

Background

The NIST cybersecurity framework is used by organizations to manage and mitigate their risk to cybersecurity threats. There are five core functions of the NIST CSF framework: identify, protect, detect, respond, and recover. In this assignment we will utilize the **Identify** and **Protect** functions of the NIST core framework to analyze the Equifax cyber security data breach.



Image: 5 core functions of the NIST CSF

Summary

Equifax is one of the 3 major credit rating agencies in the United states. In 2017 it reported a data breach that resulted in the compromise of 143 million Americans sensitive data. Data that included names, home addresses, phone numbers, dates of birth, social security numbers and driver's license numbers.

Identify

A key security patch for the apache struts framework was released on March 7th 2017 and all users were urged to immediately update their systems. The breach of Equifax's systems began on May 12th 2017 as a result of the companies failure to properly patch and update its systems. The initial data breach gave hackers access to equifax's internal corporate servers. In addition to the initial vulnerability, poor network design let hackers move around the network once they had breached the servers and gave them access to the customer database. Equifax also failed to properly encrypt

Personally identifiable information which would have significantly mitigated some of the effects of the attack. Furthermore Equifax's failure to implement an IPS/IDS gave the intruders time to perform more than 9000 scans of the databases, extract information into small temporary archives then transfer them off the Equifax servers to avoid detection. According to the incident report the activities went on for 76 days until July 29, 2017 when Equifax discovered the breach

Protect

As a matter of priority Equifax should have applied the critical patch as soon as it was available to prevent the data breach. Equifax should have properly encrypted personally identifiable information to ensure it was essentially useless if it was stolen. The company failed to implement a web application firewall to block malicious traffic. The company should also improve network design by segmenting the network to limit the damage caused in the future even if some parts of the network are compromised. According to the incident report information first pulled by the hackers included internal credentials for Equifax employees, which then allowed the hackers to search the credit monitoring databases under the guise of an authorized user. This suggests that employee credentials were not encrypted in the database and Equifax did not employ 2FA authentication on these employee accounts. As a part of their cybersecurity policy Equifax should encrypt all sensitive data and employ 2FA on all employee accounts.

The protect component of the NIST framework provides a comprehensive set of guidelines and best practices for implementing safeguards that help to reduce the likelihood and impact of successful cyberattacks. In the wake of the cyber attack Equifax was forced to settle numerous lawsuits. By following the guidelines and policies in the Protect component of the NIST CSF framework, companies can reduce the likelihood and impact of cyberattacks, which can lead to lower costs. The safeguards outlined in the protect component can make it more difficult for attackers to gain access to companies systems and data. This can help to reduce the risk of successful cyberattacks, such as data breaches, ransomware attacks, and denial-of-service attacks. The protect component of the framework specifically outlines policies for access control, employee training, data protection, protective technology and Information Protection Processes and Procedures

A post mortem of the Equifax data breach revealed several shortcomings in the company's cybersecurity policies and procedures. Equifax failed to implement a comprehensive cyber security policy which would have ensured that all critical assets were patched and updated in a timely manner. In addition from the known information about the breach it can be assumed that employees lacked training to properly respond to the breach once the systems were initially hacked. The company failed to implement encryption, network segmentation 2FA and other security hardening techniques. In addition the company also failed to implement technical solutions like web application firewalls and intrusion detection systems to help strengthen cyber security posture

Checklist

1. Identify security risks through regular audits of internal networks,
2. Implemented a regular schedule for patching and updating servers
3. Ensure that all personally identifiable information is encrypted
4. Implement a web application firewall to block malicious traffic.
5. Implement intrusion detection system
6. Develop policies to regularly scan for vulnerabilities on the companies servers and network
7. Implement 2FA authentication on all employee accounts.

Appendix

Prompts

1. Summarize the equifax data breach

The Equifax data breach was a major data breach that occurred in 2017. It was one of the largest data breaches in history, affecting over 147 million people in the United States, Canada, and the United Kingdom.

The breach was caused by a vulnerability in Equifax's web application software. Attackers exploited this vulnerability to gain access to Equifax's systems and steal personal information, including names, Social Security numbers, dates of birth, addresses, and driver's license numbers.

Equifax did not discover the breach until July 2017, and did not disclose it to the public until September 2017. This delay was met with widespread criticism, as it gave attackers time to exploit the stolen data.

The Equifax data breach had a significant impact on those affected. Many people experienced identity theft and fraud as a result of the breach. Equifax has offered affected individuals free credit monitoring and other services, but many people have still incurred financial losses and other hardships.

The Equifax data breach was a major wake-up call for businesses and consumers alike. It showed that even large and well-established companies can be vulnerable to cyberattacks. It also showed that consumers need to be vigilant about protecting their personal information.

Here are some key takeaways from the Equifax data breach:

- Businesses need to take cybersecurity seriously and invest in appropriate security measures.
- Consumers need to be careful about how they share their personal information and take steps to protect themselves from identity theft and fraud.
- Governments need to do more to regulate the data collection and sharing practices of businesses.

The Equifax data breach is a reminder that cybersecurity is a shared responsibility. Businesses, consumers, and governments all need to work together to protect our data and our systems from cyberattacks.

2. Define the NIST framework

The NIST Cybersecurity Framework (NIST CSF) is a voluntary framework of standards, guidelines, and best practices to help organizations manage and improve their cybersecurity risk. It is designed to be flexible enough to integrate with the existing security processes within any organization, in any industry.

The NIST CSF is organized around three main components:

1. Core

The Core is a set of cybersecurity activities that are considered essential for all organizations, regardless of size or industry. It is divided into five functions:

- Identify: Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.
- Protect: Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.
- Detect: Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.
- Respond: Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.
- Recover: Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

2. Implementation Tiers

The Implementation Tiers provide a way for organizations to measure their progress in implementing the NIST CSF. There are four tiers, with Tier 1 being the most basic and Tier 4 being the most advanced.

3. Profiles

A Profile is a document that describes an organization's current cybersecurity posture and its plans for improvement. It can be used to communicate cybersecurity risks and priorities to stakeholders, and to track progress over time.

The NIST CSF is a valuable tool for organizations of all sizes and industries. It can help organizations to:

- Identify and manage cybersecurity risks
- Improve their cybersecurity posture
- Communicate their cybersecurity risks and priorities to stakeholders
- Track their progress in improving their cybersecurity posture

The NIST CSF is also widely accepted by regulators and insurers. This means that organizations that implement the NIST CSF may be able to reduce their regulatory burden and insurance costs.

Benefits of using the NIST CSF

There are many benefits to using the NIST CSF, including:

- It is a voluntary framework, so organizations can implement it at their own pace and level of maturity.
- It is flexible and adaptable to any organization, regardless of size or industry.
- It is based on existing standards, guidelines, and best practices.
- It is widely accepted by regulators and insurers.
- It can help organizations to identify and manage cybersecurity risks, improve their cybersecurity posture, and communicate their cybersecurity risks and priorities to stakeholders.

How to get started with the NIST CSF

If you are interested in getting started with the NIST CSF, there are a few things you can do:

1. Download the NIST CSF from the NIST website.
2. Review the Framework and identify the areas where your organization can improve.
3. Develop a plan for implementing the NIST CSF.
4. Implement the NIST CSF and track your progress over time.

There are many resources available to help you implement the NIST CSF, including online training, templates, and tools. You can also find a community of NIST CSF users who can provide support and advice.

3. Apply the nist framework to the equifax data breach

The NIST Cybersecurity Framework (NIST CSF) is a voluntary framework that provides a common language and approach to managing cybersecurity risk. It is based on five core functions: identify, protect, detect, respond, and recover.

The NIST CSF can be applied to the Equifax data breach as follows:

Identify

Equifax failed to identify and assess the risks associated with a known vulnerability in its Apache Struts software. This vulnerability was publicly disclosed in March 2017, and Equifax did not patch the vulnerability until July 2017. This gave attackers a four-month window to exploit the vulnerability and gain access to Equifax's systems.

Protect

Equifax also failed to implement adequate security controls to protect its data. For example, Equifax did not have a web application firewall in place to block malicious traffic. Additionally, Equifax did not encrypt sensitive data, such as Social Security numbers, at rest or in transit.

Detect

Equifax did not have adequate systems in place to detect suspicious activity on its network. As a result, attackers were able to go undetected for several weeks and exfiltrate a massive amount of data.

Respond

Once Equifax discovered the data breach, it took six weeks to notify the public. This delay made it more difficult for affected individuals to take steps to protect themselves from identity theft and other fraud.

Recover

Equifax has taken steps to improve its security posture since the data breach. However, the company has not been able to fully recover from the damage caused by the breach. Millions of people have been affected by the breach, and many are still dealing with the consequences.

Recommendations

Equifax could have applied the NIST CSF to prevent the data breach or mitigate its impact. For example, Equifax could have:

- Implemented a process to identify and patch vulnerabilities promptly.
- Implemented a web application firewall to block malicious traffic.
- Encrypted sensitive data at rest and in transit.
- Implemented systems to detect suspicious activity on its network.
- Developed a plan to notify the public promptly in the event of a data breach.

Organizations can use the NIST CSF to improve their cybersecurity posture and reduce the risk of data breaches. The NIST CSF is a flexible framework that can be tailored to the specific needs of any organization

4. Why should companies follow the protect component of the NIST CSF framework?

Companies should follow the Protect component of the NIST CSF framework to protect their systems, assets, data, and capabilities from cybersecurity threats. The Protect component provides a comprehensive set of guidelines and best practices for implementing safeguards that help to reduce the likelihood and impact of successful cyberattacks.

Some of the key benefits of following the Protect component of the NIST CSF framework include:

- **Reduced risk of cyberattacks:** By implementing the safeguards outlined in the Protect component, companies can make it more difficult for attackers to gain access to their systems and data. This can help to reduce the risk of successful cyberattacks, such as data breaches, ransomware attacks, and denial-of-service attacks.
- **Improved compliance:** Many industry regulations and standards require companies to implement certain cybersecurity safeguards. The Protect component of the NIST CSF framework can help companies to comply with these requirements.
- **Reduced costs:** The cost of recovering from a cyberattack can be significant. By following the Protect component of the NIST CSF framework, companies can reduce the likelihood and impact of cyberattacks, which can lead to lower costs.

The Protect component of the NIST CSF framework is organized into five categories:

- **Access Control:** This category focuses on controlling who has access to systems and data.
- **Awareness and Training:** This category focuses on educating employees about cybersecurity threats and how to protect against them.

- Data Protection: This category focuses on protecting data from unauthorized access, use, disclosure, disruption, modification, or destruction.
- Information Protection Processes and Procedures: This category focuses on developing and implementing processes and procedures to protect information.
- Protective Technology: This category focuses on implementing technical security solutions to protect systems and assets.

Companies can use the Protect component of the NIST CSF framework to assess their current cybersecurity posture and identify areas for improvement. They can then develop and implement a plan to implement the necessary safeguards.

Overall, following the Protect component of the NIST CSF framework is a good way for companies to improve their cybersecurity posture and reduce the risk of cyberattacks.

5. Apply the Identify component of the NIST CSF to the Equifax data breach

The Identify component of the NIST Cybersecurity Framework (NIST CSF) is critical to preventing data breaches. By understanding the assets that need to be protected, the threats that exist, and the vulnerabilities that could be exploited, organizations can develop effective security strategies.

Equifax failed to adequately identify and assess the risks associated with a known vulnerability in its Apache Struts software. This vulnerability was publicly disclosed in March 2017, and Equifax did not patch the vulnerability until July 2017. This gave attackers a four-month window to exploit the vulnerability and gain access to Equifax's systems.

To apply the Identify component of the NIST CSF to the Equifax data breach, Equifax should have:

- Identified the assets that needed to be protected, such as its customer data and its IT systems.
- Identified the threats that existed, such as the known vulnerability in Apache Struts.
- Identified the vulnerabilities that could be exploited, such as the lack of a web application firewall.

Once Equifax had identified these assets, threats, and vulnerabilities, it could have developed effective security strategies to protect its data.

Here are some specific examples of how Equifax could have applied the Identify component of the NIST CSF to prevent the data breach:

- Equifax could have used a vulnerability scanner to identify the known Apache Struts vulnerability on its systems.

- Equifax could have conducted a risk assessment to determine the likelihood and impact of an exploit of the Apache Struts vulnerability.
- Equifax could have prioritized the remediation of the Apache Struts vulnerability based on the risk assessment.
- Equifax could have developed a plan to monitor its systems for suspicious activity, such as unauthorized access attempts.

By taking these steps, Equifax could have identified and mitigated the risks associated with the Apache Struts vulnerability before it was exploited by attackers.

Organizations of all sizes can benefit from applying the Identify component of the NIST CSF. By understanding their assets, threats, and vulnerabilities, organizations can develop effective security strategies to protect their data from breaches.