Impediments to Cybersecurity Policy Implementation in Organisations: Case Study of Windhoek, Namibia

Iyaloo WAIGANJO, Jude OSAKWE, Ambrose AZETA

Faculty of Computing and Informatics Namibia University of Science and Technology (NUST)

DOI: https://doi.org/10.51244/IJRSI.2024.1110046

Received: 09 October 2024; Accepted: 14 October 2024; Published: 15 November 2024

ABSTRACT

The increasing dependence on digital infrastructure has exposed organisations to heightened risks of cyber-attacks, necessitating the implementation of comprehensive cybersecurity policies. These policies aim to safeguard organisational data by establishing security requirements, ranging from acceptable use and access controls to incident response and encryption protocols. However, despite the critical importance of these policies, their effective implementation often encounters significant challenges. This study investigates the impediments to cybersecurity policy implementation within Namibian organizations, focusing on the perspectives of IT managers and employees. Using a qualitative research approach, interviews were conducted with 8 IT managers and 12 employees across various organisations to identify the key obstacles faced in adhering to and enforcing these policies. The findings reveal that the major impediments include a lack of executive and leadership support, challenges with compliance and policy adherence by employees, insufficient training and awareness, budget and resource constraints, poor communication, and the influence of human factors. This research underscores the need for a multifaceted approach to overcoming these impediments, emphasizing the importance of strong leadership, continuous and practical training, adequate resource allocation, and transparent communication. Building a cybersecurity culture within organizations is essential to mitigate these challenges and ensure the effective implementation of cybersecurity policies, thereby enhancing organizational resilience against cyber threats. The study recommends that future research should expand the sample size to include a more diverse group of participants from various organizations and sectors across Namibia. This broader representation would provide a more comprehensive understanding of the issues, reveal sector-specific challenges, and ensure that the findings are more generalizable across different industries and contexts.

Key Words: Cybersecurity Challenges, Namibian Organizations, Cybersecurity Policy Implementation, Compliance

INTRODUCTION

While organisations reaped the benefits of connectivity, they simultaneously opened themselves to cyber-attacks, necessitating the development of robust monitoring systems through the establishment of comprehensive cybersecurity policies. These policies, a strategic response to safeguard organisational data and information, were envisioned to articulate security requirements applicable across the organisational spectrum, extending to every employee member and anyone granted access to the organisation's Internet infrastructure (Li et al., 2019). These policies define acceptable use, access controls, incident response procedures, and encryption protocols among others (Grispos, 2019). They establish a framework for employees to adhere to security measures and enforce compliance with cybersecurity standards.

However, in this well-intentioned quest of cyber resilience, organisations faced an enduring challenge employee compliance. Despite the careful crafting of cybersecurity policies, employees often exhibited carelessness and indifference, overlooking, or underestimating the gravity of these protocols (Safa et al., 2016; Li et al., 2019). Recognising that employees constitute the weakest link in the cybersecurity chain, organisations found themselves grappling with the potential consequences of non-compliance. The actions of employees, particularly violations of security policies and regulations, could render the organisation susceptible to cyber threats and attacks (Williams, Chaturved, & Chakravarthy, 2020). In the absence of a

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XI Issue X October 2024

comprehensive policy implementation plan coupled with harsh employees adherence, these policies risked relegation to the status of inconsequential artifacts within the organisational framework (Alias, 2019).

Implementing cybersecurity policies within organizations is fraught with numerous challenges, which can significantly undermine the effectiveness of these policies. One of the primary obstacles is the lack of employee compliance, which remains a persistent issue across various industries. Employees often fail to adhere to cybersecurity protocols due to insufficient awareness, inadequate training, or a general disregard for the importance of these policies (Omoyiola & McKeeby, 2023; Teoh & Mahmood, 2018). The lack of necessary skills among employees, coupled with human errors—both intentional and unintentional—further exacerbates the difficulty of ensuring robust cybersecurity measures (Teoh & Mahmood, 2018).

Organizational challenges also play a critical role in impeding the successful implementation of cybersecurity policies. Inadequate implementation plans, the misallocation of human resources, and budget constraints are frequently cited as significant barriers (Teoh et al., 2018). The rapid pace of technological advancements introduces additional complexities, as policies may quickly become outdated, necessitating continuous updates and revisions to keep pace with evolving threats and technologies (Teoh et al., 2018).

Specific studies highlight these challenges within particular regional contexts. For instance, in West Africa, cybersecurity leaders often fail to enforce cybersecurity policies effectively, largely due to poor employee compliance. This noncompliance not only leads to increased security risks but also to potential breaches, undermining the overall security posture of organizations (Omoyiola & McKeeby, 2023; Alotaibi et al., 2016). Ademola and Uk (2019) found that misalignment between Information Technology (IT) Governance and business policies further complicates cybersecurity policy implementation. They noted that a lack of awareness regarding both global and local cybersecurity threats, coupled with inadequate security infrastructures and the absence of expert input in decision-making processes, poses significant challenges.

The financial aspect also plays a crucial role in the implementation of cybersecurity policies. Naguib et al. (2024) observed that the budget allocated to IT departments directly influences IT governance and, consequently, the effective execution of cybersecurity policies. Without sufficient financial resources, organizations may struggle to implement necessary security measures, leaving them vulnerable to threats.

In the Malaysian context, Teoh et al. (2018) identified several impediments to cybersecurity policy implementation, including a shortage of skills in both policy development and cybersecurity governance. Human errors, lack of comprehensive implementation plans, and the rapid evolution of technology were also noted as critical challenges. Alotaibi et al. (2016) categorized these challenges into four main groups: promotion of security policies, employee noncompliance, management and updating of policies, and the phenomenon of "shadow security" where unauthorized security measures are implemented by employees.

The role of government and its interventions through laws and regulations cannot be understated in addressing these challenges. Schneider (2018) argues that government involvement is essential for the successful implementation of cybersecurity policies. Without government-backed regulations and support, the efforts of organizations to enforce cybersecurity measures may be insufficient, leaving them vulnerable to cyber threats. To mitigate these barriers, organizations are advised to invest in comprehensive security awareness training programs, establish effective communication channels, and secure management support for cybersecurity initiatives (Omoyiola & McKeeby, 2023). Regular reviews of employee compliance and the appointment of a Chief Information Security Officer (CISO) are also recommended as critical measures (Omoyiola & McKeeby, 2023). Furthermore, aligning IT Governance with business policies is essential for maintaining competitiveness and ensuring robust cybersecurity (Ademola & Uk, 2019). Continuous, targeted awareness campaigns and dynamic monitoring of user adherence to security policies are key strategies for enhancing compliance levels (Alotaibi et al., 2016).

Considering the growing global reliance on digital infrastructure, the implementation of robust cybersecurity policies has become essential to safeguarding organizational assets. However, despite the clear need for these measures, many organizations face persistent challenges in effectively enforcing them. The barriers range from employee non-compliance and lack of awareness to resource limitations and outdated technologies. Given the

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XI Issue X October 2024

critical role that cybersecurity plays in protecting against evolving threats, understanding these impediments is crucial for developing strategies that ensure better adherence to policy frameworks. This study focuses on the Namibian context, aiming to identify and address the specific challenges organizations in Windhoek face in implementing cybersecurity policies.

METHODOLOGY

This research employed a qualitative approach, which is ideal for exploring the complex and contextual nature of cybersecurity policy implementation in organizations. Convenience sampling was used to select 20 participants based on their availability and willingness to participate. The sample comprised 8 IT managers and 12 employees, all drawn from different organizations based in Windhoek. This participant group was chosen because IT managers are responsible for overseeing the implementation of cybersecurity policies, while employees play a critical role in adhering to and executing these policies at the operational level.

Data collection was conducted using two methods: semi-structured interviews with the IT managers and focus group discussions with the employees. The semi-structured interviews provided in-depth insights into the experiences and perspectives of IT managers regarding policy implementation, challenges faced, and strategies adopted to address these challenges. This method allowed for flexibility in exploring emerging topics while ensuring that key research questions were addressed.

The focus group discussions with the employees, on the other hand, facilitated a dynamic exchange of ideas, enabling the researcher to capture a range of viewpoints and collective reflections on how cybersecurity policies are experienced in practice. This method was particularly useful in identifying shared challenges and the impact of organizational culture on policy compliance.

Thematic analysis was used to analyze the data collected, following a systematic process of coding and identifying patterns across the data. Themes were generated based on recurring concepts and issues raised by the participants, and these themes are discussed in detail in the findings section. This method allowed the researcher to distill complex data into meaningful categories, providing a nuanced understanding of the barriers and enablers of effective cybersecurity policy implementation within the selected organizations.

DATA ANALYSIS

Participants were asked a series of questions designed to explore the barriers to effective cybersecurity policy implementation from both managerial and employee perspectives. The responses from IT managers and employees highlighted several critical challenges.

Questions for IT Managers

1. In your view, how does organizational culture affect compliance with cybersecurity policies?
2. What are the main obstacles preventing employees from adhering to the organization's cybersecurity policies?
3. What challenges have you encountered when implementing cybersecurity policies within your organization?

Questions for Employees

1. From your experience, what challenges do you face in complying with cybersecurity policies in your day-to-day work?
2. Have there been instances where cybersecurity policies were unclear or difficult to follow? If so, could you provide specific examples?
3. What do you think the organization could do to improve staff understanding and compliance with cybersecurity policies?

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XI Issue X October 2024

The thematic analysis of the interview and focus group discussions revealed several key themes related to the impediments to cybersecurity policy implementation. These themes, which are discussed in detail below, offer insights into the common barriers faced by both IT managers and employees.

Executive and Leadership Support

A lack of executive and leadership support is a significant challenge in implementing cybersecurity policies. Loonam et al. (2020) emphasize the critical role of senior leaders in shaping and supporting cybersecurity strategies, while Banks (2016) highlights the importance of leaders promoting a culture of cybersecurity through example. This study found that lack of top management support was a notable impediment to successful cybersecurity policy implementation. For instance, Organisation E reported that despite having technological protocols, high-level management's reluctance to change due to perceived inconvenience created significant hurdles. In contrast, Organisations A and B experienced minimal challenges due to strong executive support and involvement. Executive and leadership support is crucial, especially in a cyber economy where senior management must initiate and enforce security plans and policies (Dutta & McCrohan, 2002).

I. Compliance and Policy Adherence

Compliance and policy adherence present significant challenges, often exacerbated by human factors such as resistance to frequent security updates and lack of commitment. Alotaibi, Furnell, and Clarke (2016) and Onumo (2021) both emphasize the difficulties employees face in complying with cybersecurity policies. Organisation B addressed low compliance rates through personalized training and quizzes following internal phishing tests. Organisation D faced challenges with older employees resisting compliance due to ignorance and cultural resistance. Employees from Organisation A struggled with constant security updates and notifications, which distracted them from their primary tasks, while Organisation D highlighted difficulties managing compliance due to frequent password changes, leading to memory issues and reduced productivity.

II. Lack of Training and Awareness

The lack of comprehensive cybersecurity training and awareness significantly impacts organizations, often leading to successful cyber-attacks (Aldawood & Skinner, 2019). Traditional awareness programs are often ineffective, necessitating new training models (Sabillon, Serra-Ruiz, & Cavaller, 2021). Organisation C indicated that the lack of comprehensive policies and formal training left employees unprepared for cyber threats. Employees expressed the need for better awareness and education, with Organisation D noting that insufficient training for new or temporary staff created vulnerabilities. Limited and ineffective training sessions did not provide the practical knowledge necessary for robust cybersecurity practices.

III. Budget and Resource Constraints

Budget constraints significantly compromise cybersecurity measures, leading to vulnerabilities (Saini, 2019). This is particularly evident in the government and public sectors (Saini, 2020). Organisation B identified budget constraints as a major challenge, particularly given the high costs associated with cybersecurity. Despite these limitations, continuous feedback mechanisms and resource sharing helped foster a culture of cybersecurity awareness. Organisation C highlighted that focusing on IT infrastructure resulted in insufficient staffing for cybersecurity initiatives, underscoring the need for better resource allocation and investment.

IV. Communication and Transparency

Effective communication and transparency are crucial for building a cybersecurity culture and managing crisis events (Corradini, 2020). Normalizing transparency, including communication to staff, investors, and the public, is essential for effective cyber incident responses (Hellemann, 2023). Organisation E reported that poor communication regarding cybersecurity policies led to employee confusion and frustration, while Organisation D's employees felt excluded due to insufficient internal communication, relying instead on external sources for cybersecurity knowledge. These gaps underscored the need for better communication and transparency within organizations.

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XI Issue X October 2024

V. Technological and Human Factors

Human factors play a critical role in cybersecurity challenges, particularly in the context of social engineering. Organisation E emphasized the importance of continuous awareness and training to create a strong cybersecurity culture. Organisation A highlighted the proactive approach of their security team, including regular training sessions and updates, which helped manage the constant stream of security tasks. However, the demanding nature of these tasks and the pressure to comply with guidelines remained significant challenges for employees.

- Technological Factors

Technological factors often complicate cybersecurity policy adherence due to the operational burden they impose on employees. For instance, Organisation A's employees faced challenges with frequent security updates and notifications, which distracted them from their core tasks. These findings align with studies that highlight the impact of excessive system notifications on employee productivity and focus (Alotaibi, Furnell, & Clarke, 2016). Additionally, Organisation D's struggle with managing frequent password changes, leading to memory issues and reduced productivity, reflects broader research on password management challenges in the workplace. According to Alotaibi et al. (2016), such frequent updates, although essential for security, often frustrate employees, contributing to poor adherence. The technological and human factors as the main influence of cybersecurity policy adherence, as outlined in the analysis, differ in several keyways.

- Human Factors

Human factors, on the other hand, primarily concern the behavioral and cognitive responses to cybersecurity policies. Organisation D’s resistance to policy compliance, especially among older employees due to cultural resistance and ignorance, mirrors findings in the literature where human behavior is a key impediment to cybersecurity (Onumo, 2021). Moreover, Organisation C's lack of comprehensive training left employees unprepared for cybersecurity challenges, a common issue noted by Aldawood and Skinner (2019). Social engineering attacks, which exploit human vulnerabilities rather than technical weaknesses, emphasize the significance of human factors (Sabillon, Serra-Ruiz, & Cavaller, 2021). Human factors, therefore, necessitate a focus on continuous education, awareness, and training to improve adherence.

- Technological factors

Technological factors involve the practical demands of security systems, such as the constant stream of updates and password management protocols, which can overwhelm employees. In contrast, human factors revolve around the behavioral and psychological responses to these security measures, including resistance to compliance, lack of awareness, and vulnerability to social engineering attacks (Aldawood & Skinner, 2019; Alotaibi, Furnell, & Clarke, 2016). Both dimensions require careful consideration when implementing and enforcing cybersecurity policies within organizations.

The study’s finding shows that the implementation of cybersecurity policies faces several impediments across organizations, including a lack of executive support, compliance and adherence issues, insufficient training and awareness, budget constraints, poor communication, and human factors. Addressing these challenges requires a multifaceted approach, involving strong leadership, comprehensive and continuous training programs, adequate resource allocation, and transparent communication. Building a culture of cybersecurity within organizations is essential for mitigating these impediments and ensuring robust protection against cyber threats.

CONCLUSION

This study highlights the multifaceted challenges Namibian organizations face in implementing cybersecurity policies. The findings reveal that these impediments span across organizational, technological, and human factors. Critical barriers include a lack of executive and leadership support, insufficient training and awareness, frequent noncompliance with security policies, budgetary constraints, and ineffective communication

strategies. Human factors, such as employee resistance to change, inadequate understanding of cybersecurity risks, and the complexities of managing compliance, also play a pivotal role.

Organizations that have garnered leadership support and fostered a culture of cybersecurity tend to navigate these challenges more effectively, ensuring higher compliance and policy adherence. However, in many cases, employees struggle with the increasing complexity of cybersecurity requirements, especially in environments lacking adequate training and engagement.

To strengthen the implementation of cybersecurity policies, organizations should prioritize leadership support by ensuring that executives actively promote and enforce these policies, fostering a culture of security. Continuous and practical training programs should be provided to employees across all departments to enhance compliance and awareness of risks. Improved internal communication is essential, with clear explanations of policies and the rationale behind security measures. Adequate budgeting and resource allocation must be ensured to support cybersecurity initiatives, including hiring skilled personnel and implementing advanced tools. A culture of shared responsibility for cybersecurity should be fostered through employee engagement and recognition for adherence to security practices. Additionally, aligning IT governance with business objectives is crucial to maintain competitiveness and secure organizational operations. For future research, studies could explore the impact of emerging technologies, such as artificial intelligence and machine learning, on enhancing cybersecurity policy enforcement, as well as investigating the role of government regulations in shaping cybersecurity frameworks in developing economies. Also, the study recommends that future research should expand the sample size to include a more diverse group of participants from various organizations and sectors across Namibia. This broader representation would provide a more comprehensive understanding of the issues, reveal sector-specific challenges, and ensure that the findings are more generalizable across different industries and contexts.

REFERENCES

1. Aldawood, H., & Skinner, G. (2019). Reviewing cyber security social engineering training and awareness programs—Pitfalls and ongoing issues. Future internet, 11(3), 73. https://doi.org/10.3390/fi11030073
2. Alias, R. A. (2019). Information security policy compliance: Systematic literature review. Procedia Computer Science, 161, 1216-1224.
3. Alotaibi, F., Furnell, S., Stengel, I., & Papadaki, M. (2016). A review of using gaming technology for cyber-security awareness. Int. J. Inf. Secur. Res.(IJISR), 6(2), 660-666.
4. Banks, C. (2016). Leadership in cybersecurity: Roles and responsibilities. International Journal of Business and Management, 11(5), 123-132. https://doi.org/10.5539/ijbm.v11n5p123
5. Banks, N. (2016). Practise what you preach. Computer Fraud & Security, 2016, 5-8.
6. Corradini, I. (2020). Communication and transparency in cybersecurity: The key to crisis management. Journal of Cyber Policy, 5(3), 301-318. https://doi.org/10.1080/23738871.2020.1818821
7. Dutta, A., & McCrohan, K. (2002). Management's role in information security in a cyber economy. California Management Review, 45(1), 67-87. https://doi.org/10.2307/41166148
8. Grispos, G. (2019). Cybersecurity: Practice. Encyclopedia of Security and Emergency Management, 1-6.
9. Hellemann, J. (2023). Radical transparency in cybersecurity: Communication strategies for modern threats. Cybersecurity Journal, 2(1), 89-107. https://doi.org/10.1057/s41284-022-00311-4
10. Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. International Journal of Information Management, 45, 13-24. https://doi.org/10.1016/j.ijinfomgt.2018.10.017
11. Loonam, J., Kumar, V., & Derksen, L. (2020). Leadership and cybersecurity: Strategies for securing the digital organization. Journal of Business Strategy, 41(6), 9-17. https://doi.org/10.1108/JBS-03-2020-0044
12. Naguib, H. M., Kassem, H. M., & Naem, A. E. H. M. A. (2024). The impact of IT governance and data governance on financial and non-financial performance. Future Business Journal, 10(1), 15.
13. Omoyiola, B. O., Mckeeby, J., & Whyte, S. T. (2023). The Strategies for Mitigating the Human Insider Factor in Cybersecurity. Available at SSRN 4680255.
14. Sabillon, R., Serra-Ruiz, J., & Cavaller, V. (2021). New models for cybersecurity awareness and training. Computers & Security, 99, 102073. https://doi.org/10.1016/j.cose.2020.102073

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XI Issue X October 2024

15. Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information security conscious care behaviour formation in organizations. Computers & Security, 53, 65-78.
16. Saini, M. (2020). Resource management in cybersecurity: Addressing vulnerabilities through strategic allocation. Public Sector Cybersecurity Journal, 4(2), 55-70. https://doi.org/10.1108/PSCJ-02-2020-0004
17. Teoh, C. S., & Mahmood, A. K. (2018). Cybersecurity workforce development for digital economy. The Educational Review, USA, 2(1), 136-146.
18. Teoh, C. S., Mahmood, A. K., & Dzazali, S. (2018, August). Cyber security challenges in organisations: A case study in Malaysia. In 2018 4th International Conference on Computer and Information Sciences (ICCOINS) (pp. 1-6). IEEE.
19. Williams, C. M., Chaturvedi, R., & Chakravarthy, K. (2020). Cybersecurity risks in a pandemic. Journal of medical Internet research, 22(9), e23692.

Ethical Considerations

Ethical Approval: All the participants signed a content form as a way of giving approval to take part in the research.

Conflict of Interest: All authors have not in conflict of interest.

Data Availability

Statement: Not available.