Breaking into the State: Analyzing the 2012 South Carolina Department of Revenue Data Breach

A Case Study

Daniel Londoño Bohorquez

Author Note

Daniel Londoño Bohorquez, B.Sc. Systems and Computing Engineering, University of Los Andes (Colombia); Postgraduate Degree in Cybersecurity, George Brown College (Canada).

This research is done for the Legality and Compliance in Security course at George Brown for Professor John Wang.

Correspondence concerning this article should be addressed to Group 5, T443 Program, George Brown College, Toronto, ON M5R 1M3.

Abstract

In 2012, the State of South Carolina made the headlines as the victim of one of the largest data breaches in the U.S history at the time. The breach occurred when a state IT contractor at the Department of Revenue clicked on a malicious link, setting off a chain of events that lead to widespread disruption. Not only for the state government but also for the millions of residents whose private information was compromised.

As CISO of the Department of Revenue, the main objective of this report is to establish a set of recommendations and active measures to mitigate the effects of the breach and prevent future incidents. This analysis will be conducted within the McCumber Cube framework, exploring the relevant intersections to illustrate a comprehensive understanding of the vulnerabilities and controls involved. The focus will specifically be on how the breach impacted the security goals of Confidentiality and Integrity primarily, considering there were no disclosed Availability issues, while determining its corresponding information states (processing, storage, and transmission). By addressing these aspects, the report aims to deliver practical recommendations for enhancing the protection of sensitive information.

In August 2012, the South Carolina Department of Revenue (SCDOR) fell victim to a major cybersecurity breach that compromised the personal data of millions of residents. According to Mandiant, the cybersecurity firm hired by the SCDOR to handle the incident response, the breach began with a targeted phishing attack on August 13, 2012 (Mandiant, n.d., p. 2). Malicious emails were sent to multiple employees within the department, which ultimately allowed the attacker to gain unauthorized access to sensitive data. The breach exposed sensitive information such as taxpayer information, Social Security numbers (SSN), bank account details, and even driver's license numbers, making it one of the most significant data breaches in U.S history. This firstly indicates that the attack vector was an email-based phishing campaign aimed at gaining an initial foothold within the organization. At the time, that is approximately 12 years ago, email security measures were not as sophisticated as they are today. It's not surprising that these phishing emails managed to bypass the company's filters, if there were any in place (none were disclosed), and went undetected. The attacker logged into the remote access service using the credentials obtained from on of the victims (Mandiant, n.d., p. 3). *Rescator*, alias for the alleged author of the attack (Krebs, 2024), gained then the ability to perform lateral movement across six different servers (Mandiant, n.d., p. 3) by performing credential dumping. Finally, he got access to crucial databases containing the personally identifiable information (PII) —as stated previously— of millions of South Carolina residents. The cyberattack resulted in the exfiltration of this sensitive data belonging to over 3.6 million residents (Krebs, 2024). The breach not only caused significant disruption to the state's operations but also resulted in considerable financial losses and a widespread loss of trust among the citizens.

Although the exact type of malware and the specific payload executed remain undisclosed, it is known that the malware was capable of dumping credentials. Hash dumping is a common technique used for privilege escalation and unauthorized access, among other tactics. Famous *dumping* binaries, such as Mimikatz, released in 2011, could have potentially been employed in this attack. The Public Incident Response Report (PIRR) states, "*The attacker executed utilities designed to obtain user account passwords on six servers*" (Mandiant, n.d., p. 3). Identifying the potential programs used, such as Mimikatz, is crucial for us moving forward since many countermeasures for these tools share common strategies.

First and foremost, Confidentiality is the most critical aspect in this case. The breach exposed sensitive user information, enabling the attacker to commit tax refund fraud and sell the exfiltrated data. Alarmingly, this information was made available on cyber forums, significantly increasing the overall risk. According to Mandiant's PIRR, the attacker exfiltrated over 74GB of data from twenty-three database backup files (Mandiant, n.d., p. 3), along with other important documents, including the encrypted version of the data encryption key (Mandiant, n.d., p. 4). This incident explains the urgent need for stronger safeguards to protect confidential data and prevent unauthorized access.

Regarding integrity, while the breach itself did not directly impact the involved parties, the criminals who exploited the exfiltrated data to commit tax fraud represent a significant Integrity issue for both the SCDOR and the federal government. According to a 2013 report by the Treasury Inspector General, the U.S Internal Revenue Service (IRS) disbursed nearly $4 billion in fraudulent tax refunds in 2012 and over $5.8 billion in 2013 (Krebs, 2024). This demonstrates how the exfiltration of sensitive data can serve as a precursor to broader Integrity issues. That's why this report will also offer recommendations for other involved parties, such as the IRS, considering the fact that the SCDOR was the point of failure.

Lastly, regarding Availability, it is important to clarify that the breach did not result in any availability issues. According to Mandiant's report, there were no disruptions or interference with the system during the time the attacker had access. The breach primarily affected Confidentiality, which is why availability will not be considered in the McCumber Cube analysis.

Although the exact phishing technique the attacker used to gain an initial foothold remains unclear (Mandiant, n.d., p. 2), it is essential that every SCDOR employee maintains updated antivirus software and avoids clicking on unknown links or downloading files without first verifying the sender's identity and the legitimacy of the content. Social engineering can take many forms, so all potential entry points must be proactively secured to counter threats effectively. However, these measures only protect the perimeter, much like a fence around a house. To secure the internal system, additional safeguards are needed to prevent lateral movement as effortlessly as Rescator did in this case. This includes ensuring that credentials are never stored in plaintext, implementing robust access control measures, and applying the principle of least privilege.

Literature Review

The nature of the malware remains unknown. However, as previously mentioned, it is very likely that during the post exploitation phase the attacker used a password dumping tool to collect unprotected credentials. Tools like Mimikatz, arguably on of the most famous applications in Red Teaming operations, work by extracting credentials stored in memory, such as plaintext passwords, password hashes, and even Kerberos tickets (Newman, n.d.). In spite of the fact that the exact method remains unknown, the attack could have involved a simple shell that enabled Remote Code Execution (RCE), which then served as a gateway for executing password-dumping binaries. Regardless of the specific tool or technique used, it’s clear that the source of the breach was fundamentally due to human factors. The SCDOR’s systems themselves had no major issues, indicating that the technical aspects alone were not sufficient to prevent the intrusion. This is why the following analysis will have a strong focus on addressing the human factor.

The U.S Department of Justice, the FBI, and even the U.S Secret Service have been leading independent investigations yet none have been able to establish the exact identity of the individual responsible for this breach (Krebs, 2023). The individual seems to also have been behind Home Depot and Target’s data breach in 2014, using similar delivery techniques.

The complexity of cyber threats, such as those associated with the SCDOR breach, highlights the necessity for comprehensive security frameworks. One such model that addresses numerous aspects of cybersecurity is the McCumber Cube. This three-dimensional framework provides a structured approach to understand and manage information security by incorporating the information being protected, the security measures employed, and the stages of information processing. In order to appropriately understand the implications of these dimensions, it is essential to explore the intersections within the McCumber Cube. By examining each cell of this framework, we will analyze how the characteristics of the compromised data, its locations, and the corresponding security controls relate to the vulnerabilities exploited in the SCDOR breach.

While we could examine all twenty-seven intersections of the McCumber Cube, it's crucial to identify those that hold actual significance in relation to the events that unfolded in this case study. Mayhem began with the exfiltration of sensitive information that was at rest, categorizing this incident primarily as a Confidentiality breach.

Literature defines Confidentiality as “*limiting access to information only to those who need it, and preventing access by those who do not*” (Whitman and Mattord, 2014, pg. 8) However, the consequences went beyond mere theft. The actions taken by third parties clearly revealed integrity issues related to the fraudulent use of the stolen data. This manipulation of sensitive information not only sabotaged the authenticity of tax records but also weakened the overall trust in the tax system, that’s why Integrity is part of this discussion. By focusing on these critical intersections, we can gain a clearer understanding of the complexities of this breach and its wider implications.

Confidentiality

Storage.

The McCumber Cube model emphasizes the importance of maintaining confidentiality during all stages of data. These include the storage, processing, and transmission stage. In the context of the SCDOR data breach, the attacker compromised sensitive data primarily through database backup files. The attacker copied and compressed 23 backup files, for a total of 8.2 GB of data (Mandiant, n.d., p. 4). The SCDOR had in place a two-key encryption scheme based on AES-256 to protect this data, with one key encrypting the data itself and the second key securing the encryption key (Mandiant, n.d., p. 4). Despite this, the attacker was able to exfiltrate and subsequently sell the data, indicating that the encrypted version of the encryption key was likely accessible somewhere within the system. We assume this as a fact, given that breaking AES-256 encryption through brute force is computationally infeasible. Even with a quantum computer, it would take approximately 2.29×10^{32} years to crack (Ubiq Security, n.d.). This points out a critical vulnerability in the encryption key management process. Either the key was poorly protected, or an improperly secured access point allowed the attacker to retrieve it.

Technology: Strengthening encryption key management is crucial. One effective approach would be to use Hardware Security Modules (HSMs) or Key Management Systems (KMS), which provide secure, tamper-resistant storage for encryption keys (Entrust, n.d.). These significantly reduce the risk of unauthorized access. Additionally, multi-factor authentication (MFA) should be enforced for any system that accesses sensitive encryption keys, adding an extra layer of protection against unauthorized access. Regularly performing security audits with tools like WinPeas, a binary used to identify security weaknesses on Windows systems, such as misconfigured permissions and leftover credentials, can also help system administrators detect vulnerabilities that could facilitate privilege escalation or lateral movement within the network. Often, these loose credentials are easily accessible and can serve as a gateway to unauthorized access of additional systems or, in the case of an Active Directory environment, provide attackers with the means to compromise domain controllers, potentially gaining full control of the network. With these measures set up, the likelihood of a similar breach occurring on the technical side would be significantly reduced. Collectively they would strengthen the security posture making it much harder for attackers to exploit vulnerabilities and gain unauthorized access.

Policy: This case study demonstrates a failure by the department of revenue to enforce the principle of least privilege and proper access control policies. Additionally, it's important to mention that the SCDOR has not publicly disclosed any formal cybersecurity policies, likely because its a government agency. As a result, the analysis for this intersection of the McCumber Cube (Confidentiality-Storage-Policy) will be developed under the assumption that there were no formal policies in place to govern access control or data protection at the time of the breach.

We also assume that the compromised account had a considerable level of unrestricted access to sensitive files, or even entire systems, allowing the attacker to move laterally across the network and escalate privileges. The assumption that the compromised account had a considerable level of unrestricted access to sensitive files is justified based on the behavior observed in the breach, disclosed by Mandiant. The attacker's ability to exfiltrate a large volume of data, including sensitive database backup files, suggests that the compromised account had more than just limited access. Additionally, the report indicates that the attacker was able to perform lateral movement across six different servers (Mandiant, n.d., p. 3). Lateral movement is typically facilitated by accounts with elevated privileges or broad access rights (Microsoft, n.d.), as attackers often exploit these privileges to navigate through the network undetected. This level of access would have been necessary to escalate privileges and exfiltrate sensitive data without triggering immediate alarms.

To address the risk of unauthorized access and data exfiltration, an Issue-Specific Policy (ISP) will be implemented to reinforce the Confidentiality of data during storage. In the first place, a robust email filtering system will be implemented to prevent phishing emails from reaching inboxes, particularly those that may attempt to gain access to data stored within sensitive systems. Email authentication protocols, especially Sender Policy Framework (SPF), will also be enforced in order to block fraudulent emails that could be used to gain access to sensitive information, given the fact that this protocol helps verify that incoming emails are sent from authorized mail servers, reducing the risk of email spoofing and ensuring that only legitimate communications reach the inbox (Cloudflare, n.d.). Additionally, the policy will enforce multi-factor authentication (MFA) for email accounts, adding an extra layer of security to prevent unauthorized access to sensitive credentials, which could have been used to access files stored on the servers, as was the case in this breach.

In addition, we assume that the decryption key was stored in close proximity to the server containing the encrypted backup files, based on the attacker's ability to decrypt and exfiltrate data without requiring extensive additional compromises. This proximity creates a significant security weakness, as storing the encrypted files and their decryption key in such close locations clearly weakens the effectiveness of encryption. To address this, we propose implementing robust segmentation policies to ensure that backup files and decryption keys are stored on highly isolated systems, separated from the primary infrastructure. This segmentation would mitigate the risk of attackers gaining access to both the encrypted data and the keys, greatly enhancing the overall security framework.

Finally, in order to strengthen data confidentiality during storage, the SCDOR will implement role-based access controls (RBAC) to limit access to sensitive data based on the principle of least privilege. Sensitive data should only be accessible to those who require it for their role, and unnecessary access to stored data should be eliminated. Segregation of Duties (SoD) will be enforced to ensure that personnel responsible for managing encryption keys do not have access to the encrypted data itself. Regular audits of access controls will be conducted to ensure that no misconfigurations, loose credentials, or unmonitored access points allow unauthorized access to stored sensitive data.

By combining email security measures with strict access control practices, this ISP will significantly reduce the risk of unauthorized access to sensitive data at rest, safeguarding its confidentiality and ensuring that it is properly protected during storage.

Training & Education: Employee training is essential in order to prevent similar breaches in the future. System administrators and IT staff will receive specialized training on best practices for encryption key management, as well as how to properly configure Access Control Lists (ACLs) to enforce strict access controls. This training will ensure that ACLs are effectively used to define and manage user permissions, restricting access to sensitive data based on the principle of least privilege. By properly configuring ACLs, the organization can reduce the risk of unauthorized access to our systems. Taking into account that the breach originated from the compromised account of a contractor (Krebs, 2024), it's vital that all third-party users—such as contractors, vendors, and partners—who have access to the organization's systems receive training on the same security protocols and best practices as full-time employees, as long as it is relevant to their level of access. The staff must be educated on the dangers of social engineering, particularly phishing attacks, the initial point of entry in this breach. Regular security awareness programs should also focus on credential management and the importance of not leaving improperly secured data in the system. Additionally, mandatory phishing simulations should be conducted to help employees recognize suspicious emails or activities, aiming to reduce the overall risk.

Processing.

The McCumber Cube model highlights the importance of maintaining confidentiality during the information processing phase. In the context of this data breach, while the attacker's actions—such as copying database backup files, compressing them into encrypted 7-zip archives, and exfiltrating the data—are documented, it is also reasonable to work under the assumption that data actively being processed at the time could have been compromised.

While the Mandiant report does not explicitly confirm that actively processed data was affected, the attacker's ability to interact with servers and execute administrative commands indicates a plausible risk to the confidentiality of data during processing. For example, the attacker performed reconnaissance activities on multiple live systems, including web servers handling payment maintenance information (Mandiant, n.d., p. 3). Although the report notes that no malicious actions were confirmed during these interactions, the possibility of observing or accessing up and running data cannot be dismissed. Additionally, the use of "multiple generic utilities to execute commands against databases," as reported (Mandiant, n.d., p. 3), suggests the attacker may have interacted directly with the systems handling live data. These utilities often allow CRUD operations in real time, depending on the permissions granted. When combined with the attacker's installation of a backdoor (a persistent access point) it becomes very likely they could read or manipulate data as it was being processed.

Technology. In order to mitigate risks during data processing, more robust technologies are essential to protect sensitive information. A Data Loss Prevention (DLP) system could have significantly reduced the impact of the SCDOR data breach. DLP systems monitor and regulate data access and transfers, which could have blocked the unauthorized exfiltration of taxpayer records. These tools also enforce encryption and access policies, ensuring sensitive data remains secure even if accessed. It also provides real-time alerts for unusual activity, meaning this system would have allowed faster detection and response, minimizing the breach's scope. Additionally, real-time monitoring solutions and a logging mechanism are essential. They enable live surveillance of system interactions, allowing immediate detection of any suspicious and unusual events. Together these technologies form a multi-layered defense, significantly reducing the opportunity for attackers to exploit vulnerabilities during active data processes. As an extra security measure, technologies such as Runtime Application Self-Protection (RASP) can detect and immediately block malicious behaviors at the application level during runtime (Check Point, n.d.). With these recommendations in place, the likelihood of Confidentiality being compromised while being processed is greatly diminished.

Policy. Protecting data during processing requires addressing the specific risks that arise at the processing stage. A key focus should be on implementing effective approval mechanisms in the processing environment. To mitigate these risks, an ISP should be developed to rule administrative operations on live systems. This policy would require pre-authorization for any commands involving sensitive data, managed through a secure approval platform to ensure that every action is validated and well documented. The platform should also maintain detailed audit trails, creating a clear record of the approval process for accountability. With these measures in place, the department can significantly reduce the risk of unauthorized actions and secure sensitive data during processing.

The proposed ISP tackles a critical gap in the protection of sensitive data during processing. Administrative operations on live systems represent one of the highest-risk activities in any environment, as they often involve direct interaction with sensitive information. Without pre-authorization and proper documentation, these activities can lead to errors, misuse, or exploitation by malicious actors, as demonstrated in this case. By requiring pre-authorization through a secure approval platform, this ISP ensures that every action is deliberate, justified, and executed with accountability. Even if an attacker were able to gain a backdoor or escalate privileges to the highest level, such as NT AUTHORITY\SYSTEM, their actions would still require approval to proceed, significantly reducing their ability to exploit the system and thus limiting the potential impact of such a breach.

Keeping detailed audit trails adds another layer of security by creating a clear and thorough record of every action taken. This helps discourage unauthorized activities and makes it easier to carry out forensic investigations or meet compliance requirements. Systems like Microsoft's Privileged Access Management (PAM) or CyberArk's workflows already use similar pre-authorization mechanisms for sensitive administrative actions, showing that requiring approval for high-risk tasks is both practical and effective. With this policy in place, the organization can be in control in a more effective way and monitor live data processes with ease, ensuring sensitive information stays protected.

Training and Education: Any employee or authorized third parties involved with active data processes, such as database administrators, system operators, or IT support staff handling live systems, must receive specific training on the secure use of approval platforms and the authorization of sensitive administrative operations. This training should cover step-by-step procedures for submitting, reviewing and interpreting commands and audit logs, and identifying unauthorized or suspicious activity during processing. A PowerShell and Bash crash course is also highly recommended due to the fact that these scripting languages are commonly used in administrative operations and log analysis. Apart from automating processes, it can also be very helpful to understand anomalies and respond effectively to potential threats. By understanding the approval process, employees can effectively prevent unauthorized actions and ensure accountability.

Such training should also focus on real-world scenarios, such as identifying anomalies similar to those observed during the breach, when the alleged hacker, *Rescator*, exploited compromised credentials to gain server access. Employees should learn to recognize patterns of malicious activity, like repeated failed login attempts or unexpected database interactions, and escalate them promptly. Given that the breach originated from a contractor, it is crucial that contractors and other third parties participate in this training to ensure they comply to the same security protocols and standards as full-time employees.

Transmission. While the McCumber Cube emphasizes the importance of securing data during transmission, this intersection doesn't play a significant role in this case study as the breach primarily involved unauthorized access to data at rest. The Mandiant report shows no evidence of intercepted data during transmission, with the attacker's efforts focused on stored data, such as database backup files. Because of this, measures like encryption protocols or secure communication channels for data in transit were not at all a factor in this incident. That said, securing data during transmission is always important and could have been essential if the breach had involved data in transit.

Availability

As previously mentioned, there were no availability issues associated with the data breach. Neither KrebsOnSecurity, Mandiant, nor any other source reported any availability disruptions during the incident. The breach was primarily a confidentiality issue.

Integrity

Although the South Carolina Department of Revenue and the Department of Treasury are two separate entities, the SCDOR should have taken a more proactive approach by promptly informing the IRS, credit bureaus, and other relevant parties about the breach. This would have allowed more protective measures to be implemented to mitigate identity theft and tax refund fraud, reducing the financial losses caused by the compromised system. This breach primarily affected the confidentiality of taxpayer information. Nevertheless, it escalated into a significant integrity issue, demonstrating how a breach targeting one dimension of the McCumber Cube, Confidentiality, can transition into another, Integrity. Hackers used the exfiltrated SSNs and financial details to commit tax refund fraud by filing false returns under fake identities (Krebs, 2024). In this case, the Integrity-Processing intersection of the McCumber Cube was the most affected, as fraudulent returns were processed based on compromised data. This led to significant financial losses, with the IRS disbursing over $5.8 billion in fraudulent tax refunds in 2013 alone, illustrating the far-reaching consequences of such breaches.

As for the aftermath of the breach, the focus shifts to the Integrity-Processing intersection since it represents the point where the fraudulent use of stolen taxpayer data directly affected the federal government. The integrity of tax processing systems was compromised as they relied on exfiltrated data to process falsified returns. This intersection is particularly relevant—and worth mentioning despite being a separate occurrence—because the breach's impact extended beyond the SCDOR's systems, bringing financial trouble to federal resources. Both actions and inactions of a single state led to billions of dollars in fraudulent refunds paid by the IRS, demonstrating the urgent need for greater accountability and preventive measures at the state level.

Other intersections, such as Integrity-Storage and Integrity-Transmission, are less relevant to this scenario. While Storage-Integrity could involve ensuring that taxpayer data within SCDOR systems remains unaltered, there is no evidence suggesting that the attackers tampered with stored data, they exploited its confidentiality rather than its integrity. In a similar way, secure transmission of data is crucial for prevention but did not play a role at all in the actual fraud, which occurred after the stolen data had been used within separate systems. Therefore, Integrity-Processing remains the most relevant focus in this context.

To address these issues within the Integrity-Processing intersection of the McCumber Cube framework, the SCDOR proposes a Breach Response and Fraud Prevention Framework in cooperation with the IRS. This includes a real-time breach notification and alert system for securely transmitting details of the compromised taxpayer records. While this system will serve as an important tool for mitigating the consequences of a breach, it is part of a layered approach to ensure timely coordination with the IRS to flag or reject fraudulent returns before further damage occurs. A Compromised Taxpayer List will also be shared with the IRS to identify and scrutinize tax filings linked to stolen data. Furthermore, the records of compromised taxpayers will be stored in an isolated, secure system to enhance protection against future unauthorized access. This segregation allows for stricter access controls, improved monitoring, and a more detailed list of audit trails to track all interactions with the data. It also facilitates optimal coordination with the IRS by ensuring the records are well-organized and readily available for secure transmission. By implementing these measures, the SCDOR demonstrates its commitment to protecting taxpayer data, preventing further exploitation of compromised data, and addressing issues that heavily impact federal resources and public trust, thereby reinforcing the integrity of vital government operations.

Additionally, in the unfortunate case of another data breach, the SCDOR will implement a mandatory freeze on compromised taxpayer accounts, preventing unauthorized use of stolen data. Affected taxpayers will be notified and provided with a secure portal to verify their identity as a means to lift the freeze as needed. Finally, a public awareness campaign will encourage taxpayers to enroll in the IRS Identity Protection PIN (IP PIN) program and monitor their accounts for unauthorized activity. By mainly focusing on this intersection, this approach addresses the core issue of tax refund fraud, reducing the risk of future fraudulent refunds and restoring trust in the tax system.

Conclusion

The 2012 SCDOR data breach highlights the far-reaching consequences of compromised confidentiality, including collateral impacts on data integrity and federal financial systems. This case study applies the McCumber Cube framework to analyze the breach and its aftermath, focusing on the Confidentiality dimension and the Integrity-Processing intersection, where fraudulent tax returns resulted in billions of dollars in losses to the IRS. The assumptions made throughout this investigation are supported by solid arguments and logical conclusions about the breach and all its consequences. While Mandiant's report lacked important details on key aspects, such as system versioning and security policies at the time, this analysis aims to fill those gaps through evidence-based reasoning. The recommendations focus on strengthening data security, improving collaboration with federal agencies, and implementing measures to protect taxpayer information while minimizing the risk of future fraud.

References

1. Krebs, B. (2023, December). Ten years later: New clues in the Target breach. Krebs on Security. Retrieved fromhttps://krebsonsecurity.com/2023/12/ten-years-later-new-clues-in-the-target-breach/
2. Newman, L. H. (n.d.). How Mimikatz became the go-to hacker tool. Wired. Retrieved from https://www.wired.com/story/how-mimikatz-became-go-to-hacker-tool/
3. National Cyber Security Centre (NCSC). (n.d.). Preventing lateral movement. Retrieved from https://www.ncsc.gov.uk/guidance/preventing-lateral-movement
4. Mandiant. (n.d.). APT1: Exposing one of China's cyber espionage units [PDF file]. Retrieved from https://oag.ca.gov/system/files/Mandiant%20Report_0.pdf
5. ManageEngine. (n.d.). Privilege escalation with WinPEAS. Retrieved from https://www.manageengine.com/log-management/cyber-security/privilege-escalation-with-winpeas.html
6. Ubiq Security. (n.d.). 128-bit or 256-bit encryption: Which to use?. Retrieved from https://www.ubiqsecurity.com/128bit-or-256bit-encryption-which-to-use/#:~:text=With%20the%20right%20quantum%20computer,than%20the%20universe%20has%20existed
7. Krebs, B. (2024, April). Who stole 3.6M tax records from South Carolina?. Krebs on Security. Retrieved from https://krebsonsecurity.com/2024/04/who-stole-3-6m-tax-records-from-south-carolina/
8. Whitman, M. E., & Mattord, H. J. (2021). Management of information security (6th ed.). Boston, MA: Cengage Learning.
9. Entrust. (n.d.). What are hardware security modules?. Retrieved from https://www.entrust.com/resources/learn/what-are-hardware-security-modules
10. Microsoft. (n.d.). Understand lateral movement paths in Defender for Identity. Retrieved from https://learn.microsoft.com/en-us/defender-for-identity/understand-lateral-movement-paths
11. Cloudflare. (n.d.). Understanding email security: DMARC, DKIM, and SPF. Retrieved from https://www.cloudflare.com/learning/email-security/dmarc-dkim-spf/
12. Check Point. (n.d.). What is Runtime Application Self-Protection (RASP)?. Retrieved from https://www.checkpoint.com/cyber-hub/cloud-security/what-is-runtime-application-self-protection-rasp/