applying this integrated approach would enhance the employees' ability to recognise and respond to cyber threats while at the same time making an improvement to the effectiveness of existing technological controls. The literature showed that persistent cyber risks cannot be attributed totally attributed to the weaknesses in cybersecurity technologies. However, they also result from the interactions between human behaviour, organisational practices and technological systems. This indicates the need for cybersecurity and privacy protection strategies that puts people at the centre while at the same time ensuring that technological solutions are aligned with organisational needs and everyday user practices. In Zimbabwe, incorporating these principles within national cybersecurity policies, organisational governance frameworks and digital transformation initiatives will be essential for strengthening cyber resilience and supporting safe, trusted and inclusive digital development.

In Zimbabwe, incorporating these principles within national cybersecurity policies, organisational governance frameworks and digital transformation initiatives will be essential for strengthening cyber resilience and supporting safe, trusted and inclusive digital development.

6. Conclusion

This study followed a systematic review of the literature to explore how human factors contribute to the persistence of cyber risks despite the widespread adoption of cybersecurity controls. This study found that despite an extensive application of cybersecurity measures, the threat of cyber-attack remains substantial. Thus, persistent cyber risks are to a greater extent influenced by an interaction between human behaviour, organisational practices and technology design. Evidence from the systematic literature review showed cybersecurity awareness, risk perception, organisational culture, system usability and insider-related behaviours being critical determinants of cybersecurity and privacy outcomes. The literature revealed that these factors could significantly influence how individuals perceive cyber threats, comply with organisational security policies and interact with technological measures.

Using the Socio-Technical Systems Theory viewpoints, the results of the study reinforce the argument that cybersecurity is not just only a technological challenge but a socio-technical phenomenon that calls for an alignment between technological infrastructure and the human and organisational systems within which it operates. The results show that while substantial empirical evidence exists internationally, research from developing countries especially Zimbabwe, remains fragmented and predominantly focused on legislative and technical aspects of cybersecurity. There is also limited integrated evidence to guide the development of human-centred cybersecurity strategies within developing countries such as Zimbabwe in a rapidly evolving digital landscape. Given this, addressing cyber risks calls for a balanced approach that integrates technological innovation with behavioural change, organisational commitment and effective governance to support secure and sustainable digital transformation.

7. Recommendations

7.1. Policy Recommendations

Instead of developing additional policies on cybersecurity, policymakers should then institutionalise the measurement of human cyber risk within national cybersecurity governance. Current regulatory approaches mainly focus on organisational compliance with technical and legal requirements, yet they rarely evaluate behavioural indicators such as cybersecurity culture, employee risk perception and security compliance. Developing a national Human Cyber Risk Assessment Framework would enable regulators to incorporate behavioural resilience indicators into cybersecurity audits, thereby providing a more comprehensive assessment of organisational cybersecurity maturity.

Government should also promote human-centred cybersecurity by design for instance, when developing digital public services and regulatory standards. The existing cybersecurity regulations put more focus on technical controls and legal compliance, with limited emphasis on usability and behavioural considerations. The integration of user-centred design principles within national digital transformation initiatives will reduce security workarounds that in most cases arise from overly intricate systems and improve both cybersecurity and privacy effects.

7.2. Practice Recommendations

The study recommends that organisations should evolve beyond awareness-driven cybersecurity programmes and embrace behavioural cybersecurity management systems. Instead of making an evaluation of employees mainly on training completion, organisations should instead monitor behavioural indicators such as policy adherence, responses to simulated cyber threats, secure system usage and recurring risky behaviours. Such behavioural metrics should then form part of the Enterprise Risk Management (ERM) as well as organisational governance to enable continuous improvement.

7.3. Areas for Further Research

The present study relied on evidence from a systematic literature review. Given this, it is suggested that future empirical quantitative research be carried to examine the human factors in Cybersecurity and Privacy.

Author Contribution

Elisha Mutize: Conceptualisation and crafting of paper
Admire Mthombeni: Conceptualisation and crafting of paper
Leonard Chitongo: Conceptualisation and crafting of paper

Conflict of Interest

The authors declared no potential conflicts of interest w.r.t. the research, authorship and/or publication of this article.

References

Akampurira, P., Edozie, E., Olaniyi Sadiq, B., & Dahiru Buhari, M. (2026). A Deep Learning-Based User Behavior Analytics Model for Proactive Cyber Threat Detection and Risk Management: A Review. *F1000Research*, *15*, Article 674. https://doi.org/10.12688/f1000research.178351.2

Akter, S., Uddin, M. R., Sajib, S., Lee, W. J. T., Michael, K., & Hossain, M. A. (2022). Reconceptualizing Cybersecurity Awareness Capability in the Data-Driven Digital Economy. *Ann Oper Res*, *350*(2), 1-26. https://doi.org/10.1007/s10479-022-04844-8

Alshaikh, M. (2020). Developing Cybersecurity Culture to Influence Employee Behavior: A Practice Perspective. *Computers & Security*, *98*, Article 102003. https://doi.org/10.1016/j.cose.2020.102003

Aslan, Ö., Aktuğ, S. S., Ozkan-Okay, M., Yilmaz, A. A., & Akin, E. (2023). A Comprehensive Review of Cyber Security Vulnerabilities, Threats, Attacks, and Solutions. *Electronics*, *12*(6), Article 1333. https://doi.org/10.3390/electronics12061333

Bishop, L. M., Asquith, P. M., Morgan, P. L., & Chakraborty, P. (2025). The Employee Cybersecurity Awareness Framework. *Human Behavior and Emerging Technologies*, *2025*(1), Article 1025045. https://doi.org/10.1155/hbe2/1025045

Chat, A. R., Anan, S. R., & Alam, M. M. (2023). *The Human Element in Cybersecurity: Bridging the Gap between Technology and Human Behaviour*. https://www.researchgate.net/publication/380270220_The_Human_Element_in_Cybersecurity_-_Bridging_the_Gap_Between_Technology_and_Human_Behaviour

Cherns, A. (1976). The Principles of Sociotechnical Design. *Human Relations*, *29*(8), 783-792. https://doi.org/10.1177/001872677602900806

Delso-Vicente, A.-T., Diaz-Marcos, L., Aguado-Tevar, O., & de Blanes-Sebastián, M. G. (2025). Factors Influencing Employee Compliance with Information Security Policies: A Systematic Literature Review of Behavioral and Technological Aspects in Cybersecurity. *Future Business Journal*, *11*(1), Article 28. https://doi.org/10.1186/s43093-025-00452-7

Emery, F. E. (1959). *Characteristics of Socio-Technical Systems*.

European Union Agency for, C. (2024). *Enisa Threat Landscape 2024* (978-92-9204-675-0). https://doi.org/10.2824/0710888

https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

Evaline, N. W. (2026). *A Model to Determine Cyber Security Human Vulnerabilities Exposure Index for Mfis (a Case Study of Nairobi County, Kenya)* Co-operative University of Kenya]. https://repository.cuk.ac.ke/xmlui/handle/123456789/541

Faotu, H., Asheshemi, O. N., & Esite, J. T. (2024). Human Vulnerabilities in Cybersecurity: Analyzing Social Engineering Attacks and Ai-Driven Machine Learning Countermeasures. *Journal of Science and Technology*, *30*(1), 72-84. https://doi.org/10.20428/jst.v30i1.2597

Govender, M., & Bussin, M. H. R. (2020). Performance Management and Employee Engagement: A South African Perspective. *SA Journal of Human Resource Management*, *18*(0), Article a1215. https://doi.org/10.4102/sajhrm.v18i0.1215

Ibm. (2024). *Cost of a Data Breach Report 2024*. https://www.ibm.com/reports/data-breach

Ifinedo, P. (2014). Information Systems Security Policy Compliance: An Empirical Study of the Effects of Socialisation, Influence, and Cognition. *Information & Management*, *51*(1), 69-79. https://doi.org/10.1016/j.im.2013.10.001

Iyer, S. S., & Raji, B. (2025). Cybersecurity Culture and Organizational Resilience: A Human-Centered Approach to Digital Risk Management. *American Journal of Industrial and Business Management*, *15*(05), 748-766. https://doi.org/10.4236/ajibm.2025.155036

Jyoti, Prajapati, N., Kulshreshtha, P., & Ghosh, A. (2026). Regulating Automated Fraud. In T. P. Fudge (Ed.), *The Intersection of Technology and Criminal Justice* (pp. 181-204). IGI Global Scientific Publishing. https://doi.org/10.4018/979-8-3373-7660-8.ch009

Khadka, K., & Ullah, A. B. (2025). Human Factors in Cybersecurity: An Interdisciplinary Review and Framework Proposal. *International Journal of Information Security*, *24*(3), Article 119. https://doi.org/10.1007/s10207-025-01032-0

Kwarteng, R. A., Idoko, I. P., Ijiga, O. M., & Enyejo, L. A. (2020). Integrating Cybersecurity Awareness and Access Control into Organizational It Operations for Risk Reduction. *International Journal of Scientific Research in Computer Science Engineering and Information Technology*, *6*(1), 243-261. https://doi.org/10.32628/cseit23906128

Lishchynsky, M. (2025). The Insider Threat: A Socio-Technical Analysis of Preventing Data Breaches and Espionage within Governmental Agencies. *Politics & Security*, *12*(2), 88-103. https://doi.org/10.54658/ps.28153324.2025.12.2.pp.88-103

Mai, N. T., & Khalid, I. (2025). Human Error Vs. System Security: Evaluating the Weakest Link in Digital Business Information Systems. *Journal of Management and Informatics*, *4*(3), 981-997. https://doi.org/10.51903/jmi.v4i3.305

National Institute of, S., & Technology. (2024). *The Nist Cybersecurity Framework (Csf) 2.0*. https://doi.org/10.6028/NIST.CSWP.29

https://www.nist.gov/publications/nist-cybersecurity-framework-csf-20

Oh, K. B., Hoang, G., Sturdy, J., & Guo, S. S. (2025). Cybersecurity and Governance. In *Cybersecurity Governance* (pp. 19-63). Springer Nature Singapore. https://doi.org/10.1007/978-981-95-3865-2_2

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D.,…Moher, D. (2021). Updating Guidance for Reporting Systematic Reviews:

Development of the Prisma 2020 Statement. *J Clin Epidemiol*, *134*, 103-112. https://doi.org/10.1016/j.jclinepi.2021.02.003

Pathirana, N., Roberts, R., Kalutarage, H., & McDermott, C. D. (2026). Integrating Human Factors into Insider Threat Detection – a Systematic Review. *ACM Computing Surveys*, *58*(10), 1-37, Article 260. https://doi.org/10.1145/3798089

Pigola, A., da Costa, P. R., Vils, L., & Meirelles, F. d. S. (2025). Enhancing Information Security Management and Performance through Social and Relational Factors: A Structural Equation Modelling Approach. *Behaviour & Information Technology*, *45*(3), 498-520. https://doi.org/10.1080/0144929x.2025.2522206

Pollini, A., Callari, T. C., Tedeschi, A., Ruscio, D., Save, L., Chiarugi, F., & Guerri, D. (2022). Leveraging Human Factors in Cybersecurity: An Integrated Methodological Approach. *Cogn Technol Work*, *24*(2), 371-390. https://doi.org/10.1007/s10111-021-00683-y

Prabhu, S. (2025). Managing Risks and Perceptions in Everyday Organisational Cybersecurity. *Australasian Journal of Information Systems*, *29*. https://doi.org/10.3127/ajis.v29.6011

Rendahl, J. (2026). Enhancing Organisational Cyber Security Resilience: A Human-Centric Approach. *Cyber Security: A Peer-Reviewed Journal*, *9*(4), 350-365. https://doi.org/10.69554/ipdb8002

Sachs, D. S. (2025). *Behavioral Insights in Cybersecurity*. CRC Press. https://doi.org/10.1201/9781003606345

Sinan, M., Shahin, M., & Gondal, I. (2025). Integrating Security Controls in Devsecops: Challenges, Solutions, and Future Research Directions. *Journal of Software: Evolution and Process*, *37*(6), Article e70029. https://doi.org/10.1002/smr.70029

Sutton, A., & Tompson, L. (2025). Towards a Cybersecurity Culture-Behaviour Framework: A Rapid Evidence Review. *Computers & Security*, *148*, Article 104110. https://doi.org/10.1016/j.cose.2024.104110

Temitayo Oluwaseun, A., Oluwatoyin Ajoke, F., Simon, K., Prisca Ugomma, U., Azeez Olanipekun, H., & Samuel Onimisi, D. (2024). Cybersecurity Awareness and Education Programs: A Review of Employee Engagement and Accountability. *Computer Science & IT Research Journal*, *5*(1), 100-119. https://doi.org/10.51594/csitrj.v5i1.708

Tran, D. V., Nguyen, P. V., Le, L. P., & Nguyen, S. T. N. (2024). From Awareness to Behaviour: Understanding Cybersecurity Compliance in Vietnam. *International Journal of Organizational Analysis*, *33*(1), 209-229. https://doi.org/10.1108/ijoa-12-2023-4147

Trist, E. L., & Bamforth, K. W. (1951). Some Social and Psychological Consequences of the Longwall Method of Coal-Getting. *Human Relations*, *4*(1), 3-38. https://doi.org/10.1177/001872675100400101

Verizon. (2024). *2024 Data Breach Investigations Report*. https://www.verizon.com/business/resources/reports/dbir/

von Solms, R., & van Niekerk, J. (2013). From Information Security to Cyber Security. *Computers & Security*, *38*, 97-102. https://doi.org/10.1016/j.cose.2013.04.004

Waiganjo, I. N., & Nandjenda, L. S. (2025). Unveiling Insider Threats: Examining Vulnerabilities in an Organizational？Structure: A Case Study of Nampost. *OALib*, *12*(01), 1-10, Article e12797. https://doi.org/10.4236/oalib.1112797

World Economic, F. (2025). *The Global Risks Report 2025*. https://www.weforum.org/publications/global-risks-report-2025/