Insider Threats in the Digital Age:

Safeguarding Your Business from Within

October 2024

25th Edition

RMG®

Table of Contents

1. Introduction

As information flows more freely every day in a world where digitisation is occurring at an exponential rate, the threat landscape has evolved dramatically. Insider threats have become a significant concern for local and global entities. The stakes are high for JSE-listed companies where consequences of a security breach may be magnified due to governance expectations, but for smaller enterprises, the risk of insider threats may pose an existential threat to the longevity of the business.

Insider threats can be either malicious or negligent, but either way, they carry a significant threat to any business. With the digital transformations and entrenchment in remote and hybrid working conditions, the need to safeguard sensitive and confidential information becomes ever more pressing.

2. Categories of Insider Threats

These insidious insider threats are particularly dangerous as they arise from within the organisation and fall into two main categories: malicious and negligent insiders.

MALICIOUS INSIDERS

are individuals within an organisation who intentionally exploit their access to sensitive information for personal gain, to harm the business, or to assist external entities, such as cybercriminals, competitive companies, or terror groups. This includes disgruntled employees leaking confidential data or collaborating with external threats to damage the organisation.

NEGLIGENT INSIDERS

are employees or contractors who unintentionally cause harm through carelessness or ignorance, such as mishandling data, clicking phishing links, or ignoring security protocols. While their actions aren't malicious, the damage they cause can be just as severe.

3. The Impact on South African Businesses

Insider threats represent significant challenges for South African businesses, especially those listed on the Johannesburg Stock Exchange (JSE). These insider threats can lead to financial losses, a decline in shareholder value, and legal or regulatory penalties from oversight bodies like the Financial Sector Conduct Authority (FSCA), making them both a financial and compliance concern.

Larger companies may have the advantage of dedicated cybersecurity teams and advanced detection systems to manage these risks, but smaller enterprises are particularly vulnerable. With limited budgets and personnel, SMEs are not always able to recover from a major insider incident, which may put the business in a state of existential flux.

4. Categories of Insider Threats

4.1 The Rise of Remote Work

The COVID-19 pandemic has fundamentally altered the work environment, making remote work a standard practice rather than an exception. While this model offers flexibility and other advantages, it also introduces significant vulnerabilities that previously did not exist. Employees working from home frequently rely on personal devices to access corporate networks, increasing the risk of data breaches. Furthermore, the lack of direct supervision can foster a lax attitude towards security protocols. To address these challenges, South African companies—both large and small—must implement stringent remote work policies. This includes requiring secure, company-approved devices, enforcing VPN usage to protect connections, and providing continuous training to keep employees alert to evolving cybersecurity threats.

4.2 Increased Access to Sensitive Information

As businesses digitise, employees gain access to more sensitive information, increasing the risk of insider threats. To manage this, companies must enforce the **principle of least privilege (PoLP)**, limiting access to only what is necessary for specific roles. Regular audits are essential to ensure only authorised personnel handle critical data, reducing the chance of misuse or breaches.

4.3 Sophistication of Insider Attacks

Insider threats are dynamic and evolve alongside advancements in security measures, becoming more sophisticated as some insiders employ advanced tactics to evade detection. In certain instances, insiders may collaborate with external hackers, complicating the threat

landscape further. To combat these challenges, businesses must proactively update their detection and prevention strategies, utilising advanced monitoring tools that leverage artificial intelligence and machine learning to identify anomalies in user behaviour. Such tools enable organisations to detect potential threats before they inflict substantial damage.

5. Implementing Robust Internal Controls

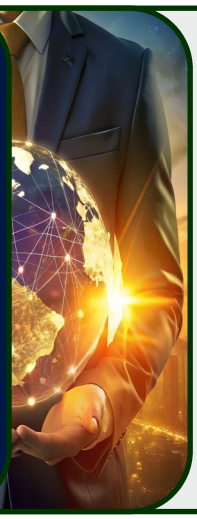
ACCESS MANAGEMENT

Effective access management is vital for mitigating insider threats. By enforcing the principle of least privilege (PoLP), businesses can limit access to sensitive information, ensuring employees only see what is necessary for their roles. Regularly reviewing and updating access controls is essential, especially when employees change roles or leave the company, to prevent any potential misuse.

MONITORING AND DETECTION SYSTEMS

Robust monitoring and detection systems are crucial for spotting unusual behaviour that may signal insider threats. In South Africa, tools like User and Entity Behaviour Analytics (UEBA) can analyse user patterns using machine learning, helping identify deviations that suggest malicious activity. Implementing these systems provides real-time insights, enabling quick responses to potential threats and minimising damage.

EMPLOYEE TRAINING AND AWARENESS



Even the best security systems rely on user effectiveness. Regular training on cybersecurity best practices empowers employees to recognise and respond to threats. For JSE-listed companies, this training should be integrated into a broader governance and compliance framework, ensuring all staff, from executives to entry-level employees, understand the significance of cybersecurity in protecting against insider threats.

6. Case Studies: Lessons from South African Companies

6.1 JSE-Listed Companies

Case Study 1:

A prominent JSE-listed financial services firm encountered an insider threat when a disgruntled employee attempted to leak sensitive client information. Fortunately, the company's robust insider threat programme, which included access management, monitoring systems, and employee training, enabled early detection of the threat, preventing significant harm. This incident highlights the necessity of a comprehensive approach to insider threat management.

Case Study 2:

In the retail sector, another JSE-listed company faced an insider threat when an employee inadvertently exposed customer data by mishandling a phishing email. While unintentional, this incident underscored the need for ongoing employee training and awareness. In response, the company enhanced its training initiatives and implemented stricter email security protocols.

6.2 Small to Medium Enterprises (SMEs)

Case Study 3:

A small South African tech start-up experienced an insider threat when a former employee attempted to steal proprietary code to launch a competing business. Lacking a comprehensive insider threat programme due to limited resources, the company later recognised the need to protect its intellectual property and invested in access management and monitoring systems. This case illustrates the vulnerability of SMEs and the importance of affordable security solutions.

Case Study 4:

A medium-sized manufacturing company encountered an insider threat when an employee accidentally exposed sensitive supplier information due to a lack of awareness. Acknowledging the importance of cybersecurity, the company implemented a targeted training programme focused on data handling and security best practices. This proactive measure helped prevent further incidents and emphasised the value of employee education.

7. Regulatory Considerations

South African businesses must navigate a complex regulatory landscape to effectively safeguard against insider threats, with the Protection of Personal Information Act (POPIA) being a critical piece of legislation governing the processing of personal data. JSE-listed companies face additional obligations related to governance and risk management, with insider threat management being a key component that ensures they fulfil their responsibilities to shareholders, regulators, and stakeholders. Non-compliance can lead to severe penalties, reputational risks, and diminished investor confidence. Therefore, these companies must develop comprehensive insider threat programmes that not only meet regulatory standards but also incorporate best practices in cybersecurity.

8. Best Practices for Mitigating Insider Threats

Developing a Comprehensive Insider Threat Programme

To effectively mitigate insider threats, South African businesses should create a comprehensive insider threat programme tailored to their unique needs. This programme should encompass several key components:

Risk Assessment	Conduct thorough assessments to identify potential insider threats and vulnerabilities within the organisation.
Policy Development	Establish clear policies and procedures for managing insider threats, including access management, monitoring, and response protocols.
Incident Response Planning	Develop a detailed incident response plan outlining the steps to take in the event of an insider threat, including communication strategies, legal considerations, and post-incident analysis.

Regular Audits	Conduct periodic audits of the insider threat programme to evaluate its effectiveness and identify areas for improvement.
Inter-Departmental Collaboration	Effective insider threat management necessitates collaboration between IT and HR departments. HR can offer valuable insights into employee behaviour and potential risks, while IT implements the technical controls needed to mitigate these threats.

9. Conclusion

Insider threats pose a significant risk to businesses of all sizes in South Africa. Whether driven by malicious intent or simple negligence, the potential damage from an insider threat can be severe. By implementing robust internal controls, monitoring systems, and employee training programmes, businesses can protect themselves against these threats and ensure their long-term security and success.

10. Bibliography

1. **Geldenhuys, P.** (2020). "Understanding Insider Threats in South Africa." *South African Journal of Information Management*, 22(1), 10-19.
2. **PwC South Africa**. (2022). "The Rise of the Insider Threat: How to Protect Your Organisation." Available at: www.pwc.co.za.
3. **FSCA**. (2023). "Governance and Compliance Frameworks for JSE-Listed Companies." Available at: www.fsca.co.za.
4. **Pillay, S.** (2021). "Data Protection and POPIA Compliance in South Africa." *Journal of Legal Studies*, 15(2), 87-105.
5. **Deloitte South Africa**. (2023). "Insider Threats: Current Trends and Challenges." Available at: www.deloitte.co.za.
6. **Van Zyl, L.** (2022). "Cybersecurity in the Age of Remote Work: A South African Perspective." *Information & Computer Security*, 30(3), 201-216.
7. **KPMG South Africa**. (2023). "Mitigating Insider Threats: Best Practices for South African Businesses." Available at: www.kpmg.co.za.
8. **Popov, V.** (2022). "User and Entity Behaviour Analytics (UEBA): The Future of Insider Threat Detection." *Cybersecurity Today*, 14(4), 55-66.
9. **South African Law Review**. (2022). "Regulatory Requirements for JSE-Listed Companies: Insider Threat Management." *SA Law Review*, 28(6), 112-123.