Kesha Williams

Professor Cartledge

CS 465-25069

April 16, 2019

IA Policies and Procedures

 QIR, LLC is a small yet successful company that many have come to appreciate and value over the years. This popularity can come with a price however, due to the attention it has recently gained from malicious parties that hunt for its valuable information. This has resulted in a breach, thus leading to proprietary information and communications being exposed to the public domain. While this can have crippling consequences, the company is doing their best in mitigating the damage through misleading statements and mounting a public relations campaign. As for the future, there will be new information assurance policies and procedures implemented to prevent future incidents of unauthorized access of restricted data. This will be explained after addressing what assets this company currently has, a summary of the recent incident, and the consequences that came as a result of its occurrance.

This company is in possession of crucial financial data of many government officials and lawmakers as it is a financial advising firm for campaigns and marketing. With this in mind, it would be a prime target for opposing officials, should they be willing to hack our systems or hire a third party to do it for them. Of course the company has plenty of safeguards in the system to prevent breaches, however, some may slip through the cracks, thus bringing us to need new policies implemented. Also, there are several strategic alliances with other companies and organizations that share our interests, abilities, and drive to deliver measurable and sustainable results for our clients and communities. A multinational accounting organization, Deloitte Touche Tohmastu Limited, is one of the main organizations that we associate with as they understand the importance of using proactive cyber risk management as they advise accordingly to the needs of each unique business. Another would be Boston Consulting Group, which is an American multinational management consulting firm that has locations in 50 countries. This company also understands technology’s role in business and develops strategies for clients to thrive in today’s volatile business environment.

We now come to a brief analysis of the breach as it will contribute to the overall reflection process of what went wrong. Around May 2016 is where we first became aware that there was an intrusion in our systems, thus leading to a security company being hired to assist in the investigation to find the person or persons behind the incident. They came to the conclusion that the hackers were Russian and sought to sabotage the U.S. presidential campaign of Hillary Clinton, who is also one of our clients. In order to do this, data that included sensitive documents and personal email accounts, were compromised and released on WikiLeaks, which is an online anti-secrecy organization that became the main platform for the Russians to display their trove of hacked emails (The Washington Post). Factors that led to the breach were unfortunately aimed at our employees and allies through spear phishing attacks that obtained login and password credentials, X-Agent malware that was used to hack the company, keystroke loggers that let them see what was being typed, along with computer screenshots, and once inside, they conducted keyword searches that let them find documents and other data that was beneficial for their cause.

As with any incident, there are consequences as a result and must be addressed if there is to be any progress made. First, we must determine the appropriate action to deal with the employees that were victims of the spear phishing attack. While the emails may have seemed legit, there should have been some sort of precautionary measures utilized to ensure that the email received had come from a legit source. From there, we need to look at our training policies for our employees because this may have happened due to the lack of knowledge of the varying dangers of cyberspace. We need to make it so our workforce are all well versed on these potential risks that our sensitive data can attract. We may also face some legal action from our clients whose data may have been exposed and could cost us a hefty sum if we cannot find a way to defend ourselves. Lastly, we unfortunately will lose some credibility, clients, and some partners that we strategically align ourselves with. With us being a small company, this aspect will be a devastating loss and will certainly take some time to recover from.

 To ensure that incidents won’t happen again, there are some information assurance policies and procedures that will be implemented, as well as some clarifications of the organizational structure to understand what role each person has in its contribution. We must also understand that we have to fortify these policies so that the five pillars of information assurance will be maintained. From what we have observed from the breach, the confidentiality was not upheld due to the data being disclosed to unauthorized individuals, the integrity may not have been maintained because once they obtained the information, it is very possible that it could have been modified, and authentication was not upheld due to various log in credentials being stolen. As for the availability and non-repudiation, they were properly maintained despite the unfortunate circumstances.

In order to properly understand the organizational structure of the company, we must first see what roles need to be filled to create a proper information assurance program. This would be a set of information assurance policies that protect QIR’s information and information systems from unauthorized access, use, disclosure, disruption, modification, and destruction (nationalservice.gov). Due to the purpose of this document, it is apparent that the development and maintenance of the information assurance policies is under the jurisdiction of the Chief Information Assurance Officer. The CIAO carries out the Chief Information Officer’s (CIO’s) security and privacy responsibilities under the Federal Information Security Management Act. The CIO is responsible for the overall information technology program and is the one that gives authority to the CIAO to manage the information assurance program. Lastly, it would then come to the Chief Executive Officer that ensures that the IAP is developed and implemented in accordance with regulatory and business requirements (nationalservice.gov).There are some other roles that have a smaller impact, however, these are the main contributors to the IAP’s development and implementation.

This IAP is broken up into five sections that incorporates security vision and strategy, senior management commitment, training and awareness programs, and information assurance management structure.

**1. Assessment and Diagnostic Services**

According to netwrix.com, a risk Assessment is a process used to identify, estimate, and prioritize risks to organizational operations and assets resulting from the operation and use of information systems (netwrix.com). In order to complete this assessment, there are a few steps that need to be taken:

* Find all valuable assets. This can include servers, customer data, websites, etc.
* Identify potential consequences such as system failure or data loss.
* Identify threats and their level. This can range from natural disasters to individuals with ill intent that would purposefully harm the system.
* Assess risk by using the logical formula (Risk = Asset X Threat X Vulnerability). Afterwards, develop solutions for every high and moderate risk, including a cost estimate.
* 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: 
* Create a risk mitigation plan. This would involve identifying the activities or steps to reduce the chance or impact of a risk and creating a contingency plan if the risk should occur.

Penetration Testing and Analysis would be useful as well. According to imperva.com, it is also known as a pen test and is a simulated cyber-attack against your computer system to check for vulnerabilities that can be exploited (Impervia). This process is completed in 5 steps. First would be planning and reconnaissance, which is defining the scope and goals of the test and gathering intelligence to better understand the system’s potential vulnerabilities. Then you would scan the system via two types of analysis to see how the target would respond to intrusion attempts. It can be either static analysis, which inspects an application’s code to estimate how it behaves while running or dynamic analysis that inspects it while it is running. Next would be the utilization of web application attack to gain access, such as XSS or SQL injection and afterwards, you would attempt to maintain access to the exploited system. Once the steps are completed, an analysis will be composed to report what vulnerabilities were exploited, what data was accessed, and how long the intruder stayed in 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.
* 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 evaluate 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)).

Having some form of education training and awareness would be pertinent in this situation. 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**

Security architecture and design is a component of a 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 several services that would be beneficial to use in lieu of the recent attack.

* Encryption involves the process of encoding data, making it unintelligible unless you had a particular key. This encryption key is a collection of unique algorithms that can either lock or unlock the information, depending of the type of encryption that is being used. It can be asymmetric encryption that uses two different keys or symmetric encryption that uses only one key.
* Varying forms of authentication are available and this process would ensure that a user’s identity has been confirmed. Rather than simply having a 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, having a single sign on system would enable users to access multiple applications with that one set of log in credentials
* Having 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 numerous 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 overall 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.

Having 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 your IAP is, there will always be some people looking for ways of circumnavigating it.

Works Cited

“A New Unmanned Aerial Surveillance Platform.” *SI110: Information Assurance*, www.usna.edu/Users/cs/wcbrown/courses/si110AY13S/lec/l21/lec.html.

“BCG Approach.” *Https://Www.bcg.com*, www.bcg.com/en-us/about/mission/approach.aspx.

Engelbert, Cathy, and Deloitte. “About Deloitte | Our Global Network of Member Firms.” *Deloitte United States*, www2.deloitte.com/us/en/pages/about-deloitte/articles/about-deloitte.html.

“Information Assurance Program.” *Corporation for National and Community Service*, Nov. 2012, nationalservice.gov/sites/default/files/upload/IAP\_082112\_Final Public.pdf.

*Information Security Risk Assessment Checklist*. www.netwrix.com/information\_security\_risk\_assessment\_checklist.html.

Lainhart, John W. *Information Assurance/Information Security*. 13 June 2002, csrc.nist.gov/CSRC/media/Events/CSSPAB-JUNE-2002-MEETING/documents/Lainhart-06-2002.pdf.

Libfeld, Roey. “What Is Smart Card Authentication ? | Security Wiki.” *Secret Double Octopus*, doubleoctopus.com/security-wiki/authentication/smart-card-authentication/.

Nakashima, Ellen, and Shane Harris. “How the Russians Hacked the DNC and Passed Its Emails to WikiLeaks.” *The Washington Post*, WP Company, 13 July 2018, www.washingtonpost.com/world/national-security/how-the-russians-hacked-the-dnc-and-passed-its-emails-to-wikileaks/2018/07/13/af19a828-86c3-11e8-8553-a3ce89036c78\_story.html?noredirect=on&utm\_term=.52b83591bf95.

*Security Architecture and Design*. en.wikibooks.org/wiki/Security\_Architecture\_and\_Design.

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

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