Article

Data Security: Approaches to Local Government Cybersecurity

Shandukani Tshilidzi Thenga *

Posted Date: 8 July 2025

doi: 10.20944/preprints202507.0651.v1

Keywords: cybersecurity; digitalisation; modern technology; decentralisation; machine learning; artificial intelligence; blockchain

 doi:10.20944/preprints202507.0651.v1

Article

Data Security: Approaches to Local Government Cybersecurity

Shandukani Tshilidzi Thenga

British University College, South Africa; candythenga@gmail.com

Abstract

Data security at the local government departments is discusses the dangers associated with cybersecurity tat ocal governments level hand the possibilities of cyberattacks and data breaches. As the government goes deeper into its digital push, the municipalities are even more vulnerable because they operate practically exclusively on outdated infrastructures and are strangled by skimpy budgets. These governments preserve a lot of sensitive data of the citizens, including identification, health, tax, and crime history, and thus, they are easy to attack by cybercriminals. Another aspect indicated in the paper is the lack of good resources, qualified personnel, and modern technology that can be possessed by the local governments and contribute to the security problem as well. The article also explains the cybersecurity threats currently facing municipalities; these include old-age IT systems, financial limitations, and the shortage of in-house cybersecurity specialists. In the majority of the municipalities, third-party vendors are used, which leads to inefficiencies and loopholes in security. The IT systems within the various departments of city governments are also decentralised, thus causing variation in security practice. The paper states that one of the solutions to the said challenges is the adoption of cybersecurity frameworks such as the NIST Cybersecurity Framework, because they provide a systematic way of handling and managing cyber threats. The paper also describes the role of emerging technologies in promoting cybersecurity in local governments. Artificial intelligence (AI), machine learning (ML), and blockchain are the most popular data protection and threat detection enforcement processes. AI and ML can help identify cyber threats in real time by analysing a large amount of data. Blockchain ensures the integrity of the data and its resistance to unauthorised access. The essay also discusses the prospects of cloud computing since it offers flexible and scalable security provisions to mitigate the threat posed by the legacy environment. The paper analyses successful and unsuccessful initiatives at municipal cybersecurity based on a case study of Los Angeles and Gloucester City. The secure security tools based on the cloud, available to the towns in Los Angeles, and real-time monitoring of the threats are a good example of the benefits of periodic modernisation of information technology infrastructure. In the meantime, the experience of Gloucester City's ransomware attack demonstrates the disastrous outcomes of non-observance of cybersecurity planning and the importance of funds spent on security. Lastly, the writer points out that cybersecurity is an issue that local governments should prioritise through research, development, and implementation of the latest technology, employee education, and the adoption of best practices to maintain the confidentiality of information. In so doing, cities can employ cyber resilience to achieve market trust and maintain key services' business continuity.

Keywords: cybersecurity; digitalisation; modern technology; decentralisation; machine learning; artificial intelligence; blockchain

1. Introduction

The issue of data security is an increasing problem for local governments since cities are entrusted to manage the sensitive data of their citizens, including personal identification information, health, and financial details. The digitalisation of government services and infrastructure has led to

 doi:10.20944/preprints202507.0651.v1

improved efficiency of operations; however, digital systems pose significant cyberattack risks. The smaller size of municipalities and the control of sensitive data are often associated with unique difficulties, including small budgets, outdated IT infrastructure, and the absence of specialists (Bisceglia, 2023). In the absence of adequate cybersecurity, local governments may become the primary targets of cyberattacks, which can erode people's trust in their government, interrupt services, and cause substantial financial losses (Larson, 2025). This study explores the issue of data safety in local governments, determines the struggles that local governments encounter, and presents the best possible practices and technologies that can aid in improving cybersecurity. This study is an actionable proposal to improve data security in local governments based on recent case studies, cybersecurity frameworks, and expert advice.

2. Literature Review

2.1. The Requirement of Data Security in Local Governments

The sensitive information that local governments manage is enormous, such as voter information, criminal records, healthcare data, tax records, and utility services (Cagigal, 2023). With the increasing use of digital systems by municipalities to enhance their efficiency and service delivery, cybersecurity threats have increased considerably. A growing issue that local governments should address is the phenomenon of digital threats, including cyberattacks, data breaches, and identity theft (Dinapoli, 2016). The ransomware attack on the City of Atlanta government in 2018 is a reminder of how poor cybersecurity can interfere with municipal government operations. The attack led to massive system shutdowns and economic losses, revealing weak points in the local government's infrastructure (New Hampshire Municipal Association, 2018).

Maintaining the security of sensitive data is important in facilitating operations and ensuring that people have faith in their government. The loss of personal data may severely affect people's trust in the capability of the government to handle and secure personal data, which may have both long-term reputation and economic impacts (Eugene, 2024). Cities that do not respond appropriately to such threats risk lawsuits, reputation damage, and even monetary fines. As technology is developing quickly, cities are forced to reconcile the introduction of new technologies, including cloud computing, smart city infrastructure, and IoT, with effective measures to enforce cybersecurity (New Hampshire Municipal Association, 2023). The security of citizen data should be a significant priority for municipalities, and to ensure the security of their systems, digital systems should be subject to regular vulnerability monitoring (Hatter, 2024).

2.2. Issues Confronting Local Governments

Local governments are increasingly experiencing various difficulties in the protection of sensitive information. A lack of sufficient funding is one of the major obstacles. Municipal governments usually have limited budgets, and cybersecurity may not be prioritised over other urgent requirements. Harmon (2025) notes that local authorities often fail to justify the costs of acquiring the services of cybersecurity specialists or the purchase of new security technologies. This is primarily due to a lack of resources; in many cases, the existing IT infrastructure continues to be utilised instead of implementing improvements and new technologies. Outdated systems do not possess the security required to counter new attacks (Hatcher et al., 2020). The utilisation of legacy systems further complicates the issue. Legacy technologies in the majority of local governments do not possess the required security patches and are vulnerable to attacks (Harmon, 2025).

Without modern systems, cities are unable to implement modern cybersecurity systems and protect sensitive data. Moreover, there is a lack of qualified cybersecurity experts available to implement these changes. Furthermore, municipal governments do not have suitable in-house experts to carry out this work, according to Cagigal (2023); therefore, these governments are forced to hire the services of outside contractors or suppliers. This reliance on third-party providers is among the reasons why inefficiencies and security vulnerabilities exist, especially if a third-party provider

 doi:10.20944/preprints202507.0651.v1

proves to be unable to meet the security requirements of a local government. The second problem is that municipal IT systems are dispersed. The range of solutions implemented across different departments within a municipal administration leads to inconsistency in the security solutions and a lack of capability to enforce a uniform strategy for cybersecurity. Ibrahim et al. (2018) assert that such heterogeneous systems leave vulnerabilities in security that are only identified after catastrophic breaches, as exemplified by the City of Atlanta administration hack.

2.3. Security Guidelines and Principles

In order to address these issues, efficient models and best practices for city cybersecurity are required. One of the most widely used frameworks of local government cybersecurity mechanisms is the NIST Cybersecurity Framework (NIST, 2024). This framework has a formal response plan to identify, guard against, detect, and respond to cyberattacks. VisioneerIT (2025) notes that the framework provides municipalities with steps that they can follow to protect their IT infrastructure and enhance cybersecurity. Best practices such as regularly conducting vulnerability assessments, encrypting sensitive information, multi-factor authentication (MFA), and training employees are critical (Bisceglia, 2023). Moreover, municipalities should back up and store their data at off-site locations in order to ensure immunity to ransomware attacks. VisioneerIT (2025) also recommends proactive defences to prevent cybersecurity threats and to store sensitive information where it cannot be accessed by unauthorised users. Governments at the local scale should also be proactive in conducting regular audits to evaluate the effectiveness of their security measures and identify vulnerabilities before they are exploited by attackers.

2.4. Innovations and Technological Solutions

New technologies are becoming instrumental in improving the cybersecurity of municipalities. For example, technologies such as artificial intelligence (AI) and machine learning (ML) can review extensive portions of data in order to identify cybersecurity threats in real time. Such tools enable municipalities to recognise patterns and identify abnormalities in their networks, making it easier to react to possible cyberattacks (Larson, 2025). Threat detection using AI is a necessary measure that municipalities require to manage changing cyber threats. Blockchain technology is another innovation with the potential to assist municipalities in improving their cybersecurity. Li and Liao (2018) believe that blockchain provides tamper-resistant, decentralised data storage. This technology can be invaluable in securing municipal transactions, including voting systems and money records. Blockchain is a perfect tool for ensuring data integrity and preventing unauthorised data access because of its transparency and immutability.

Another notable technology that can significantly assist local governments in enhancing their cybersecurity is cloud computing. According to Fedson (2025), through cloud-based services, municipalities can obtain real-time updates and constant monitoring of their security systems in order to identify threats before they occur. Cloud computing is also scalable; municipalities can change their cybersecurity facilities accordingly. Such flexibility is of particular significance to local governments with shifting requirements or minimal resources. Moreover, cloud providers can offer high-level encryption methods and redundant storage, which ensures that a security breach does not endanger municipal data.

2.5. Case Studies

Several cities have experienced serious cybersecurity incidents; however, these experiences can offer guidance to others. The ransomware attack on Gloucester City Council in 2020 is one of the most significant examples of how inexperienced municipalities can be victims of cyberattacks. According to Smith (2024), Gloucester's reaction to the attack demonstrates the significance of a proactive cybersecurity approach. After the attack, the city invested in improving its security infrastructure, such as data backup protocols and a better incident response plan. Conversely, Los Angeles presents

 doi:10.20944/preprints202507.0651.v1

an example of a municipality that has implemented cloud-based security solutions to enhance its cybersecurity status. With cloud-based services, Los Angeles has expanded its cybersecurity and minimised the risks of using legacy systems (Fedson, 2025). The Los Angeles case demonstrates that IT infrastructure modernisation and implementation of the best cybersecurity practices can assist a municipality in considerably increasing its cyber threat resistance.

2.6. Methodology

This study was conducted using a qualitative method to evaluate the current issue of data security in local governments with a focus on municipalities. Considering the nature of the challenges regarding data security, especially in institutions within the public sector, qualitative approaches can assist in understanding the nature of the challenges that municipalities have to address and the efficiency of the strategies they use to secure the data. An extensive literature search, including academic sources, government reports, case studies, and expert interviews, provided a comprehensive overview of the subject. These sources were selected to cover a broad spectrum of perspectives so that the research results are comprehensive and applicable to the difficulties municipalities face while providing resolutions to protect their data.

2.7. Data Collection

The primary data review approach employed in this study was the critical analysis of the scholarly literature, which provided a theoretical background of cybersecurity practices combined with a review of government reports that present information about the policies, frameworks, and practical implementation of these practices in local governments. A large part of the literature comprises peer-reviewed articles, reports of cybersecurity agencies, white papers of different government agencies, etc., all of which comment on trends, challenges, and cybersecurity opportunities in local governments. The data collection also involved case studies of local government cybersecurity activities. These case studies, selected in cities and towns of diverse geographical locations, provide practical evidence of how local governments have addressed data security challenges and their approaches to surmounting funding barriers and inadequate infrastructure while ensuring a skilled workforce.

The presented case studies also indicate what can go wrong with cybersecurity and what others can learn to make their municipalities safer. As an example, the City of Atlanta government ransomware attack in 2018 is mentioned numerous times in research studies and reports as one of the critical events that highlighted municipalities' vulnerability to cyberattacks (Smith, 2024). This study highlights trends and best practices of enhancing cybersecurity in municipalities by examining the causes and consequences of such incidents. The other important feature of the data collection process is expert interviews. Interviews were conducted with IT administrators of municipalities and cybersecurity professionals who have had experience working with local governments and are familiar with the data security peculiarities of these local governments. These professionals offered applicable considerations regarding data security, such as challenges encountered, which include the lack of sufficient funds, the use of old IT systems, and the lack of qualified professionals (ResoluteGuard, 2025). Cagigal (2023) believes that most municipalities cannot hire cybersecurity professionals because of financial constraints. In addition, Hatcher, Meares, and Heslen (2020) emphasise that decentralised municipal systems, where several departments can work without coordination, make the data security task even more challenging.

2.8. Data Analysis

Thematic analysis was employed to analyse the data gathered during the literature review, case studies, and interviews, as this is a standard methodology in qualitative research. This approach includes the detection of similarities and regularities in the information, which can assist in understanding the key data security problems that should be addressed in local governments. This

 doi:10.20944/preprints202507.0651.v1

analysis started by coding the data to point out the key themes, which included the effectiveness of the current cybersecurity practices, the role of emerging technologies, and the obstacles municipalities encounter in integrating effective data security solutions. Among the major themes was the prevalence of the NIST Cybersecurity Framework in local governments. As one of the most effective cybersecurity tools, this framework assists municipalities in evaluating and enhancing their security position by systematically determining and addressing risks (NIST, 2024). According to the literature and the interviews conducted with experts, although a significant number of municipalities have embraced the NIST Cybersecurity Framework, it is still challenging to effectively implement. This also encompasses the inadequacy of the staff and resources, which prevents adequate implementation of the framework's guidelines.

The second theme in the data analysis process was how emerging technologies can help enhance cybersecurity. Machine learning and AI were cited as possible technologies that could assist local governments in being proactive in detecting and responding to cybersecurity attacks. Li and Liao (2018) state that systems based on AI can analyse large volumes of data in real-time and identify anomalies, allowing municipalities to prevent breaches before they occur. On the same note, cloud computing and blockchain were also identified as possible remedies to improve local government data security, with the benefits of scalability, real-time updates, and enhanced data integrity (Fedson, 2025). Data analysis also indicated some general challenges municipalities have experienced in securing data. These challenges include inadequate budgets, old IT systems, a lack of qualified human resources, and uniformity in cybersecurity policies among the departments. According to Cagigal (2023), not all municipalities have a specific cybersecurity budget, so they must contact third-party vendors to assist them. In addition, Hatcher et al. (2020) mention the UCM problem of having one comprehensive cybersecurity plan for every department, in which every department may have different systems and other priorities.

2.9. Ethical Implications

Ethical considerations were taken into account in the course of this research when engaging with IT administrators and cybersecurity experts at the local government level. To guarantee confidentiality and transparency, all the interview participants were informed about the purpose of this study and offered an opportunity to provide informed consent. In addition, any data exchanged during the interviews was made anonymous to preserve the interviewees' privacy. Furthermore, the study findings are reported in a manner that protects the privacy of the participating individuals and municipalities.

3. Findings/Results

3.1. Important Literature Findings

The literature review revealed significant data protection issues that cities encounter. One of the main problems identified is the absence of dedicated cybersecurity personnel. For many local governments, the difficulty of overcoming this challenge is due to small budgets (Cagigal, 2023). Because many municipalities are subject to limited budgets, they cannot hire in-house cybersecurity specialists who possess the knowledge to assist in the management and protection of their IT systems. As a result, many municipalities rely on third-party vendors or consultants to cover their cybersecurity requirements. Although this is a cost-efficient solution, it may cause inefficiency and vulnerability to data control and protection (Bisceglia, 2023). Moreover, obsolete IT infrastructures have continued to be a significant issue for most local governments. Despite the increased awareness of cybersecurity risks, most municipalities still rely on legacy systems that cannot address the demands of contemporary security (Harmon, 2025). Outdated systems do not provide the required security patches, encryption mechanisms, and extra functions that new systems do. This complicates local governments' decision-making regarding the application of efficient cybersecurity measures.

 doi:10.20944/preprints202507.0651.v1

The weaknesses of legacy systems make municipalities susceptible to cyberattacks such as ransomware, which can cripple their operations and affect important information.

Some of the best practices for enabling local governments to improve their data security were mentioned in the literature. Among the main recommendations, the risk-based approach to cybersecurity enables municipalities to allocate their resources and efforts to addressing the security of each system depending on the degree of the associated risk (Bisceglia, 2023). Moreover, it is also important to regularly train employees about the best cybersecurity practices to ensure that every employee is informed about possible security risks and trained on how to avoid the most common mistakes, including becoming a victim of a phishing attack. It is also possible to create an organisational culture based on security awareness through training, eliminating the risk of human error, which is one of the most frequent causes of successful cyberattacks (Harmon, 2025). The next best practice is using multi-factor authentication (MFA), which implements an additional layer of user account protection by requiring more than one type of confirmation to log in to a digital system (Harmon, 2025). This is an especially critical tool in systems with sensitive information, as it considerably minimises the chances of unauthorised access. In addition, it is crucial to encrypt all sensitive information during both data transfer and storage to avoid data breaches (Bisceglia, 2023). Data encryption ensures that even when information is stolen or intercepted by other parties, it cannot be read.

One of the main conclusions found in the literature was the identification of the NIST Cybersecurity Framework as a powerful tool that can be used by local governments to enhance their cybersecurity strategies (Cook, 2017). The NIST Cybersecurity Framework provides an organised method for the identification, protection, detection, response, and recovery of cybersecurity incidents. NIST (2024) asserts that municipalities using the framework can effectively define their cybersecurity requirements, concentrate on security improvements, and address the pertinent approaches to defend their IT infrastructure.

3.2. Case Studies

Several case studies can be utilised to provide valid conclusions in terms of implementing cybersecurity practices within local governments. Cyberattacks may drastically destabilise municipal systems, as was experienced in the City of Gloucester, Massachusetts, in 2020. The attack was connected with a ransomware virus that encrypted the city's systems and caused inefficiency. As a response, Gloucester immediately acquired enhanced cybersecurity solutions in the form of improved data backup systems, advanced security devices, and a fortified incident response strategy (Smith, 2024). This example showed that it is necessary to be proactive and have a well-planned cybersecurity plan. As the recovery process was taking place, it became apparent that the absence of a good security infrastructure in the city initially led to the attack's intensity. Nevertheless, the experience led to the city improving its cybersecurity stance. The experience of Gloucester underlines the importance of municipalities having a cybersecurity plan in place that is continually revised and enhanced. Moreover, municipalities should carry out regular risk assessments and modernise their infrastructure to protect sensitive information.

On the other hand, the example of the City of Los Angeles, California, can serve as evidence of a municipality that has been able to implement modern security tools and improve its cybersecurity position. Los Angeles has migrated most of its critical systems to cloud-based systems, which have provided scalable, flexible, and more secure solutions to the city. Through cloud-based services, Los Angeles can respond to emerging threats promptly because cloud-based systems can be updated in real time with the latest security patches and updates (Fedson, 2025). This move to the cloud also reduced the use of legacy systems that were high risk to cybersecurity for the city. Adopting cloud-based security solutions has provided Los Angeles with several benefits, such as an opportunity to increase or reduce its cybersecurity infrastructure according to the city's requirements. Moreover, cloud providers often offer advanced encryption and constant monitoring services, which further contribute to the increased safety of the city. The effectiveness of Los Angeles in enhancing its

 doi:10.20944/preprints202507.0651.v1

cybersecurity by adopting a cloud-based security solution indicates that IT systems require updating and the application of advanced technologies to minimise risks.

3.3. Technological Solutions

New technologies are also playing a vital role in making the cybersecurity of cities robust. The most notable evolving pattern is the use of artificial intelligence (AI) and machine learning (ML) to detect and track cybersecurity threats in real time. With AI and ML, it is feasible to manage gigantic amounts of data, recognise anomalies, and anticipate potential attacks before they become full-fledged security breaches. According to Larson (2025), AI threat defence mechanisms enable municipalities to avert security attacks, which lowers the risk of data leakage and loss of functionality in services. By using AI and ML, municipalities can increase their ability to respond to current cyber threats and reduce them. Blockchain technology can also aid in the security of municipal systems. As Ibrahim et al. (2018) report, blockchain provides support for decentralised storage and protection of data; hence, blockchain is more reliable against tampering and unauthorised access. The immutability of records and transparency can be ensured through blockchain platforms, thus protecting private information in municipalities. Moreover, blockchain technology may be beneficial in financial transactions, voting systems, and citizen data management, where data integrity and transparency are key to public trust. AI and blockchain are the latest technologies that may assist local governments in addressing some of the most urgent cybersecurity issues they face. Although these technologies are still developing, their capability to improve municipal cybersecurity strategies is immense. Furthermore, municipalities that implement these technologies early have a significant edge in protecting their data.

4. Discussion

The results of this research present some of the most important facts about cybersecurity challenges in local government. Among the most crucial obstacles is the inadequate funding of cybersecurity programs. Most local governments work with limited budgets, and, as Harmon (2025) states, cybersecurity is a lower priority than other urgent requirements, such as infrastructure or public safety. Limited funding prevents municipalities from investing in new security systems, recruiting professional cybersecurity staff, and replacing ageing IT infrastructure. Consequently, local governments become susceptible to many types of cyberattacks, including ransomware and data breaches. Moreover, Cagigal (2023) adds that numerous municipalities have external vendors providing cybersecurity solutions, which is inefficient and renders them not in control of their data security. Although third-party vendors might provide an affordable solution, their services are likely inadequate to meet a municipality's specific requirements and priorities, which may cause security vulnerabilities.

The advantage of applying a holistic approach to cybersecurity instead of only focusing on the technical side of security is one of the key findings of this study. An effective cybersecurity plan should have policies, practices, and an organisational culture that supports security awareness at every level. As municipalities increasingly utilise the digital infrastructure, employee training funding, security scans on a regular basis, and detailed incident response plans are necessary (Bisceglia, 2023). Employee training, in particular, stands out because human oversight is still one of the most common reasons that successful cyberattacks occur. Municipal employees should also be trained on how to recognise threats, i.e., phishing emails or social engineering, and the appropriate action to take in response (Brown et al., 2020). Municipalities must also perform regular security vulnerability scans and maintain up-to-date systems with current patches. Having a well-planned incident response plan that allows local governments to respond appropriately and promptly in the event of a security breach is crucial to minimise potential damage.

The case studies analysed in the current study also set the stage for the significance of proactive cybersecurity measures. A clear example of the consequences of a late reaction to a cyberattack is the City of Gloucester, Massachusetts. In 2020, the city was targeted by ransomware that majorly

 doi:10.20944/preprints202507.0651.v1

disrupted its systems, which cost the city millions of dollars to restore. The absence of a proactive cybersecurity plan further predisposed the city to such an attack, as Smith (2024) explains. The slow response, old systems, and poor backup procedures worsened the damage. The experience of Gloucester demonstrates that municipalities should invest in preventing cyberattacks before they occur. The Gloucester case also highlights the significance of an effective incident response plan and data backup mechanisms to reduce the effects of a breach.

Conversely, Los Angeles offers an appropriate example of how investing in modern security infrastructure early may enhance the cybersecurity position of a municipality. Los Angeles has effectively deployed cloud-based security, which has enabled the city to scale their cybersecurity and act against security threats (Fedson, 2025). The move to cloud computing has provided the city with real-time updates, high-end encryption techniques, and constant monitoring, which are the key factors in safeguarding sensitive information. In addition, the city's use of AI-based threat recognition technologies makes it possible to identify any potential security breach before it escalates into a massive attack. This kind of pre-emptive approach is proof of the ability of contemporary technologies to assist cities in limiting the risks of legacy technologies and provide an additional layer of overall security.

Emerging technologies, such as artificial intelligence (AI), machine learning (ML), and blockchain, have the potential to boost cybersecurity in local governments to a greater extent. AI and ML can process vast amounts of data in real time and detect anomalies and potential attacks, allowing municipalities to promptly address security problems (Larson, 2025). It is feasible for local governments to mechanise the majority of the threat detection process with such technology, thereby saving substantial time in discovering and responding to security intrusions. The tamper-evident and decentralisation features of blockchain technology provide an excellent solution for ensuring data integrity within municipal systems. Blockchain has been shown to secure sensitive data at the municipal level so that tampering or alteration of any information is traced, according to Ibrahim et al. (2018). Such technology can be integrated into an extended cybersecurity system to further protect municipal information and IT security.

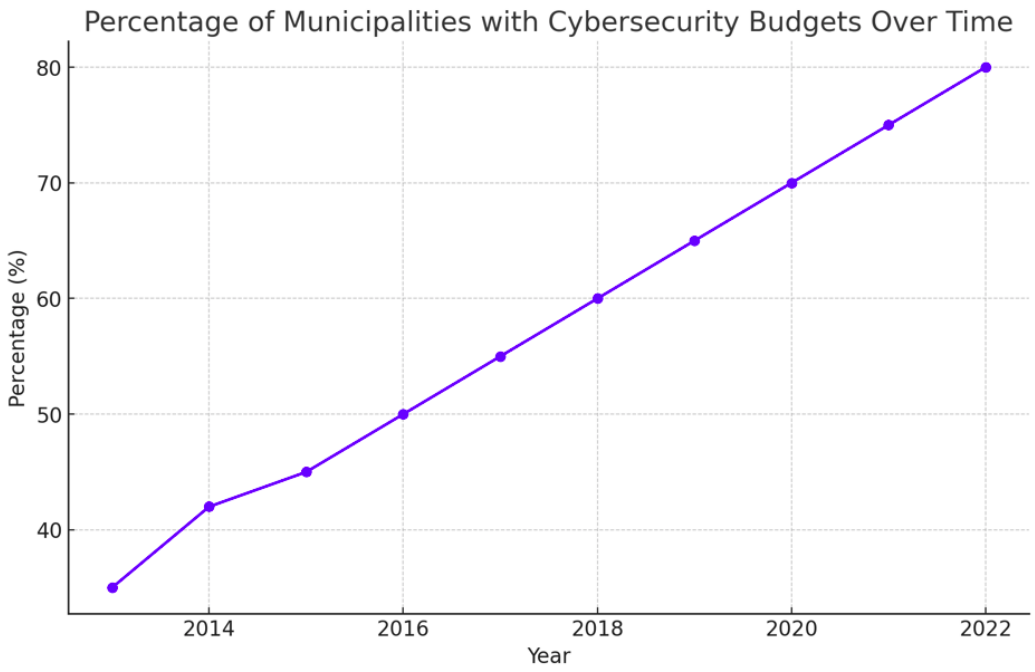
However, it should be emphasised that new technologies are not silver bullets. While new technology systems have much promise, they must be supported by a sophisticated cybersecurity infrastructure comprised of risk management, education of employees, and third-party collaboration with specialists. In concurrence with Fedson (2025) and Cagigal (2023), it is the overall strategy that is key to developing a safe environment through which municipal data can be effectively safeguarded against modern cyberattacks. Therefore, municipalities should ensure that they are technology-led and developing cultures of resilience and security within their organisations.

5. Conclusions

In summary, data security is again a widespread issue for local authorities. Increased municipal digitalisation of operations and services has exposed local governments to new cyber threats, and the majority of municipalities are not in a position to defend their systems. However, applicable solutions and technologies can be utilised to improve local government data security. The security of local governments can be guaranteed through the implementation of cybersecurity frameworks, such as the NIST Cybersecurity Framework (NIST, 2024) and emerging technologies such as AI, machine learning, and blockchain (Ibrahim et al., 2018). Municipalities should invest in training employees, carrying out frequent security audits, and deploying new IT infrastructures to fend off the risks of archaic systems (Bisceglia, 2023). With an active and concerted policy for cybersecurity, local governments can be well placed to protect sensitive data, provide citizen security, and ensure essential services are not disrupted. In the long term, all government levels must be dedicated to cybersecurity to protect the public interest and ensure that government activities are secure in the cyber world.

 doi:10.20944/preprints202507.0651.v1

Appendix



References

1. Bisceglia, N. (2023, July 23). *Data Security in Local Government: Best Practices for Protection*. TeamPassword. https://teampassword.com/blog/data-security-in-local-government?utm
2. Brown, I., Marsden, C. T., Lee, J., & Veale, M. (2020). Cybersecurity for elections: A Commonwealth guide on best practice.
3. Cagigal, D. (2023, September 26). *Cybersecurity Challenges and Opportunities for Local Government - GovLoop*. GovLoop. https://www.govloop.com/community/blog/cybersecurity-challenges-and-opportunities-for-local-government/?utm

 doi:10.20944/preprints202507.0651.v1

4. Cook, K. D. (2017). *Effective cyber security strategies for small businesses* (Doctoral dissertation, Walden University).
5. Dinapoli, T. (2016). *Protecting Sensitive Data and Other Local Government Assets: A Non-Technical Cybersecurity Guide for Local Leaders*. https://www.osc.ny.gov/files/local-government/publications/pdf/cyber-security-guide.pdf?utm
6. Eugene N. (2024, March). *Cyber security best practices to support local governments*. https://www.municipalworld.com/feature-story/cyber-security-best-practices/?utm
7. Fedson, A. (2025, June 26). *A guide to best cybersecurity practices for local governments and utilities*. Raftelis. https://www.raftelis.com/insight/a-guide-to-best-practices-of-cybersecurity-for-local-governments-and-utilities/?utm
8. Harmon, P. (2025, March 14). *Cybersecurity challenges faced by local governments in 2025*. Americancityandcounty.com. https://www.americancityandcounty.com/government-technology/cybersecurity-challenges-faced-by-local-governments-in-2025?utm
9. Hatcher, W., Meares, W. L., & Heslen, J. (2020). The cybersecurity of municipalities in the United States: An exploratory survey of policies and practices. *Journal of Cyber Policy*, *5*(2), 302-325.
10. Hatter, D. (2024, April 18). *Cybersecurity Strategies for Municipalities: 8 Expert Tips - Intrust IT*. Intrust IT. https://www.intrust-it.com/cybersecurity-strategies-for-municipalities/?utm
11. Ibrahim, A., Valli, C., McAteer, I., & Chaudhry, J. (2018). A security review of local government using NIST CSF: a case study. *The Journal of Supercomputing*, *74*(10), 5171–5186. https://doi.org/10.1007/s11227-018-2479-2
12. Larson, K. (2025). *Municipal Cybersecurity: How to prepare as cybercriminals go hyperlocal*. Citizensbank.com. https://www.citizensbank.com/corporate-finance/insights/municipal-cybersecurity.aspx?utm
13. Li, Z., & Liao, Q. (2018). Economic solutions to improve cybersecurity of governments and smart cities via vulnerability markets. *Government Information Quarterly*, *35*(1), 151-160.
14. National Cybersecurity Centre. (2023, April 19). *Cybersecurity Best Practices for Smart Cities*. https://www.cisa.gov/sites/default/files/2023-04/cybersecurity-best-practices-for-smart-cities_508.pdf?utm_source
15. New Hampshire Municipal Association. (2018). *Cybersecurity Best Practices for Municipalities*. New Hampshire Municipal Association. https://www.nhmunicipal.org/town-city-magazine/july-august-2019/cybersecurity-best-practices-municipalities?utm
16. NIST. (2024, February 26). *The NIST Cybersecurity Framework (CSF) 2.0*. National Institute of Standards and Technology. https://www.nist.gov/cyberframework
17. Norris, D. F., Mateczun, L., Joshi, A., & Finin, T. (2018). Cybersecurity at the grassroots: American local governments and the challenges of internet security. *Journal of Homeland Security and Emergency Management*, *15*(3), 20170048.
18. ResoluteGuard. (2025, April 17). *Cybersecurity Challenges for Local Governments in 2025: What Every City and Town Must Know - ResoluteGuard*. ResoluteGuard - ResoluteGuard. https://resoluteguard.com/cybersecurity-challenges-for-local-governments-in-2025-what-every-city-and-town-must-know/?utm
19. Smith, E. (2024). *Local Government Transformation: Gloucester City Council Cyber Attack*. Govnet.co.uk. https://blog.govnet.co.uk/technology/local-government-transformation-gloucester-city-council-cyber-attack
20. VisioneerIT. (2025, January 2). *10 best practices for improving cyber security in Local Governments*. Visioneerit.com; publisher. https://www.visioneerit.com/blog/cyber-security-local-gov?utm