Open Access Library Journal
2025, Volume 12, e12797
ISSN Online: 2333-9721
ISSN Print: 2333-9705

Unveiling Insider Threats: Examining Vulnerabilities in an Organizational Structure: A Case Study of NamPost

Iyaloo N. Waiganjo, Linekela S. Nandjenda

Faculty of Information Communication Technology, International University of Management, Windhoek, Namibia
Email: i.waiganjo@ium.edu.na, linekela.sh@gmail.com

How to cite this paper: Waiganjo, I.N. and Nandjenda, L.S. (2025) Unveiling Insider Threats: Examining Vulnerabilities in an Organizational Structure: A Case Study of NamPost. *Open Access Library Journal*, **12**: e12797.
https://doi.org/10.4236/oalib.1112797

Received: December 9, 2024
Accepted: January 5, 2025
Published: January 8, 2025

Abstract

Insider threats pose significant risks to organizations, particularly in cybersecurity, where individuals with authorized access can misuse their privileges to cause data breaches, financial losses, or operational disruptions. This study explores the vulnerabilities within NamPost's organizational structure that could be exploited by insider threats, aiming to develop a tailored detection and prevention model. A qualitative research approach was employed, involving semi-structured interviews with 10 participants from NamPost's ICT department. The findings reveal that high stress, job dissatisfaction, inadequate access controls, and insufficient employee training contribute to insider threats. Participants emphasized the need to foster a supportive organizational culture and implement robust access control measures to mitigate risks. This article discusses these findings, situates them within broader literature, and provides actionable recommendations to strengthen NamPost's resilience against insider threats.

Subject Areas

Cybersecurity

Keywords

Insider Threats, Cybersecurity Risks, Organizational Vulnerabilities, Access Control

1. Introduction

Insider threats refer to security risks posed by individuals within an organization who have authorized access to its systems, networks, or data [1]. Factors such as

financial difficulties, relationship conflicts, substance abuse, blackmail, dissatisfaction with the organisation and job increase the instances of insider threats [2]. These threats often arise from employees, contractors, or business partners who abuse or inadvertently mishandle their access, leading to data breaches, financial loss, or operational disruptions [3]. Insider threats are particularly concerning cybersecurity because insiders are already within the organization's security perimeter, making it difficult to detect malicious activity compared to external attacks [1].

The motivations behind insider threats vary widely and can include personal gain, ideological beliefs, dissatisfaction with the organization, or coercion by outside forces [4]. Insiders with privileged access, such as system administrators or senior managers, often represent a higher risk due to the extent of their access to sensitive systems and data. Furthermore, insider threats are difficult to predict, as they may stem from individuals with no previous red flags [5]. [1] state that inside threats cause so many challenges in securing organisations cyber space.

Detecting insider threats poses a unique challenge for organizations, as the activity may appear normal and can blend in with legitimate operations [6]. Traditional security measures like firewalls and intrusion detection systems are less effective against insider threats, which require advanced behavioral monitoring and data analytics to detect anomalies. Additionally, maintaining a balance between security and employee privacy adds to the complexity of insider threat management [7].

The impact of insider threats on organizations can be severe, leading to financial loss, reputational damage, and regulatory penalties. For instance, an insider attack involving sensitive data theft may expose an organization to significant liabilities, including lawsuits and regulatory fines [8]. Insider threats are especially prevalent in industries dealing with highly sensitive data, such as financial institutions, healthcare providers, and government agencies, where the potential consequences of data breaches are particularly high [9].

[10] highlighted that substantial research has been conducted globally on various strategies to prevent and mitigate insider threats, particularly concerning the leakage of sensitive information. However, in Namibia, studies on insider threats remain scarce. Consequently, this study aimed to identify vulnerabilities within NamPost's organizational structure that could be exploited by insider threats.

This article is organized into the following sections: introduction, methodology, results, analysis, discussion, and conclusion.

2. Methodology

This study employed qualitative research methods to gather narrative and visual data, aiming to gain in-depth insight into the vulnerabilities and risk factors within NamPost's organizational structure that contribute to insider cybersecurity threats. A qualitative research approach was selected as it allows for the exploration of complex phenomena through rich, detailed data. This approach was deemed suitable for understanding insider threats, a nuanced issue requiring insights into

organizational dynamics, employee behavior, and systemic vulnerabilities.

The target population for this study consisted of staff members within NamPost's ICT department, based in Windhoek. The study focused on this specific population due to their direct involvement with organizational cybersecurity systems and protocols. The sample size was determined using the principle of data saturation, defined as the point at which no new information or themes emerge from the data [11]. Data saturation ensures the comprehensiveness and reliability of qualitative findings. For this study, saturation was achieved with a sample size of 10 participants.

Data was collected through face-to-face, semi-structured interviews, each lasting approximately 15 to 20 minutes. This method was chosen for its flexibility and ability to elicit detailed responses while allowing the researcher to probe further into specific areas of interest. An interview guide was used to ensure consistency across interviews while allowing room for participants to share their experiences and insights. The study adhered to ethical research practices, including obtaining informed consent from all participants. Confidentiality was maintained throughout, and participants were assured that their responses would be used solely for research purposes.

3. Prepare Your Paper before Styling

The participants were asked to describe any specific technological or procedural vulnerabilities that they have identified within NamPost that could be exploited by insiders.

Here are the responses from the participants.

> "When employees are under high stress or dissatisfied with their jobs, they may become more susceptible to engaging in malicious activities or negligence, driven by feelings of frustration or disengagement. This negative emotional state can erode their commitment to organizational policies and ethical standards, making them more likely to bypass security protocols or seek personal gain through unauthorized access to sensitive data".
>
> "High stress and job dissatisfaction can exacerbate the risks associated with insider cyber-attacks by influencing employees' cultural behavior and decision-making. When employees are under significant stress or unhappy in their roles, they may become more prone to engaging in risky or malicious behavior as a coping mechanism or due to a sense of resentment".
>
> "High stress and job dissatisfaction can profoundly affect employee performance and relationships within an organization. When employees experience significant stress or dissatisfaction, their performance often suffers due to decreased motivation, focus, and productivity. They may struggle with meeting deadlines, producing high-quality work, or maintaining the efficiency required for their roles".
>
> "My views on the relationship between performance and cultural or behavioral factors at NamPost are that employees generally perceive a significant rela-

tionship between performance, interpersonal relationships, and cultural or behavioral factors when it comes to insider cyberattacks. I recognize that a positive work environment, characterized by strong relationships and a supportive culture, can enhance overall performance and reduce the likelihood of insider threats".

"When access controls are inadequate, unauthorized individuals may gain entry to confidential information, leading to potential data breaches or misuse of sensitive resources. This lack of control can result in various threats, including data theft, unauthorized alterations, and disruptions to operational processes. Additionally, insufficient access controls can undermine compliance with regulatory requirements, exposing NamPost to legal penalties and reputational damage. The risk is further amplified if insiders exploit these weaknesses for personal gain or malicious purposes".

"The risks of Insider cyber-attack that I know of Insufficient access controls expose an organization to several risks, including unauthorized data access, data breaches, and system vulnerabilities".

"When access controls are weak, unauthorized users, whether external hackers or internal employees, may exploit these gaps to gain access to sensitive data and systems. This lack of control can be exacerbated by technological vulnerabilities, such as outdated software or unpatched systems, which can be easily exploited to facilitate unauthorized access or data breaches".

"In my opinion, firstly, clear and well-communicated policies and procedures help employees understand their role in maintaining cybersecurity, which can foster a culture of vigilance and responsibility. By involving employees in the development process and actively seeking their feedback, organizations can address potential concerns and tailor strategies to fit the actual work environment, making them more practical and effective".

"Employees feel that they are not valued. Some employees feel that regular training and awareness programs engage them, keeping them informed about emerging threats and best practices for preventing insider attacks. When employees feel valued and included in the security process, they are more likely to cooperate and adhere to security measures, enhancing overall organizational defense".

"I would say it's both good and bad; on the positive side, effective development of these strategies fosters a culture of security awareness and responsibility among employees, which is crucial for preventing insider threats. Engaged employees are more likely to adhere to security policies, participate in training, and report suspicious activities, thus enhancing the organization's overall security posture".

4. Analysis of Findings

The findings reveal critical themes related to technological and procedural vulnerabilities at NamPost, emphasizing insider threats, cultural and behavioural factors,

access control issues, and the role of organizational strategies in cybersecurity. Below is the thematic analysis based on the participants' responses.

4.1. Stress and Job Dissatisfaction as Drivers of Insider Threats

Stress and job dissatisfaction have been identified as critical factors contributing to insider threats. According to [12], both stress and lack of satisfaction can serve as precursors to insider crimes, with stressed employees more likely to engage in behaviors that compromise organizational security. Emerging approaches, such as stress recognition through keystroke dynamics, offer non-invasive methods for detecting potential insider threats [13]. Furthermore, environmental factors, such as improper ambient temperatures, have been shown to induce stress, thereby increasing the risk of insider threats among both blue- and white-collar workers [14].

To mitigate these risks, organizations should adopt strategies that prioritize positive reinforcement. As suggested by [15], fostering perceived organizational support and promoting a sense of justice through positive incentives can effectively complement traditional negative deterrents. Key measures include enhancing job engagement, cultivating a sense of connectedness among coworkers, and demonstrating organizational support, all of which align employee interests with those of the organization [15]. Moreover, implementing a psychosocial model to assess employee behavior and identify individuals at risk can serve as an effective tool for insider threat prevention [12].

Key Considerations

- **Emotional State:** Chronic stress and job dissatisfaction can lead to frustration and disengagement, undermining employees' commitment to ethical standards and security policies.
- **Behavioral Risks:** Employees under stress may exhibit risky or malicious behaviors, often such as coping mechanisms or expressions of resentment, further exacerbating organizational vulnerabilities.
- **Performance Impact:** Job dissatisfaction can erode productivity, impair focus, and hinder adherence to deadlines, indirectly contributing to security lapses and operational inefficiencies.

A stressed and dissatisfied workforce represents a significant vulnerability, as emotional and behavioral issues can compromise employees' ability to adhere to security protocols and contribute effectively to organizational objectives. Addressing these challenges through proactive stress management, employee engagement, and organizational support is crucial for reducing the risk of insider threats and fostering a secure and productive work environment [1].

4.2. Cultural and Behavioral Influences on Security Practices

Cultural differences play a significant role in moderating relationships within behavioral models for protective information technologies. As highlighted by [16], this underscores the critical need for culturally-tailored security policies and practices to address the diversity of organizational environments. Recognizing the pivotal

role of human factors in cybersecurity, researchers have increasingly examined the interplay of culture, behavior, and social media usage to assess individuals' susceptibility to cybercrime. Such insights are instrumental in designing more effective information security awareness training programs [17].

To mitigate insider threats and foster a robust cybersecurity culture, organizations should consider the following measures.

- **Work Environment:** Cultivating a supportive workplace culture that emphasizes strong interpersonal relationships enhances employee performance and reduces the likelihood of insider threats. A collaborative and trust-driven environment can significantly decrease malicious or negligent behavior.
- **Engagement and Inclusion:** Actively involving employees in the development and implementation of cybersecurity strategies fosters a sense of ownership and cooperation. When employees feel valued and included, they are more likely to adhere to security protocols and contribute positively to organizational security.
- **Responsibility Culture:** Encouraging a culture of vigilance and accountability is essential for promoting adherence to security measures. Employees who are trained to recognize and report suspicious activities can act as the first line of defense against potential threats.

The integration of positive cultural and behavioral factors into organizational practices enhances overall security by reducing risks associated with insider threats. Therefore, prioritizing cultural alignment and employee engagement within cybersecurity frameworks is not only a strategic necessity but also a practical approach to safeguarding organizational assets.

4.3. Technological and Procedural Weaknesses

Technological factors frequently complicate adherence to cybersecurity policies due to the operational burden they place on employees. As noted by [18], the practical demands of security systems—such as the continuous stream of software updates, multifactor authentication, and password management protocols—can overwhelm employees, leading to fatigue and decreased compliance. Furthermore, technological and procedural controls alone are often insufficient in preventing data theft and other malicious actions by insiders [19]. The increasing reliance on interconnected systems and cyberspace further amplifies organizational vulnerabilities to insider threats, as highlighted by [20].

Key Vulnerabilities

- **Access Control Gaps:** Inadequate access controls enable unauthorized individuals to access sensitive information, resulting in potential breaches, misuse of resources, and compromised confidentiality.
- **Outdated Systems:** Unpatched software and outdated IT systems exacerbate vulnerabilities, creating exploitable gaps that both internal and external actors can leverage.
- **Regulatory Compliance Risks**: Weak technological controls can lead to non-

compliance with regulatory standards, exposing organizations to significant reputational and financial penalties.

To mitigate these risks, organizations must prioritize the strengthening of access control mechanisms and ensure that systems and software are regularly updated and patched. Proactive measures such as role-based access controls (RBAC), timely software updates, and robust compliance monitoring are essential for minimizing exploitation opportunities, enhancing cybersecurity resilience, and maintaining adherence to legal and regulatory requirements.

4.4. Importance of Training, Awareness, and Policies

According to [18], employees often struggle with the growing complexity of cybersecurity requirements, particularly in organizations that lack sufficient training and engagement initiatives. The authors emphasize that to enhance the implementation of cybersecurity policies, organizations must prioritize continuous and practical training programs for employees across all departments. Such initiatives are critical for fostering compliance and raising awareness of cybersecurity risks [18].

To mitigate insider threats effectively, organizations should consider the following strategies.

- **Employee Training:** Regular and targeted training programs keep employees informed about emerging cybersecurity threats and equip them with best practices to handle potential risks.
- **Policy Clarity:** Clearly communicating cybersecurity policies ensures that employees understand their roles and responsibilities, thereby fostering a culture of vigilance and accountability.
- **Employee Value Perception:** Employees who feel valued and included in the cybersecurity process are more likely to demonstrate cooperation and commitment to adhering to security measures.

Engaging employees in security awareness initiatives and involving them in strategy development enhances policy adherence and strengthens the organization's overall security posture. A workforce that is well-informed, valued, and actively engaged becomes a key asset in mitigating insider threats and safeguarding organizational assets.

5. Discussions

Research highlights the critical impact of employee well-being on organizational security. High stress and dissatisfaction correlate with increased risks of insider threats, as employees may engage in malicious activities out of frustration or disengagement. [21] suggests that job dissatisfaction can erode commitment to security policies and ethical standards, making employees more susceptible to insider attacks. Similarly, [22] emphasizes that stress can impair decision-making, leading to negligence or risky behavior that compromises security.

A positive work environment and supportive culture can significantly reduce

the risk of insider threats. [23] found that organizations with strong interpersonal relationships and a culture of mutual trust are less likely to experience insider-related incidents. Furthermore, [24] stresses that fostering a sense of responsibility and vigilance among employees enhances adherence to security protocols and proactive threat reporting, thereby strengthening organizational defense mechanisms.

The literature underscores the importance of robust access controls and updated systems in mitigating cybersecurity risks. Weak access management is a critical vulnerability that can be exploited by insiders and external attackers alike [4]. Additionally, outdated software and unpatched systems exacerbate these risks, as highlighted by [25], who argue that maintaining updated technological infrastructure is key to preventing unauthorized access and ensuring compliance with regulatory standards.

Employee training and clear communication of security policies are pivotal in mitigating insider threats. [26] suggest that regular training programs enhance employees' ability to recognize and respond to emerging threats. Moreover, engaging employees in developing and implementing cybersecurity strategies fosters a sense of inclusion and cooperation, reducing the likelihood of non-compliance [8]. Employees who feel valued and informed are more likely to adhere to security measures, as supported by [27], who advocate for inclusive and participatory approaches in organizational cybersecurity initiatives.

6. Conclusions

Insider threats present a critical challenge to NamPost, as they exploit vulnerabilities inherent in organizational structures, employee behavior, and technological systems. The findings of this study highlight the interconnectedness of stress, job dissatisfaction, insufficient access controls, and a lack of training in amplifying the risks of insider threats.

To mitigate insider threats, NamPost should foster a supportive workplace environment to address employee stress and dissatisfaction, enhance engagement, and reduce potential risks. Strengthening access control mechanisms, such as multi-factor authentication and role-based access policies, is essential to restrict unauthorized access to sensitive information. Regular cybersecurity awareness training, incorporating simulated insider threat scenarios, can empower employees to recognize and prevent malicious activities. Additionally, NamPost should implement advanced monitoring tools, such as behavioral analytics, to detect anomalous activities and conduct regular system audits to identify and address vulnerabilities. Clear cybersecurity policies, coupled with confidential reporting channels for suspected threats, will further promote a culture of vigilance and responsibility, ensuring enhanced organizational resilience.

Conflicts of Interest

The authors declare no conflicts of interest.

References

[1] Cappelli, D.M., Moore, A.P. and Trzeciak, R.F. (2020) The CERT Guide to Insider Threats: How to Prevent, Detect, and Respond to Information Technology Crimes. 2nd Edition, Addison-Wesley Professional.

[2] Nassir, N.F.M., Rauf, U.F.A., Zainol, Z. and Ghani, K.A. (2024). Revealing the Multi-Perspective Factors Behind Insider Threats in Cybersecurity. *Journal of Media and Information Warfare*, **17**, 65-82.

[3] Homoliak, I., Toffalini, F., Guarnizo, J., Elovici, Y. and Ochoa, M. (2019) Insight into Insiders and It. *ACM Computing Surveys*, **52**, 1-40. https://doi.org/10.1145/3303771

[4] Greitzer, F.L., Strozer, J.R., Cohen, S.L., Moore, A.P., Mundie, D. and Cowley, J. (2019) Analysis of Internal and External Threat Awareness in Organizational Cybersecurity. *Cybersecurity Studies Quarterly*, **11**, 118-135.

[5] Liu, X. and Cheng, T. (2020) Factors Contributing to the Insider Threat. *Journal of Organizational Security*, **12**, 179-198.

[6] Mills, D., Zaffar, F. and Parveen, T. (2021) Challenges in Detecting Insider Threats. *Cybersecurity Challenges Journal*, **6**, 120-134.

[7] Pfleeger, S.L. and Caputo, D.D. (2020) Insider Threats: Mitigation Strategies and Lessons Learned. *Computer Security Review*, **19**, 223-238.

[8] Chang, W. and Yeh, M. (2019) The Financial Impact of Data Breaches and Cyberattacks. *Financial Management Journal*, **45**, 102-118.

[9] Inayat, U., Farzan, M., Mahmood, S., Zia, M.F., Hussain, S. and Pallonetto, F. (2024) Insider Threat Mitigation: Systematic Literature Review. *Ain Shams Engineering Journal*, **15**, Article 103068. https://doi.org/10.1016/j.asej.2024.103068

[10] Kim, A., Oh, J., Ryu, J. and Lee, K. (2020) A Review of Insider Threat Detection Approaches with IoT Perspective. *IEEE Access*, **8**, 78847-78867. https://doi.org/10.1109/access.2020.2990195

[11] Naeem, M., Ozuem, W., Howell, K. and Ranfagni, S. (2024) Demystification and Actualisation of Data Saturation in Qualitative Research through Thematic Analysis. *International Journal of Qualitative Methods*, **23**, Article 16094069241229777. https://doi.org/10.1177/16094069241229777

[12] Greitzer, F.L., Kangas, L.J., Noonan, C.F., Dalton, A.C. and Hohimer, R.E. (2012) Identifying At-Risk Employees: Modeling Psychosocial Precursors of Potential Insider Threats. 2012 45*th Hawaii International Conference on System Sciences*, Maui, 4-7 January 2012, 2392-2401. https://doi.org/10.1109/hicss.2012.309

[13] Sultanov, A.B. and Kogos, K. (2020) Insider Threat Detection Based on Stress Recognition Using Keystroke Dynamics.

[14] Sergiu, E. (2020) Insider Threats and Thermal Stress in the Working Environment. *Scientific Bulletin of Naval Academy*, **24**, 271-276. https://doi.org/10.21279/1454-864x-20-i1-038

[15] Moore, A.P., Perl, S.J., Cowley, J., Collins, M.L., Cassidy, T.M., VanHoudnos, N. and Rousseau, D.M. (2016) The Critical Role of Positive Incentives for Reducing Insider Threats. SEI Technical Report CMU/SEI-2016-TR-014.

[16] Dinev, T., Goo, J., Hu, Q. and Nam, K. (2009) User Behaviour Towards Protective Information Technologies: The Role of National Cultural Differences. *Information Systems Journal*, **19**, 391-412. https://doi.org/10.1111/j.1365-2575.2007.00289.x

[17] Collier, H., Morton, C., Alharthi, D. and Kleiner, J. (2023) Cultural Influences on Information Security. *European Conference on Cyber Warfare and Security*, **22**, 143-

150. https://doi.org/10.34190/eccws.22.1.1127

[18] Waiganjo, I., Osakwe, J. and Azeta, A. (2024) Impediments to Cybersecurity Policy Implementation in Organisations: Case Study of Windhoek, Namibia. *International Journal of Research and Scientific Innovation*, **11**, 540-546. https://doi.org/10.51244/ijrsi.2024.1110046

[19] McCormick, M. (2008) Data Theft: A Prototypical Insider Threat. In: *Advances in Information Security*, Springer, 53-68. https://doi.org/10.1007/978-0-387-77322-3_4

[20] Warkentin, M. and Willison, R. (2009) Behavioral and Policy Issues in Information Systems Security: The Insider Threat. *European Journal of Information Systems*, **18**, 101-105. https://doi.org/10.1057/ejis.2009.12

[21] Shaw, T., Chen, C., Harris, A. and Huang, H. (2018) Examining the Antecedents of Insider Threats on Organizations: The Impact of Job Satisfaction, Stress, and Organizational Commitment. *Information & Computer Security*, **26**, 1-16. https://doi.org/10.1108/ICS-03-2017-0013

[22] Whitty, M.T. (2015) Mass-Marketing Fraud: A Growing Concern. *IEEE Security & Privacy*, **13**, 84-87. https://doi.org/10.1109/msp.2015.85

[23] Mourad, A., Soeanu, A., Laverdière, M. and Debbabi, M. (2009) New Aspect-Oriented Constructs for Security Hardening Concerns. *Computers & Security*, **28**, 341-358. https://doi.org/10.1016/j.cose.2009.02.003

[24] D'Arcy, J. and Greene, G. (2014) Security Culture and the Employment Relationship as Drivers of Employees' Security Compliance. *Information Management & Computer Security*, **22**, 474-489. https://doi.org/10.1108/imcs-08-2013-0057

[25] Ahmed, M., Pathan, A.-S.K. and Ullah, S. (2020) Security Challenges in Modern Cyber Systems. Springer.

[26] Parsons, K., McCormac, A., Pattinson, M., Butavicius, M. and Jerram, C. (2014) A Study of Information Security Awareness in Australian Government Organizations. *Information Management & Computer Security*, **22**, 334-345. https://doi.org/10.1108/imcs-10-2013-0078

[27] Ngoqo, B. and Flowerday, S. (2015) Employee Perceptions of Insider Threats to Information Security: A Case Study. *South African Journal of Information Management*, **17**, 1-9. https://doi.org/10.4102/sajim.v17i1.632