Kesha Williams

Professor Karahan

CYSE 495

April 30, 2019

How IA Policies and Procedures Respond to a Cybersecurity Breach

 With the rise of technologies, many have come to appreciate the benefits that they bring. This can range from a regular household that contains a small network of devices such as a cell phone, laptop, and even a refrigerator to something in a large business like a server, some switches, and various workstations. Dan Panesar, who is author of the article “The Role of Information Assurance in Managing Data Security,” says it best. “Networks can quickly become a web of users, devices and applications, all requiring different access controls and requirements to keep the data safe.” In either case, there can come a time where the data within the network is a target of an outside party and they will jump through many hoops to exploit it. If this were to occur, it would be defined as a breach and must be handled accordingly. This is where cybersecurity has a role in protecting the data and other assets as it employs multiple layers of protection to safeguard systems, networks, and programs from digital attacks. Take notice that cybersecurity mainly encompasses the security of digital assets however, when there is a large company with many pages of hard copy records and data, what security is there? This is where information assurance comes in. Since this field is able to cover the security policies and procedures for digital and non-digital data, a cyber-attack on a network would be mitigated if the company follows the IA policies that are put in place.

 In order to see how a risk can be mitigated, it would be best to view this process through an example. A fair sized company called Maxim, LLC has been successful for about 15 years. This company deals in financial advising for many famous people, including government officials and big names in politics. They are even partners with other advising companies such as Capital One and USAA that share strategies and information that would be mutually beneficial for them to share. Through knowing this, it is apparent that many would love to get their hands on the sensitive data within Maxim’s systems as it could provide a competitive advantage for opponents and bring in big money on the deep web. Companies such as this would already have systems in place to prevent unauthorized access into the system, however, there is no system that has guaranteed security. A breach has occurred as a result and an analysis must be done to see who the perpetrator is, what was exploited, and how can we secure the system.

 As a reflection process, analyzing the breach will assist in understanding what went wrong and how to prevent it. In some companies, they can choose to hire a security company to assist in investigating the person or group that was behind the breach. In this case, there was a specialist on hand that was able to determine that the hacker group “Anonymous” was responsible for the breach. This group sought to sabotage a local governor’s chances in a race because his opponent decided that he needed to hire the hacker group to gain an advantage. Due to the nature of this company, many documents containing financial data and other sensitive information is within the system and was exploited by this group. Some factors that led to the breach was from spear phishing attacks on employees with administrative privileges to gain log in credentials, malware that was used to hack the company, keystroke loggers that monitored everything that was typed, and screenshots of other documents and data they thought was pertinent for their malicious cause.

 When looking at the consequences of this breach, we must first see if this was only an attack on this particular client, or if was more. To best save face, it would be the responsible thing to address the public that our systems have been compromised and that the company is doing all that they can to mitigate the threat. To all parties involved, the company should provide identity protection until everything has been settled. Next, the employees that were victims of the spear phishing attack need to be dealt with appropriately. While the messages or emails may have seemed valid, precautionary measures should have been used as it is stated in the policy. This can be a large indicator that refresher courses on the company’s security policies should be implemented since some employees don’t have appropriate knowledge of the potential cyber threats. This is a crucial aspect of this company, therefore, everyone must understand how these dangers can have even more crippling consequences than this incident has brought on. Lastly, this could bring about some legal trouble, especially with some of the clients having an image to upkeep. This could be devastating to their future finances and careers if any data is exposed. All of these consequences will take much effort to recover from, which is why it is important to prevent it from happening again.

 To prevent incidents like this from reoccurring, there are some information assurance policies and procedures that would be beneficial to implement, as well as understanding the organizational structure of the company to know what role each individual has in its contribution. It is also a must that the five pillars of information assurance is maintained. This would be integrity, availability, authentication, confidentiality, and nonrepudiation. With this situation, confidentiality was not upheld due to the fact that unauthorized parties were able to access this information, integrity wasn’t guaranteed because they could have changed that data how they saw fit, and authentication was not maintained since a number of employees’ log in credentials were taken. Despite the situation, availability and nonrepudiation has been upheld which can be seen as a small positive in some eyes.

 When analyzing the organizational structure of the company, it is best to first view what roles need to be filled to craft an effective information assurance program. This is essentially a set of information assurance policies to protect Maxim’s data and systems from unauthorized access, use, disclosure, disruption, modification, and destruction. The Chief Information Assurance Officer or CIAO, is responsible for the creation and upkeep of information assurance policies. This person reports to the Chief Information Officer and carries out the security and privacy responsibilities under the Federal Information Security Management Act. The CIO has the responsibility of the information technology program and is the one that gives the CIAO the power to manage the information assurance program. Last, would be the Chief Executive Officer that is at the very top of the chain of command. This person keeps the business requirements in mind and ensures that the IAP is developed and implemented in tandem with the requirements.

 For the IAP to be effective, it is broken into four different sections that includes security vision and strategy, senior management commitment, training and awareness, and information assurance management structure (csrc.nist.gov).

**1. Assessment and Diagnostic Services**

According to synopys.com, a risk Assessment is a process used to identify, assess, and implement security controls in applications and preventing risks to organizational operations and assets resulting from the operation and use of information systems (synopsys.com). In order to complete this assessment, there are a few steps that need to be taken:

* Determine the critical assets. This can include servers, customer data, websites, etc. Then identify the information that passes through these assets
* Determine the consequences that could result from system downtime, legal issues, etc.
* Identify the threats and their level. This can range from unforeseen natural disasters to malicious people that want to bring harm to the system and data.
* Assess risk by using the logical formula (Risk = Asset X Threat X Vulnerability). Afterwards, formulate solutions for all but the low risks, including a cost estimate.

From the data that is collected, you can then create a risk management plan. This is a plan that lays out all the risks with their levels and the response for each risk. Example: 

* The keys to information assurance are understanding and mitigating risks, therefore, a risk mitigation plan should be created (C. Quick). This would determine the activities or steps that are needed for reducing the risk impact and create a contingency plan should the risk occur.

To test the solidity of the company’s security, penetration testing would be beneficial. This would essentially be a simulated cyber-attack against the computers and network and would be able to show what vulnerabilities that were exploited during the test. This process is executed into five different steps and the first would be planning and reconnaissance. If this were to be a real hacker, this would be where they are gathering intelligence such as domain names and mail severs, to understand a target’s vulnerabilities. Then a scan will be done to determine how the target application responds to the intrusion and can be done with two different types of scans. A static analysis inspects an application’s code to estimate how it will behave when running, and a dynamic analysis inspects the code while it is running and gives a real time view into an application’s performance. Next would come the use of web application attacks such as SQL injection, backdoors, or XSS attacks to uncover the vulnerabilities to further understand the damage that can be caused, and afterwards, the person executing the test will attempt to maintain access within the system. This is to imitate persistent threats that can remain undetected in the system for long periods of time. Last, would be the overall analysis that explains the specific vulnerabilities that were exploited, what data was accessed, and the amount of time the tester was able to remain undetected within the system.

**2. Management Services**

IAP Metrics is a system that serves the purpose of expressing a quantitative means to compare different systems, vulnerabilities, attacks, costs, etc. By using this, it provides the organization a means of measuring security to further prevent attack. There are three major types:

* Compliance Metrics are used to measure the compliance with standards such as HIPAA, PCIDSS, ISO 27001/27002, etc. These standards are essentially guidelines or put in place to best manage cybersecurity risks and are many different variations created to fit each business. For example, PCIDSS is the Payment Card Industry Data Security Standard which is one of the most frequently used frameworks and was developed to ensure the security of cardholder data that spans the different card companies available.
* Resilience Metrics that measure the ability to foresee, withstand, recover, and adapt to stress, attack, or compromise of cyber resources.
* Return on investment metric is a performance measure used to determine the efficiency of an investment or the efficiency of a several different investments. The formula is (ROI = (Current Value of Investment – Cost of Investment) / Cost of Investment)).

Executing a training and awareness course would be beneficial for this situation. With the employees having an ineffective level of knowledge of this topic, developing a schedule through which employees are frequently trained on the cyber risks that emerge would assist in the prevention of future phishing attacks.

**3. Architecture Services**

According to Wikibooks, security architecture and design is one component of a product or system’s overall architecture and is developed to provide guidance during the design of the system. This would describe the security controls and countermeasures’ positions in the architecture and serve the purpose of maintaining the system’s quality attributes of confidentiality, integrity, and availability (Wikibooks.org).

**4. Implementation Services**

There are numerous services that would be best to use in response to the breach

* Cryptography is a set of techniques and applications based on the basis of mathematical methods, which allows two or more parties communicating with each other to make the exchange of information securely and grounds on a protection by transforming information into a form that unwanted people cannot understand (Y. Yalman).It can either be asymmetric encryption that uses two different keys or symmetric encryption that uses only one key.
* Different forms of authentication are available and this process would ensure that a user’s identity has been confirmed. Instead of a simple username and password, more secure methods such as Public Key Infrastructure, biometrics, or smart cards can be used. PKI is an authentication method that enables the use of digital signatures and encryption across large user populations. Since these establish the identities of people, devices, and services, it enables their access to the system to be controlled and accountable. With biometric authentication, it is the process of verifying your identity by measuring the unique characteristics of your body. This can be a retina scan, fingerprint scan, voice recognition, or the measurement of your gait. As for a smart card, it is a microcontroller that is typically used for generating, storing, and operating on cryptographic keys (Security Wiki). This is a very secure form of authentication due to the cards needing to be carried around by the user and that they need to be inserted into the host computer every time the user wants to authenticate with it. While this does have plenty of benefits, it is also fairly expensive to administer since they require instillation on host computers and physical distribution to users.
* Once authenticated, utilizing a single sign on system would allow users to access multiple applications with that one set of log in credentials
* Maintaining an updated firewall enables the network to effectively monitor incoming and outgoing traffic, while deciding what to block or allow through. This is the first line of defense for many networks, so it is something that cannot be overlooked.

**5. Incident Investigation and Assurance Services**

Data forensics is an important concept during the investigation process. It is the general study of digital data and how it is created and used and it is the identification, preservation, recovery, analyzation, and presentation of digital information. There are two types of data that can be collected which are persistent data and volatile data. Persistent is data that is permanently stored on a drive while volatile is elusive data that is not permanent, thus making it more difficult to recover and analyze.

Implementing an intrusion detection system would assist in monitoring network traffic for suspicious activity and issues alerts if any is discovered. There are different types of systems and include network intrusion detection systems, host intrusion detection system, signature based, and anomaly based (Whatis.com).

* NIDS: This is deployed as certain points within the network where inbound and outbound traffic is monitored
* HIDS: This runs on all computers or devices in the network and is able to detect anomalous network packets that originate from inside the organization or any malicious traffic that a NIDS failed to detect
* Signature Based: This monitors all packets in the network and compares them to a database of known malicious threats
* Anomaly Based: This monitors the network against a previously established baseline and is able to determine what is considered normal in respect to bandwidth, protocols, ports, and other devices.

Overall, this is just a small portion of what Information Assurance can provide to end users and businesses either large or small. In lieu of the phishing attack, new training protocols can be implemented for all personnel and enables them to discern a fake email or message from an unauthorized party. As for the malware intrusion, it can be mitigated through penetration testing, risk assessment procedures, and proper security architecture implementation. These policies will also mitigate the key logger risks by assessing any back doors or ports that hackers try to get through. Keep in mind that having good Information Assurance involves the art of communication (E. McFadzean). Efficient team work in developing and implementing these policies are key, especially since it doesn’t matter how good the IAP is, there will always be some people looking for ways of circumnavigating it (J. Mitchell).

Works Cited

Security Risk Assessment | Synopsys. https://www.synopsys.com/software-integrity/resources/knowledge-database/security-risk-assessment.html.

https://opentextbc.ca/projectmanagement/wp-content/uploads/sites/3/2014/06/risk-breakdown-structure-johns-apartment.jpg.

“What Is Penetration Testing | Step-By-Step Process & Methods | Imperva.” Learning Center, www.imperva.com/learn/application-security/penetration-testing/.

Security Architecture and Design - Wikibooks, Open Books for an Open World. https://en.wikibooks.org/wiki/Security\_Architecture\_and\_Design.

What Is Smart Card Authentication? | Security Wiki. https://doubleoctopus.com/security-wiki/authentication/smart-card-authentication/.

“What Is Intrusion Detection System (IDS)? - Definition from WhatIs.com.” SearchSecurity, searchsecurity.techtarget.com/definition/intrusion-detection-system.

Panesar, Dan. “The Role of Information Assurance in Managing Data Security.” Database & Network Journal, vol. 49, no. 1, Feb. 2019, p. 20. EBSCOhost, search.ebscohost.com/login.aspx?direct=true&db=iih&AN=135309501&site=ehost-live&scope=site.

McFadzean, Elspeth, et al. “Information Assurance and Corporate Strategy: A Delphi Study of Choices, Challenges, and Developments for the Future.” Information Systems Management, vol. 28, no. 2, Spring 2011, pp. 102–129. EBSCOhost, doi:10.1080/10580530.2011.562127.

Mitchell, John. “Information Systems Assurance.” ITNOW, vol. 59, no. 2, Summer 2017, pp. 10–11. EBSCOhost, doi:10.1093/itnow/bwx035.

Yalman, Yildiray, and Murat Yesilyurt. “Information Security Threats and Information Assurance.” TEM Journal, vol. 2, no. 3, Aug. 2013, pp. 247–252. EBSCOhost, search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=90416853&site=ehost-live&scope=site.

Quick, Christopher. “Redefining Information Assurance Compliance.” Army Communicator, vol. 37, no. 3, Fall 2012, pp. 37–39. EBSCOhost, search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=127150026&site=ehost-live&scope=site.