Peertechz

ENGINEERING GROUP

Trends in
Computer Science and Information Technology
OPEN ACCESS JOURNAL

ISSN: 2641-3086 Journal DOI: https://dx.doi.org/10.17352/tcsit

Literature Review

Malicious Insider Threat to Data Security: Mitigation Strategy for municipalities

Shandukani Tshilidzi Thenga* and S Arunmozhi Selvi

British University College, 4524 Turnberry Street, South Africa

Received: 01 December, 2025
Accepted: 16 December, 2025
Published: 17 December, 2025

***Corresponding author**: Shandukani Tshilidzi Thenga, British University College, 4524 Turnberry Street, South Africa, E-mail: candythenga@gmail.com

Keywords: Malicious insider threats; Municipal data security; Socio-technical risk management; Governance and policy controls in cybersecurity; Behavioral analytics and UEBA; Defense-in-depth strategy; Privileged Access Management (PAM); Ethical and privacy-aware monitoring; Public sector cyber resilience

https://www.engineegroup.us

Check for updates

Abstract

The municipal governments are the custodians of huge volumes of sensitive information, including personally identifiable information (PII), financial information, law enforcement intelligence, and control of essential infrastructure. Although external cyber-threats are the most discussed, deliberate insider threats, malicious actions of authorised personnel, are an equally serious, but underestimated threat to municipal data security. The paper is a holistic formulation of a mitigation strategy, which is specific to the local government setting. The proposed solution, based on such standard frameworks as the NIST SP 800-53, ISO/IEC 27001, and CERT Insider Threat Model, and incorporating socio-technical and risk management concepts, will build a multi-layered defence. This model is a combination of governance policies, technical controls, behavioural monitoring, and reforms in the organisational culture. It focuses on active prevention, ongoing surveillance, as well as organised incident recovery and response. The paper also covers some very important ethical and legal issues, especially how to strike a balance between the privacy of employees and the required monitoring. A gradual implementation scheme and performance indicators are proposed to guarantee feasible implementation, which is based on municipal budget and regulatory factors. The study finds that insider risk mitigation goes beyond technology, as a complex and culture-entrenched challenge necessitating an overhaul of the municipal operations to instill trust, accountability, and resilience.

Introduction

The municipal governments handle huge quantities of sensitive government information that ensures that the city operations run smoothly. This consists of personal data of citizens, tax and financial data, police databases, and the systems that manage utilities and transportation. This information must also be kept safe to ensure the trust of the population and the legal requirements. Although most individuals are concerned with cyberattacks by external hackers, insider threats posed by individuals within the organisation can also be as deadly as external attacks. These attacks occur when workers or contractors gain access to information through their privileged access and abuse it to steal information, disrupt, or leak information. Local governments are particularly vulnerable since they usually have small budgets, outdated computer systems, and most of them have numerous departments, each sharing data on various networks. Problems in security can also be a challenge when there exist political pressures or excessive competing priorities [1]. One insider attack can be very damaging, such as data loss, service interruption, and destruction of trust in the population.

This paper will outline an insider threat prevention and response strategy in municipal governments. Insider threat mitigation extends beyond technical safeguards and requires the integration of governance structures, organisational culture, and human-centred controls, as technical measures alone are insufficient to address trusted insider misuse [2].

Citation: Thenga ST, Selvi SA. Malicious Insider Threat to Data Security: Mitigation Strategy for municipalities. Trends Comput Sci Inf Technol. 2025;10(3):089-096. Available from: https://dx.doi.org/10.17352/tcsit.000102

Literature review and theoretical framework

Insider threats are among the largest and most ancient issues of cybersecurity, particularly when it concerns city governments that have access to public information, financial systems, and local infrastructures. These threats are perpetrated by individuals who already have access to systems, making them hard to detect. Some insiders have ill motives, whereas others harm unintentionally [3]. Researchers admit that insider threats have to be addressed both technologically and humanly with the combination of technology, behaviour, and leadership [2].

Defining insider threats and context

There are two categories of insider threats: malicious and non-malicious. Bad insiders intentionally steal information, destroy systems, or defraud. Non-malicious insiders are harmful by accident, usually due to neglect. Alsowail and Al-Shehari [2] put forward a model that integrates technology, behaviour, and organisational practices to curb insider threats. They state that tools such as access control or system monitoring cannot exist independently. Powerful recruitment, reference checking, and moral consciousness are also required. This is particularly true in those municipalities that rely on outdated systems and minimal IT personnel.

The challenges are even more in the case of municipal governments, which have limited budgets and numerous departments. Vestad and Yang [4] discovered that the majority of local governments are using cybersecurity plans developed by national or personal agencies without modifying them to local requirements. The consequences of this are usually poor supervision, inadequate access control, and poor detection of insider activities.

Organizational and behavioral dimensions.

Individuals are the key contributors to insider threats. Safa and Abroshan [5] discovered that transparency in leadership, motivation of employees, and a feeling of equity have a significant influence on whether employees become responsible. When employees feel trusted and valued, they are unlikely to damage the organisation. This applies especially in city offices where strict management styles may dishearten Communication and accountability.

Steinmetz [6] further notes that organisations can promote insider advocates, who are employees who promote security, report risks, and develop good behaviour. The concept relates to the Social Exchange Theory, according to which organisations should treat employees fairly and in return, employees give loyalty and sincerity. This concept can be applied by the municipal leaders through promoting fairness, inclusion, and open Communication to minimise the possibility of insider threats.

Technical and procedural frameworks

Technology remains essential in combating insider threats, but it should act with prompt detection and response. According to Savchenko, et al. [7], damage is enhanced by the presence of slow responses. They suggest constant monitoring and automatic notifications so that IT teams can respond more quickly.

Nagel, et al. [8] propose that cities should implement a formal program of insider threats, which matures over time. Their ISACA model is geared towards governance, training, detection, and response. To local governments, it implies a way of incorporating insider threat management in the cybersecurity policy with clear coordination and periodic review.

Municipal data environment and emerging challenges

Municipal cybersecurity has become more complicated due to the new smart city systems. According to Cornelius and Van Rensburg [9], weak authentication, low accountability, and weak data governance contribute to risks. They recommend zero-trust and privacy-by-design practices, whereby no one is trusted. Vestad and Yang [4] also mention that outside contractors are dangerous since they can get extensive access without appropriate control. Cities can address this by revising vendor access regularly and executing more robust contracts.

Synthesis and implications

In general, the research indicates that the security of municipal data involves both human and technical strategies. Alsowail and Al-Shehari [2] emphasise technical controls, Safa and Abroshan [5] emphasise the organisational culture, and Steinmetz [6] also introduces positive engagement among employees. Savchenko, et al. [7] emphasise the necessity of quicker response, whereas Cornelius and Van Rensburg [9] pay attention to risks of smart cities. When they are combined, they demonstrate that the right combination of policy, culture, and technology can assist municipalities in minimising insider threats and ensuring trust by the population.

Nature and impact of intentional insider threats in municipalities

Types and sources of intentional insider threats

Municipal governments are most vulnerable to the insider threats that are intentional since sensitive systems and data are regularly accessed by those who are trusted. IT administrators, finance officers, human resources, and third-party contractors maintaining or overseeing municipal systems are considered to be the prominent members of the list of common sources of malicious activities by insiders [6]. These insiders usually have valid credentials and higher privileges, enabling them to escape perimeter security rules and act unnoticed, at least in the short term.

Besides the permanent workers, municipalities are now increasingly using external vendors and contractors to assist with the specialised IT infrastructure. Such extended insiders often have a similar level of system access as internal employees, but might lack the equivalent number of regular audits, background checks, and behavioural surveillance [9]. Such a broadened insider threat perimeter poses a major threat surface to municipal settings.

Citation: Thenga ST, Selvi SA. Malicious Insider Threat to Data Security: Mitigation Strategy for municipalities. Trends Comput Sci Inf Technol. 2025;10(3):089-096. Available from: https://dx.doi.org/10.17352/tcsit.000102

Nature and motivations of malicious insider behaviour

Premeditated insider threats are usually motivated by factors that can be traced. Theoretical models like the Fraud Triangle (opportunity, pressure, and rationalisation) and the MICE framework (money, ideology, coercion, and ego) are also popular models upon which malicious insiders act [2]. Opportunities in municipal settings can be very common because of the decentralised structure, aging infrastructure, and the lack of coordinated access restrictions between departments.

The factors in organisations contribute to insider risk. Poor budgets, political influence, job insecurity, and poor managerial control can lead to conditions in which the disgruntlement or rationalisation of misconduct may become more prone to occurrence [5]. In combination with these human factors and privileged system access, municipalities become highly vulnerable to purposeful misuse of data and systems.

Impact of insider threats on municipal operations

The effects of willful insider threats in localities are not limited to technical harm. Potentially operational effects are data exfiltration, unauthorized manipulation of records, interference with vital services, and destruction of vital infrastructure systems [7]. Municipally, a significant amount of money could be spent on incident response, system recovery, litigation, and fines.

Nevertheless, reputational damage and the loss of social trust are typically the most unbearable and prolonged effects. Violations of data that includes personally identifiable information (PII), law enforcement data, or systems of service delivery diminish confidence of citizens in local governance, as well as institutional legitimacy [4]. In addition to operational and financial losses, insider incidents can cause reputational damage and loss of trust, which, in particular, is harmful in municipal situations where the legitimacy and accountability are key governance factors [4].

Illustrative case: Insider threat in municipal government

Another case in point that illustrates the seriousness of the issue of insider threats in the municipal setting is the case of Terry Childs, which took place in San Francisco in 2008. Childs, a top network manager, declined to hand over administrative privileges to the FiberWAN network of the city, virtually denying the city officials access to systems serving over sixty departments of the city. The event interfered with the core services and caused huge financial and operational losses.

According to Nagel, et al. [8], the present case revealed significant failures related to the governance, such as excessive concentration of the privileged access mechanism, the absence of role separation, and of sufficient control over high-risk individuals. The attack highlights the vulnerability of the entire municipal infrastructure to a single trusted insider who is poorly managed.

Summary

All in all, the convergence of privileged access, organisational vulnerabilities, and personal motivations leads to intentional insider threats in municipalities. Although outsiders pose more serious cybersecurity risks, insiders may be equally detrimental as they are insiders who are trusted but seriously harm the municipal systems [2]. The damages incurred are not only in terms of the lost data but also in terms of service, financial loss, and loss of confidence in the system, and this is the ultimate purpose of systematic and system outage mitigation efforts (Figure 1).

Risk assessment framework for municipal insider threats

Municipalities need to develop a viable risk assessment model that would help the.m to detect, analyse, and address insider threats in a systematic manner. Since municipal institutions work in an interrelated and data-rich environment, the systematic approach will make sure that both technical and human risk factors are addressed. The following framework is a combination of situational awareness, behavioural analysis, and the modelling of adaptive risks in order to offer a practical and evidence-based methodology for insider risk identification.

Asset identification and situational awareness

The initial process of evaluating insider threats is to map the municipal assets, users, and data flows in order to know how information flows across departments and systems. Chandra, et al. [10] emphasise that situational awareness frameworks assist organisations in visualising user-system and data interaction relationships. At a municipal level, this would entail defining key datasets, like citizen personal records, financial information, and infrastructure control data,

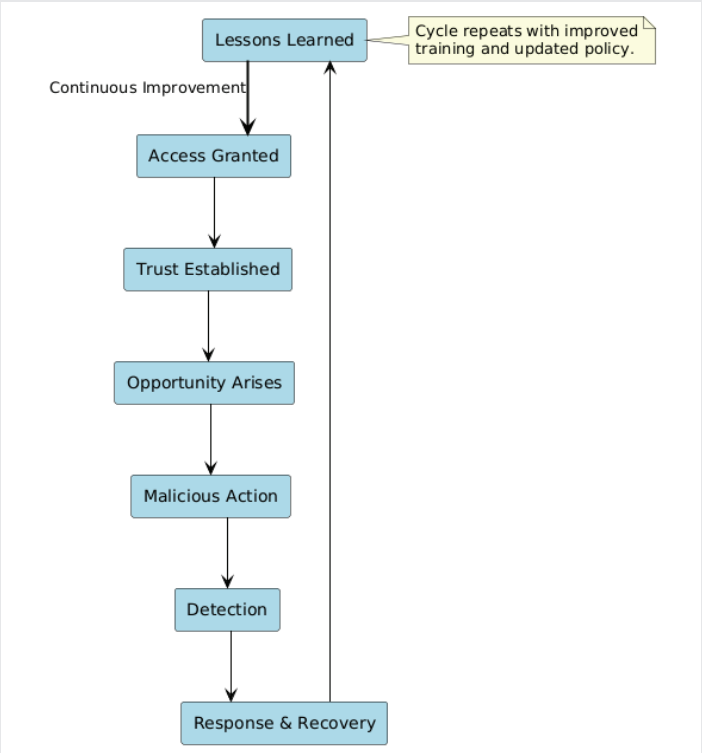

Figure 1: Insider Threat Lifecycle

Citation: Thenga ST, Selvi SA. Malicious Insider Threat to Data Security: Mitigation Strategy for municipalities. Trends Comput Sci Inf Technol. 2025;10(3):089-096. Available from: https://dx.doi.org/10.17352/tcsit.000102

and defining who should have authorised access to them and by whom. Using the principles of situational awareness, the municipalities may identify access anomalies and exposure points before they become exploitable.

Human and technical risk modelling

After the documentation of assets and data flows, municipalities ought to simulate insider threat cases on a human-based risk approach. Zeng, Dian, and Wei [11] suggest a model, IHFACS-BN (Insider Human Factors Analysis and Classification System-Bayesian Network), that calculates the probability of insider risks by combining psychological, organisational, and environmental factors [12]. This model allows municipalities to evaluate the possibility of increasing the risk of insider incidents due to employee stress, weak supervision, or poor policy enforcement. Combined with a likelihood-versus-impact matrix, this strategy will enable the decision-makers to make mitigation decisions on the most critical vulnerabilities.

Dynamic and explainable risk management

In the fast-changing digital space, the evaluation of static risk cannot be used. Islam, et al. [13] suggest intelligent, dynamic cybersecurity systems based on AI-driven analytics to track in real-time, with the backdrop of explainability and interpretability. These systems can detect abnormal behaviour-like mass file access or inconsistent privilege utilisation- and deliver interpretable information that helps a security team to make informed decisions. The adaptive approach enables municipalities with available human resources to be more responsive without exposing the staff to false positives.

Socio-technical integration and governance

Lishchynsky [14] points out the fact that insider threat prevention needs to consider a socio-technical approach with human, organisational, and technological aspects. This is a socio-technical approach that implies that the municipalities are supposed to integrate human, managerial, and technical activities into a single coordinated system. As an illustration, the cybersecurity units should collaborate closely with human resources, legal, and management teams to gain a better insight into behavioural red flags before they develop into critical issues. Frequent training of employees, background checks, and other explicit offboarding practices can help minimise the risk, as only trusted and verified people have access to the systems.

Simultaneously, the user behaviour must be constantly monitored by technical protection measures, including access control, monitoring of the system, and a log of activities. A combination of social awareness and technology can result in cities developing a balanced, flexible, and effective insider threat defence suited to the realities of work in the public sector (Table 1).

Table 1: Risk Factors for Insider Threats in Municipalities.

Category	Key Risk Factors	Examples
Organizational	Lack of oversight, weak policies, and decentralisation	Lack of admin privileges review
Human	Disgruntled employees, personal stress, and low morale	The employee is angry about the demotion
Technical	Legacy systems, excessive privileges, and poor logging	Old servers with weak access controls

Multi-layered response to violence

This section is organised based on five complementary mitigation aspects (governance and policy controls, technical and system controls, human and behavioural controls, incident response and recovery controls, and integrated defence-in-depth and resource prioritisation) to depict a socio-technical and layered approach to insider threat mitigation in municipal settings. The based structure relies on the principles of defence-in-depth of well-known standards, including NIST SP 800-53, ISO/IEC 27001, and the CERT Insider Threat Model, which states that no single control is adequate to deal with insider risk [15].

Each of the mitigation aspects focuses on a unique aspect of the insider threat exposure: governance mechanisms create strategic oversight and accountability; technical controls minimise system-level vulnerabilities; human and behavioural controls address organisational and psychological risk factors and incident response capability helps to ensure the timely containment and recovery of incidents; integrated defence-in-depth helps municipalities prioritize limited resources using controls with the most significant reduction potential. All these layers create a unified and flexible structure that balances technical protection with organisational operations and human factors, which is the multifaceted nature of real-time operations of municipal governments.

Governance and policy controls

1. **Establishing an insider threat program:** An effective insider threat strategy begins with effective governance. Governments of cities should develop an official program that will specify roles and organization of IT, HR, legal, and public safety departments. NIST [15] states that an insider threat management program must be incorporated within an overall cybersecurity framework with leadership support. Having departments come together makes everything monitored and allows for everything to be done in one action.

2. **Role-based access and least privilege:** Role-based access control (RBAC) and the principle of least privilege are quite critical in minimising insider threats. Municipal IT systems are likely to be distributed among numerous departments, so access must be limited to what is required by each employee. NIST [15] recommends access enforcement and separation of duties control to reduce risks related to privilege abuse. Frequent access rights reviews, especially after employees have transferred or left, ensure that there are no orphans and accounts with unauthorised access continue to exist.

3. **Personnel security and offboarding procedures:** According to Safa and Abroshan [5], insider attacks

Citation: Thenga ST, Selvi SA. Malicious Insider Threat to Data Security: Mitigation Strategy for municipalities. Trends Comput Sci Inf Technol. 2025;10(3):089-096. Available from: https://dx.doi.org/10.17352/tcsit.000102

may escalate when employees are dissatisfied and experience stress. Background checks, regular testing of sensitive positions, and secure offboarding that terminates access upon the termination of employment should be used as personnel security measures by the municipalities. Making HR policies consistent with cybersecurity policies makes them accountable during the duration of employment in the organisation.

4. **Data classification and data handling policies:** Municipalities keep very sensitive information, such as records of citizens and financial records. A policy on data classification assists in identifying the information that must be the most secure. NIST [5] states that labelling sensitive data, establishing retention regulations, and erasing old files securely are the keys to making protection in line with the risks of data. The response teams are also guided by these policies in recovering from an incident.

Technical and system controls

1. **Prevention: Patch Management, Authentication, and Segmentation:** Safe systems are a starting point for prevention. Multi-factor authentication (MFA), frequent updates to software, and network segmentation restrict insiders from accessing critical systems (utilities and payroll). These measures minimise the possibility of insider abuse and contribute to sealing security breaches [16].

2. **Detection: Analytics and Behavioural Monitoring:** Prevention is essential, but early detection of suspicious behaviour is also important. Behavioural monitoring and analytics, including UEBA and SIEM systems, enable earlier detection of insider threats by identifying anomalous access patterns and deviations from baseline behaviour, thereby reducing the time between malicious activity and response [7]. According to Savchenko, et al. [7], the time lag between the malicious activity and its detection is minimised by real-time monitoring, which minimises the total harm. Cities should make sure that these systems are in line with privacy laws and labour laws [17].

3. **Deterrence: Privileges, Access Control, and Auditing Records:** Technical deterrence measures such as Privileged Access Management (PAM) systems) contain administrative privileges, provide logging of session use, and generate unalterable audit trails. The perception of constant monitoring is a deterrent since it raises the risk of being caught. Extensive auditability is useful not only in investigations but also offers due diligence evidence that is crucial in terms of social responsibility [15].

Human and behavioural controls

1. **Role-specific security awareness training:** The most vulnerable part of any system is human error [18]. Periodic, role-based training will be used to ensure that the staff is aware of the warning signs and how insiders can become threats. Educated employees are less prone to mistakes or negligence towards suspicious activity [5].

2. **Promoting a positive security culture:** Surveillance is not the sole aspect of insider threat prevention. Empirical studies indicate that organisational trust, fairness, and transparent leadership are associated with reduced insider threat risk, as employees who feel valued and treated equitably are less likely to engage in malicious or negligent behaviour [5]. Safa and Abroshan [5] discovered that organisational trust reduces the risk of insider incidents. There is a culture of verified trust that makes the employees responsible yet not over-policed.

3. **Reporting mechanisms and whistleblower protections:** The municipalities ought to establish secure and confidential ways through which employees can report suspicious activities. Whistleblower policies protect individuals against being punished after speaking up. A trained team should fairly review reports. Integration of reporting systems and monitoring enhances prompt detection and trust in security procedures by the employees.

Incident response and recovery controls

1. **Planning of insider-specific response:** Conventional response strategies consider the external attacks, but insider attacks demand discretion. The municipalities are supposed to come up with silent and organised reactions that reduce interference but maintain evidence. NIST [15] suggests open communication between IT, HR, and legal divisions to make sure that all roles involved in the response process are familiar.

2. **Forensic preparedness and law enforcement preparedness:** IT personnel should be able to maintain digital evidence by collecting logs and protecting systems after a breach. Operating in collaboration with the law enforcement agencies provides a way of ensuring that investigations are conducted in a manner that is legal and free of any corruption. The preparation is time-saving and assists the city in fulfilling disclosure requirements.

3. **Continuous improvement and post incident recovery:** After restoring the systems, leaders are supposed to analyse what went wrong and reformulate the policies or training accordingly. According to Savchenko, et al. [7], incident recovery and learning make incidents less harmful in the long term. Lessons learned should be used to inform future prevention plans.

Integrated defence-in-depth and resource prioritisation

All protection layers should be in cooperation. Governance offers form, technology protects systems, human nature influences behaviour, and response strategies provide

Citation: Thenga ST, Selvi SA. Malicious Insider Threat to Data Security: Mitigation Strategy for municipalities. Trends Comput Sci Inf Technol. 2025;10(3):089-096. Available from: https://dx.doi.org/10.17352/tcsit.000102

resilience. According to Sektas-Bilusich, et al. [16], the priority of limited budgets should be on high-value controls, including access management and training employees. Insider threat is especially effectively addressed with defence-in-depth methods since such methods decentralise control mechanisms over governance, technical, and human domains, thereby closely coupling to no specific control mechanism, and they stress resistance against insider abuse [15]. The ongoing review helps keep the defences updated because of the changing risks and technologies (Figure 2).

Implementation framework and resource considerations

Implementing an insider threat mitigation strategy on the municipal level needs a resource-sensitive, phased approach, where governance, technology, and human capital are balanced. An effective model starts with the implementation of original governance mechanisms, such as the formation of a cross-departmental insider threat program and the establishment of formal risk ownership functions. Chandra, et al. [10] found that situational awareness and structured assessment frameworks can be used to improve the decisions made at the initial stages of implementation to identify high-risk data assets and access points.

The implementation may be structured into four stages.

Phase 1: Foundation aimed at the creation of insider threat policies, training, and awareness.

Phase 2: Technical Integration is the implementation of multi-factor authentication, privileged access management, and audit logs to apply principles of least privilege.

Phase 3: Behavioural Analytics and Automation is the third phase that implements AI-based anomaly detection systems to improve monitoring, which fits the explainable AI system [13].

Phase 4: Continuous Improvement involves performance audits, lessons learned, and Proactive training based on emerging threat intelligence (Table 2).

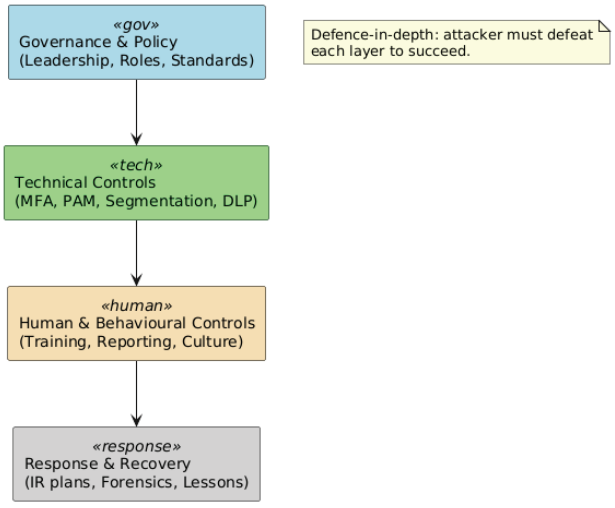

Figure 2: Multi-Layered Mitigation Strategy Model.

Table 2: Implementation phase and Key accounts.

Phase	Focus Area	Activities	Expected Outcomes
Foundation	Governance & Policy	Form an insider threat team, develop a policy, and conduct awareness training.	Establish governance and awareness.
Deployment	Technical Controls	Implement MFA, PAM, and DLP tools	Improved access and data control
Monitoring	Analytics & Detection	Monitor activity using SIEM and UEBA	Early detection of malicious behaviours
Improvement	Review & Audit	Conduct audits, policy updates, and staff retraining	Continuous resilience

Resource allocation is a significant challenge to municipalities. Budgetary limitations can be countered by utilising joint cybersecurity services or federal/state grants. According to Rajagopalan, Lynch, and Burbach [19], the idea of reliability in personnel and specific investment into training is as important as the purchase of technology. Economies of scale can also be facilitated in cybersecurity infrastructure through inter-municipal collaboration and through public-private partnerships [20]. In addition, preventive controls can be enhanced with human intelligence elements, including counterintelligence tests performed on critical positions [21]. Finally, successful implementation is achieved by matching the technical measures to organisational culture and regular assessment of the programme's maturity.

Ethical, legal, and privacy considerations

Insider threat mitigation in a municipal setting needs to resolve security needs with ethical and legal considerations to safeguard the privacy of the employees and trust in communities. Strict compliance regimes, including the data protection laws, labour controls, and transparency requirements, govern municipalities. Ethical supervision can also make sure the monitoring systems do not infringe on privacy at the expense of attaining reasonable security goals. Following Lishchynsky [14], social technical governance insists that insider monitoring must be visible, fair, and accountable to avoid the depletion of employee morale and institutional trust.

Legal risks may arise in terms of the utilisation of behavioural monitoring technologies, insofar as the digital footprints of employees or their Communication are examined. Alsowail and Al Shehari [22] state that the countermeasure frameworks should be based on direct policy guidelines and informed consent procedures to guarantee lawful surveillance. Interpretability is also an issue because of the integration of AI-based detection systems, which are powerful. According to Islam, et al. [13], explainable and interpretable AI is required in cybersecurity decisions to curb algorithmic bias and to avoid the due process in investigations.

Local authorities must also adhere to local privacy regulations including GDPR or local privacy regulations, by ensuring a balance between the level of monitoring and the level of risk. Ethical Communication and whistleblower safeguarding systems also add to the development of trust

Citation: Thenga ST, Selvi SA. Malicious Insider Threat to Data Security: Mitigation Strategy for municipalities. Trends Comput Sci Inf Technol. 2025;10(3):089-096. Available from: https://dx.doi.org/10.17352/tcsit.000102

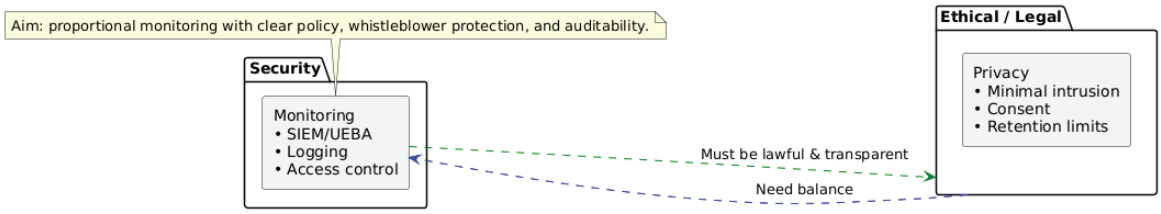

Figure 3: Ethical and Legal Balance in Employee Monitoring.

and motivate timely reporting of suspicious activity [21]. Legally, proper documentation, chain-of-custody procedures, and policies to notify the organisation and individuals guard against procedural violations [19]. Simply, the concepts of fairness, transparency, and accountability should be reflected in city insider threat programmes, in which the level of proper security is highly reliant on long-term public trust as well as on the technical control maturity (Figure 3).

Limitations and directions for future research

This research is mainly conceptual in essence, and it is based on a broad overview and integration of stakeholder literature, standards, and theoretical frameworks of insider threat mitigation. In this regard, the proscribed multi-layered mitigation framework has not undergone an empirical validation process over case studies or field-based applications in municipal settings. Although the methodology facilitates the generalisability of the wide choice and integrates with the theories, it is hampered by the inability to directly estimate the operational effectiveness of the framework in a variety of municipal settings.

The limitation could be mitigated by future studies, which involve case study research and pilot application of the proposed framework to small, medium, and large cities to test the viability over time and costs, as well as quantifiable security results. The framework can also be improved through comparative analysis in terms of jurisdictions and the systems of governance in order to formulate contextual factors that define the effectiveness in curbing insider threats. Also, longitudinal research on the organisation and behavioural changes would offer useful empirical evidence on the effectiveness of integrated insider threat programmes in resource-constrained public-sector settings in the long term.

Conclusion and recommendations

The increasing complexity of insider threats is a significant threat to the security of municipal data. This research has suggested that the mitigation process ought to be holistic and incorporate governance, technical, behavioural, and ethical facets. As municipalities hold sensitive data about citizens, the municipality has to transform into a defensive mechanism that is responsive to active and intelligence-driven systems of defence. Studies emphasise the importance of encouraging situational awareness, 24-hour observation, and a sense of responsibility as the key to insider threat prevention [10].

Policy suggestions are institutionalising specific insider threat programmes into the cycles of municipal governance, using ongoing training and employee vetting as a vital element of human resources, and using explainable AI tools to manage risks [13] dynamically. Moreover, interagency partnerships can lead to the sharing of security services and skills between small and mid-sized municipalities with the help of State or federal grants. According to Kanellopoulos [21] and Rajagopalan, et al. [19], introducing human intelligence and counterintelligence factors increases the resistance to espionage or politically oriented insider attacks.

Lastly, all insider threat strategies should consider ethical and privacy issues. The transparency of oversight, accurate policies of data use, and a continuous discussion of privacy implications are the means of building the trust of people and employees. Future studies ought to discuss the patterns of predictive models in low-resource municipal settings and comparative studies on the framework of insider threats as they exist in different jurisdictions. The leaders of a municipality need to understand that insider threat reduction is not only a technical procedure but a foundation of democratic data custodianship and robust citizen administration.

References

1. Inayat U, Farzan M, Mahmood S, Zia MF, Hussain S, Pallonetto F. Insider threat mitigation: systematic literature review. Ain Shams Eng J. 2024:103068. Available from: https://doi.org/10.1016/j.asej.2024.103068

2. Alsowail RA, Al-Shehari T. A multi-tiered framework for insider threat prevention. Electronics. 2021;10(9):1005. Available from: https://doi.org/10.3390/electronics10091005

3. Akinsola FA, Ogwueleka FN, Mbanaso UM. A comprehensive survey of insider threat landscape and detection indicators. Int J Eng Inf Technol. 2025;2(3):146-177. Available from: https://ejournal.yasin-alsys.org/KIJEIT/article/view/7704

4. Vestad A, Yang B. Municipal cybersecurity—A neglected research area? A survey of current research. In: Springer proceedings in complexity. 2023. p. 151-165. Available from: https://doi.org/10.1007/978-981-19-6414-5_9

5. Safa NS, Abroshan H. The effect of organizational factors on the mitigation of information security insider threats. Information. 2025;16(7):538. Available from: https://doi.org/10.3390/info16070538

6. Steinmetz M. The insider threat and the insider advocate. In: Oxford University Press eBooks. 2021;348-358. Available from: https://doi.org/10.1093/oxfordhb/9780198800682.013.21

7. Savchenko V, Dzyuba T, Matsko O, Novikova I, Havryliuk I, Polovenko V, et al. Time aspect of insider threat mitigation. Adv Mil Technol. 2024;19(1):149-164. Available from: https://doi.org/10.3849/aimt.01830

8. Nagel K. Establishing a foundation and building an insider threat program. ISACA J [Internet]. 2021;5. Available from: https://www.isaca.org/resources/

Citation: Thenga ST, Selvi SA. Malicious Insider Threat to Data Security: Mitigation Strategy for municipalities. Trends Comput Sci Inf Technol. 2025;10(3):089-096. Available from: https://dx.doi.org/10.17352/tcsit.000102

isaca-journal/issues/2021/volume-5/establishing-a-foundation-and-building-an-insider-threat-program

9. Cornelius FP, Van Rensburg SKJ. Emerging South African smart cities: data security and privacy risks and challenges. S Afr J Inf Manag. 2024;26(1). Available from: https://sajim.co.za/index.php/sajim/article/view/1847/2948

10. Chandra NA, Ramli KA, Putri Ratna AAP, Gunawan TS, et al. Information security risk assessment using situational awareness frameworks and application tools. Risks. 2022;10(8):165. Available from: https://doi.org/10.3390/risks10080165

11. Zeng M, Dian C, Wei Y. Risk assessment of insider threats based on IHFACS-BN. Sustainability. 2022;15(1):491. Available from: https://doi.org/10.3390/su15010491

12. Al-Mhiqani MN, Ahmad R, Zainal Abidin Z, Yassin W, Hassan A, Abdulkareem KH, et al. A review of insider threat detection: classification, machine learning techniques, datasets, open challenges, and recommendations. Appl Sci. 2020;10(15):5208. Available from: https://doi.org/10.3390/app10155208

13. Islam S, Basheer N, Papastergiou S, Ciampi M, Silvestri S. Intelligent dynamic cybersecurity risk management framework with explainability and interpretability of AI models for enhancing security and resilience of digital infrastructure. J Reliab Intell Environ. 2025;11(3). Available from: https://doi.org/10.1007/s40860-025-00253-3

14. Lishchynsky M. The insider threat: a socio-technical analysis of preventing data breaches and espionage within governmental agencies. Politics Secur. 2025;12(2):88-103. Available from: https://doi.org/10.54658/ps.28153324.2025.12.2.pp.88-103

15. National Institute of Standards and Technology. Security and privacy controls for information systems and organizations. NIST Spec Publ 800-53 Rev 5 [Internet]. 2020. Available from: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

16. Sektas-Bilusich D, Nunes-Vaz NA, Chim L, Lord S. A risk-based framework to inform prioritisation of security investment for insider threats. Int J Saf Secur Eng. 2020;10(1):49-57. Available from: https://www.iieta.org/journals/ijsse/paper/10.18280/ijsse.100107

17. Gheyas IA, Abdallah AE. Detection and prediction of insider threats to cyber security: a systematic literature review and meta-analysis. Big Data Anal. 2016;1(1). Available from: https://doi.org/10.1186/s41044-016-0006-0

18. Ismail WBW, Widyarto S. A classification of human error factors in unintentional insider threats. Eur Proc Multidiscip Sci. 2022;3:667-676.

19. Rajagopalan RP, Lynch P, Burbach T. Mitigating insider threats and ensuring personnel reliability. In: Springer eBooks. 2024. p. 29-69. Available from: https://link.springer.com/chapter/10.1007/978-3-031-56814-5_2

20. Whitty MT. Developing a conceptual model for insider threat. J Manag Organ. 2018;27(5):911-929. Available from: https://doi.org/10.1017/jmo.2018.57

21. Kanellopoulos A-N. Insider threat mitigation through human intelligence and counterintelligence: a case study in the shipping industry. Def Secur Stud. 2024;5:10-19. Available from: https://doi.org/10.37868/dss.v5.id261

22. Alsowail RA, Al-Shehari T. Techniques and countermeasures for preventing insider threats. PeerJ Comput Sci. 2022;8:e938. Available from: https://doi.org/10.7717/peerj-cs.938

23. Saxena N, Hayes E, Bertino E, Ojo P, Choo KKR, Burnap P, et al. Impact and key challenges of insider threats on organizations and critical businesses. Electronics. 2020;9(9):1460. Available from: https://doi.org/10.3390/electronics9091460

Citation: Thenga ST, Selvi SA. Malicious Insider Threat to Data Security: Mitigation Strategy for municipalities. Trends Comput Sci Inf Technol. 2025;10(3):089-096. Available from: https://dx.doi.org/10.17352/tcsit.000102