Enhancing Government Efficiency Through Cybersecurity Hardening

Shreyas Kumar[a], Anika Garg[b], Maitreya Niranjan[c]

[a]Texas A&M University, College Station, TX, USA, shreyas.kumar@tamu.edu, https://orcid.org/0009-0009-7035-9768
[b]Texas A&M University, College Station, TX, USA, https://orcid.org/0009-0000-6704-1761
[c]Texas A&M University, College Station, TX, USA, https://orcid.org/0009-0002-6282-3670

Submitted: 31 January 2025, Revised: 26 March 2025, Accepted: 21 April 2025, Published: 13 June 2025

Abstract. The rapid digitization of public sector services has fundamentally reshaped how governments operate, manage resources, and interact with citizens. From digital identity platforms to AI-enabled service portals, technology enables faster decision-making, seamless operations, and more responsive governance. Yet, this digital transformation introduces growing cyber risks, including ransomware, insider threats, and nation-state attacks. These risks not only threaten data privacy and national security but also undermine service reliability and institutional trust. To mitigate such threats and sustain innovation, cybersecurity hardening has emerged as a critical enabler of government efficiency. It includes proactive strategies such as continuous threat monitoring, network segmentation, encryption, and Zero Trust frameworks that reinforce operational continuity. While existing literature often frames cybersecurity as a compliance necessity, our research recasts it as a core strategic asset for enhancing public service performance. Specifically, we examine how cybersecurity contributes to resilience, reduces service disruptions, and improves resource allocation—three pillars of efficient governance. This approach aligns with emerging policy shifts, notably the formation of the U.S. Department of Government Efficiency (DOGE) in January 2025, which identifies cybersecurity as central to improving operational outcomes. Supported by similar initiatives in Texas, Kansas, and Louisiana, this paper situates cyber defense as a linchpin of modern administrative reform. By exploring real-world breach case studies and integrating economic modeling with cybersecurity strategy, we demonstrate how protecting systems is not just a cost-saving imperative but a means to power smarter, faster, and safer governance.

Keywords. Cybersecurity Hardening, Government Efficiency, Risk Management, Automation, Cost-Benefit Analysis.
Research paper, DOI: https://doi.org/10.59490/dgo.2025.1047

1. Introduction

The digitization of government services has transformed public administration, enabling efficient resource management, streamlined operations, and enhanced citizen engagement. From online tax filings to e-governance platforms, technology has become integral to the functioning of modern governments. However, this increasing reliance on digital infrastructure has also made governments vulnerable to an array of cybersecurity threats, including ransomware, data breaches, and state-sponsored cyberattacks. The consequences of these threats are far-reaching, impacting not only operational continuity but also national security, public trust, and the overall efficiency of government systems. Cybersecurity hardening has emerged as a critical strategy to mitigate these risks. This involves implementing advanced measures such as encryption, network segmentation, and continuous threat monitoring to safeguard sensitive data and ensure uninterrupted service delivery. While the technical aspects of cybersecurity hardening are well-documented, its broader implications for government efficiency remain underexplored. This paper examines how enhancing cybersecurity measures can improve the operational efficiency of government agencies, reduce costs associated with cyber incidents, and build resilience in the face of evolving threats. Government efficiency refers to the ability of public agencies to deliver services, manage resources, and execute operations in a timely, cost-effective, and streamlined manner that maximizes public value and minimizes waste or redundancy.

The intersection of cybersecurity and government efficiency highlights the critical role of robust digital transformation in modern governance, where technology streamlines operations, enhances service delivery, and fosters effective decision-making. Centralized data systems enable faster retrieval and updates, improving productivity and collaboration across departments while minimizing errors and redundancies. Real-time access to information equips decision-makers with actionable insights, transforming static data into dynamic tools for effective resource allocation. Digital transformation also fosters responsive public services, enabling governments to adapt to evolving priorities and citizen needs with agility. However, the rapid digitization of government operations exposes vulnerabilities to cyber threats such as data breaches and ransomware, which can disrupt services, compromise sensitive data, and erode public trust. Strong cybersecurity measures are essential to secure these digital systems, ensuring continuity of operations and reinforcing public confidence. By aligning cybersecurity with digital transformation efforts, governments can achieve operational resilience, sustain innovation, and deliver efficient, citizen-centric services in an increasingly complex digital landscape.

Drawing on computer science to analyze technical security measures, public administration to assess operational impacts, and economics to evaluate cost-benefit considerations, this study provides a holistic analysis of the intersection between cybersecurity and government efficiency. It includes case studies of significant government-related cyber incidents, shedding light on the financial, operational, and societal impacts of cyberattacks. By focusing on actionable strategies and policy recommendations, the study aims to inform decision-makers on how cybersecurity hardening can improve the operational efficiency of government agencies, mitigate the financial and operational impacts of cyber incidents, and build resilience against evolving cyber threats.

The U.S. Department of Government Efficiency (DOGE) has identified cybersecurity hardening as a cornerstone of its mission to optimize public service delivery and enhance the resilience of critical infrastructure (Gianfortune, 2025). As federal, state, and local governments accelerate their digital transformation efforts, the risk of cyberattacks has grown exponentially. High-profile incidents, such as the SolarWinds breach and the ransomware attack on the city of Atlanta, highlight the urgent need for robust cybersecurity measures to protect sensitive data and ensure the continuity of essential services.

The U.S. government has prioritized cybersecurity as a key component of its strategic goals, reflected in initiatives such as the Cybersecurity and Infrastructure Security Agency's (CISA) Continuous Diagnostics and Mitigation (CDM) program. These efforts aim to strengthen the security posture of federal agencies by providing real-time threat monitoring, vulnerability management, and automated incident response capabilities. Moreover, the Biden Administration's 2023 National Cybersecurity Strategy emphasizes public-private collaboration, supply chain security, and workforce development to address the growing complexity of cyber threats. (Jaikaran, 2023) Small- and medium-sized government entities face unique challenges, often lacking the resources and expertise needed to implement advanced cybersecurity measures. This paper underscores the importance of equipping such agencies with cost-effective tools and strategies to enhance their cyber resilience. By addressing these gaps, governments can minimize service disruptions, reduce remediation costs, and foster public trust in digital systems.

At its core, this research is motivated by the dual need to protect national assets and improve the efficiency of government operations. The focus on cybersecurity hardening not only aligns with DOGE's mission but also contributes to broader national priorities, including economic stability, public safety, and democratic integrity. By highlighting the intersection of cybersecurity and government efficiency, this paper seeks to provide actionable insights that support the development of resilient, cost-effective, and citizen-centric governance models.

2. Background

2.1. The rising cost of governance due to data breaches

As digitization accelerates, the frequency and sophistication of cyber threats continue to grow exponentially. The global cost of cybercrime is projected to surge from $9.22 trillion in 2024 to $13.82 trillion by 2028, as shown in 1. This alarming trajectory emphasizes the critical need for robust cybersecurity measures. Additionally, IBM's 2024 report on data breach costs highlights the increasing prevalence of cybersecurity incidents, with the global average cost of a data breach reaching $4.88 million in 2024—a 15% increase since 2020.

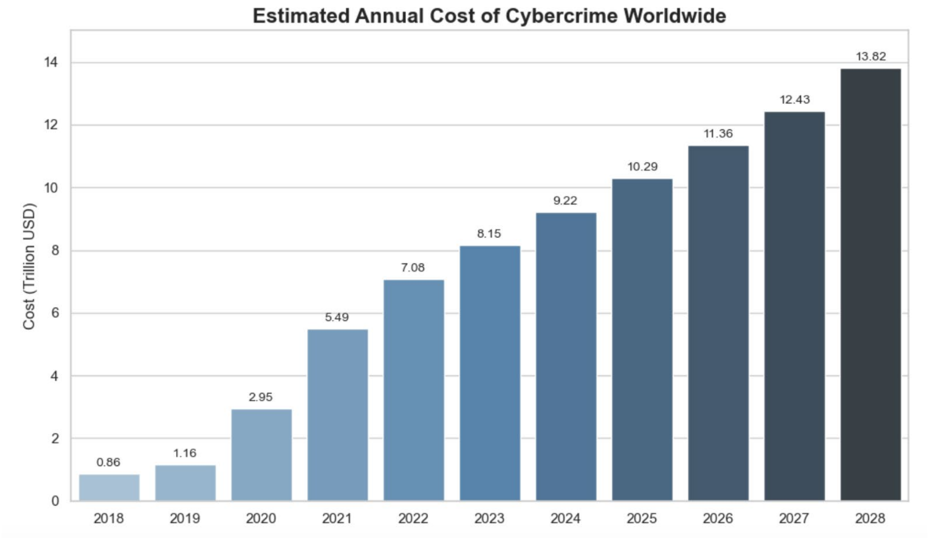

Fig. 1 – Estimated global cost of cybercrime and the rising cost of data breaches. Data sourced from Statista.

Governments and organizations face a diverse range of cyber threats, each with significant potential to disrupt operations and compromise sensitive information. Ransomware attacks, where malicious actors encrypt critical data and demand ransom payments for its release, pose a serious risk. For instance, the Costa Rica ransomware attack in 2022 paralyzed essential public services, causing widespread economic and operational damage (Nato, 2022). Phishing and social engineering tactics exploit human vulnerabilities through deceptive emails and messages to gain unauthorized access to systems (Kumar et al., 2024). Such attacks can lead to data breaches, as evidenced by the 2015 Office of Personnel Management (OPM) hack, where stolen credentials compromised millions of sensitive records (Gootman, 2016). State-sponsored cyber espionage, often in the form of advanced persistent threats (APTs) backed by nation-states, targets critical infrastructure and sensitive government data. The SolarWinds hack of 2020 exposed vulnerabilities in numerous U.S. federal agencies, raising national security concerns (Alkhadra et al., 2021). Furthermore, Distributed Denial of Service (DDoS) attacks represent another significant threat. These attacks overwhelm systems with excessive traffic, disrupting essential services. Governments and public institutions often become targets, impeding their ability to serve citizens. The diverse nature of these cyber threats demonstrates the need for comprehensive cybersecurity strategies and robust defense mechanisms to protect critical infrastructure and sensitive information.

The impacts of these cyber threats extend beyond financial losses. They compromise public trust, disrupt essential services, and expose sensitive data, which can have long-term implications for national security and societal stability. Recognizing the direct correlation between the rate of digitization and the scale of cybersecurity risks, governments must prioritize cybersecurity hardening to mitigate these threats effectively and ensure the continuity of public services.

In December 2015, a significant data breach exposed personal information of around 191 million U.S. voters due to a misconfigured database that was publicly accessible without security measures. This breach revealed sensitive data, including names, addresses, and party affiliations. The lack of basic security protocols and poor database configuration underscored the need for stringent data security measures and clear data ownership. The breach delayed remediation and highlighted the importance of proper configuration management and ownership accountability (Finkle, 2015).

Similarly, in 2022, Costa Rica faced a series of devastating ransomware attacks that targeted 27 public institutions, including the Ministry of Finance and the Costa Rican Social Security Fund. The attackers demanded millions in ransom, leading to severe operational disruptions. The government's refusal to pay the ransom resulted in an estimated economic loss of $125 million within the first 48 hours. The attack paralyzed essential services, including tax systems and healthcare records, demonstrating the far-reaching consequences of ransomware on public institutions and the economy. The national emergency declaration underscored the importance of robust cybersecurity defenses and incident response plans. (Nato, 2022)

While many governments have faced cyberattacks, some have proactively strengthened their security frameworks, preventing major incidents and ensuring the continued resilience of their digital infrastructures. Estonia, often hailed as a global leader in e-governance and cybersecurity, stands out with its robust infrastructure, including its Data Embassy and blockchain-secured systems (Bitton, 2022). These measures, combined with a focus on citizen education and strong public-private collaboration, have significantly reduced cyber incidents, bolstering the nation's digital governance. Estonia's proactive measures have established it as a leader in cybersecurity, setting an example for other nations. Similarly, Singapore, with its Smart Nation initiative, integrates both technological innovation and cybersecurity at its core. The country's Cybersecurity Act and the work of the Cybersecurity Agency of Singapore (CSA) have made cybersecurity a key element of the nation's digital transformation (Cyber Security Agency of Singapore, 2025). By embedding security measures within its evolving digital infrastructure, Singapore has ensured the secure and efficient delivery of public services, becoming a model for how digital security and innovation can work hand-in-hand. These case studies illustrate the financial and operational impacts that data breaches can have on both public institutions and private organizations. From the misconfigured U.S. voter database to the crippling ransomware attacks in Costa Rica, each incident highlights the urgent need for robust cybersecurity frameworks, proactive risk management, and swift incident response. In contrast, countries like Estonia and Singapore demonstrate the effectiveness of strategic investments in cybersecurity. With well-established national cybersecurity agencies, public-private collaborations, and innovative security technologies, these nations have created more resilient digital infrastructures. They've built strong foundations that have not only mitigated cyber risks but have also enhanced their ability to innovate securely in the digital age. While the United States has taken significant steps to bolster its cybersecurity, particularly through initiatives like the Cybersecurity and Infrastructure Security Agency (CISA) and the Continuous Diagnostics and Mitigation (CDM) program, these efforts, though valuable, are not enough. The U.S. has made progress in strengthening federal systems and reducing downtime, but as recent breaches have shown, there is still much work to be done to protect critical infrastructure. The country's current cybersecurity framework needs to evolve more rapidly to keep pace with the growing sophistication of cyber threats.

These successful models, however, provide valuable insights for nations and organizations seeking to safeguard their digital infrastructures. They show that the cost of data breaches goes far beyond financial losses—impacting public trust, operational continuity, and even national security. To mitigate these risks, governments and organizations must prioritize cybersecurity, continually adapt to emerging threats, and make significant investments in both technology and human resources. Only through these sustained, concerted efforts can we hope to build resilient digital governance frameworks capable of standing up to the challenges of an increasingly interconnected and cyber-vulnerable world.

2.2. Government Efficiency initiatives in the United States

The establishment of the US Department of Government Efficiency (DOGE) in January 2025 highlights the commitment of the federal government to improving operational efficiency through strategic technological and organizational measures. The formal purpose of DOGE, as stated in the executive order that established it, is to "modernize federal technology and software to maximize government efficiency and productivity" (The White House, 2025). Several U.S. states, including Texas, Kansas, and Louisiana, have recently undertaken similar initiatives to enhance government efficiency. In Texas, the Committee on Delivery of Government Efficiency has been formed to reduce inefficiencies, increase transparency, and promote the use of science and technology. (Texas House of Representatives, 2024). As digitization reshapes public administration, these organizations play a pivotal role in driving initiatives that ensure seamless service delivery while addressing systemic vulnerabilities. These initiatives focus on preventing service disruptions, safeguarding critical public services such as healthcare and emergency response, and optimizing resource allocation by reducing financial and reputational losses linked to cyber incidents. A key way to achieve this is through cybersecurity hardening - proactive securing systems to enhance resilience, reduce downtime, and ensure seamless operations. Strong cybersecurity prevents costly breaches, minimizes reactive spending, and compliance burdens while supporting DOGE's mission to cut inefficiencies. Hardened systems also foster trust in digital services, ensuring secure and frictionless operations. Without a strong security foundation, modernization efforts risk being undermined by cyber threats. Our approach helps to achieve the broader objectives of government efficiency while suggesting the addition of cybersecurity jobs and the reinvestment, leading to not only efficiency of government operations, but also potentially avoiding multi-million dollar costs of data breaches. Our research demonstrates that cybersecurity improvements are integral to government efficiency by improving operational resilience, reducing the likelihood and impact of service disruptions, enabling smarter resource allocation, and strengthening public trust in digital infrastructure.

Sl	State	Committee Name	Cybersecurity Agenda
1	Kansas	Senate Committee on Govt Efficiency	Not specified
2	Louisiana	Fiscal Responsibility Program	Not specified
3	Texas	Committee on Delivery of Govt Efficiency	Cybersecurity, privacy, and identity theft

Tab. 1 – Government Efficiency Committees Launched in the USA (Oct 2024–Feb 2025)

2.3. The Role of Cybersecurity Hardening

The National Institute of Standards and Technology (NIST) defines hardening as the process of reducing attack opportunities by addressing vulnerabilities and disabling unnecessary services. Cybersecurity hardening is a holistic strategy designed to protect organizations from cyber threats and reduce risks. By limiting the attack surface, organizations can lower their susceptibility to breaches and bolster their overall security framework. Organizations can enhance cybersecurity hardening by addressing key vulnerabilities through measures like strengthening password security, replacing default passwords with strong, unique ones to prevent breaches, and providing regular employee and client training on emerging threats and best practices. Automated updates and patching are crucial for efficiently managing zero-day vulnerabilities across complex IT environments. Encrypting network traffic ensures sensitive data is protected during transmission, while regular audits help identify and resolve misconfigurations in servers, routers, firewalls, and other systems. These steps collectively reduce risks, safeguard data, and strengthen overall network security. To achieve a robust cybersecurity framework, organizations should regularly assess their data storage and sharing processes. This includes reviewing the security of collaboration tools and addressing any gaps in system configuration to mitigate risks effectively.

3. Related Work

3.1. Regulatory Frameworks and Governance

The regulatory landscape of cybersecurity has evolved significantly, with governments and organizations developing comprehensive frameworks to address emerging threats. This evolution is driven by the increasing frequency and sophistication of cyber attacks, as well as the growing importance of data protection and privacy. Karabacak et al., 2016 demonstrated how nations can develop and implement regulatory frameworks for critical infrastructure protection. This approach is mirrored in other countries, such as the United States, where sector-specific regulations like HIPAA for healthcare and FISMA for government agencies have been implemented (Federal Information Security Management Act of 2002, 2002; Health Insurance Portability and Accountability Act of 1996, 1996). The European Union has taken a more comprehensive approach with the General Data Protection Regulation (GDPR) and the Network and Information Systems (NIS) Directive, setting global benchmarks for data protection and network security.

Furthermore, Bechara and Schuch, 2021 examined the challenges of creating unified global regulatory standards, particularly highlighting the complexities of cross-border cooperation. This is evident in the difficulties faced by businesses operating internationally, who must comply with multiple, sometimes conflicting, regulations. Albalas et al., 2022 provided a foundational understanding of cybersecurity governance structures and their implementation across different sectors. This understanding is crucial as the regulatory landscape continues to evolve, with new cybersecurity rules being enacted in major economies worldwide in 2024. These new laws aim to provide enhanced cybersecurity guardrails to effectively counter evolving cyber threats, including those leveraging advanced technologies like artificial intelligence.

Adding to this body of work, Hiller et al., 2024 proposed an innovative approach that breaks away from traditional regulatory frameworks by introducing a ”carrots and sticks” tax strategy to incentivize stronger cybersecurity postures. Their framework for a Federal Cybersecurity Investment Tax Credit, combined with a cyber insecurity tax, offers a more flexible and adaptive approach to cybersecurity governance that goes beyond conventional compliance-based requirements.

3.2. Economic and Resource Allocation

The economic aspects of cybersecurity hardening remain a critical concern for organizations in 2025, as they navigate uncertain economic times (Kissoon, 2020). Despite the growing need for robust cybersecurity measures, businesses are scrutinizing their budgets closely. Recent studies indicate that cybersecurity budgets have seen slower growth, with average increases dropping from 17% to 6% year-over-year (Krishna & Sebastian, 2021). However, cybersecurity spending remains relatively resilient, accounting for an increasing proportion of total IT costs, rising from 8.6% in 2020 to 11.6% in 2023 (IANS Research & Artico Search, 2023). This trend reflects the strategic importance of cybersecurity in organizational growth and continuity plans. CISOs are facing pressure to justify their budgets, leading to a focus on cost-effective solutions such as automation and security tool consolidation. Organizations are prioritizing basic cyber hygiene practices over investing in new technologies, emphasizing the need to maximize the outcome of every dollar spent on cybersecurity (Argyridou et al., 2023). As the global cybersecurity spend approaches $100 billion annually, with potential losses nearing $1 trillion, the economic imperative for effective resource allocation in cybersecurity hardening has never been more apparent. (Falco et al., 2019)

3.3. E-Government Implementation

The incorporation of cybersecurity into e-government initiatives is crucial for ensuring their success and resilience. Alrubaiq and Alharbi, 2021 identify key cybersecurity threats in e-government implementations, including data breaches, denial-of-service attacks, and insider threats. Their study highlights the need for a comprehensive cybersecurity framework that addresses both technical vulnerabilities and human factors in e-government projects. Recent advancements in e-government implementation include the development of more sophisticated risk assessment models. Ganin et al., 2020propose a novel cybersecurity risk assessment framework specifically tailored for e-government applications, incorporating dynamic threat landscapes and interdependencies between different government systems. This approach allows for more accurate prediction and prioritization of potential vulnerabilities in government networks. The National Institute of Standards and Technology (NIST) has developed Cybersecurity Framework 2.0, which provides a comprehensive approach to managing cybersecurity risks in critical infrastructure, including e-government systems. This updated framework now emphasizes six core functions: Govern, Identify, Protect, Detect, Respond, and Recover, offering a structured approach to cybersecurity implementation in e-governance initiatives.(National Institute of Standards and Technology, 2024)

The concept of ”security by design” has gained significant traction in e-government implementations. Alreemy et al., 2016 propose a framework for integrating security considerations throughout the entire lifecycle of e-government projects, ensuring that cybersecurity measures are not an afterthought but are embedded in the design and development phases. This approach aligns with a demonstration by Conklin and White, 2006 of the practical value of cybersecurity exercises in strengthening government organizations’ security posture and incident response capabilities. As e-government systems become more sophisticated and widespread, the need for robust, adaptive, and comprehensive cybersecurity strategies becomes increasingly important, necessitating ongoing research and development in this critical area.

4. Methodology

This study integrates qualitative and quantitative analyses to assess how cybersecurity hardening enhances government efficiency and resilience. The methodology consists of three key components: a comprehensive literature review, an in-depth case study analysis, and economic modeling to evaluate the financial impact of cybersecurity investments. The literature review involves a systematic analysis of academic research, government reports, and industry publications to establish a foundational understanding of cybersecurity hardening strategies, digital transformation, and their effects on government operations. This review focuses on identifying key challenges in cybersecurity, evaluating best practices, and exploring how robust security frameworks improve public sector efficiency. It provides a theoretical basis for assessing the economic and operational benefits of proactive cybersecurity measures, guiding the case study selection and subsequent financial analysis. The case study analysis examines five major government-related cyber breaches to illustrate the financial and operational consequences of cyberattacks. The selected cases include the SolarWinds Attack (2020), which exposed vulnerabilities in supply chain security across U.S. federal agencies; the OPM Breach (2015), which compromised 22.1 million security clearance records; a U.S. Voter Data Breach, highlighting risks to election integrity; and the Costa Rica Government Ransomware Attack (2022), which paralyzed public services and caused significant economic losses. These cases were chosen based on their scale, relevance to government operations, and the financial and reputational damages incurred. The analysis identifies common vulnerabilities, assesses incident response effectiveness, and extracts key lessons to inform best practices for cybersecurity hardening. The economic modeling component synthesizes findings from the literature review and case studies to evaluate the financial impact of cybersecurity investments. It identifies cost patterns across breaches, estimates potential losses that could have been mitigated through proactive security measures, and highlights best practices for maximizing return on investment (ROI). The study leverages risk reduction frameworks and historical breach cost data to assess how cybersecurity spending can lead to long-term cost savings and improved operational stability in government agencies. This study acknowledges certain limitations, including reliance on publicly available data, which may not fully capture remediation costs, classified response strategies, or long-term policy changes following breaches. Additionally, quantifying indirect costs such as reputational harm, erosion of public trust, and political fallout remains complex. However, by triangulating insights from multiple sources, this study provides a comprehensive assessment of cybersecurity's role in strengthening government efficiency and resilience while offering actionable recommendations for policymakers and security professionals.

5. Case Studies and Analysis

5.1. SolarWinds Incident

The SolarWinds hack was a supply chain attack where malicious actors breached the SolarWinds Orion software system (Alkhadra et al., 2021). A supply chain attack exploits weaker points in an organization's network, often through third-party vendors, to gain unauthorized access to systems and data. In this case, over 18,000 SolarWinds customers installed software updates containing malicious code, unknowingly enabling attackers to infiltrate their networks. The attack had a far-reaching impact on government and private organizations alike. According to the White House, nine federal agencies—including the Departments of Homeland Security, State, Treasury, Justice, Energy, and Defense—along with over 100 technology companies, were compromised (Cybersecurity and Infrastructure Security Agency & Federal Bureau of Investigation, 2021). A report by Roll Call estimated that American businesses and government agencies could spend upwards of $100 billion over months to contain and mitigate the damage (Pexton, 2021). The indirect costs compounded the financial toll, with companies losing an average of 11% of their annual revenue. The United States faced the highest financial impact, where companies suffered losses averaging 14% of their annual revenue, compared to 8.6% in the United Kingdom and 9.1% in Singapore (Fortinet, 2021). Beyond monetary losses, the attack tarnished the reputations of affected organizations, increased their operational costs, triggered legal actions and customer refunds, and compromised sensitive data. Moreover, a ProPublica investigation revealed that the U.S. government had spent $2.2 million on a cybersecurity system that, if implemented, might have prevented the SolarWinds attack.(ProPublica, 2021)

5.2. US Office of Personnel Management Incident

The 2015 Office of Personnel Management (OPM) data breach targeted sensitive information contained in Standard Form 86 (SF-86) records, which are used for U.S. government security clearances. This breach exposed critical data retained by OPM, affecting 22.1 million individuals, including federal employees, contractors, and their associates.(Gootman, 2016) OPM reported two separate but related cybersecurity incidents stemming from malicious activity on its network. The breach was traced back to a compromised contractor credential, as revealed by a collaborative investigation by the FBI and the Department of Homeland Security. By 2017, the breach had cost the U.S. government over $1 billion, primarily to provide identity theft protection for affected individuals. Two contracts were signed with ID Experts to address these concerns: the first for $340 million in credit monitoring and identity theft protection services, and the second for up to $416 million in extended services. In 2022, an additional $63 million settlement was reached for individuals who could demonstrate financial hardship caused by the breach (Giaritelli, 2022). This incident highlighted vulnerabilities in the bureaucratic system, which some argue contributed to inadequate protection of proprietary information. Others place the blame on senior leadership for failing to implement necessary security protocols to protect sensitive data. Warnings of such a breach were not unforeseen. According to Boyd, 2015, government auditors had warned the Office of Personnel Management (OPM) and other federal agencies about vulnerabilities in their systems. Security experts had recommended enhancing defenses through encryption and deploying software tools to mitigate risks. Unfortunately, these warnings went unheeded.(Brown, 2019)

5.3. Economic Modeling and Analysis

A comprehensive review of existing literature underscores the critical need for economic frameworks that balance cybersecurity investments with organizational risks and outcomes. The Gordon-Loeb Model has long served as a cornerstone in cybersecurity economics, offering a structured approach to determining optimal spending on security measures (Gordon & Loeb, 2002). However, as technology advances and cyber risks evolve, it is imperative to adapt this model to reflect contemporary challenges. This section explores the Gordon-Loeb Model's insights, integrates findings from IBM's 2024 report on breach costs, and incorporates emerging considerations from research on cyber risk quantification, including the work of Böhme et al., 2018.(Ponemon Institute, 2023)

5.4. The Gordon-Loeb Model: Foundational Insights

The Gordon-Loeb Model provides a mathematical framework to help organizations determine the optimal level of investment in protecting their information assets. It offers several key insights into cybersecurity investment strategies. First, the model highlights the principle of diminishing returns on investment. It suggests that the optimal level of security investment should not exceed 37% of the expected loss from a potential security breach. Investing beyond this threshold often results in diminishing returns, making additional expenditures less effective in mitigating risks. Second, the model emphasizes the importance of focusing on mid-vulnerability information. Protecting high-vulnerability information can demand significant resources, which may not always justify the costs. Similarly, securing low-vulnerability data often provides limited returns on investment. Therefore, the model advises prioritizing information assets with medium vulnerability, where security investments are likely to be most cost-effective. Lastly, the model underscores the need for strategic resource allocation. Organizations are encouraged to categorize their information assets based on their value and susceptibility to breaches, enabling a more rational and efficient distribution of security resources. This framework provides a valuable guide for balancing investment and risk in cybersecurity.

5.5. Adapting the Gordon-Loeb Model to Current Challenges

While the Gordon-Loeb Model provides a solid theoretical foundation, adapting its principles to today's dynamic cyber threat landscape involves addressing key developments. Insights from IBM's 2024 report highlight several pressing issues. The global average cost of a data breach has surged to $4.88 million, marking a 10% increase over the previous year and emphasizing the financial stakes of inadequate cybersecurity measures. Additionally, organizations that leverage security AI and automation can save an average of $2.22 million per breach, demonstrating the return on investment in technologies like AI-driven threat detection, encryption, and endpoint protection. Another growing concern is the proliferation of shadow data, which now plays a role in one-third of breaches. This trend complicates the task of tracking and securing sensitive information, necessitating the implementation of advanced data governance frameworks and visibility tools (IBM, 2024).

Furthermore, public sector entities face distinct cybersecurity challenges due to their responsibility for protecting critical infrastructure and citizen data. High-profile breaches, such as the Office of Personnel Management (OPM) hack, have resulted in substantial direct and indirect costs, highlighting the need for optimal budget allocation (Brown, 2019). Unlike private organizations, governments must also address externalities, including public trust, national security, and economic stability. Meanwhile, cyber risk insurance remains an underutilized tool for managing financial exposure to breaches. Böhme et al., 2018 argue that its adoption is hindered by the lack of actuarial data and the unpredictable nature of emerging threats. They advocate for data-sharing frameworks to improve risk quantification, which would help insurers price policies more effectively and incentivize better security practices. As cyber threats evolve, insurers may also need to collaborate with software vendors to mitigate vulnerabilities proactively, creating a feedback loop that benefits both parties.

Emerging technological paradigms further complicate cyber risk modeling. The rise of distributed ledger technologies, such as blockchain, introduces new risks that require novel analytical approaches. These systems rely on cryptographically enforced rules and autonomous algorithms, posing unique challenges for cybersecurity. Moreover, broader trends like the Internet of Things (IoT) and the Fourth Industrial Revolution underscore the necessity for dynamic, predictive models capable of addressing interconnected risks. Adapting the Gordon-Loeb Model to these realities will require a more nuanced approach that integrates evolving technological, economic, and policy considerations. Leveraging Gordon-Loeb's research, we have modeled the optimal cybersecurity investment based on the average annual cost of a data breach in 2. This investment is projected to reduce the risk of a data breach by 26%, potentially saving organizations millions of dollars per incident (Accenture, 2023).

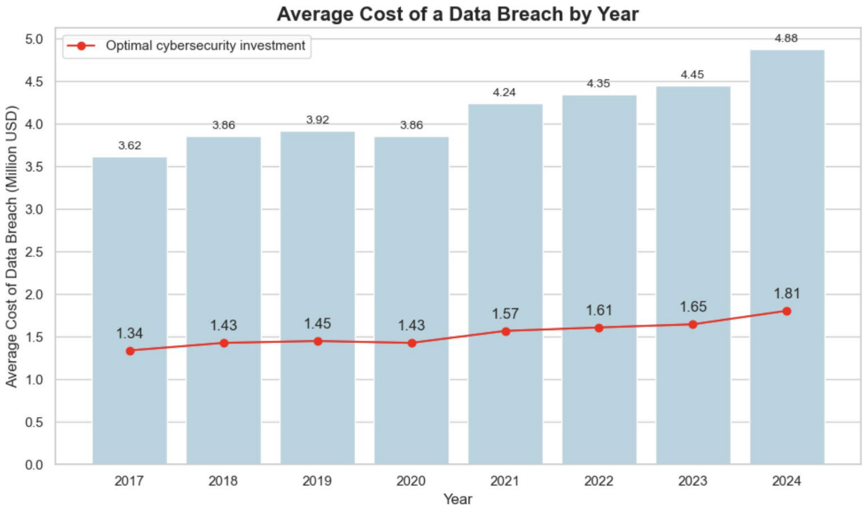

Fig. 2 – Yearly average data breach cost and recommended cybersecurity spending. Data sourced from IBM.

Analyzing the SolarWinds and OPM data breaches through the Gordon-Loeb model demonstrates the importance of optimizing security investments to address vulnerabilities effectively. In both cases, proactive spending on cybersecurity measures—such as robust identity verification systems, privileged access management (PAM) solutions, and AI-driven threat detection—could have mitigated vulnerabilities and reduced overall costs. The model's principle that security investments should be proportional to potential losses and risk levels underscores the need for strategic allocation of resources to areas with the highest impact. An equally critical component of risk mitigation is investing in human capital. Both the SolarWinds and OPM breaches highlight the importance of recruiting skilled security engineers and providing employee training to recognize and respond to potential threats. For example, the average salary of a DevOps Security Engineer in 2025 is approximately $140,000 annually—a cost that pales in comparison to the billions of dollars in direct and indirect costs resulting from these breaches. Organizations should aim to have at least one dedicated security engineer per development team, with larger enterprises requiring a centralized, specialized security team to oversee and manage the overall security posture. Finally, adopting advanced security technologies, such as endpoint protection, encryption, and AI-enabled threat detection systems, combined with a disciplined approach to patch management, is essential to reducing vulnerabilities. Although these measures involve significant upfront costs, they provide a high return on investment by reducing risk exposure and strengthening organizational resilience. By leveraging economic models like Gordon-Loeb and implementing smarter spending strategies, organizations can mitigate the likelihood and impact of future breaches, turning cybersecurity investments into a long-term safeguard for operational and financial stability.

5.6. Application to Government Efficiency

By integrating insights from the Gordon-Loeb Model and Böhme et al.'s research, governments can enhance cybersecurity investments in ways that align with their broader goals of efficiency and resilience. Strategic investments in AI, automation, and encryption can significantly reduce breach costs. Proactive measures to manage shadow data can mitigate risks stemming from poor data governance. According to Gordon and Loeb, the optimal level of security investment (S) should not exceed 37% of the expected loss (L) from a breach, expressed mathematically as **$S \leq 0.37 \times L$**, which helps avoid over-investment while addressing critical vulnerabilities (Gordon & Loeb, 2002). Governments can use data-sharing frameworks to assess risk at both individual and systemic levels, improving decision-making. The shortage of skilled cybersecurity professionals presents a significant challenge to maintaining secure systems, so investing in training programs for existing employees and recruiting specialized security engineers can dramatically improve an organization's ability to detect and mitigate threats. By employing Security Operations (SecOps) teams equipped with advanced tools and knowledge, governments can enhance real-time threat monitoring and incident response capabilities. Training initiatives can also extend to non-technical personnel, fostering a culture of cybersecurity awareness and reducing human errors, often a major source of breaches. Cyber insurance can play a pivotal role in promoting security best practices, with premium differentiation, as proposed by Böhme et al., 2018, encouraging organizations to adopt secure-by-design approaches and prioritize risk mitigation throughout the supply chain. Finally, a robust cybersecurity posture fosters trust in digital public services, which is critical for successful digital transformation initiatives The Gordon-Loeb Model offers a robust framework for optimizing cybersecurity investments, and its relevance has become increasingly critical in the context of rising breach costs, and the rapid evolution of technological landscapes. As demonstrated in the research, organizations and governments can adopt a more comprehensive approach to managing cyber risks by balancing investments with expected losses, embracing cutting-edge technologies such as AI, automation, and Privileged Access Management (PAM) solutions, investing in human capital through the recruitment of skilled security professionals and employee training programs, and leveraging cyber insurance to incentivize better practices and mitigate risk exposure. By integrating economic models such as the Gordon-Loeb framework with predictive analytics, dynamic risk assessments, and a forward-thinking approach to emerging threats, organizations can enhance their resilience, ensuring their ability to navigate the complexities of a rapidly advancing digital landscape.

6. Strategies for Cybersecurity Hardening

Governments must adopt a multi-pronged approach to harden cybersecurity systems, especially as threats grow in sophistication and impact. Strategic investments, technical controls, workforce development, and public-private partnerships all play critical roles in strengthening national cybersecurity postures. Strategic investments in cybersecurity are often shaped by economic constraints, policy priorities, and perceived risks. Governments tend to increase funding when the cost of inaction—such as fallout from major cyberattacks—surpasses the cost of implementation. High-impact events like ransomware incidents or geopolitical tensions prompt accelerated adoption of Zero Trust Architectures (ZTA), Endpoint Detection and Response (EDR), and AI-powered threat intelligence platforms. Frameworks like NIST CSF, FedRAMP, and ISO 27001 promote investment by enforcing compliance, while partnerships with the private sector offer access to funding and technical expertise (Cybersecurity and Infrastructure Security Agency, 2023; National Institute of Standards and Technology, 2022).

On the technical front, scalable defenses are necessary to safeguard sensitive government systems against nation-state actors and cybercriminals. Following the SolarWinds attack, U.S. agencies prioritized ZTA, which enforces continuous verification through identity and access management (IAM), micro-segmentation, multi-factor authentication (MFA), and conditional access policies (Alkhadra et al., 2021; Cybersecurity and Infrastructure Security Agency, 2023). Broader deployment of EDR, mobile device management (MDM), and automated threat intelligence tools enhances detection while balancing operational efficiency (National Institute of Standards and Technology, 2022).

Given that human error remains a leading cause of breaches, workforce training and cyber hygiene are essential. However, enforcing best practices across large public institutions can be challenging. Integrating mandatory cybersecurity training, gamified learning, and phishing simulations boosts employee engagement and adoption (European Union Agency for Cybersecurity, 2023; Ogundare, 2024). Practices like strong password policies, MFA, secure access management, and automated patching reduce exploitable vulnerabilities (National Institute of Standards and Technology, 2022). Regular audits and assessments help evaluate the effectiveness of these initiatives and ensure compliance.

Finally, public-private partnerships are vital for accessing cutting-edge technologies and real-time threat intelligence. Collaborations with cybersecurity vendors, ISACs, and CISA's Joint Cyber Defense Collaborative (JCDC) support proactive threat mitigation and rapid incident response (Cybersecurity and Infrastructure Security Agency, 2023). Joint cyber exercises improve crisis coordination and expose vulnerabilities in existing systems. Academic partnerships also contribute to workforce development by advancing research and specialized training.

By integrating strategic investments, technical defenses, workforce preparedness, and cross-sector collaboration, governments can enhance resilience, minimize disruptions, and respond more effectively to the evolving cybersecurity threat landscape.

7. Discussion

7.1. Benefits of Cyber Security Hardening

Improved Service Reliability: Secure systems play a pivotal role in ensuring the uninterrupted availability of critical services, ranging from emergency response systems to welfare distribution networks. For instance, a study by Zhani et al., 2021 highlights that robust cybersecurity measures significantly reduce the downtime of essential services during cyberattacks, ensuring operational continuity even under duress. This reliability not only minimizes disruptions but also builds public confidence in digital governance frameworks. Furthermore, high service reliability mitigates the ripple effects of service outages, such as economic losses and reputational damage, thereby stabilizing broader societal systems reliant on these services.

Cost Savings: Preventing cyber incidents reduces the financial burden of remediation, legal liabilities, and lost productivity. Investments in cybersecurity yield substantial financial benefits by preempting the high costs associated with cyber incidents. According to Ponemon Institute's 2023 Cost of a Data Breach Report, organizations with advanced security frameworks reported an average cost reduction of 28% per breach compared to those with minimal defenses (Ponemon Institute, 2023). This cost efficiency is achieved through reduced expenditures on incident remediation, legal liabilities, regulatory fines, and the indirect costs of lost productivity. Moreover, proactive measures such as network segmentation and endpoint security can significantly decrease the financial impact of potential threats, transforming cybersecurity from a cost center to a strategic investment with measurable returns (Böhme & Schwartz, 2022).

Enhanced Public Trust: A strong cybersecurity posture not only protects sensitive information but also fosters public trust in digital systems. Citizens are more likely to engage with government-led technological initiatives, such as e-voting platforms or digital health records, when assured of their data's safety. Research by Smith and Duggan, 2020 reveals that public trust in digital services increases by 45% when organizations visibly demonstrate adherence to cybersecurity best practices. Additionally, transparent communication about security measures and regular audits can reinforce this trust, creating a virtuous cycle of increased adoption and innovation in public service delivery.

Strategic Advantage: Cybersecurity hardening equips organizations and governments with a proactive approach to risk management, enabling them to allocate resources toward innovation rather than crisis mitigation. As noted by Johnson et al., 2022, governments that prioritize cybersecurity are better positioned to leverage emerging technologies, such as artificial intelligence and blockchain, without the fear of compromising system integrity. This strategic advantage not only enhances operational efficiency but also bolsters national security by preempting cyber threats. Furthermore, strong cybersecurity frameworks provide a competitive edge in the global arena, as they attract international investments and partnerships by demonstrating robust risk management capabilities.

7.2. Challenges

Budget Constraints: Implementing comprehensive cybersecurity measures demands substantial financial resources, which can be a significant hurdle, particularly for developing nations. Many governments face competing priorities, such as healthcare, education, and infrastructure, making it difficult to allocate sufficient funds for cybersecurity. The high costs of acquiring advanced security technologies, maintaining robust infrastructure, and ensuring continuous monitoring and response capabilities further strain limited budgets. As a result, governments may resort to outdated security systems, increasing their vulnerability to cyber threats. Cost-effective solutions, such as leveraging open-source security tools and fostering public-private partnerships, can help mitigate these financial challenges.

Talent Shortages: The global shortage of skilled cybersecurity professionals remains a pressing issue, making it difficult for governments to build and maintain resilient security systems. A lack of trained personnel can lead to gaps in threat detection, incident response, and overall security posture. Many developing nations struggle with brain drain, where skilled professionals seek higher-paying opportunities in the private sector or abroad (Reuters, 2024). To address this, governments must invest in workforce development initiatives, such as specialized training programs, cybersecurity education in universities, and incentives to retain talent within the public sector. Additionally, collaboration with international organizations and private companies can help bridge the talent gap by providing training and expertise.

Evolving Threats: Cyber threats are constantly evolving, with attackers developing more sophisticated techniques to bypass security measures. Governments must stay ahead of emerging risks, including artificial intelligence-driven attacks, advanced persistent threats (APTs), and zero-day vulnerabilities. One of the most pressing future challenges is the potential impact of quantum computing, which could render current encryption standards obsolete. Proactive investment in quantum-resistant cryptographic solutions and adaptive cybersecurity frameworks will be essential to mitigate this risk. Continuous threat intelligence gathering, regular security audits, and agile policy adjustments are necessary to ensure that security measures remain effective against emerging cyber threats.

Bureaucratic Hurdles: The implementation of cybersecurity measures within government institutions often faces significant bureaucratic challenges. Lengthy procurement processes, rigid administrative structures, and inter-agency coordination difficulties can delay the adoption of critical security solutions (U.S. Government Accountability Office, 2024). Additionally, differing priorities among government departments can lead to fragmented security policies and inconsistent implementation. Overcoming these hurdles requires streamlined governance structures, clear cybersecurity mandates, and enhanced collaboration between agencies (Report of Commission on the National Defense Strategy, 2024). Establishing centralized cybersecurity authorities and implementing clear accountability frameworks can improve decision-making and accelerate the deployment of effective security measures.

7.3. Limitations

The foundation of our economic modeling relies heavily on accurate estimations of data breach costs, which are inherently difficult to measure and can vary significantly. While we have utilized industry-standard reports like IBM's Cost of a Data Breach study, these figures represent averages across diverse organizations and may not perfectly reflect the unique circumstances of government entities. The long-term and indirect costs of breaches, such as reputational damage or loss of public trust, are particularly challenging to quantify accurately.

Furthermore, we propose that investing in cybersecurity might lead to a substantial decrease in risk. Our proposal relies on generalized models, such as the Gordon-Loeb Model, which are built on theoretical assumptions like diminishing returns on security investments and a linear correlation between spending and risk reduction. These assumptions may oversimplify real-world complexities, such as interdependencies between different security measures and organizational processes. The effectiveness of security investments can vary greatly depending on factors such as the quality of implementation and operation, the maturity of existing security measures, and the specific threat landscape faced by an organization. As a result, the actual outcomes of security investments may deviate from our projections.

Overall, cybersecurity is a rapidly evolving field, with new threats, technologies, and defensive strategies emerging continuously. As a result, our research may become outdated over time as novel attack vectors and mitigation techniques reshape the security landscape. Excessive cybersecurity controls can hinder the efficiency and responsiveness of government operations, while too little leaves critical systems vulnerable to attack. Striking the right balance between security and functionality is essential to ensure both resilience and operational success.

Additionally, while we have relied on industry reports and established models, these sources may age quickly, potentially limiting their applicability to future cybersecurity challenges. Continuous updates and reassessments will be necessary to ensure the relevance and accuracy of our findings.

8. Future Directions

The future of cybersecurity will be shaped not just by cutting-edge technologies, but also by how well we collaborate globally and engage everyday people. Artificial intelligence (AI) is already transforming the field by helping detect threats faster, automate responses, and find system vulnerabilities before attackers do. These systems learn over time, getting better at spotting unusual behavior and taking action quickly, which helps security teams focus on big-picture strategy. But while AI makes defense smarter, quantum computing introduces new risks. Encryption methods we rely on today—like RSA and ECC—could be broken by quantum computers in the next couple of decades (Vermeer & Peet, 2020). That's why there's a growing push to develop quantum-safe alternatives like lattice-based and hash-based algorithms. On the global stage, cyber threats don't stop at borders. International efforts—like the Budapest Convention, the Five Eyes alliance, and INTERPOL's cybercrime programs—are becoming essential for sharing threat intelligence and coordinating response efforts (Council of Europe, 2025; INTERPOL, 2025; Rix, 2023). And beyond governments and tech, people play a key role too. When citizens are educated about digital risks and know how to report suspicious activity, they become part of the solution. Strong cybersecurity in the future will depend not only on smart machines and strong laws but also on an informed and engaged public.

9. Conclusion

Cybersecurity hardening has evolved from a defensive measure to a strategic imperative for modern governance. As governments accelerate their digital transformation, safeguarding critical infrastructure and sensitive data against cyber threats must remain a top priority. Case studies of significant cyber incidents, such as the SolarWinds attack and the OPM breach, highlight the severe financial and operational consequences of insufficient security measures. Despite challenges like budget constraints, talent shortages, and the rapidly changing nature of cyber threats, a proactive, multilayered cybersecurity approach can greatly enhance government efficiency. This paper emphasizes that cybersecurity hardening is not merely a cost, but a vital enabler of innovation and operational effectiveness. Governments that prioritize cybersecurity will be better positioned to harness emerging technologies, optimize resource allocation, and uphold public trust. Looking ahead, international collaboration, workforce development, and investment in quantum-resistant cryptography will be essential to sustaining secure and effective digital governance in an increasingly complex threat landscape. By integrating cybersecurity into the core of governance strategies, nations can protect their digital futures while advancing efficient and secure public administration.

References

Accenture. (2023, June). Aligning cybersecurity to business objectives helps drive revenue growth and lower costs of breaches [Access]. https://newsroom.accenture.com/news/2023/aligning-cybersecurity-to-business-objectives-helps-drive-revenue-growth-and-lower-costs-of-breaches-accenture-report-finds

Albalas, T., Modjtahedi, A., & Abdi, R. (2022). Cybersecurity governance: A scoping review. *International Journal of Professional Business Review*, *7*(4), e0629. DOI: https://doi.org/10.26668/businessreview/2022.v7i4.629.

Alkhadra, R., Abuzaid, J., AlShammari, M., & Mohammad, N. (2021). Solar winds hack: In-depth analysis and countermeasures. *2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, 1–7. DOI: https://doi.org/10.1109/ICCCNT51525.2021.9579611.

Alreemy, Z., Chang, V., Walters, R., & Wills, G. (2016). Critical success factors (csfs) for information technology governance (itg). *International Journal of Information Management*, *36*(6), 907–916. DOI: https://doi.org/10.1016/j.ijinfomgt.2016.05.015.

Alrubaiq, A., & Alharbi, T. (2021). Retracted: Developing a cybersecurity framework for e-government project in the kingdom of saudi arabia [Retracted: 10 October 2024]. *Journal of Cybersecurity and Privacy*, *1*(2), 302–318. DOI: https://doi.org/10.3390/jcp1020017.

Argyridou, E., Nifakos, S., Laoudias, C., Panda, S., Panaousis, E., Chandramouli, K., Navarro-Llobet, D., Mora Zamorano, J., Papachristou, P., & Bonacina, S. (2023). Cyber hygiene methodology for raising cybersecurity and data privacy awareness in health care organizations: Concept study. *Journal of Medical Internet Research*, *25*, e41294. DOI: https://doi.org/10.2196/41294.

Bechara, F. R., & Schuch, S. B. (2021). Cybersecurity and global regulatory challenges. *Journal of Financial Crime*, *28*(2), TBD. DOI: https://doi.org/10.1108/JFC-04-2020-0061.

Bitton, M. (2022). The estonian miracle: E-estonia and the future of digital infrastructure. *Metaverse Blog, NYU School of Professional Studies*. https://www.sps.nyu.edu/homepage/metaverse/metaverse-blog/the-estonian-miracle-e-estonia-and-the-future-of-digital-infrastructure.html

Böhme, R., & Schwartz, G. (2022). Economic incentives for cybersecurity investments. *Journal of Cybersecurity Economics*, *9*(2), 121–138.

Böhme, R., Laube, S., & Riek, M. (2018). A fundamental approach to cyber risk analysis. https://api.semanticscholar.org/CorpusID:49526942

Boyd, A. (2015). *Could opm have prevented the breach?* [Accessed: January 30, 2025]. https://www.federaltimes.com/smr/opm-data-breach/2015/06/18/could-opm-have-prevented-the-breach/

Brown, I. (2019). Cybers' cost: The potential price tag of a targeted trust attack [Accessed: 2025-01-29]. *MCU Journal*, *10*(1). https://doi.org/10.21140/mcuj.2019100105

Conklin, W. A., & White, G. B. (2006). E-government and cyber security: The role of cyber security exercises. *Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS'06)*, 79–79. DOI: https://doi.org/10.1109/HICSS.2006.133.

Council of Europe. (2025). The budapest convention [Accessed on January 30, 2025]. *Council of Europe*. https://www.coe.int/en/web/cybercrime/the-budapest-convention

Cyber Security Agency of Singapore. (2025, January). Cybersecurity act: Information on the cybersecurity act [Last updated 28 January 2025]. https://www.csa.gov.sg/legislation/cybersecurity-act

Cybersecurity and Infrastructure Security Agency. (2023). Cybersecurity best practices for government agencies.

Cybersecurity and Infrastructure Security Agency & Federal Bureau of Investigation. (2021). *Joint statement from the federal bureau of investigation (fbi) and the cybersecurity and infrastructure security agency (cisa)* [Accessed: January 30, 2025]. https://www.cisa.gov/news-events/news/joint-statement-federal-bureau-investigation-fbi-cybersecurity-and-infrastructure-security-agency-0

European Union Agency for Cybersecurity. (2023). Cybersecurity culture guidelines: Behavioral aspects of cybersecurity awareness.

Falco, G., Noriega, A., & Susskind, L. (2019). Cyber negotiation: A cyber risk management approach to defend urban critical infrastructure from cyberattacks. *Journal of Cyber Policy*, *4*(1), 90–116. DOI: https://doi.org/10.1080/23738871.2019.1586969.

Federal Information Security Management Act of 2002 (2002).

Finkle, J. (2015). Database of 191 million u.s. voters exposed on internet: Researcher. *Reuters*. https://www.reuters.com/article/world/us/database-of-191-million-us-voters-exposed-on-internet-researcher-idUSMTZSAPEBCT4IJVCW/

Fortinet. (2021). *Impact of the solarwinds cyber attack on organizations* [Accessed: January 30, 2025]. https://www.fortinet.com/resources/cyberglossary/solarwinds-cyber-attack#:~:text=Impact%20Of%20Attack%20On%20Organization's,additional%20information%20with%20government%20agencies

Ganin, A. A., Quach, P., Panwar, M., Collier, Z. A., Keisler, J. M., Marchese, D., & Linkov, I. (2020). Multicriteria decision framework for cybersecurity risk assessment and management. *Risk Analysis*, *40*(1), 183–199. DOI: https://doi.org/10.1111/risa.12891.

Gianfortune, R. (2025, January). *Proposed doge reforms target technology, efficiency* [Accessed: 2025-01-23]. https://govciomedia.com/proposed-doge-reforms-target-technology-efficiency/

Giaritelli, A. (2022). Judge finalizes $63m opm hack settlement for feds, two months of damages [Accessed: 2025-01-29]. *Government Executive*. https://www.govexec.com/pay-benefits/2022/10/judge-finalized-63m-opm-hack-settlement-feds-two-months-damages/378950/

Gootman, S. (2016). Opm hack: The most dangerous threat to the federal government today. *Journal of Applied Security Research*, *11*(4), 517–525. DOI: https://doi.org/10.1080/19361610.2016.1211876.

Gordon, L. A., & Loeb, M. P. (2002). The economics of information security investment. *5*(4). DOI: https://doi.org/10.1145/581271.581274.

Health Insurance Portability and Accountability Act of 1996 (1996).

Hiller, J. S., Kisska-Schulze, K., & Shackelford, S. (2024). Cybersecurity carrots and sticks. *American Business Law Journal*, *61*(1), 5–45. DOI: https://doi.org/10.1111/ablj.12238.

IANS Research & Artico Search. (2023). *2023 security budget benchmark summary report* (tech. rep.). IANS Research. https://cdn.iansresearch.com/Files/Marketing/2023SurveyContent/IANS+ArticoSearch-2023SecurityBudgetBenchmarkSummaryReport.pdf

IBM. (2024). Cost of a data breach report 2024 [Accessed: 2025-01-23]. https://www.ibm.com/reports/data-breach

INTERPOL. (2025). Interpol innovation centre [Accessed on January 30, 2025]. *International Criminal Police Organization*. https://www.interpol.int/en/How-we-work/Innovation/INTERPOL-Innovation-Centre

Jaikaran, C. (2023, July). The national cybersecurity strategy—going where no strategy has gone before [Accessed: 2025-01-23]. https://crsreports.congress.gov/product/pdf/IN/IN12123

Johnson, K., Li, X., & Patel, M. (2022). Leveraging cybersecurity for strategic governance. *International Journal of Digital Strategy*, *14*(3), 203–219.

Karabacak, B., Yildirim, S. O., & Baykal, N. (2016). Regulatory approaches for cyber security of critical infrastructures: The case of turkey. *Computer Law Security Review*, *32*(3), 526–539. DOI: https://doi.org/10.1016/j.clsr.2016.03.005.

Kissoon, T. (2020). Optimum spending on cybersecurity measures. *Transforming Government: People, Process and Policy*, *14*(3), 417–431. DOI: https://doi.org/10.1108/TG-11-2019-0112.

Krishna, B., & Sebastian, M. P. (2021). Examining the relationship between e-government development, nation's cyber-security commitment, business usage and economic prosperity: A cross-country analysis. *Information and Computer Security*, *29*(5), 737–760. DOI: https://doi.org/10.1108/ICS-12-2020-0205.

Kumar, S., Menezes, A., Giri, S., & Kotikela, S. (2024). What the phish! effects of ai on phishing attacks and defence [05–06 December]. *Proceedings of the 4th International Conference on AI Research (ICAIR)*.

National Institute of Standards and Technology. (2022). Framework for improving critical infrastructure cybersecurity.

National Institute of Standards and Technology. (2024, February). Nist releases version 2.0 of landmark cybersecurity framework. https://www.nist.gov/news-events/news/2024/02/nist-releases-version-20-landmark-cybersecurity-framework

Nato. (2022). Costa rica ransomware attack (2022) [Retrieved January 29, 2025]. https://cyberlaw.ccdcoe.org/wiki/Costa_Rica_ransomware_attack_(2022)

Ogundare, E. (2024). The human factor in cyber security.

Pexton, P. (2021, January). Cleaning up solarwinds hack may cost as much as $100 billion [Accessed: 2025-01-29]. https://www.rollcall.com/2021/01/11/cleaning-up-solarwinds-hack-may-cost-as-much-as-100-billion/

Ponemon Institute. (2023). Cost of a data breach report [Retrieved from Ponemon Institute website]. https://www.ponemon.org

ProPublica. (2021, December). How the solarwinds cybersecurity system was breached [Accessed: 2025-01-29]. https://www.propublica.org/article/solarwinds-cybersecurity-system

Report of Commission on the National Defense Strategy. (2024). *Report of commission on the national defense strategy*. Commission on the National Defense Strategy. https://www.armed-services.senate.gov/imo/media/doc/nds_commission_final_report.pdf

Reuters. (2024). Borderless europe fights brain drain as talent heads north [Accessed: 2025-01-29]. *Reuters*. https://www.reuters.com/world/europe/borderless-europe-fights-brain-drain-talent-heads-north-2024-11-14/?utm_source=chatgpt.com

Rix, M. (2023). Why the five eyes? power and identity in the formation of a multilateral intelligence grouping. *Journal of Cold War Studies*, *25*(1), 101–140. DOI: https://doi.org/10.1162/jcws_a_01109.

Smith, J., & Duggan, R. (2020). Public trust in digital governance: The role of cybersecurity. *Digital Society Quarterly*, *18*(1), 45–67.

Texas House of Representatives. (2024). Committee on delivery of government efficiency [Accessed: 2025-03-23]. https://house.texas.gov/committees/committee/233

The White House. (2025). Establishing and implementing the president's department of government efficiency [Accessed: 2025-03-23]. https: / / www. whitehouse. gov/ presidential- actions/ 2025/ 01/ establishing-and-implementing-the-presidents-department-of-government-efficiency/

U.S. Government Accountability Office. (2024, June). What are the biggest challenges to federal cybersecurity? (high risk update). https://www.gao.gov/blog/what-are-biggest-challenges-federal-cybersecurity-high-risk-update

Vermeer, M. J. D., & Peet, E. D. (2020). *Securing communications in the quantum computing age: Managing the risks to encryption* (tech. rep.). RAND Corporation. https://www.rand.org/pubs/research_reports/RR3102.html

Zhani, M., Karim, R., & Taylor, P. (2021). Cyber resilience in public infrastructure. *Journal of Information Security Studies*, *11*(4), 345–361.