Cyberattacks in government organizations: A systematic literature review of attack types and mitigation strategies.

Dimaz Cahya Ardhi [a], Dwi Puspita Sari[b], Benjamin Yankson[c]*

[a] College of Emergency Preparedness, Homeland Security and Cybersecurity, University at Albany, State University of New York, USA, dardhi@albany.edu, 0009-0006-9306-0820

[b] College of Emergency Preparedness, Homeland Security and Cybersecurity, University at Albany, State University of New York, USA, dsari@albany.edu, 0009-0002-7451-439X

[c] College of Emergency Preparedness, Homeland Security and Cybersecurity, University at Albany, State University of New York, USA, byankson@albany.edu, 0000-0003-3306-3748

Submitted: 31 January 2025, Revised: 26 March 2025, Accepted: 21 April 2025, Published: 22 May 2025

Abstract. In the digital government era, the government must protect citizens' data from cyberattacks to gain public trust. This study aims to identify the type of cyberattack incidents in government organizations and the implementation strategies to prevent cyberattacks. In this study, we conduct the Preferred Reporting Items for Systematic Reviews and Meta-Analysis (PRISMA) approach to answer our research questions. It performs a detailed analysis based on 50 peer-reviewed articles published in the conference proceedings and journals from January 2020 to December 2024. Those articles are retrieved from five databases: ACM Digital Library, Engineering Village, IEEE Xplore, the University at Albany Library, and Web of Science. The results revealed six types of cyberattacks in government organizations: malware, denial-of-service attacks, phishing attacks, false data injection, supply chain attacks, and advanced persistent threats. Furthermore, our review showed that four strategies have been implemented to prevent cyberattacks: 1) developing national cybersecurity strategies and frameworks, 2) building cyber defense capacity, 3) enhancing infrastructure resilience, and 4) education, training, and awareness. This study contributes to the field by providing different types of cyberattacks associated with government organizations and presenting a centralized and comprehensive analysis of research work in security, which is an excellent resource for other researchers in a similar field. Finally, this study also offers practical implications for government organizations, providing strategies to help them prevent cyberattacks.

Keywords. Cyberattack, cybersecurity, public sector, government organization.
Poster, DOI: https://doi.org/10.59490/dgo.2025.1021

1. Introduction

It is undeniable that the use of information and communication technologies (ICTs) in government organizations has become essential as a part of the digital government and modern society. The digital government aims to expedite the administrative process in government organizations (Frandell & Feeney, 2022). Furthermore, ICT integration has become increasingly prevalent, but at the same time, it is also associated with cyber risks, including cyberattacks (Frandell & Feeney, 2022). The risk can be caused by the fact that, in the digital government, the government stores its data online or in the cloud. Cyberattacks have occurred globally in both the private and public sectors, including financial services, government administration, insurance, and other industries. The increase in cyberattack incidents has drawn the attention of many researchers to study cyberattacks in organizations.

The existing literature concentrates on the private sector due to prominent cases, including data breaches at big companies such as Yahoo, Equifax, and Capital One (Khan et al., 2022). For example, Starbucks, a company with chain stores worldwide, experienced a ransomware attack that impacted 11,000 of its branches in North America, requiring employees to be scheduled manually (Watkins, 2024). However, there is scarce literature focusing on cyberattacks in government organizations. This study aims to shed light on various types of cyberattack incidents in government organizations and the strategies these organizations have implemented to prevent and address cyberattacks. Two research questions guided our study: (1) What type of cyberattacks occurred in government organizations? and (2) What strategies has the government employed to prevent cyberattacks? In order to answer these research questions, this study employed a Systematic Literature Review (SLR) approach. In particular, in this study, we apply the PRISMA approach to answer our research questions.

2. Research Design

The research design section is divided into two sub-sections: search strategies and review method. First, we describe the search strategies apply in this SLR, including the keywords used and the various sources of articles included in our search. Second, we elaborate on the steps involved in identifying the articles included in this study.

2.1 Search strategies

In our study, we include five databases for articles searches in our analysis: ACM Digital Library, Engineering Village, IEEE Xplore, the University at Albany Library, and Web of Science. In all our searches, we use the following search words: “cyber attack” OR “cyber-attack” OR “cyberattack” AND “public sector” OR “government”.

2.2 Review method

In order to ensure the clarity, transparency, and quality of this systematic literature review, this study follows the SLR using the PRISMA approach to help us better understand the cyberattack types and strategies to prevent and mitigate those different attacks in government organizations (see Figure 1 below). Figure 1 below illustrates a flow diagram of the PRISMA approach, which outlines our method, divided into two main stages: identification and screening. Initially, we identified 785 articles that included the keywords. However, we excluded 735 articles because those do not meet the eligibility criteria. Finally, after reading the full text and checking the eligibility criteria, we included 50 articles for the review.

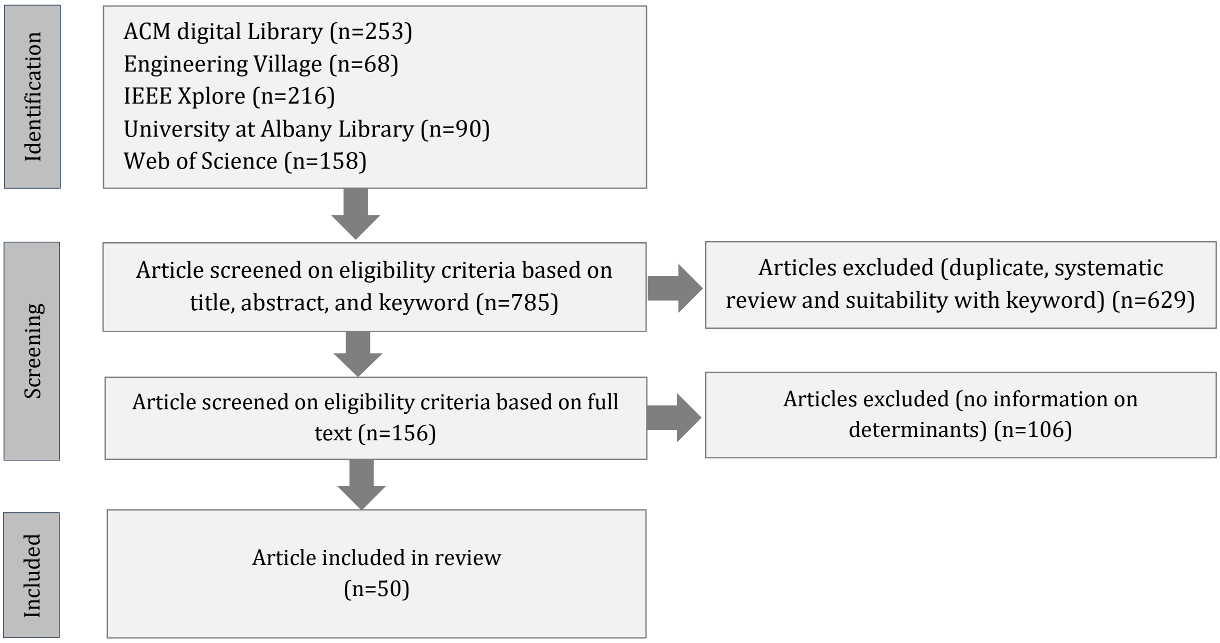
Identification
ACM digital Library (n=253)
Engineering Village (n=68)
IEEE Xplore (n=216)
University at Albany Library (n=90)
Web of Science (n=158)
Screening
Article screened on eligibility criteria based on title, abstract, and keyword (n=785)
Articles excluded (duplicate, systematic review and suitability with keyword) (n=629)
Article screened on eligibility criteria based on full text (n=156)
Articles excluded (no information on determinants) (n=106)
Included
Article included in review (n=50)

Fig. 1 – Flow diagram with PRISMA approach.

Table 1 below presents the characteristics of the included studies, which illustrate the selection of articles from five different database resources. Table 1 below shows the characteristics of the studies included in our review, including the number of articles retrieved from the database and selected for our review.

Tab. 1 – Sources of included studies.

Database Resource	Article Retrieved	Article Selected
ACM Digital Library	253	5
Engineering Village	68	6
IEEE Xplore	216	18
University at Albany Library	90	16
Web of Science	158	5

Table 2 below shows the characteristics of the studies included in our systematic literature review. It showcases the diversity of article publications in terms of sources, methods, and geographical regions. Out of the 50 articles included in this review, 28 were published in conference proceedings, while 22 were published in journals.

Tab. 2 – Characteristics of included studies.

		Number of publication(s)
Source	Journal	22
	Conference proceeding	28
Method	Qualitative	22
	Quantitative	13
	Mix Method	15
Geographic Region	Europe	8
	North America	10
	Central America	1
	South America	4
	East Asia	4
	Middle East Asia	1
	South Asia	1
	Southeast Asia	2
	Africa	1
	Oceania	1
	Multiple countries	8

3. Findings and Discussion

3.1 Cyberattack types

Our study indicates that the three most common government cyberattacks are malware, denial of service (DoS) and denial-of-service (DDoS), and phishing. First, ransomware attacks disrupt operations or steal sensitive data, compromising grid reliability and security (Atkins, 2021; Avraam et al., 2023). Second, DoS and DDoS attacks cause significant disruption to the government system, including communication disruption, data breaches, and attacks on the cloud service (Byeon & Suh, 2020; Aljuaid & Alshamrani, 2024). Porter and Tan (2022) in their study discuss distributed DDoS attacks as the primary method used in the first cyberattack on Estonian government organizations in 2007, targeting parliaments, banks, and ministries. Third, phishing attacks are a common cyberattack technique that targets government organizations (Drummonds et al., 2022; Park et al., 2023). In addition to these three attacks, the literature also discusses more sophisticated threats, such as code injection attacks.

Our review reveals that government organizations were vulnerable to three other types of cyberattacks: False Data Injection (FDI), supply chain attacks, and advanced persistent threats (APTs). FDI presents crucial threats to High-Voltage Direct Current (HVDC) systems under an Exchange Frequency Containment Reserve control (Avraam et al., 2023; Ramadhan et al., 2023). Furthermore, supply chain attacks indirectly target third-party vendors to infiltrate government systems. For example, the 2020 SolarWinds hack exemplifies a supply chain attack within the Orion software updates of the Texas-based IT firm SolarWinds, and government organizations, including the Department of Homeland Security and Microsoft (Porter & Tan, 2022; Wang, 2021). Attackers compromised the software build system to insert malware into legitimate Orion updates, which were then unknowingly installed by thousands of governments and corporate users. Finally, APTs, also known as national cyber-attacks, target the government in any organization and are hard to detect (Atkins, 2022; Kumar et al., 2022).

3.2 Strategies to prevent and mitigate cyberattacks

We discover four key strategies commonly implemented by governments to prevent cyberattacks. First, government organizations develop a national cybersecurity strategy. The existing literature shows that the United Kingdom government established a national cybersecurity strategy to strengthen resilience at the organizational and national levels (Klumpes, 2023). The literature mentions that national cybersecurity is updated periodically in 2011, 2016, and 2022 (Klumpes, 2023). Additionally, Swedish government organizations implemented the ISO/IEC 27001 framework for compliance in government organizations, including municipalities and regions (Magnusson et al., 2023). Furthermore, Japan has implemented strategies and measures to strengthen cybersecurity, covering legal, policy, and operational aspects, starting from an action plan in 2000, the national strategy on information security since 2006, and a cyber security strategy in 2013 (Ukhanova, 2022).

Second, government organizations build a strong cyber defense capacity, which includes establishing a cyber defense unit, command, and response (Porter & Tan, 2022) or cyber response (Mahima, 2021). For example, the Estonian government established the Estonian Defense League Cyber Unit, which united computer programmers from the private and public sectors. Additionally, in 2018, Estonia established a cyber command comprising 300 military and civilian professionals, including those from the private sector. Besides developing a defense cyber unit, government organizations' action to build a strong cyber defense is creating an emergency response team (Hossain et al., 2021; Riebe et al., 2021).

Third, government organizations have started to enhance cybersecurity infrastructure by developing resilient infrastructure and implementing a detection system (Ramadhan et al., 2023; Suresh & Madhavu, 2021). For example, using sensors and normalized correlation to detect anomalies in HVDC systems effectively identifies cyberattacks, such as measurement delay, missing data, and false data injection, as demonstrated through simulations in Jeju Island, South Korea (Ramadhan et al., 2023).

Fourth, education, training, and awareness programs are essential to foster a cybersecurity-aware workforce and informed public. Keshvadi (2023) suggested the importance of specialized cybersecurity education programs designed for non-technical staff based on the results of a research survey of senior cybersecurity leaders from public and private sectors in different countries, including Australia, Europe, and the United States.

4. Conclusion

Our review shows six cyberattacks that occurred in government organizations: malware, DoS and DDoS, phishing attack, FDI, supply chain attack, and APTs. In this study, the review shows prevention strategies for cyberattacks: developing national cybersecurity strategies and frameworks, building strong cyber defense capacity, enhancing the resilience of infrastructure, and providing education, training, and awareness. Our study reveals a notable lack of empirical study examining cyberattacks and strategies to prevent and mitigate them in government organizations.

This study has two main contributions to the field. First, this study contributes to the limited literature by proposing a specific type of cyberattack explicitly associated with government organizations. Second, this study presents a centralized and comprehensive analysis of research work in security, which will serve as an excellent resource for other researchers in a similar field. Limitation of our study focuses exclusively on two primary keywords: cyber-attack/cyber attack/cyberattack and public sector/government. In the future, we need to incorporate additional keywords into our searches, like cybersecurity and cyber resilience.

Acknowledgement

- **Contributor Statement***: Author 1: conceptualization, data curation, formal analysis, investigation, and methodology, writing - original draft; Author 2: conceptualization, formal analysis, investigation, and methodology, writing - original draft; Author 3: supervision and writing - review and editing.
- **Use of AI***: During the preparation of this work, the authors used Grammarly in order to check the writing grammar. After using this tool/service, the author(s) reviewed, edited, made the content their own and validated the outcome as needed, and take(s) full responsibility for the content of the publication.
- **Conflict Of Interest (COI)***: There is no conflict of interest.

References

Aldabbagh, A. M., & Ilyas, M. (2021). Smart city GIS mapping and analysis of intrusion detection. *IEEE Xplore*. https://doi.org/10.1109/ICECCT52121.2021.9616943

Aljuaid, W. H., & Alshamrani, S. S. (2024). A deep learning approach for intrusion detection systems in cloud computing environments. *Applied Sciences*, *14*(13), 5381. https://doi.org/10.3390/app14135381

Atkins, S., & Lawson, C. (2021). An improvised patchwork: Success and failure in cybersecurity policy for critical infrastructure. *Public Administration Review*, *81*(5). https://doi.org/10.1111/puar.13322

Atkins, S., & Lawson, C. (2022). Integration of effort: Securing critical infrastructure from cyberattack. *Public Administration Review*, *82*(4), 771-775. https://doi.org/10.1111/puar.13493

Avraam, C., Ceferino, L., & Dvorkin, Y. (2023). Operational and economy-wide impacts of compound cyber-attacks and extreme weather events on electric power networks. *Applied Energy*, *349*, 121577-121577. https://doi.org/10.1016/j.apenergy.2023.121577

Byeon, S., & Suh, W. (2020). A study on the government's countermeasures against cyber attacks. *IEEE Xplore.*

https://doi.org/10.1109/BigComp48618.2020.00-17

Drummonds, A. O., Henry, J., & Mirpuri, K. (2022). An analysis of website phishing awareness in Jamaica. *IEEE Xplore*. https://doi.org/10.1109/SoutheastCon48659.2022.9764050

Frandell, A., & Feeney, M. (2022). Cybersecurity threats in local government: A sociotechnical perspective. *The American Review of Public Administration*, *52*(8), 558–572. https://doi.org/10.1177/02750740221125432

Hossain, Z., Zaman, G. K., & Taher, K. A. (2021). Cyber emergency response team for Bangladesh. *IEEE Xplore*. https://doi.org/10.1109/ICICT4SD50815.2021.9396922

Keshvadi, S. (2023). Enhancing western organizational cybersecurity resilience through tailored education for non-technical employees. *IEEE International Humanitarian Technology Conference (IHTC)*, 1-6. https://doi.org/10.1109/ihtc58960.2023.10508824

Khan, S., Kabanov, I., Hua, Y., & Madnick, S. (2022). A systematic analysis of the Capital One data breach: Critical lessons learned. *ACM Transactions on Privacy and Security*, *26*(1). https://doi.org/10.1145/3546068

Klumpes, P. (2023). Coordination of cybersecurity risk management in the U.K. insurance sector. *The Geneva Papers on Risk and Insurance - Issues and Practice*. https://doi.org/10.1057/s41288-023-00287-9

Kumar, G. K. S., Prakasha, K. K., & Muniyal, B. (2022). ACH reference model - A model of architecture to handle advanced cyberattacks. *2022 Second International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies (ICAECT)*. https://doi.org/10.1109/icaect54875.2022.9808076

Magnusson, L., Dalipi, F., & Elm, P. (2023). Cybersecurity compliance in the public sector: Are the best security practices properly addressed? *Communications in Computer and Information Science*, 219-226. https://doi.org/10.1007/978-3-031-36001-5_28

Mahima, D. (2021). Cyber threat in public sector: Modeling an incident response framework. *IEEE Xplore*. https://doi.org/10.1109/ICIPTM52218.2021.9388333

Park, H., Lim, K., Kim, D., Yu, D., & Koo, H. (2023). Demystifying the regional phishing landscape in South Korea. *IEEE Access*, 11, 130131-130143. https://doi.org/10.1109/access.2023.3333883

Porter, T., & Tan, N. (2022). An integrated complex adaptive governmental policy response to cyberthreats. *Journal of Economic Policy Reform*, 1-15. https://doi.org/10.1080/17487870.2022.2125390

Ramadhan, U. F., Lee, J., & Yoon, M. (2023). A comprehensive study of cyber attack mitigation with the exchange of frequency containment reserves control in a multi-infeed direct current power system. *Sensors*, *23*(4), 1964. https://doi.org/10.3390/s23041964

Riebe, T., Kaufhold, M.-A., & Reuter, C. (2021). The impact of organizational structure and technology use on collaborative practices in computer emergency response teams: An empirical study. *Proceedings of the ACM on Human-Computer Interaction*, *5*(CSCW2), 1-30. https://doi.org/10.1145/3479865

Suresh, P., & Madhavu, M. L. (2021). Insider attack: Internal cyber attack detection using machine learning. *12th International Conference on Computing Communication and Networking Technologies (ICCCNT)*. https://doi.org/10.1109/icccnt51525.2021.9579549

Ukhanova, E. (2022). Cybersecurity and cyber defence strategies of Japan. *SHS Web of Conferences*, *134*, 00159. https://doi.org/10.1051/shsconf/202213400159

Wang, X. (2021). On the feasibility of detecting software supply chain attacks. *IEEE Xplore*. https://doi.org/10.1109/MILCOM52596.2021.965290

Watkins, A. (2024). *Starbucks among companies affected by ransomware attack*. The New York Times. https://www.nytimes.com/2024/11/26/business/blue-yonder-ransomware-attack-starbucks.html