INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact Factor: 6.078
(Volume 10, Issue 1 - V10I1-1246)
Available online at: https://www.ijariit.com

Cyber security and government: safeguarding the public sectors in the digital era

Oluwasola Yunusa Smith
smitholuwasola@gmail.com
Eastern Illinois University, IL 61920, United States

Abstract
This publication emphasizes the critical importance of bolstering cybersecurity in the public sector due to the increasing reliance on digital technologies and the significant risks posed by cyber threats. It discusses the vulnerability of government agencies to cyberattacks, highlighting examples such as the OPM breach, the Colonial Pipeline ransomware attack and the Solar Winds supply chain attack amongst others. The public sector's vulnerability to cyber threats is attributed to factors such as the wealth of sensitive data it holds, outdated technology and security measures, and the potential for public disclosure that can lead to widespread impact and public scrutiny. Moreover, geopolitical strategies and cyberwarfare play a significant role, with cyberattacks on government organizations having profound implications for national security and international relations. This publication also explores the strategies to safeguard the public sector in the digital era, including security awareness training, multi-factor authentication, endpoint security, network segmentation, regular patches and updates, incident response planning, backup and disaster recovery, zero trust architecture, and continuous vulnerability assessments. Overall, it underscores the urgent need for robust cybersecurity measures to protect sensitive data and critical infrastructure from cyber threats.

Keyword: Cybersecurity, Government operations, Cyber threats, Data breaches, Public sector, Cybercrime, Critical infrastructure, Cyber-attacks, Risk management, National security, Governance framework, Safeguarding

1. INTRODUCTION

It is impossible to overestimate the significance of bolstering cybersecurity in our increasingly linked world. Essentially, cybersecurity is the discipline of protecting digital networks and systems to guarantee the security of cyberspace. Government operations depend heavily on it because it acts as a digital barrier against emerging cyber threats. Data that governments handle is extremely sensitive in nature. The national security could be seriously threatened if such information ended up in the wrong hands. For this reason, cybersecurity is crucial for the government since the sensitive data it stores must safeguard.[5]

In addition, governments are gradually utilizing digital platforms in a variety of operational domains in order to improve functionality and transparency. But the increased reliance on digital technologies raises the unintentional risk of cybercrime, including data breaches. Strong cybersecurity measures are therefore essential in the current digital era—not just important, but indispensable. With the constant threat of cybercrime, the public sector is depending more and more on digital technology for daily operations, which is very convenient but also risky.[17] Hackers who are enthralled with disrupting critical infrastructure, the backbone of our society, are drawn to government agencies, healthcare providers, academic institutions, and public infrastructure.

Recent findings from the European Union Agency for Cybersecurity (ENISA) highlight the vulnerability of the public sector, particularly in governments and public administration, which are considered prime targets for cyber attackers.[22] With a whopping 24% share, this sector tops the list of most targeted areas. Adding another layer to this complicated picture is the financial resonance of cyber threats. According to IBM's Cost of a Data Breach 2023 report,[4] the global *average cost* of a *data breach* in *2023* was USD 4.45 *million*, a 15% increase over 3 years.

In a world where ones and zeros are the new battlefield, things are undeniably on the rise. Cybercriminals are constantly evolving and finding new ways to circumvent cybersecurity measures. At this crucial moment, when the public sector stands out as a key target in their playbook, joining forces and sharing knowledge is crucial to strengthen defenses. These cyberattacks have become a significant threat to governments worldwide. The United States, with its multitude of government agencies and critical infrastructure, is no exception.[15] Cybersecurity threats impacting the public sector range from state-sponsored attacks to financially motivated hacking groups.

U.S. Government and Cybercrime

The increasing digitalization of all aspects of modern life has not stopped excluding the government. With increasing online and data usage, government databases have become prime targets for hacker attacks and cyber warfare. According to Richard Clarke,[3] former presidential adviser and counterterrorism expert, cyber warfare is the action of one nation-state to penetrate another state's computers or networks and cause damage or disruption. Broader definitions also include non-state actors such as terrorist groups, corporations, political or ideological extremist groups, criminal organizations and hacktivists. In the United States, cyberattacks from these sources have been a concern for years, as not only the frequency of data breaches has increased, but also their complexity and (economic) impact. In 2018, the U.S. was the country most affected by cybercrime in terms of financial damage, according to Statista, industry experts estimate that cyberattacks cost the U.S. government over $13.7 billion.

The United States is one of the countries with the highest commitment to cybersecurity, based on the Global Cyber Security Index.[21] In terms of budget allocation, the Department of Defense (DoD) is the primary recipient of federal cybersecurity spending, as the agency is responsible for protecting the United States from both offline and online attacks. According to the Department of Defense's latest cyber strategy doctrine, its cyber objectives include building and sustaining forces to conduct cyberspace operations, securing and defending DoD data, preparing for disruptive and destructive cyberattacks, and integrating Cyber options and turn alliances into plans.

Considering the number and scale of data breaches in the U.S. in recent years, the increasing federal spending and focus on cybersecurity becomes increasingly understandable. In 2018, 13,107 cybersecurity incidents were reported by federal agencies. The following year, the U.S. government accounted for 5.6 percent of data breaches and 2.1 percent of all exposed records. With more than 198 million records compromised, the US voter database hack in December 2015 is one of the largest online data breaches in the world.[20] This incident is particularly interesting because the connection between cybercrime and the US electoral process gained global attention during the 2016 US presidential election.

2 SAFEGUARDING THE PUBLIC SECTOR IN THE DIGITAL AGE

A good definition of safeguarding is taking proactive measures to prevent harm and misuse. At the same time, good safeguarding practice means knowing what to do if harm or abuse ever occurs: who to contact, what to tell them and how to help the person who has experienced abuse. Therefore, digital protection is the same idea but in a digital space. Digital safeguarding simply means taking steps to stay safe online.

Why is Safeguarding the Public Sector Important in the Digital Age?

When it comes to protection, prevention is always better than cure. It is always better to prevent abuse in the first place than to react to an incident of abuse. Digital protection is no different. We should know how to use the Internet safely and sensibly, and we should all be aware of the risks we face online.[23]

In 2020, many people in the United States may have spent more time online than ever before due to government-imposed lockdowns,[7] with internet usage continuing to increase to this day. From work meetings to school lessons to training sessions, even within public administration, many things that we used to do offline, we now do online.

The information that government agencies contain is very important and can be very harmful to the country if breached. Let's take a look at some examples of cyberattacks that targeted government agencies:

Office of Personnel Management (OPM) Breach (2015)

One of the most significant cyberattacks on the U.S. government occurred in 2015 when hackers believed to be linked to China infiltrated the Office of Personnel Management. This breach compromised the confidential information of over 22 million current and former federal employees.[14] The stolen data included personnel files, security clearance information and background investigation files. The OPM breach highlighted the vulnerability of government agencies to sophisticated cyber threats.

Solar Winds Supply Chain Attack (2020)

This was a massive, highly innovative supply chain attack discovered in December 2020 and named after its victim, Austin-based IT management company Solar Winds. The incident was carried out by APT 29, an organized cybercrime group with ties to the Russian government. In this incident, malicious actors compromised the software update mechanism of Solar Winds' Orion software platform. During the attack, threat actors injected malware, later known as Sunburst or Solorigate malware, into Orion's updates. The updates were then distributed to Solar Winds customers. The Solar Winds attack is considered one of the most serious cyber

espionage attacks against the United States for successfully targeting the U.S. military, many U.S.-based federal agencies, including those responsible for nuclear weapons, critical infrastructure services, and the majority of Fortune 500 organizations. This cyberattack revealed the extent of supply chain vulnerabilities in modern cybersecurity.[16]

Democratic National Committee (DNC) hack (2016)
The 2016 DNC hack made headlines during the US presidential election. Russian hackers allegedly linked to the Russian government broke into the DNC's email servers and leaked sensitive information and documents to the public via WikiLeaks.[15] The incident sparked concerns about foreign interference in American elections and led to increased scrutiny of cybersecurity practices in political organizations.\

Stuxnet Worm (2010)
Stuxnet is a sophisticated computer worm believed to have been developed by the governments of the United States and Israel.[24] Their target was Iran's nuclear facilities, particularly the Natanz uranium enrichment plant. Stuxnet caused physical damage by manipulating the programmable logic controllers of centrifuges, slowing Iran's nuclear program. While not a traditional cyberattack, Stuxnet represents a new era of digital warfare with physical consequences.

WannaCry ransomware attack (2017)

The attack was a major security incident that impacted organizations all over the world. On May 12, 2017, the WannaCry ransomware worm spread to more than 200,000 computers in over 150 countries. Notable victims included some US government agencies, FedEx, Honda, Nissan, and the UK's National Health Service (NHS), the latter of which was forced to divert some of its ambulances to other hospitals.[25] This ransomware exploited a Windows vulnerability and encrypted users' data, within hours of the attack, WannaCry was temporarily neutralized. A security researcher discovered a "kill switch" that essentially turned off the malware. However, many affected computers remained encrypted and unusable until the victims paid the ransom or were able to reverse the encryption. Although the primary target of the attack was not the government, however, this incident highlighted the potential impact of ransomware on critical infrastructure and government services.

Colonial Pipeline Ransomware Attack (2021)
The 2021 Colonial Pipeline ransomware attack highlighted the vulnerability of critical infrastructure to cyber threats. Dark Side, a ransomware group, has targeted the largest fuel pipeline in the United States, causing fuel shortages and widespread disruption along the East Coast.[11] While this incident was not a direct attack on the government, it highlighted the interconnectedness of the public and private sectors in the face of cyber threats.

Cyberattacks on the Pentagon (Continuous)
The Pentagon, the headquarters of the US Department of Defense, is a constant target of cyberattacks.[16] These attacks, often attributed to state-sponsored hackers, aim to gather intelligence, disrupt military operations or gain the upper hand in potential conflicts. The U.S. government continues to invest heavily in cybersecurity measures to protect its military and national security interests.

Microsoft Exchange Remote Code Execution Attack (2021)
In March 2021, a large-scale cyberattack was carried out against Microsoft Exchange, a popular corporate email server. It exploited four separate zero-day vulnerabilities discovered in Microsoft Exchange servers. These vulnerabilities allow attackers to spoof untrusted URLs and use them to access an Exchange Server system and provide a direct server-side storage path for malware. It is a Remote Code Execution (RCE) attack that allows attackers to completely compromise a server and gain access to all of its data. On affected servers, attackers stole sensitive information, injected ransomware, and deployed backdoors that were nearly undetectable. In the United States alone, the attacks affected nine government agencies and more than 60,000 private companies.[12]

III. WHAT MAKES THE PUBLIC SECTOR A MAGNET FOR CYBERATTACKS?

In the rapidly evolving technology landscape, where innovation and Digital transformation is at the forefront as we constantly push the boundaries of what is possible, a parallel and equally significant development is taking place. This is the evolution of cyber threats aimed at exploiting the digital landscape. These threats are becoming increasingly sophisticated and complex. The increasing trends in cyber threats require organizations to prioritize robust network security measures. It is of utmost importance to protect critical assets, protect sensitive data and ensure uninterrupted business operations. As cyber threats continue to increase, companies must prioritize protecting their networks to ensure data security.
Government agencies' digital servers contain confidential information and if the server is encrypted or the data is breached, it can have drastic implications at the national level.[2] From defense secrets to information about citizens, the government has the most important information about the country. This makes government agencies prime targets for cyber attackers. Therefore, why cybersecurity is important to the government is evident from the national security concerns arising from cyberattacks. It is not by chance that cybercriminals target the public sector. From the high volume of data to the attractiveness of public disclosure, there are many reasons why the public sector attracts cybercriminals as they plan their next big attack.

The goldmine of public sector data

Public sector organizations are entrusted with a wealth of sensitive and valuable data, including citizen records, government operations and critical infrastructure.[9] This breadth and depth of information is inherently attractive to cybercriminals who want to exploit it for various purposes. With the public sector overseeing critical infrastructure for public transportation, healthcare and education, the potential harm from exploited data is widespread. Login credentials, personal email addresses, addresses, identification information, payment details and more could be at risk if cyber security measures fail.

Outdated technology and security measures

Public sector organizations often struggle to keep up with the latest technology and cybersecurity measures. Outdated IT systems and software contain vulnerabilities that are well documented and known to cyber attackers. These vintage technologies lack the security features of their modern counterparts and provide cybercriminals with a treasure trove of entry points. Connecting legacy government systems can also increase the impact of a successful cyberattack. A breach in one department can potentially spread to other agencies and systems, creating a cascading effect.

Limited Security Budgets and Understaffed Teams

Compared to private sector companies with larger budgets, many public sector organizations are not fully prepared to defend against a cyberattack, especially in the most vulnerable departments: security, finance and IT. The public sector's heavy reliance on taxpayer dollars creates budget constraints and red tape, which in turn makes it difficult to implement comprehensive cybersecurity measures appropriate to the level of risk. A 2021 International City/County Management Association (ICMA) report concluded that the top three barriers to cybersecurity for local governments are the inability to pay competitive wages, insufficient cybersecurity staffing, and a general lack of funding.[10]

The lure of public disclosure for hackers

Public sector companies handle vast amounts of sensitive information, from citizen data to classified national security details, and the public's trust in these institutions means that any security breach can have widespread impact and public scrutiny. Cybercriminals are motivated by the opportunity to disrupt operations, steal valuable data, or threaten public trust. Therefore, the public sector becomes an attractive target because of its potential to gain notoriety, spark political unrest, and exploit the fear and uncertainty that a data breach or cyberattack can create among the public.[13]

Geopolitical Strategy and Cyberwarfare

Disruption or infiltration of public sector organizations can have profound geopolitical implications, allowing cybercriminals to exert pressure, gain strategic advantages, and advance their political and military goals.[19] For example, by compromising critical infrastructure and stealing sensitive data. Cybercriminals can destabilize governments, undermine public trust and manipulate international relations. The public sector represents a high-value target for cybercriminals seeking to exploit vulnerabilities for geopolitical purposes, making it a key battleground in the complex environment of cyberwarfare and state-sponsored hacking.

IV. STRATEGIES TO SAFEGUARD THE PUBLIC SECTOR IN THE DIGITAL ERA

Now that real-life examples have exposed the serious impact of cyberattacks on the public sector, there is more urgency than ever to protect public organizations from these digital attacks. The strategies listed below form a dynamic arsenal designed to protect public sector entities from the relentless evolution of cyber threats and strengthen the resilience of critical systems.

Security Awareness Training: Ensure all employees receive regular training on the importance of cybersecurity, current threats, and best practices. Use real-world examples, run simulations, and make sure everyone understands their role in protecting the company's data.

Multi-Factor Authentication (MFA): Implement MFA across all systems, especially for privileged accounts. This additional layer of security ensures that unauthorized access can be effectively prevented even if credentials are compromised.

Endpoint Security: Use advanced endpoints Protection platforms that outperform traditional antivirus solutions. These platforms should provide real-time monitoring, threat detection, and automated responses to suspicious activity.

Network Segmentation: Isolate sensitive data by segmenting your network.[1] This precaution ensures that even if attackers gain access to part of the network, reaching critical systems or data becomes a daunting challenge.

Regular Patches and Updates: Keep all systems, applications and devices secure by regularly updating them to the latest security.[1] Automated patch management solutions can efficiently streamline this process.

Incident Response Plan: Develop and update a comprehensive incident response plan.[17] Conduct regular drills to ensure everyone involved is familiar with their roles and responsibilities in the event of a breach.

Backup and Disaster Recovery: Back up important data and systems regularly and store backups both on-site and off-site. Routine testing of the recovery process ensures data integrity and availability.[18]

Zero Trust Architecture: Leverage a zero trust framework where every access request is subject to thorough vetting, regardless of its origin. This approach minimizes the likelihood of internal threats and breaches due to compromised credentials.

Continuous Vulnerability Assessments: Conduct regular vulnerability assessments and penetration testing to identify vulnerabilities in your systems and applications.[6] Remediate discovered vulnerabilities promptly to maintain robust defenses.

V. CONCLUSION

In conclusion, the imperative of bolstering cybersecurity in our interconnected world cannot be overstated. Cybersecurity is the linchpin for safeguarding government operations and protecting sensitive data from emerging cyber threats. As governments increasingly rely on digital platforms to enhance functionality and transparency, the risk of cybercrime, including data breaches, unintentionally escalates. The public sector, with its wealth of valuable information, is a prime target for cyber attackers, as evidenced by recent findings highlighting its vulnerability. The financial repercussions of cyber threats underscore the urgent need for robust cybersecurity measures.

The United States, like many other nations, faces persistent cyber threats, ranging from state-sponsored attacks to financially motivated hacking groups. With the government's commitment to cybersecurity evident in budget allocations and strategic objectives, efforts to defend against cybercrime remain a top priority. However, the complexity and economic impact of cyberattacks continue to escalate, necessitating a proactive approach to cybersecurity.

The public sector's attractiveness to cybercriminals stems from various factors, including the volume of sensitive data, outdated technology, and the potential for public disclosure. Moreover, cyberattacks on government agencies can have profound geopolitical implications, making them a battleground in the evolving landscape of cyberwarfare.

To safeguard the public sector in the digital age, organizations must prioritize robust cybersecurity strategies. These include security awareness training, multi-factor authentication, advanced endpoint security, network segmentation, regular patches and updates, incident response planning, backup and disaster recovery, zero trust architecture, and continuous vulnerability assessments. By adopting these proactive measures, public sector entities can enhance their cyber resilience and mitigate the risks posed by cyber threats in the digital era.

VI. REFERENCES

1. Auxin. (2023b, July 31). Network Security: Safeguarding major industries in a digital era. *Medium*. https://auxinsec.medium.com/network-security-safeguarding-major-industries-in-a-digital-era-e1e90502674c
2. Ccoeseo. (2023, November 1). Why Cybersecurity is Crucial for Government: Protecting Our Nation in the Digital Age. *Medium*. https://medium.com/@ccoeseo/why-cybersecurity-is-crucial-for-government-protecting-our-nation-in-the-digital-age-b79cec688423
3. Clarke, Richard A. *Cyber War*, HarperCollins (2010) ISBN 9780061962233
4. *Cost of a data breach 2023 | IBM*. (n.d.). https://www.ibm.com/reports/data-breach
5. *Cybersecurity Is Critical for all Organizations – Large and Small*. (2023, October 23). IFAC. https://www.ifac.org/knowledge-gateway/preparing-future-ready-professionals/discussion/cybersecurity-critical-all-organizations-large-and-small
6. Dimitris. (2022, March 21). Vulnerability assessments vs. penetration testing. *Hack The Box*. https://www.hackthebox.com/blog/vulnerability-assessments-vs-pentesting
7. Drouin M., McDaniel B.T., Pater J., Toscos T. How parents and their children used social media and technology at the beginning of the COVID-19 pandemic and associations with anxiety. Cyber psychology, Behavior, and Social Networking. 2020;23(11):727–736.
8. *Exploring Zero Trust: Navigating the digital Security maze*. (2024, February 22). TECKPATH | Managed IT Services | Business IT Support. https://teckpath.com/navigating-the-digital-labyrinth-the-zero-trust-model-explained/
9. *Guarding Governance: Cybersecurity in the public sector | UPGuard*. (n.d.). https://www.upguard.com/blog/cybersecurity-in-the-public-sector
10. *Inadequate Funding Biggest Barrier to Local Governments Achieving High Levels of Cybersecurity*. (2017, May 2). icma.org. https://icma.org/articles/press-release/inadequate-funding-biggest-barrier-local-governments-achieving-high-levels-cybersecurity
11. Kerner, S. M. (2022, April 26). *Colonial Pipeline hack explained: Everything you need to know*. https://www.techtarget.com/whatis/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know
12. Levy, M. (2023, December 20). *What is a Cyber Attack | Types, Examples & Prevention | Imperva*. Learning Center. https://www.imperva.com/learn/application-security/cyber-attack/
13. Lillian Ablon, *Data Thieves: The Motivations of Cyber Threat Actors and Their Use and Monetization of Stolen Data*, Santa Monica, Calif.: RAND Corporation, CT-490, 2018 https://www.rand.org/content/dam/rand/pubs/testimonies/CT400/CT490/RAND_CT490.pdf
14. *OPM hack hit over 22 million people | Congressman Ted Lieu*. (2015, July 13). Congressman Ted Lieu. https://lieu.house.gov/media-center/in-the-news/opm-hack-hit-over-22-million-people
15. *Satter, Raphael; Donn, Jeff; Day, Chad (November 4, 2017). "Inside Story: How Russians Hacked the Democrats' Emails: How did Russian hackers pry into Clinton campaign emails? Huge effort made quick work". US News. Associated Press. Retrieved November 28, 2017.*

16. SecurityScorecard. (2024, January 18). *The Top 7 Cyberattacks on U.S. Government A closer look at the evolving landscape of cybersecurity | SecurityScorecard*. https://securityscorecard.com/blog/top-cyberattacks-on-us-government
17. Sevefjord, M. (2023, January 26). *Magnus Sevefjord on LinkedIn: 2023 cybersecurity predictions that should be on your radar*. https://www.linkedin.com/posts/magnus-sevefjord-54372111_2023-cybersecurity-predictions-that-should-activity-7024435419236679681-XcwF
18. SoSafe. (2024, February 23). Top 5 cyber threats facing the public sector. *SoSafe*. https://sosafe-awareness.com/blog/top-5-cyber-threats-facing-the-public-sector
19. Team, C. T. I. (2023, December 18). *Geopolitical factors shaping the future of the cyber domain*. Critical Start. https://www.criticalstart.com/geopolitical-factors-shaping-the-future-of-the-cyber-domain/
20. The Hacker News. (n.d.). *Database of over 198 million U.S. voters left exposed on unsecured server*. https://thehackernews.com/2017/06/us-voters-data-leaked.html
21. *Topic: U.S. government and cybercrime*. (2024, February 29). Statista. https://www.statista.com/topics/3387/us-government-and-cyber-crime
22. *Trending Topics: all about IT security | Myra Security*. (2023, December 21). Myrasecurity.com. https://www.myrasecurity.com/en/news/it-security-news-december-2023/
23. Trust, O. A. (n.d.). *Ormiston Ilkeston Enterprise Academy - Digital Safeguarding*. Ormiston Academy Trust. https://www.oiea.co.uk/key-info/safeguarding/digital-safeguarding
24. *What is Stuxnet? | Trellix*. (n.d.). Trellix. https://www.trellix.com/security-awareness/ransomware/what-is-stuxnet/
25. *What was the wannacry ransomware attack?* | Cloudflare, https://www.cloudflare.com/learning/security/ransomware/wannacry-ransomware/

