المجلة الدولية فى العلوم القانونية والمعلوماتية

The Role of Insurance and Cyber Security Protection in Government Institutions

Yasser Elmalik Ahmed Seleman[1,*] *and Naglaa Abdel Lateef Saeed Fadul*[2]

[1] Assistant professor, College of Computer Science, University of Technology, Sudan.
[2] Assistant professor, Information Systems Department, Islamic University of Minnesota.

Received: 10 Sep. 2025, Revised: 30 Sep. 2025, Accepted: 20 Oct. 2025.
Published online: 1 Jan. 2026.

Abstract: The role of insurance and cybersecurity protection in government institutions has become a critical global concern. Information security is now intrinsically linked to national security in most countries, as cyberattacks targeting vital infrastructures—such as communication and electronic systems—can have widespread effects that transcend national borders. Such attacks can disrupt services, compromise sensitive information, and threaten the stability of entire regions. Therefore, cybersecurity in government institutions plays a vital role in protecting sensitive data, ensuring the availability and integrity of essential public services, safeguarding national interests, and maintaining citizens' trust in digital governance. Achieving these goals requires robust technical defenses, comprehensive governance frameworks, and coordinated strategies to defend against sophisticated cyber threats and ensure operational continuity.

Keywords: cyber security, cybercrime, digital environment, cultural Invasion, information systems, computers, electronic.

*Corresponding author e-mail: Dr.yaserking359@hotmail.com

دور التأمين وحماية الأمن السيبراني في المؤسسات الحكومية

ياسر الملك أحمد سليمان[1] و نجلاء عبد اللطيف سعيد فضل[2]

1 أستاذ مساعد، كلية علوم الحاسوب، جامعة التكنولوجيا، السودان.
2 أستاذ مساعد، قسم نظم المعلومات، الجامعة الإسلامية في مينيسوتا.

الملخص: أصبح دور التأمين وحماية الأمن السيبراني في المؤسسات الحكومية مصدر قلق عالمي بالغ الأهمية. يرتبط أمن المعلومات ارتباطًا وثيقًا بالأمن القومي في معظم الدول، إذ يمكن أن تُخلّف الهجمات السيبرانية التي تستهدف البنى التحتية الحيوية - مثل أنظمة الاتصالات والأنظمة الإلكترونية - آثارًا واسعة النطاق تتجاوز الحدود الوطنية. ويمكن لهذه الهجمات أن تُعطّل الخدمات، وتُعرّض المعلومات الحساسة للخطر، وتهدد استقرار مناطق بأكملها. لذلك، يلعب الأمن السيبراني في المؤسسات الحكومية دورًا حيويًا في حماية البيانات الحساسة، وضمان توافر الخدمات العامة الأساسية وسلامتها، وحماية المصالح الوطنية، والحفاظ على ثقة المواطنين في الحوكمة الرقمية. ويتطلب تحقيق هذه الأهداف دفاعات تقنية متينة، وأطر حوكمة شاملة، واستراتيجيات منسقة للدفاع ضد التهديدات السيبرانية المعقدة وضمان استمرارية العمليات.

الكلمات المفتاحية: التأمين، حماية، الأمن السيبراني، المؤسسات الحكومية، أمن المعلومات.

1. Introduction

In today's digital era, government institutions face unprecedented cybersecurity challenges as they strive to protect sensitive data and critical infrastructure from a growing array of cyber threats. Ensuring cybersecurity is essential not only for maintaining public trust but also for safeguarding national security. Cyberattacks targeting government systems can disrupt essential services, compromise classified information, and undermine public confidence in digital governance. Government cyber security practices increasingly involve implementing advanced strategies and solutions designed to protect networks at the local, state, and international levels. Since the public sector manages vast amounts of data—including citizen records, financial transactions, and national intelligence any breach could lead to severe consequences such as compromised national security and threats to public safety.

As a result, information security has become a top priority for policymakers worldwide. Governments, as the largest producers and custodians of public and private data, carry the responsibility of establishing strong cybersecurity frameworks, developing relevant regulations, and enforcing compliance mechanisms that define the boundaries and responsibilities of digital protection. 2 .Research Problems:
Despite growing awareness and investment, government institutions continue to face significant cybersecurity risks due to the complexity and sensitivity of their operations. Key research problems include:

- Supply chain vulnerabilities: Government agencies rely on multiple external vendors and contractors, increasing the risk of supply chain attacks. Ensuring the security of the entire supply chain is crucial to prevent exploitation of weak links (e.g. agencies have been impacted by software supply chain compromises.
- Sophisticated cyber threats: The evolving nature of cyberattacks demands equally advanced defense mechanisms. Government systems are frequent targets for highly skilled attackers seeking to compromise critical national infrastructure.
- High exposure risk: Even single system vulnerability can result in large-scale consequences, including data breaches, operational disruption, loss of public trust, and threats to national security.

These challenges highlight the urgent need for advanced cybersecurity measures, proactive threat detection, and resilient incident response strategies within the public sector.

2. Importance of Research:

Studying cyber security in government institutions is vital to ensure the protection of sensitive citizen data, national intelligence, and critical infrastructure. It helps governments prevent, detect, and respond effectively to cyber incidents, thus maintaining operational continuity and reinforcing public trust in digital government services.

Furthermore, cyber security education and awareness programs empower government employees to recognize and respond to threats such as phishing, ransomware, and social engineering. By minimizing human error, such initiatives enhance the overall cyber resilience of government institutions and strengthen the protection of national interests in an increasingly interconnected world.

3. Research Questions:

The study seeks to address key questions related to the protection of government institutions against cyber threats and the role of cybersecurity insurance in mitigating their effects.

The main research questions are as follows:

1. What are the primary threats and risks associated with cybersecurity breaches in government institutions?
2. How do cyberattacks and electronic intrusions target the information systems of ministries and state agencies?
3. What technical and procedural measures are currently in place to prevent or limit electronic violations?
4. To what extent do technical measures and cybersecurity insurance mechanisms contribute to protecting government institutions from cyberattacks?
5. How can a comprehensive framework enhance cybersecurity resilience and ensure operational continuity across public sector systems?

These questions guide the research toward understanding both the technical and managerial dimensions of cybersecurity within government institutions. They also aim to explore how insurance mechanisms can support national digital resilience by mitigating financial and operational risks arising from cyber incidents.

4. Research objectives:

The objectives of this study are to:

1. Analyze the current cybersecurity strategies implemented in government institutions and assess their effectiveness.
2. Identify the major risks and vulnerabilities affecting government networks and supply chains.
3. Explore the role of cybersecurity insurance in mitigating the financial and operational impacts of cyber incidents.
4. Examine best practices for identity and access management (IAM) to prevent insider threats.
5. Recommend a comprehensive framework to enhance cybersecurity readiness and resilience across government sectors.

Cybersecurity and insider threat management underscore the need for robust identity and access control policies. While many institutions have begun updating their strategies in line with global cybersecurity trends, others still struggle with challenges related to inadequate training, outdated systems, and limited awareness of emerging threats.

5. Research Methodology:

This study employs a descriptive–analytical research methodology, combining both qualitative and conceptual approaches to examine the intersection between cybersecurity protection and insurance in government institutions.

- Descriptive Approach:

The descriptive component provides a detailed overview of the current cybersecurity landscape within government agencies. It outlines existing policies, types of threats, and the protective measures in place to secure sensitive data, national infrastructure, and digital services.

- Analytical Approach:

The analytical component evaluates the effectiveness of these measures, identifying gaps, vulnerabilities, and potential areas of improvement. It also analyzes how cyber insurance can complement traditional cybersecurity strategies by providing financial resilience and risk mitigation.

Data for this research is derived from:

- Review and synthesis of existing literature and case studies on cybersecurity in government institutions;
- Analysis of international frameworks and standards such as the Government Cyber Security Strategy (GCSS) and Government Security Operation Coordination (GSOC) models;
- Examination of academic journals, reports, and policy documents to explore best practices in digital governance, risk management, and cyber insurance.

The study aims to connect theoretical insights with practical applications to develop a comprehensive understanding of how governments can strengthen their cyber defense posture through multi-layered protection strategies and insurance-based risk management.

Chapter Two

Practical applications

6. Introduction:

In the modern digital era, government institutions have become prime targets for cyber threats due to their management of sensitive data, critical infrastructure, and national security operations. The increasing dependence on digital systems for governance, communication, and public services has expanded the potential attack surface, exposing governmental entities to threats ranging from ransomware and phishing attacks to large-scale breaches of national databases. Cyber security in the public sector is no longer merely a technical concern it is a cornerstone of national resilience and public trust. Government agencies are responsible for protecting extensive networks that store personal information, economic data, and classified intelligence. Any compromise of these systems can have severe consequences, including

operational disruption, economic loss, and erosion of citizen confidence in digital governance. To address these challenges, governments worldwide are developing comprehensive cybersecurity strategies that integrate policy frameworks, advanced defense technologies, and organizational governance. Such strategies focus on protecting public sector systems, detecting and responding to incidents, and strengthening supply chain security. They also emphasize capacity building through education, awareness, and collaboration among government, academia, and private industry.

In addition to preventive measures, modern government cybersecurity frameworks incorporate risk management, incident response, and insurance mechanisms to mitigate financial losses from cyber incidents. As Csonka (2020) noted, the interconnectedness of digital systems means that attacks on one nation's critical infrastructure can have global repercussions—making international cooperation in cyber security essential.

Therefore, this research explores the role of cybersecurity protection and insurance in government institutions, focusing on the mechanisms, strategies, and layered defenses necessary to secure government systems and ensure the continuity of national digital operations. The study highlights the importance of the Government Security Operation Coordination (GSOC) model, the core objectives of national cybersecurity strategies, and the essential layers of protection—ranging from IoT and cloud security to data, network, and endpoint defense.

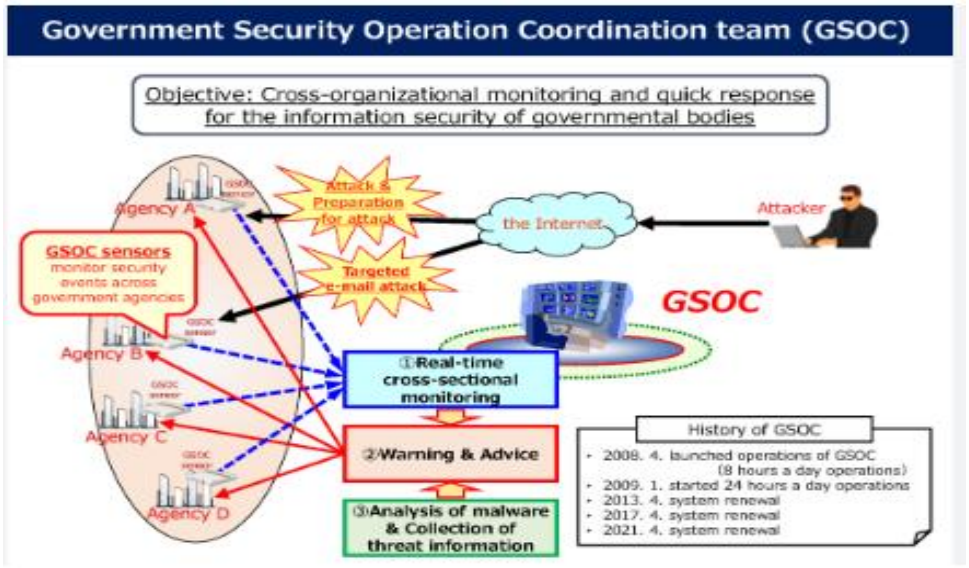

Fig. 1: Government Security Operation Coordination Team (GSOC) [1]

Government Security Operation Coordination Team (GSOC) and its role in cross-organizational monitoring and response to cyber threats.

Cybercrime represents a significant threat to public services, businesses, individuals, and society at large. Therefore, cybersecurity is a priority area for government institutions, which must work collaboratively with business, academia, and other stakeholders to ensure that national infrastructure (NI) is protected as effectively as possible. Governments bear responsibility for ensuring that public services maintain trust and resilience by safeguarding personal and organizational data.

The Government Cyber Security Strategy (GCSS) typically represents a comprehensive plan to protect citizens, organizations, and critical infrastructure from cyber threats. Its main goals include[2]:

1. Hardening public sector systems against attacks.
2. Detecting and responding effectively to incidents.
3. Securing digital supply chains.
4. Promoting a skilled cybersecurity workforce through national and international collaboration.

1 _ *D'Souza, 2021; Tsohou & Kokolakis, 2023*

2 - Ramirez, M, Ariza, L., 2022,14(3).

5. Disrupting attackers through intelligence sharing and coordinated monitoring.
6. Investing in future capabilities, such as real-time threat analysis and cyber insurance adoption.

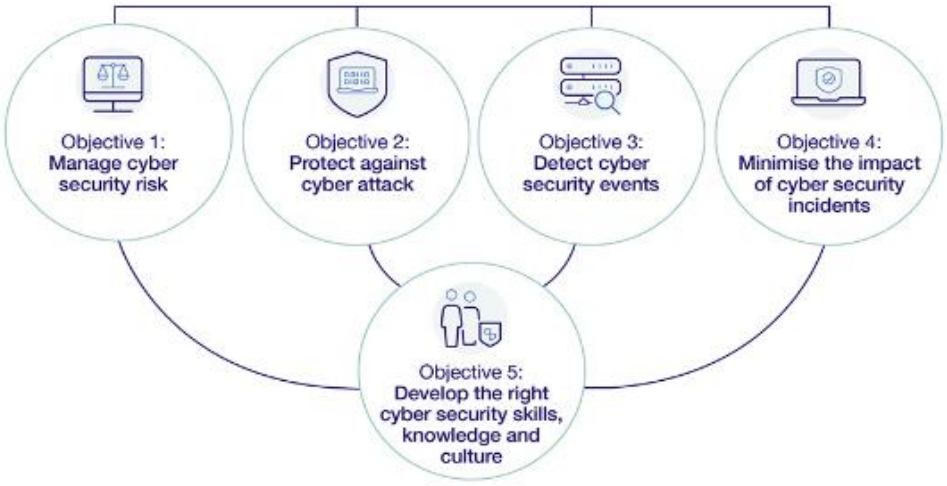

Fig. 2: Government Cyber Security Strategy [3]

Types of Protections in Government Institutions:

To meet these objectives, government agencies must implement a range of layered protections that address the most common and severe cyber threats. These include:

- Internet of Things (IoT) Security: Many critical infrastructures are managed by IoT devices, which often contain unpatched vulnerabilities. Proper IoT security ensures devices are not exploited by botnets or used as unauthorized access points.
- Data Security: Governments handle vast volumes of sensitive information, including citizen records and classified intelligence. Protecting this data against breaches, ransomware, and unauthorized disclosure is vital for both national security and public trust.
- Cloud Security: With rapid adoption of cloud services for scalability and efficiency, misconfigurations and weak access controls present significant risks. Strong governance and third-party risk management are necessary to secure cloud-based assets.
- Network Security: Network defenses are foundational to cybersecurity. Effective network monitoring and controls prevent unauthorized access and restrict lateral movement of attackers within government systems.
- Application Security: Government services (e.g., tax portals, healthcare systems) rely on applications that must be protected from denial-of-service attacks, injection attacks, and data compromise. Application security tools such as Web Application Firewalls (WAFs) safeguard both services and data.
- Endpoint Security: Government-issued laptops, desktops, and mobile devices are frequent attack targets. Endpoint detection and response (EDR) solutions are critical to prevent malware infections and enable rapid remediation.
- Mobile Security: As mobile devices become more common in government operations, ensuring their protection against mobile malware, insecure apps, and unauthorized access is vital for maintaining secure communication and services.

7. Government Cyber security Strategy and Protections:

Government institutions require a comprehensive cybersecurity strategy to safeguard sensitive information, critical infrastructure, and public trust. Effective strategies integrate both technical defenses and organizational governance

3 _ *D'Souza, 2021; Tsohou & Kokolakis, 2023*

mechanisms to ensure resilience, coordination, and rapid response to cyber incidents[4].

7.1 Government Security Operation Coordination (GSOC)

As illustrated in Figure 1, the Government Security Operation Coordination Team (GSOC) plays a pivotal role in cross-organizational monitoring and quick response for government information systems. GSOC sensors are deployed across multiple agencies to:

- Conduct real-time cross-sectional monitoring of threats.

- Provide warnings and advice to government institutions.

- Enable analysis of malware and the collection of threat intelligence.

This coordinated monitoring helps prevent attacks such as targeted email phishing, denial-of-service attempts, and infrastructure-level disruptions. By enabling shared situational awareness, GSOC strengthens the government's ability to detect and mitigate sophisticated attacks before they escalate into national crises [5].

7.2 Cyber security Strategy Objectives:

A robust government cyber security strategy must go beyond detection and response to address resilience, awareness, and proactive protection. Figure 2 highlights five key objectives that governments should pursue:

1. Manage cybersecurity risk – Establishing risk-based policies to prioritize resources and address vulnerabilities.
2. Protect against cyberattacks – Deploying strong defenses to prevent unauthorized access and disruption.
3. Detect cybersecurity events – Implementing monitoring systems to identify incidents in real time.
4. Minimize the impact of incidents – Ensuring continuity of critical government services during and after cyberattacks.
5. Develop skills and culture – Building human capacity, awareness, and resilience among government employees and stakeholders.

5.3 Types of Cyber security Protections:

To achieve the above objectives, government agencies must adopt layered cybersecurity protections tailored to their unique environments. These protections include:

- Internet of Things (IoT) Security: Protecting IoT devices in critical infrastructure from botnets and unpatched vulnerabilities [6] .
- Data Security: Safeguarding citizen records, financial transactions, and classified intelligence against breaches and ransomware[7].
- Cloud Security: Managing risks in cloud-based systems by strengthening configuration management, access controls, and vendor oversight [8].
- Network Security: Implementing network defenses that prevent intrusions and limit lateral attacker movement.
- Application Security: Securing government services (e.g., tax portals, healthcare systems) against exploitation through AppSec and Web Application Firewalls (WAFs) .
- Endpoint Security: Deploying endpoint detection and response (EDR) solutions on government devices to prevent malware infections.
- Mobile Security: Protecting mobile devices used for official operations against malware and unauthorized access.

These layers of defense form a comprehensive security ecosystem that enhances protection across devices, networks, and applications, ensuring the resilience of critical government services.

8. Conclusion:

4 -D'Souza, 2021; Tsohou & Kokolakis, 2023

5 -Wang et al., 2019.

6 -Csonka, 2020.

7 - Tsohou & Kokolakis, 2023

8 - Wang et al., 2019; Woods, 2017

Cybersecurity has become an indispensable pillar of governance in the modern digital era. As government institutions increasingly rely on information systems to manage critical infrastructure, citizen data, and national security operations, they are exposed to a growing spectrum of cyber threats. This research emphasized that cybersecurity protection and insurance are vital mechanisms for safeguarding public sector systems and ensuring operational continuity during and after cyber incidents.

The study revealed that Government Security Operation Coordination (GSOC) plays a central role in strengthening cyber resilience by enabling cross-agency monitoring, early detection, and coordinated incident response. Moreover, the Government Cyber Security Strategy (GCSS) highlights five essential objectives risk management, protection, detection, mitigation, and capacity building that collectively forms the foundation of an effective national cyber security framework.

Implementing layered protections, including IoT, data, cloud, network, application, endpoint, and mobile security, is crucial to defending against sophisticated attacks. These measures, when combined with cyber insurance policies, not only minimize financial and operational damage but also enhance institutional preparedness and public trust.

The research further supports the argument that cybersecurity is not merely a technical concern but a matter of national resilience and policy governance. Governments must therefore adopt a holistic approach that integrates technological defenses, regulatory frameworks, and human resource development. Collaboration among public institutions, private sectors, and academic organizations is equally essential to maintain adaptive and proactive defense mechanisms.

In conclusion, protecting government systems from cyber threats requires a synergy between prevention, preparedness, and recovery.

The incorporation of cyber insurance as a financial safeguard complements traditional cybersecurity strategies, ensuring long-term sustainability and trust in digital governance. Continuous investment in innovation, capacity building, and international cooperation remains imperative to address the evolving landscape of global cyber risks.

References:

[1] Ramirez, M, Ariza, L., and Miranda, M., The disclosure of information on security in listed companies in Latin America- proposal for a cyber-security disclosure index), journal of sustainability ,2022,14(3).

[2] Fortin, Anne and Heroux, S., (2020), (Cyber security disclosure by the companies on the SPP/TSX60, index, vol: 19, issue: 2, June, pp: 73-100.

[3] Reddt, M., & Reddy, G. (2020). A Study of Cyber Security Challenges and Its Emerging Trends on Latest Technologies, Peridot Technologies, 26 (9), 202-2020.

[4] Csonka P., (2020): Internet Crime, the Draft Council of Europe Convention on Cyber- Crime: A Response to the Challenge of Crime in the Age of the internet, Computer Law & Security Report, Vol.28, No.15.

[5] D'Souza, V. A., (2021): *CYBERSECURITY: Federal Agencies Need to Implement Critical Actions to Address Major Challenges*, U.S. Government Accountability Office (GAO-21-594T), Washington D.C.

[6] Tsohou, A., & Kokolakis, S., (2023): Cyber Insurance: State of the Art, Trends and Future Directions, Journal of Cybersecurity, Vol.9, No.1.

[7] Wang, S. S., Chen, Y., & Zhu, L., (2019): An Integrated Framework for Information Security Investment, Pacific-Basin Finance Journal, Vol.57, No.7.

[8] Romanosky, S., (2019): Content Analysis of Cyber Insurance Policies: How Do Carriers Underwrite Risk?, Journal of Cybersecurity, Vol.5, No.1.

[9] Woods, D., (2017): Policy Measures and Cyber Insurance: A Framework, Journal of Cyber Policy, Vol.2, No.2.