South African Journal of Information Management
ISSN: (Online) 1560-683X, (Print) 2078-1865

Cloud leakage in higher education in South Africa: A case of University of Technology

Authors:
Tshepiso Ntloedibe[1]
Thato Foko[1]
Mmatshuene A. Segooa[1]

Affiliation:
[1]Department of Informatics, Faculty of Information & Communication Technology, Tshwane University of Technology, Tshwane, South Africa

Corresponding author:
Tshepiso Ntloedibe,
ntloedibet@tut.ac.za

Dates:
Received: 12 Oct. 2023
Accepted: 11 Dec. 2023
Published: 16 Feb. 2024

How to cite this article:
Ntloedibe, T., Foko, T. & Segooa, M.A., 2024, 'Cloud leakage in higher education in South Africa: A case of University of Technology', *South African Journal of Information Management* 26(1), a1783. https://doi.org/10.4102/sajim.v26i1.1783

Background: Users with knowledge of an organisation can pose risks to Cloud Computing, including current and past employees and external stakeholders with access to the organisation's cloud. These insiders may engage in intentional or unintentional disruptive behaviors, causing significant harm to the organisation. A study focused on insider threats in South African higher education examined the tactics used by cybersecurity leaders to enforce cybersecurity policies.

Objectives: The goal of this study was to develop a comprehensive insider mitigation framework for cloud leakage in a South African University.

Method: The study employed qualitative methodologies and a case study approach. Open-ended interviews were conducted to collect data from the participants. The collected data was coded and analysed using ATLAS.ti 22.

Results: The study's findings revealed that some of the major sources of cloud leakage are a lack of effective training, ineffective information security (IS) policy regulation, and the implementation of information security awareness workshops that provided advice on how information security should be managed in the university.

Conclusion: Insider threats pose a serious risk to organisations. To mitigate this threat, it is crucial for organisations to establish strong security policies and closely monitor employee activities. By conducting a thorough assessment of insider threats, organisations can enhance their understanding of this dynamic threat and strengthen their defenses.

Contribution: Although every employee is ultimately responsible for an organisation's security, the most effective IS programmes demonstrate strong top-level leadership by setting a 'tone at the top' and promoting the benefits of IS through careful policy and guidance.

Keywords: cloud computing; data leakage; insider threat; information security; information systems security policies.

Introduction

When businesses opt to migrate their data to the Cloud, many people think that the duty for data security is transferred to the Cloud provider, and this idea appears to be plausible. After all, putting sensitive information onto a third-party system gives up some control over the information security (IS) (ISACA 2020). Users of information systems frequently engage in risky behaviour that jeopardises confidentiality, integrity and availability (CIA) by revealing sensitive information. Insider threats account for a significant portion of security breaches that happen in companies. These are individuals who engage in any malevolent behaviour that results in harm, either as users or as staff members (Singh et al. 2023)

Because of the increasing use of technologies over the past few decades, concerns about security and privacy have grown significantly. Enterprises possess confidential resources (like customer data, business blueprints, intellectual property, etc.) that could potentially cause significant damage to their operations and reputation in the case of a breach. Thus, in order to protect the confidentiality, availability and integrity of their sensitive assets, it is imperative that all businesses take precautions against insider threats (Alsowail & Al-Shehari 2022). Insider threats are considered to be one of the largest security risks that businesses, institutions and governmental bodies face, according to both the scientific community and security experts (Georgiadou, Mouzakitis & Askounis 2021). Organisations are forced to deal with a variety of internal and external cyber risks as a result of an environment where cyber threats are becoming more

complicated. A significant percentage of IS issues in organisations are caused by human factor exploitation. Put another way, most security incidents – which include both intentional and unintentional misbehaviours, are caused, directly or indirectly, by human error (Khando, Gao & Salman 2021). Organisations all over the world invest a lot in technology defences against IS (Li & Liu 2021). However, organisations frequently fall short in protecting their information assets because they rely primarily on technical solutions such as IPS/IDS – Intrusion Protection Systems/ Intrusion Detection Systems, Firewalls and NSM – Network Security Monitoring tools that are insufficient and not contextually appropriate. In actuality, a sizable portion of organisational IS problems is attributable to the misuse of human elements, which either directly or indirectly results in the majority of security incidents (Khando et al. 2021). With this in mind, the study adopted the Theory of Planned Behaviour (TPB) and Protective Motive Theory (PMT) as a foundation to design a framework to lessen Cloud insider risks in a South African university, focussing on the human or insider element. The following research questions were addressed in the study:

- What are the organisational proactive controls that aid in developing a mature security posture?
- What is the university's level of analysing behaviour to make more intelligent access decisions?
- How does the university effectively monitor critical assets?
- How does the privilege users handle the university's sensitive data?

The TPB (Ajzen 1991) and the PMT (Rogers 1983), two pertinent theories, were combined to improve our understanding of privileged users' compliance with IS in higher education.

All of the variables were taken from the PMT. It was possible to determine three variables using the TPB, namely subjective norms, attitude towards compliance, and self-efficacy. According to Ajzen's (1991) TPB, three paradigms – behavioural, normative and control – are responsible for shaping human behaviour. The behavioural beliefs take into account the results of the behaviour and assess these results to decide which behaviour to choose. Normative beliefs, also known as subjective norms, propose that a person will successfully complete a task if they have a positive relationship with the higher authority at work. Conversely, control beliefs are associated with variables that either enhance or lessen the performance of the actions' outcome. The combination of these behavioural paradigms results in behavioural intention to act, which in turn leads to actual action or behaviour. Behavioural beliefs, normative beliefs and control beliefs collectively realise positive or negative attitudes towards an action. According to this theory, behavioural intention is both an immediate antecedent of behaviour and a mediating factor between behavioural factors and actual behaviour. According to this study, the TPB is pertinent as it clarifies why employees intend to follow Information Systems Security Policies (ISSPs).

The fundamental goal of PMT, according to Zuwita and Rahmatullah (2021), is to encourage people to take adaptive actions in response to environmental risks by first assessing their perceived risk vulnerability and then taking into account their ability to respond effectively and independently. During the threat assessment process, the user must determine the perceived severity of the threat and whether he believes he is vulnerable to it (perceived vulnerability). In the coping appraisal process, the user evaluates whether taking a protective action will protect him from the threat (response efficacy), whether he can carry out the protective action (self-efficacy) and whether the perceived cost of taking the action is worth it (perceived cost). Generally speaking, adaptive intentions or behaviours were aided by increases in threat severity, threat vulnerability, response efficacy and self-efficacy. Conversely, an increase in adaptive intentions or behaviours was observed when maladaptive response rewards and adaptive response costs decreased. This resulted in a conclusion that PMT components might be helpful for individual and community interventions, regardless of whether the measures were based on intentions or behaviours. As per PMT, once an insider obtains security threat information, they can assess the security through the threat appraisal process. The cost of carrying out the advised behaviour is known as the 'coping appraisal' or prevention cost (Zuwita & Rahmatullah 2021).

Literature review

Data leakage is a major problem in the contemporary business environment as it must be protected against privilege misuse. Research on data security breaches in both the public and private domains demonstrates the significance of the human element. A Verizon report states that 74% of all breaches involve human involvement, with individuals becoming involved through error, privilege abuse, the use of credentials that have been stolen or social engineering (Mikuletič et al. 2023). The unintentional or deliberate release of confidential organisational information to unapproved parties is known as data leakage (Khan et al. 2021). It is critical to guard against unauthorised users misusing the critical data (Gupta & Singh 2019). Information about patents and intellectual property rights (Protection of Personal Information Act (POPI Act) – POPIA), which lays out the procedures and guidelines that must be followed when processing data about human beings and people with legal status and functionality, are all examples of critical data (Ulven & Wangen 2021).

This important organisational information has frequently been distributed to stakeholders outside the boundaries of the company. As a result, it is challenging to find the person responsible for the data leak (Cheng, Liu & Yao 2017).

Role of privileged users in the security of cloud computing

The security architecture of an organisation is greatly threatened by insiders as they are aware of its security procedures and have permission to access its resources

(Al & Happa 2018). Insider threats may occur unintentionally (non-malicious) or maliciously (intentional). Privilege accounts can be used for applications, patches, configuration changes, user management and log file retrieval. Certain accounts can only be accessed locally, but others might be available across the entire organisation. Below are a few examples of privileged accounts with system and security features at institutions of higher learning:

- Local administration. Non-personal accounts that provide administrative access to work with workstations, networks, databases and platforms (including one's own).
- Accounts for privileged users, who have the authority to manage an enterprise network, a system or multiple systems.
- All workstations and servers within the domain have administrative access through domain administrative accounts (Active Directory).

Access to administrative computing resources, facilities and data is typically available to managers and administrative staff throughout the Tshwane University of Technology. Privileged users are those who have multiple accounts, such as database and system administrators and supervisors.

According to Elifoglu, Abel and Tasseven (2018), the privileged user is expected to operate in the organisation's best interests. Certain user accounts are necessary for the proper operation of computer operating systems and business applications. More permissions are granted to privilege accounts; administrator accounts are typical examples, but other accounts with higher levels are also included. Moreover, these elevated user accounts possess nearly limitless entry to every computer system. Therefore, once these credentials are compromised, it can be easy to compromise the most valuable assets of a company, including social media accounts, databases and unstructured data. Highly sensitive company data is also accessible to anyone with access to these computer accounts (Walker 2019). Non-malicious insider threat behaviours include careless acts like inadvertently giving important information to the wrong people or putting private information in communications that are not secure. Non-malicious insider threats frequently include phishing vulnerabilities, IS policy violations (such as failing to change passwords on a regular basis) and resistance to cybersecurity procedures and training (Harms et al. 2022).

Impact of insider threats in organisations

Cybersecurity needs to be a top priority because educational institutions now face special security challenges not seen in other industries, according to Pinheiro (2020). Furthermore, maintaining the system security from cyberattacks is a very challenging task because these institutions have a large and complex network with a large number of switches, routers and single users. Information Technology (IT) departments need to address these risk areas and identify strategies for reducing threats. For instance, thousands of people may use a university. A high vulnerability to attack results from these users potentially accessing the system via outdated, less secure hardware, like a computer or smartphone, which might not have the features needed to install the most recent software updates in order to stay protected.

Chin (2023) reports that educational institutions are frequently targeted by hackers and cybercriminals. The retail, healthcare, financial and education sectors are among those that are frequently the focus of cyberattacks. According to Check Point's Mid-Year Report, there were 44% more cyberattacks in the education sector in 2022 than the year before. On average, there were 2300 reports of attacks against educational organisations every week. The education sector is an ideal target for cyberattacks because of a confluence of significant vulnerabilities, widespread vulnerabilities and valuable data, making these figures, although conservative by some estimates, concerning.

Singar and Akhilesh (2019) state that for the past 20 years, cybersecurity has been a hotly debated topic in academia, business and government. A key component of many higher education establishments is the Internet. In today's cutting-edge educational setting, online resources are essential. In order to accommodate the needs of today's diverse student body, the higher education sector has been heavily reliant on information systems and technology, both for in-person instruction and online learning platforms. Higher education institutions are subject to risks that affect their information and data security because of an abundance of connected devices and increased use of the Internet. These risks are known as cyber threats.

Insider threats in the South African context

Pieterse (2021) claims that research reports and peer-reviewed scholarly articles around the world have comprehensive documentation of cyber incidents. Nonetheless, official reporting of cyber incidents is uncommon in South Africa, even though the number of incidents is steadily rising. Resources and statistics specific to local cyber incidents are not provided by the National Prosecuting Authority (NPA) or the South African Police Service (SAPS). The National Computer Security Incident Response Team (CSIRT) of South Africa, known as the Cybersecurity Hub, offers a mechanism for stakeholders to report cyber incidents; however, it does not notify the public about these incidents. Moreover, there are not many peer-reviewed studies that have assessed cyber incidents in South Africa. The examination of 12 South African cyber incidents that happened between 1994 and 2015 is one noteworthy exception.

Research method and design

This study was conducted using a case study research approach. The targeted population for the study was professionals (information and communication technology [ICT] managers, systems developer, network administrators) within a division of ICT in a university of technology with

legitimate access to computer systems, networks and data and information resources. A sample of five participants was purposefully selected and all five were interviewed (One manager from data centre, One network administrator, One support engineer, (One Director-ICT services and One HOD-IS & ICT policy); non-probability sampling was relevant for this study. The researcher's preference for sample selection is taken into account when using non-probability sampling techniques. The researcher's access to the study sample is the main source of this sampling technique (Obilor 2023). Non-probability sampling adopts a more sympathetic attitude than probability sampling.

Semi-structured interviews were used in this study as an instrument for gathering data to perform thematic analysis on the factors deterring privileged user from cybersecurity insider threats and ultimately their intention to reduce insider threats in an organisation. Data were collected using open-ended questions. In the interview guide, identities will not be given, and when reporting, the researcher will refer to participants as respondents. A copy of the completed thesis will be sent to each section that participated in order to provide feedback, and another copy will be given to the department's head's office so that all staff members have access to it. The library at Tshwane University of Technology will also make the thesis copy electronically accessible.

Analysis of data collected from the main case study interviews was evaluated through ATLAS.ti Scientific Software Development GmbH (2023) ATLAS.ti Mac (Version 23.2.1) [Computer program]. Available at: https://atlasti.com (Downloaded: 27 July 2023) (ATLAS. ti 22). According to Fox and Bayat (2013), data analysis for qualitative research can be carried out either manually or with the aid of suitable computer programmes. Using data-analysis tools (ATLAS. ti 22) that allowed the researcher to record the data, organise the data and give codes to the data, the researcher processed and analysed the qualitative data that were gathered.

Ethical considerations

Ethical clearance to conduct this study was obtained from the Tshwane University of Technology Information and Communication Technology Faculty Committee for Research Ethics, before the case study was conducted (ref. no. FCRE/ICT/2021/03/004). Ethical clearance was approved unconditionally on 21 February 2022. The ethical guidelines, as outlined in the approval protocol by the Ethics Committee, were followed throughout the data collection process.

Results

Presentation of results based on the responses that informed the themes from the interviews conducted.

The interviews took place over the phone and via Microsoft Teams for virtual communication. With the respondents permission, I recorded the interviews, and afterward I had them transcribed. For the purpose of data analysis, I made notes during the interviews. My analysis of the material was aided by the review process in identifying important themes, components and patterns that are important to consider when considering insider mitigation framework enforcement tactics. Five research participants were interviewed in semi-structured interviews to provide the data. Ten main themes were found through thematic analysis: Cloud benefits, security policy awareness, risk mitigation techniques, IS risks, information systems security policies, information systems security policy enforcement, information protection framework, IS culture, CIA and incident response plan.

Information security risks

From the interview results, various IS risks in the system were identified as major contributors to Cloud leakage. These include a violation of privacy policies, lack of knowledge of the processes, migration to the Cloud, inadequate maintenance, security-policy compliance, security issues relating to third parties, poor access management, employee negligence, lack of knowledge of where the university data reside, among others. These results demonstrated that the organisation was exposed to several internal and external threats because of poor IT security management. It is clear that data leaks and the exposure of private information are a few examples of internal threats. Although several technology solutions for IS have been created and others are being worked on, most organisations still face significant challenges in this area (Grant et al. 2014).

Information systems security policies

The participants' feedback on whether the university policy follows the international organisation standardisation indicated the following:

- There were sufficient safeguards in place to ensure IS, including organisational structures, software and hardware features, policies, regulations, procedures and operations. These results demonstrated that the organisation was exposed to several internal and external threats because of poor IT security management. It is clear that data leaks and the exposure of private information are a few examples of internal threats. Although several technology solutions for IS have been created and others are being worked on, most organisations still face significant challenges in this area (Grant et al. 2014).

Information systems security policy enforcement

The participants' feedback on the reasons for updating the security policy is that these reasons are because of:

- new technologies coming out, new risks, technology changes and working condition changes,
- evolution in IT space and new security threats,
- employee compliance, to enhance security measures and to look at best practices.

Information protection framework

From the interview results, participants indicated knowledge and existence of an information protection framework. It is the responsibility of the university to:

- indicate the availability of the policy and technological framework to guarantee that the relevant users have adequate access to technology resources,
- implement the framework through awareness of knowing the implications,
- implement regular trainings for everyone, especially the privilege user and ICT personnel,
- improve the university firewall.

Information security culture

From the interview results, it was clear that participants have an idea of the current security culture. The university indicated its responsibilities to:

- expand or improve end-user awareness,
- conduct regular security workshops and trainings,
- communicate the security policies and the values that determine how people are expected to think about and approach security in the organisation,
- delegate someone to champion the security culture processes,
- ensure that the system is patched,

These results point to the inefficiency of the present security culture. The International Organization for Standardization's IS management system (ISO/IEC 27001:2022) includes processes and activities related to IS awareness (Kitsios, Chatzidimitriou, & Kamariotou, 2023).

Risk-mitigation strategies

The participants indicated webmail as the only strategy for mitigating IS risks, and this is not an effective strategy. It is the university's responsibility to:

- conduct IS workshops,
- plan and execute IS campaigns,
- implementation of a disaster-management committee to perform risk assessment,
- delegate a risk champion.

These findings show that the university does not have a sufficient risk-mitigation strategy.

Security policy awareness

The participants' feedback on whether the university updates the privileged user on the latest IS policies is:

- that the institution communicates the most recent security regulations using webmail, an email service accessible via a regular web browser.

These results clearly show that the university's plan is ineffective. Security policy must act as the cornerstone for IS strategy, design and implementation in order to meet the three requirements of CIA.

Benefits of cloud to the university

It is the responsibility of the university to:

- ensure that the university avoids over-purchasing servers and storage by dynamically increasing processing capacity,
- improve adaptation to variations in workload,
- gain control over data stored on Cloud,
- have less in-house infrastructure.

From these results, it is clear that the university wants to improve Cloud infrastructure through having less in-house infrastructure and increase computing capacity to prevent over-purchasing servers and storage. Web applications have very dynamic workloads generated by a fluctuating number of users and therefore experience unanticipated peaks. As a result, dynamic resource allocation is required not only to avoid degraded application performance but also to avoid underutilised resources. The ability to adjust an application's resource allocation based on changing demand over time in order to satisfy the quality of service (QoS) standards is a key selling factor of Cloud Computing (Farokhi 2015).

Confidentiality, integrity and availability

From the interview results, participants indicated the importance of CIA triad security model that was considered an important concept within IS. The participants' feedback on the current CIA triad model was:

- Identity and access management, also known as (IAM), make ensuring that only the appropriate individuals and job functions inside an organisation have access to the resources they need to do their duties. The institution can control staff applications using identity management and access systems rather than logging in as an administrator to each application. Not every user has access to everything, you get access to certain services based on your role
- When employees have access to confidential information, such as trade secrets, proprietary procedures, customer information and lists, marketing methods and any other significant or sensitive information, the institution commonly employs non-disclosure agreements (NDAs).
- Through indemnities on the university website and enforcing authentication process (strong passwords)

Based on these findings, there is an indication that institutions of higher learning are attempting to strengthen their present CIA triad security approach in response to the university's reaction. Multi-factor authentication (MFA) fortifies each of these three security pillars. It is a secure authentication technique that requires more than one authentication mechanism chosen from various categories of credentials. Similar to single-factor authentication, MFA is gaining popularity as a means of confirming users' identities when they access online resources. Access control is the process of giving a resource privacy, and single-factor authentication is no longer a dependable way to offer strong security against unauthorised access. As a result,

research into innovative MFA techniques that combine two or more authentication factors – inherence, possession and knowledge – is growing significantly (Aleluya & Vicente 2018).

Incident response plan

The interview results suggest that participants have knowledge of the current incident response plan.

The participants' feedback on how the university responds to incidents was:

- There are enough controls (depends on the assets being protected, the possibility of an attack and the resources available to the organisation trying to safeguard its assets) in place in the institution to maintain IS, including organisational structures, software and hardware features, rules, regulations, processes, procedures and CSIRT-incident response tools and technologies such as IPS and IDS. More so, the university responds to incidents through the Tertiary Education and Research Network of South African (TENET).
- That the end user reports incidents to the IS officer and via helpdesk.

Discussion of results

Security governance and compliance

Governance of IS is essential for all enterprises. There is growing interest in the topic as a result of IT systems' fundamental usefulness and the variety of hazards they face (Moghadam 2018). Protecting an organisation's operations requires IS. To maintain the organisation's value and reputation, the institution should secure its data and assets. Furthermore, top-tier IS management demands that policies and procedures be implemented with the backing and commitment of management (Shahim 2020). Threat assessment and coping appraisal are the two main ways that PMT explains that people can be encouraged to adopt adaptive, protective behaviours (Hina, Selvam & Lowry 2019). Basically, threat appraisal is determining how serious a threat (like a potentially dangerous security breach incident) is and how likely it is to happen. It is therefore made up of two crucial components: perceived vulnerability and perceived severity. With regard to the potential damage caused by an ISP's noncompliance, for example, the former evaluates the extent or seriousness of the threat's consequences.

Security risk management

Risk management offers an approach for extending risk management guidelines into a framework for managing the resilience of critical infrastructure (Kure, Islam & Mouratidis 2022). In order to reduce risk given a limited amount of resources to implement control measures, risk management aims to build the right mix of security controls (for instance, rules, processes and technology). Risk management is in direct alignment with the TPB framework, which serves as the study's conceptual framework. Communication is consistent with the mindset surrounding the TPB behaviour construct. Put another way, security risk management is consistent with the TPB's 'attitude towards behaviour' construct, which is why the TPB framework supports the communication theme. According to Omoyiola (2020), having a positive attitude towards cybersecurity policies is associated with a good intention to adhere to them. Theoretically, employee behavioural intentions are influenced by communications. Leaders in cybersecurity update security policies and send emails informing staff members of these changes. Executives in cybersecurity employ similar tactics, like holding cybersecurity workshops, to communicate security risk management. According to Reeves, Delfabbro and Calic (2021), cybersecurity leaders employ cybersecurity help desks as a means of communication and prompt resolution of cybersecurity incidents.

Security compliance

Information leakage has grown to be a major IS concern in the era of Industry 4.0 (IR 4.0) (Saura, Ribeiro-Soriano & Palacios-Marqués 2021). Implementing an information security policy (ISP) that outlines the demands, limitations and responsibilities of IT users inside an organisation is the key strategy for addressing the vulnerabilities posed by information leakage. Protecting the accessibility, discretion and integrity of an organisation's information and technological resources is the aim of IS. Therefore, IS compliance is the observance of standards or laws for the protection of data and information. It was discovered that ISSP compliance behaviour intention was significantly positively impacted by the two components of subjective norms and attitude towards compliance from TPB. These findings suggest that the attitudes of employees towards ISSP compliance in their organisations and the opinions of their coworkers are critical factors in motivating ISSP behaviour intentions. Employee adoption of the ISSP of their organisation is more likely if they possess the necessary competence and capability to implement preventative security measures and take IS precautions. This is confirmed by the results pertaining to the third component of TPB, namely self-efficacy, which is also present when one completes coping appraisals in PMT.

Awareness and training

To protect their information systems and assets from security risks, organisations employ a variety of tactics. Nonetheless, many experts advise implementing a Security Education, Training, and Awareness (SETA) programme as part of the organisation's overall IS/cyber security strategy as it is one of the most well-known tactics for reducing IS threats and safeguarding information assets (Alyami et al. 2023). Additionally, the TPB, the research's conceptual framework and the theme of security awareness and training are directly aligned. Because security awareness is consistent with the attitude-toward-behaviour construct of TPB, the TPB framework supports the security awareness and training theme. To sum up, the TPB's attitude-toward-behaviour construct promotes security awareness and instruction. The

theory states that actual behavioural control and intentions (INT) to carry out the behaviour are what ultimately determine behaviour. The impact of intentions on behaviour is mitigated by the behavioural control. Because an individual has the ability to control their behaviour, their intention will ultimately dictate how they behave (Aigbefo, Blount & Marrone 2020). Our attitudes towards particular issues are also altered by different training techniques. Knowledge of IS has an impact on behaviour as well as attitude. According to Hassandoust and Techatassanasoontorn (2020), general deterrence theories place a strong emphasis on the idea of command and control, whereas PMT primarily concentrates on persuading people to take preventative action and explain defensive actions. When it comes to situations where users need extra encouragement to safeguard their information assets, PMT can be used to better understand users' IS awareness and intentions.

User access management

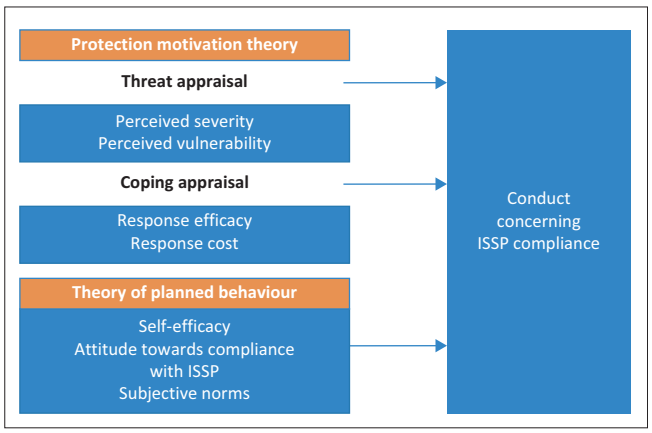
Emerging technologies are used in the identity management process to manage user identification data and to restrict access to business resources. The main objectives of an identity management system are to enhance security, boost productivity and reduce expenses related to processing user credentials and attributes. Identity systems oversee policy management, central administration, inspections, user self-service and delegated administration in addition to user authentication and authorisation (Adenola 2023).

The study's findings support the primary purpose of developing an insider mitigation framework (see Figure 2) for Cloud leakage in a South African University. Figure 1 depicts a framework based on the study's findings.

Discussion of the main elements of insider threats

Governance and oversight

One of the most important factors in safeguarding an organisation's operations is IS. To maintain their worth and reputation, organisations need to safeguard their data and



ISSP, information systems security policy.

FIGURE 1: Illustrates of the research model.

resources. Moreover, commitment and support of senior management are necessary for efficient IS management when it comes to putting policies and procedures into place (AlGhamdi, Win & Vlahu-Gjorgievska 2020). The duties and procedures that executive management performs in the area of security governance are intended to provide strategic direction, guarantee that goals are met, ensure that risks are properly managed and confirm that the enterprise's resources are being used responsibly. A lot of companies are being proactive in making sure that the goals they have for the business are directly supported by the security controls they invest in. A key component of this strategy is an organisation-wide perspective on security risks that integrates IT and physical security. Organisations can gain a competitive edge in the global economy by integrating an integrated approach to logical and physical security with superior security governance and risk management. This allows for better protection of digital, physical and human assets as well as an optimised IT infrastructure (Shahim 2020).

In order to protect sensitive data and reduce cybersecurity risks inside of enterprises, IS governance is essential. To protect information assets, it includes the strategic planning, execution and supervision of security measures. A reciprocity resource states that several essential elements are necessary for efficient IS governance. Organisations must first and foremost set up a precise framework for IS governance. The organisation's policies, practices and guidelines governing IS are outlined in this framework. It offers a road map for putting security controls in place, controlling risks and guaranteeing adherence to pertinent laws and guidelines (Squirrel 2023). According to Squirrel (2023), the identification and evaluation of risks are a crucial component of IS governance. To find possible weak points and threats to the organisation's information assets, this entails performing routine risk assessments. Organisations can effectively allocate resources to address the most critical areas and prioritise security efforts by having a clear understanding of the risks.

In addition, the governance of IS mandates the implementation of strong controls and safeguards for data assets. This involves putting in place technical safeguards like intrusion detection systems, firewalls and encryption techniques. Defining user privileges, access controls, and authentication procedures is also necessary to guarantee that sensitive data is only accessed by those who are authorised.

Continuous monitoring and reporting

According to Gowsika (2023), continuous security monitoring (CSM) continuously examines systems to look for deviations from security norms, vulnerabilities, indications of a possible data breach and insufficient security measures or incorrect configurations using intrusion detection systems. After that, it compiles information about the results and reports them.

When your organisation uses automation to continuously monitor your IT systems and networks, it is known as CSM.

In essence, you require real-time reports on the security of your system. This aids in the identification of security risks, the measurement of decreases in control-efficiency and the isolation of situations in which your internal organisational rules are broken. The primary goal is to identify and address any potential issues or threats as they arise. The following continuous monitoring solutions provide up-to-date information about the security status of your business:

- Monitor every system in use by your company, including those that your vendors utilise.
- Keeping abreast of potential dangers and continuing sly actions.
- Assembling, linking and interpreting all of the data about security.
- Verifying the effectiveness of your security measures.
- Informing everyone in your company about the current state of security.
- Managing risks by means of meticulous organisational oversight.
- Combining risk management and IS frameworks for a strong defence.

Incident response and recovery

Cyberattacks are unavoidable from an organisational standpoint for a variety of reasons. The inability of organisations to fully detect potential security flaws in their systems and to fully eliminate the human element – the weakest link in the cyber security framework – is one of the main causes. Therefore, in order to minimise the impact that cyberattacks have on their businesses, they must implement both corrective and preventive measures to deal with the threat. Using an incident methodology can assist an organisation in putting cyberattack management strategies into practice and minimising the possible impact on their customers, intellectual property and business processes. Reducing potential damage from cybercrime incidents and accelerating recovery from such incidents are the goals of incident management frameworks (Shinde & Kulkarni 2021). Incidents involving IS and privacy are growing more common. According to the CyberEdge Group 2021 Cyber threat Defence Report, 2021 'saw the largest increase in successful attacks within the last six years'. Furthermore, as per CyberEdge (2021), cybersecurity experts have realised that the question now is not if their organisation will be harmed by a data breach but rather when it will occur. Because of this, it is highly crucial than ever to teach incident response teams how to identify, manage and address cybersecurity incidents. It is imperative for organisations to conduct a thorough assessment of cybersecurity threats and attack vectors, comprehend the significance of incident response plans, evaluate response activities, carry out table top exercises, analyse the results to identify areas for improvement, oversee reporting and perform incident response plan (IRP) maintenance.

According to Shinde and Kulkarni (2021), assuring business continuity and an organisation's overall productivity requires

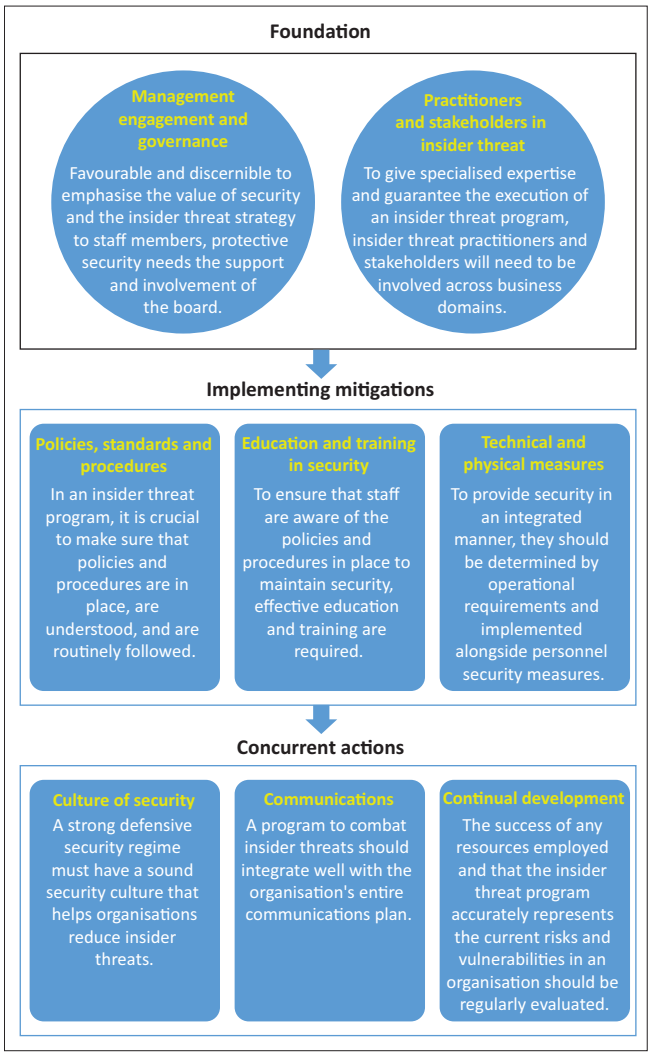


FIGURE 2: An insider mitigation framework.

effective incident management. For incident management, there are several methods. Given the unavoidability of IS risks, an organisation can identify problems and systematically address them by implementing an incident management process at a reasonable cost. Different strategies have different restrictions. Objectives and goals within the organisation also vary, though not significantly. It follows that organisations need a customised framework.

The research questions that led this study, as well as feedback from the participants, assisted in developing the framework for discussion. This framework was built on the following themes:

- Leadership and governance
- Insider risk assessment
- Ongoing personnel security
- Monitoring and assessment of employees
- Security culture and behaviour change

The limitation and future work

This study has potential methodological limitations because of its approach to employ case study, which limit the research to generalising findings of the insider security threats to

organisation's data leakage. As the study focussed on one institution and every organisation has its own IS settings, this allows the risk of bias as the researchers' personal opinions and preferences may have influenced the research. Another limitation was the data collection instrument, the use of semistructured interviews. When the discourse is not flexible during semi-structured interviews, little grasp of the issue typically kills the conversation. On the negative side, having a large number of non-responders may result in population underrepresentation, which must be investigated (Denzin 2017). It has also been demonstrated that certain candidates may reply less to 'obvious' issues or ones that the interviewees are too embarrassed to discuss (Nguyen 2015).

One of the study's strengths was the use of qualitative research approach. It has the recognition that data must always be understood in relation to the context of their production. The analytical approach taken should be described in detail and theoretically justified in light of the research question (Murphy 2010).

Implications of the study

Despite the fact that insider threats are becoming more prevalent, there has been little research on how organisations can decide whether their data security measures and insider threat mitigation practices are appropriate or most effective in the context of their operations. Researchers can expand on this study to investigate insider threats using other case studies. The study suggests conceptualisation for future research that combines PMT and TPB in the context of employees' ISSP behavioural intention. To that end, this research further suggests that combining the two theoretical frameworks improves comprehension of the kinds of variables that influence employees' ISSP behavioural compliance compared with when each is utilised separately to investigate the theme.

This study sampled the population from a higher education institution within the IT department. However, because of the nature of insider threats to Cloud Security and the unusual aspect of protecting valuable information resources at a South African university of technology, researchers in future should consider to expand their sample to cover the broader demographics of institutions beyond the higher education sector using other sampling techniques.

Conclusion

The purpose of this research was to investigate and clarify the reasons why employees in a South African university of technology are more likely to engage in Cloud leakages. The study examined elements from the TPB and PMT theories that affect an individual's reduction of intentions to break security rules for Cloud data and, as a result, diminish insider threats in this situation. The TPB is a hypothesis that helps predict and comprehend behaviour. According to this theory, attitudes toward a behaviour, subjective norms and the perception of behavioural control all play a role in determining behavioural intentions, which in turn shape behavioural actions. An insider mitigation framework has therefore been presented, which demonstrates how to lessen insider threats in organisations, based on the empirical evidence gathered from this study.

According to the findings of this study, managers should pay a closer attention to the reasons that induce privileged users to engage in Cloud leaking misbehaviour. Although every employee is ultimately responsible for an organisation's security, the most effective IS programmes demonstrate strong top-level leadership by setting a 'tone at the top' and promoting the benefits of IS through careful policy and guidance.

Acknowledgements

Competing interests

The authors declare that they have no financial or personal relationship(s) that may have inappropriately influenced them in writing this article.

Authors' contributions

T.N. was the research leader and was involved in designing the research questions, methodology used, literature review, data collection, codification and analysis and writing of the manuscript. T.F. was the research supervisor and M.A.S., the co-supervisor. They guided the researcher T.N. in designing the research questions, methodology, literature review, data collection, data analysis and discussion of findings.

Funding information

This research received no specific grant from any funding agency in the public, commercial or not-for-profit sectors.

Data availability

The data are not publicly available due to containing information that could compromise the privacy of the research participants.

Disclaimer

The views and opinions expressed in this article are those of the authors and are the product of professional research. It does not necessarily reflect the official policy or position of any affiliated institution, funder, agency, or that of the publisher. The authors are responsible for this article's results, findings, and content.

References

Adenola, V., 2023, 'Artificial intelligence based access management system', Doctoral dissertation, East Carolina University.

Aigbefo, Q.A., Blount, Y. & Marrone, M., 2020, 'The influence of hardiness and habit on security behaviour intention', *Behaviour & Information Technology* 41(6), 1151–1170. https://doi.org/10.1080/0144929x.2020.1856928

Ajzen, I., 1991, 'The theory of planned behavior', *Organizational Behavior and Human Decision Processes* 50(2), 179–211. https://doi.org/10.1016/0749-5978(91)90020-T

Al, K. & Happa, J., 2018, 'Insider-threat detection using Gaussian', *Computers & Security* 77, 838–859. https://doi.org/10.1016/j.cose.2018.03.006

Aleluya, E.R.M. & Vicente, C.T., 2018, 'Faceture ID: Face and hand gesture multi-factor authentication using deep learning', *Procedia Computer Science* 135, 147–154. https://doi.org/10.1016/j.procs.2018.08.160

AlGhamdi, S., Win, K.T. & Vlahu-Gjorgievska, E., 2020, 'Information security governance challenges and critical success factors: Systematic review', *Computers & Security* 99, 102030. https://doi.org/10.1016/j.cose.2020.102030

Alsowail, R.A. & Al-Shehari, T., 2022, 'Techniques and countermeasures for preventing insider threats', *PeerJ Computer Science* 8, e938. https://doi.org/10.7717/peerj-cs.938

Alyami, A., Sammon, D., Neville, K. & Mahony, C., 2023, 'The critical success factors for Security Education, Training and Awareness (SETA) program effectiveness: A lifecycle model', *Information Technology & People* 36(8), 94–125. https://doi.org/10.1108/ITP-07-2022-0515

Amankwa, E., Loock, M. & Kritzinger, E., 2018, 'Establishing information security policy compliance culture in organizations', *Information & Computer Security* 26(4), 420–436.

Chandarman, R., 2016, 'Cybersecurity awareness of students at a private higher education institute in South Africa', Master's dissertation, University of KwaZulu-Natal.

Cheng, L., Liu, F. & Yao, D., 2017, 'Enterprise data breach: Causes, challenges, prevention, and future directions', *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery* 7, e1211. https://doi.org/10.1002/widm.1211

Chin, K., 2023, *Why is the education sector a target for cyber attacks?* UpGuard, www.upguard.com, viewed 08 December 2023, from https://www.upguard.com/blog/education-sector-cyber-attacks.

CyberEdge Group, 2021 *Cyberthreat defense report, USA, 2021*, viewed 08 December 2023, from https://resources.perimeterx.com/c/2021-cyber-threat-defense-report?x=OxBXZ2.

Denzin, N.K., 2017, *The research act: A theoretical introduction to sociological methods*, Routledge, New York, NY.

Elifoglu, I.H., Abel, I. & Tasseven, O., 2018, 'Minimizing insider threat risk with behavioral monitoring', *Review of Business* 38(2), 61–73.

Farokhi, S., 2015, 'Quality of service control mechanisms in cloud computing environments', Doctoral dissertation, Wien.

Fox, W. & Bayat, M.S., 2013, *A guide to managing research*, Juta & Co., Cape Town.

Georgiadou, A., Mouzakitis, S. & Askounis, D., 2021, 'Detecting insider threat via a cyber-security culture framework', *Journal of Computer Information Systems* 62(4), 1–11. https://doi.org/10.1080/08874417.2021.1903367

Gowsika, 2023, *What is continuous security monitoring?* CSM, Sprinto, viewed 06 December 2023, from https://sprinto.com/blog/continuous-security-monitoring/.

Grant, K., Edgar, D., Sukumar, A. & Meyer, M., 2014, '"Risky business": Perceptions of e-business risk by UK small and medium sized enterprises (SMEs)', *International Journal of Information Management* 34(2), 99–122. https://doi.org/10.1016/j.ijinfomgt.2013.11.001

Gupta, I. & Singh, A., 2019, 'A confidentiality preserving data leaker detection model for secure sharing of cloud data using integrated techniques', in *2019 7th International Conference on Smart Computing & Communications (ICSCC)*, pp. 1–5, Sarawak, June 28.

Harms, P.D., Marbut, A., Johnston, A.C., Lester, P. & Fezzey, T., 2022, 'Exposing the darkness within: A review of dark personality traits, models, and measures and their relationship to insider threats', *Journal of Information Security and Applications* 71, 103378. https://doi.org/10.1016/j.jisa.2022.103378

Hassandoust, F. & Techatassanasoontorn, A.A., 2020, 'Understanding users' information security awareness and intentions: A full nomology of protection motivation theory', in V. Benson & J. Mcalaney (eds.), *Cyber influence and cognitive threats*, pp. 129–143, Elsevier Inc., London.

Herath, T. & Rao, H.R., 2009, 'Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness', *Decision Support Systems* 47(2), 154–165.

Hina, S., Selvam, D.D.D.P. & Lowry, P.B., 2019, 'Institutional governance and protection motivation: Theoretical insights into shaping employees' security compliance behavior in higher education institutions in the developing world', *Computers & Security* 87, 101594. https://doi.org/10.1016/j.cose.2019.101594

Homoliak, I., Toffalini, F., Guarnizo, J., Elovici, Y. & Ocha, M., 2017, 'Insight into insiders and IT: A survey of insider threat taxonomies, analysis, modeling, and countermeasures', *Journal for Applied Mathematics and Computer Science* 52(2), 1–40. https://doi.org/10.1016/j.im.2020.103392

ISACA, 2022, *Cybersecurity incident response exercise guidance*, viewed 06 December 2023, from https://www.isaca.org/resources/isaca-journal/issues/2022/volume-1/cybersecurity-incident-response-exercise-guidance#1.

Khan, F., Kim, J., Mathiassen, L. & Moore, R., 2021, 'Data breach management: An integrated risk model', *Information & Management* 58(1), 103392. https://doi.org/10.1016/j.im.2020.103392

Khando, K., Gao, S. & Salman, A., 2021, 'Enhancing employees information security awareness in private and public organisations: A systematic literature review', *Computers & Security* 106, 102267. https://doi.org/10.1016/j.cose.2021.102267

Kitsios, F., Chatzidimitriou, E. & Kamariotou, M., 2023, 'The ISO/IEC 27001 Information Security Management Standard: How to Extract Value from Data in the IT Sector', *Sustainability* 15(7), 5828. https://doi.org/10.3390/su15075828

Kure, H.I., Islam, S. & Mouratidis, H., 2022, 'An integrated cyber security risk management framework and risk predication for the critical infrastructure protection', *Neural Computing and Applications* 34(18), 15241–15271. https://doi.org/10.1007/s00521-022-06959-2

Li, Y. & Liu, Q., 2021, 'A comprehensive review study of cyber-attacks and cyber security: Emerging trends and recent developments', *Energy Reports* 7, 8176–8186. https://doi.org/10.1016/j.egyr.2021.08.126

Mikuletič, S., Vrhovec, S., Skela-Savič, B. & Žvanut, B., 2024, 'Security and privacy oriented information security culture (ISC): Explaining unauthorized access to healthcare data by nursing employees', *Computers & Security* 136, 103489.

Moghadam, R.S. & Colomo-Palacios, R., 2018, 'Information security governance in big data environments: A systematic mapping', *Procedia computer science* 138, 401–408. https://doi.org/10.1016/j.procs.2018.10.057

Murphy, E., Dingwall, R., Greatbatch, D., Parker, S. & Watson, P., 1998, 'Qualitative research methods in health technology assessment: a review of the literature', *Health technology assessment* 2(16) iii–ix, 1–274.

Nguyen, T.Q.T., 2015, 'Conducting semi-structured interviews with the Vietnamese', *Qualitative Research Journal* 15(1), 35–46.

Obilor, E.I., 2023, *Convenience and purposive sampling techniques: Are they the same?*, viewed n.d., from https://seahipaj.org/journals-ci/mar-2023/IJISSER/full/IJISSER-M-1-2023.pdf.

Omoyiola, B.O., 2020. *Exploring strategies for enforcing cybersecurity policies*. Minneapolis, Walden University, Minnesota.

Pieterse, H. 2021, 'The Cyber Threat Landscape in South Africa: A 10-Year Review', *The African Journal of Information and Communication* 28, 1–21. doi:https://doi.org/10.23962/10539/32213

Pinheiro, J., 2020, 'Review of cyber threats on educational institutions', in *Proceedings of the digital privacy and security conference*, p. 43, Universidade Lusófona do Porto, Porto.

Pol, R., Thakur, V., Bhise, R. & Kat, A., 2012, 'Data leakage detection', *International Journal of Engineering Research & Application* 2(3), 404–410.

Reeves, A., Delfabbro, P. & Calic, D., 2021, 'Encouraging employee engagement with cybersecurity: How to tackle cyber fatigue', *SAGE Open* 11(1), 21582440211000049.

Rogers, R., 1983, 'Cognitive and physiological processes in fear-based attitude change: a revised theory of protection motivation', In J. Cacioppo & R. Petty (eds), *Social Psychophysiology: A Sourcebook*, pp 153–176, Guilford Press, New York, NY.

Saura, J.R., Ribeiro-Soriano, D. & Palacios-Marqués, D., 2021, Evaluating security and privacy issues of social networks based information systems in Industry 4.0', *Enterprise Information Systems* 16(10–11), 1694–1710.

Shahim, A. and Schinagl, S., 2020. What do we know about information security governance? "From the basement to the boardroom": towards digital security governance. Information & Computer Security, 28(2), pp.261–292.

Shinde, N. & Kulkarni, P., 2021, 'Cyber incident response and planning: A flexible approach', *Computer Fraud & Security* 2021(1), 14–19.

Singar, A.V. & Akhilesh, K.B., 2020, 'Role of Cyber-security in Higher Education', In K. Akhilesh & D. Möller (eds.), *Smart Technologies*, Springer, Singapore. https://doi.org/10.1007/978-981-13-7139-4_19

Singh, M., Mehtre, B.M., Sangeetha, S. & Govindaraju, V., 2023, 'User behaviour based insider threat detection using a hybrid learning approach', *Journal of Ambient Intelligence and Humanized Computing* 14, 4573–4593. https://doi.org/10.1007/s12652-023-04581-1

Squirrel, S., 2023, *What is information security governance in cybersecurity?*, Kiteworks | Your Private Content Network, viewed 05 December 2023, from https://www.kiteworks.com/cybersecurity-risk-management/security-governance-in-cybersecurity/.

Ulven, J.B. & Wangen, G., 2021, 'A systematic review of cybersecurity risks in higher education', *Future Internet* 13(2), 39.

Walker, P., 2019, 'Why do PAM projects fail?', *Network Security* 2019(9), 15–18.

Yin, R.K., 2003, *Case study research, design and methods*, Sage, Newbury Park, CA.

Zuwita, R.M. & Rahmatullah, B., 2021, 'Relationship between PMT appraisals and Security Practice: Analysis of prevention of insider threat in organization success factor', *Ilkogretim Online* 20(4), 1118–1126.