CS 465 - Final Project

By: Bradyn Ritchie

CS 465: Information Assurance

Professor Cartledge

4/19/23

Table of Contents

(A) Incident summary 3
(B) Commercial Responsibilities, Corporate Alliances, Network Infrastructure 4
(C) Consequences of Attack 6
(D) Vulnerability Assessment 7
(E) Threat Matrix 9
(F) Communication Plans 10
(G) Proposed Controls 11

List of Tables/Figures

Table 1: Vulnerability Assessment 7
Table 2: Threat Matrix 9

To whom it may concern,

As businesses and corporations continue to develop and integrate new and advancing technologies into the workplace, the abilities of the devices improve the workload and job function of employees. However, as the capabilities of these technologies advance, so do the abilities of potential adversaries. Therefore, proper information assurance and information security is critical in order to protect the valuable data stored on the organization's computer systems. Without proper information assurance measures, companies may face a wide range of potential threats that would ultimately negatively affect the confidentiality, integrity or availability of their data, such as insider attacks, malware, social engineering, and various other types of malicious incidents. This report is primarily focused on the detrimental attack that ABC manufacturing encountered that affected its daily operations.

(A) Incident summary

Roughly a month ago, the ABC manufacturing company was subjected to a very dangerous ransomware attack. As a result, the corporation was rendered incapable of successfully billing customers or issuing payment to vendors for roughly three whole weeks before the issue was ultimately resolved. In order to resolve the incident, outside cybersecurity experts were brought in to assist our information security team. After the matter was resolved, it was revealed during the following investigation that the source of the ransomware originated from a malicious email attachment. An unsuspecting employee within ABC downloaded the malicious Microsoft Excel attachment. Within minutes of the attachment being downloaded and opened, a trojan malware, more commonly known as Zloader, began harvesting employee login credentials on systems throughout the network. Three weeks later, the systems on the

administrative and financial sectors of the company fell victim to ransom demands issued through Ryuk ransomware. Shortly after the cybersecurity experts were called in, the issue was resolved when all compromised files were removed from the affected systems and backups were implemented to fully restore company activities. Fortunately, some devices, such as the engineering and manufacturing programmable logic controllers were not affected during this attack.

(B) Commercial Responsibilities, Corporate Alliances, Network Infrastructure

As a manufacturing company, ABC possesses many different commercial responsibilities that they must meet. For example, they are expected to properly pay their vendors for selling their manufactured products and expected to issue bills to customers who purchase directly from ABC. ABC's internal systems may house various forms of intellectual property as well. This could include design or utility patents on their products or patents on the machines that they utilize to manufacture their products. In addition to this, ABC may hold trade secrets that would be devastating to the company if publicly released, such as the specific process for manufacturing or a certain combination of chemicals needed to produce their products. ABC manufacturing has a wide array of strategic and corporate alliances as well. This includes any instance where two companies combine their efforts and work together in order to benefit both parties. The vendors that ABC supplies may be considered a corporate alliance, as they are willing to combine efforts to sell products. Therefore both parties benefit from the collaboration by increasing their income revenue.

Overall, there is really only one main strength of ABC manufacturing's network infrastructure. That is the logically segmented networks that the larger network as a whole is divided into. This includes the segment containing finance and administration, and the other

segment consisting of engineering and manufacturing. Segmented networks, more commonly known as subnets, are an extremely important method to improve security and network organization in larger companies or organizations. This is because the subnets are generally completely isolated from one another and are only connected through a single router or switch so the systems within each segment can communicate. Therefore, if an attacker attempts to penetrate into one subnet, they may still need to determine a way to break into the other (Pandey, 2022). Therefore, it will take more time for an attacker and the organization's security team will have more time to respond to a potential incident. Segmenting a network is an extremely useful network architecture technique when attempting to minimize the damage done to the organization's network.

However, some may argue that subnetting is a major hindrance to an organization. This is because it increases the overall complexity of the network and may be more difficult for the IT teams to manage and audit if needed. In addition to this, subnetting increases the overall cost for an organization to maintain their network, as there is generally one switch or hub needed before every subnet in order to be effective. Therefore, the price may add up significantly, especially in larger organizations with many different subnets present. However, most believe that the benefits of subnetting strongly outweigh the negatives (Pandey, 2022). The malware attack also exemplified one primary weakness with ABC manufacturing's network. That is that there appears to be no antivirus software installed on the information assurance team's computers to use. If an antivirus software was installed and periodically run on all systems company wide, the malware hiding on the affected systems would have quickly been spotted and removed by the antivirus application. However, since the malware stayed on the system for three weeks without being noticed, it is evident that there is either no antivirus that is being used or regular, scheduled

scans are not being run by the information security team. However, it is also entirely possible that scans were being run, but the antivirus software had not been updated. Therefore, the database of malware signatures that it bases the scans off of were missing entries for the Zloader and ransomware malware. The frequent use of antivirus software is critical to ensuring the confidentiality, integrity, and availability of all information located on the company systems (Matthews, 2014). Due to this lack of use of antivirus software, all systems within ABC's local area network were vulnerable to malware attacks.

(C) Consequences of Attack

ABC manufacturing faced some rather severe consequences as a result of this detrimental cyber attack. As stated above, the ransomware attack prevented ABC from properly billing their customers or providing payouts to their vendors. Therefore, they were unable to obtain a steady, reliable form of income for three weeks before the systems were restored and the company could resume their normal operations. In addition to this, sensitive and confidential information may have been stolen both during and before the actual ransomware attack occurred. During the investigation, the cybersecurity support experts were able to determine that Zloader, a trojan designed to steal passwords, had been active in the systems and network for roughly three weeks, silently gathering employee and potentially customer login information, such as usernames and passwords. However, at this time, it is unknown just how many login credentials were compromised by the malware. During the ransomware attack, other sensitive files may have potentially been stolen, such as trade secrets created by the ABC company, customer information, and vendor information. These may have contained personally identifiable information about various individuals, therefore, ABC may face legal consequences from government organizations or the affected victims for letting sensitive information be exposed. In

addition to this, ABC's reputation may be permanently tarnished due to their inability to pay vendors and the possibility that sensitive information was potentially stolen or released during the ransomware attack.

(D) Vulnerability Assessment

A vulnerability assessment is a commonly used technique in order to identify potential threats and vulnerabilities within the organization's infrastructure and how they would potentially affect the company's ability to operate on a daily basis. These different actions that are critical to the operation of the company include issuing payments to vendors, receiving the necessary payments. In addition to this, another important aspect of a vulnerability assessment is the classification of the vulnerabilities. Different vulnerabilities are organized into specific groups, such as type or severity. Therefore, the information assurance team knows which high risk vulnerabilities to prioritize over the others. Below is a vulnerability assessment table outlining potential vulnerabilities for ABC manufacturing and their computer systems.

ID	Vulnerability	Details	Severity Rating
1	Outdated hardware	Old and outdated hardware can be exploited by attackers in order to gain access to a system.	Medium
2	Opening spam emails	Form of social engineering that may introduce malware to the systems or network or trick employees into providing sensitive information.	Critical

3	Opened ports	Opened ports on a system can provide more attack vectors for potential attackers.	High
4	Excessive user privileges	Attackers who gain access to a user account will have more privileges than necessary, therefore, they can do more damage to a system.	High
5	Missing security patches	Opens up a wide range of issues, as security patches are meant to fix current security issues, therefore the systems are still vulnerable.	Critical
6	Configuration errors	Potential flaws that are located in system settings that could leave systems vulnerable to attack.	Medium
7	Hardware failure	Potential to lose important data if there is no backup available.	Low
8	Unused user IDs	Terminated users may log into their old accounts and access potentially sensitive information.	Medium
9	Unchecked user input	Users can enter malicious code in order to alter databases, such as during an SQL injection.	High
10	Unauthorized	Unauthorized	High

	application installation	applications may contain malware that can have detrimental consequences on the individual system or network as a whole.	

Table 1: Vulnerability Assessment

(E) Threat Matrix

In many organizations, a threat matrix is utilized in order to determine the severity of potential threats to a company, similar to a risk or vulnerability analysis. It is meant to analyze the potential capabilities that threats may pose if they breach the company wide network. The proposed threat matrix below is based on the threat matrix ranking system introduced by Goel and Chen (Goel & Chen, n.d.).

Threat Matrix	**Vulnerabilities**	Databases	Physical Security	Password Strength	Insecure WiFi	Configuration errors	Hardware	Total Score	Ranking (Highest More Significant)
Threats	**Priority**	3	6	1	5	2	4		
Malware	2	5	1	3	4	2	2	17	4
Social Engineering	1	2	3	1	1	5	1	13	6
Insider Threats	6	4	9	2	1	1	7	24	2
Intrusions (Hacking)	3	6	1	6	4	3	1	21	3
System Failure	4	9	6	1	1	4	9	30	1
Denial of	5	1	1	1	2	8	3	16	5

Service Attack									

Table 2: Threat Matrix

(F) Communication Plans

Communication plans, both internal and external, are critical to the continuing function of the organization. An internal communication plan outlines the specific goals that the company has when communicating with their employees. Therefore company related news and ideas would qualify as part of the internal communication plan. An external communication plan covers various aspects of how members located inside of the company exchange information with individuals outside of the organization (Harvey, n.d.). This could include customers, stakeholders, outside investors, and the general public as a whole. An internal communication plan should outline many different aspects of the organization. One of the main topics should include the various challenges currently faced by the organization (Grossman, 2022). However, these communications need to be relayed to the correct individuals in order for the communication plan to be effective. For example, marketing challenges would be relayed to the marketing executives, and potential problems within the sales department would be addressed to the corresponding members of the sales department. In addition to this, a proper internal communication plan should outline how this information will be delivered to the proper individuals (Grossman, 2022). It may depend on the type of information, but this could include company newsletters, email, or even in person meetings to discuss the problems at hand.

External communication plans are just as critical to the success of an organization as internal plans and are more generally seen as a form of marketing, as the primary purpose is to

appeal to individuals all over the world. One of the main types of external communication includes the company website. This should inform the general public of information about the company, such as their products they produce and their company missions (Kunsman, 2022). Another could include company newsletter distributed to past or future customers that inform them on the current status of the organization. Unlike the internal communication plan, external communication plans should not outline the challenges that the organization is facing and how to fix them. This would potentially lead to a vulnerability that could be exploited by members of the general public through internet hacking, social engineering techniques, or more.

(G) Proposed Controls

In order to ensure that a detrimental cyber attack such as this does not occur again, there are quite a few factors and defensive mechanisms that ABC can implement to better improve their information security program. Since this previous attack exploited the human vulnerability in the company, I would suggest that ABC implement better procedures and protocols for training their employees (Jones, n.d.). For example, the information assurance or security team may send out fake phishing emails to employees in order to test them, and then educate the employees who unknowingly clicked the links. In addition to this, it is wise for any corporation to include a Cybersecurity Awareness policy for employees as well. This policy outlines how the information security team will pass cybersecurity related news along to the employees within the company. For example, the team may send an email to the entire company alerting them of potential phishing emails to look out for and avoid. By properly educating employees, many different forms of social engineering attacks, such as the phishing email that ABC fell victim to, can be thwarted rather easily.

Another way that this attack could have been prevented or mitigated is through the use of an intrusion detection system (IDS) or an intrusion prevention system (IPS). An IPS or IDS is a software or physical device that alerts the security team of an organization whenever suspicious activity on a system or network has been detected. Different types of IDS and IPS determine suspicious behavior through various means, such as anomaly based and signature based techniques. Signature based looks specifically for certain patterns and behaviors of a particular threat while anomaly based IDS or IPS look for network wide traffic that is not deemed to be normal. These defensive systems may have been able to recognize the Zloader malware as soon as it began maliciously harvesting the login credentials. From here, it would have issued an alert to the security team who would have manually dealt with the malware, or the IPS could have neutralized the security threat on its own without the need for human interaction. If the Zloader malware was simply caught earlier, it could have completely avoided this incident. In addition to this, the use of an IDS or IPS would potentially prevent the ransomware from encrypting the sensitive and important files. If modification occurred on certain files outlined in the IDS or IPS's settings, the security team would be immediately notified of the potential security incident. Also, a simple malware scan of the computer network conducted by the security team would have potentially revealed the Zloader malware as well. As a general rule, it's best to run a virus scan on a network or individual system at least once a week (Matthews, 2014). Therefore, if malicious malware is hiding from plain view on a system, it can quickly be located and properly dealt with by the security team.

In addition to this, modern forms of encryption should be utilized by ABC in order to protect the confidentiality of the information stored on their devices. This would have ultimately reduced the impact of the damage caused by both the ransomware and Zloader malware, as the

passwords and potentially stolen files' encryption algorithms would need to be cracked before they can be used. If the attackers do not have the proper encryption algorithm or key for decryption, the information will be of no use to them unless it is presented in readable format. Therefore, encrypted information can potentially remain confidential even after it has been exfiltrated by malicious attackers or software.

Also, two factor authentication may have prevented the attack from reaching its large scale. It's unclear exactly how the ransomware was installed onto the systems leading up to the ransomware attack. This could have been installed at the time that the employee downloaded and opened the malicious Microsoft Excel spreadsheet attachment, or the Zloader malware could have passed the logon credentials of employees back to the individuals behind the cyber attack. From there, they could have accessed employee accounts to manually install the ransomware program. If the second option is the case, this could have easily been thwarted through the use of multi factor authentication. If the attackers attempted to login through employee accounts utilizing the harvested credentials, they would be presented with an additional hurdle that they must bypass. This could take the form of a security question, personal identification number (PIN), one of the employee's biometric characteristics, and even the employee's approval on their cell phone. Therefore, the attackers would not have been able to log onto the system without knowing this information specific to each separate employee. Therefore, two factor or multifactor authentication is an extremely important security measure to include on all systems company wide. As a result of the Zloader malware, everyone within the company should immediately change their password as well, as it could have been harvested and compromised during the attack. These passwords should follow the complexity definitions outlined in the company wide password policy. This should include a minimum number of characters, inclusion

of special characters, both uppercase and lowercase letters, and whatever else the information assurance or security executives deem should be included.

Lastly, with the recent COVID-19 pandemic and remote work positions gaining popularity, working from home has been a major information security issue for many businesses and organizations around the world. Therefore, ensuring that the data transmitted both to and from the remote employee's devices is secure is critical. One method that should be implemented for workers outside of the office is the use of virtual private network (VPN) software. VPN software allows users to connect to servers and services within the company's network, as long as they provide the proper credentials. In addition to this, it encrypts the traffic between the client and server, therefore, attackers who are intercepting data will not be able to read it without the decryption key. ABC should implement a policy that requires all remote employees to use the VPN software provided by the company. In addition to this, public wifi networks should be strictly avoided unless they are utilizing the VPN software on the network. Public networks may be extremely insecure and send information in the plain text, therefore allowing potential attackers to intercept and read the data being transmitted. In addition to this, the information security team at ABC should install antivirus software on all remote computers and periodically run scans remotely in order to ensure the availability, integrity, and confidentiality of information on the systems. These are just a few of the cybersecurity related controls and safety precautions that can be implemented to make sure that an event similar to this does not occur again.

The previous ransomware attack suffered by the ABC manufacturing company exemplifies a current absence of proper security controls throughout the company wide network and individuals systems. If the various controls suggested in this report are implemented into the existing network, ABC will likely see a reduction in various types of cyberattacks, including

ransomware. In addition to this, in order to keep the information on the systems secure, the employees and information security team need to keep a watchful eye for abnormal or suspicious behavior on company systems. As technology continues to advance, so do the capabilities of the attackers, therefore, it's imperative that ABC consistently implement up to date security procedures in order to protect their sensitive information.

Works Cited

Goel, S., & Chen, V. (n.d.). *INFORMATION SECURITY RISK ANALYSIS – A MATRIX-BASED APPROACH*. University at Albany. Retrieved April 2, 2023, from https://www.albany.edu/~goel/publications/goelchen2005.pdf

Grossman, D. (2022, February 21). *Internal communications plan: 7-Step strategy and template*. The Grossman Group. Retrieved April 2, 2023, from https://www.yourthoughtpartner.com/blog/internal-communications-plan

Harvey, S. (n.d.). *External communication strategies: Finding your marketing megaphone*. Fabrik Brands. Retrieved April 2, 2023, from https://fabrikbrands.com/external-communication-strategies/

Jones, M. (n.d.). *Best practices for how to train employees for cyber security*. Cox BLUE. Retrieved April 2, 2023, from https://www.coxblue.com/8-tips-and-best-practices-on-how-to-train-employees-for-cyber-security/

Kunsman, T. (2022, March 18). *How to level up your external communications strategy*. EveryoneSocial. Retrieved April 2, 2023, from https://everyonesocial.com/blog/external-communications-strategy/

Matthews, K. (2014, March 13). *Anti-virus software: How often to run and why?* Colocation America. Retrieved April 2, 2023, from https://www.colocationamerica.com/blog/anti-virus-software-how-often-to-run-and-why

Pandey, P. (2022, September 7). *Subnetting in computer networks*. Scaler Topics. Retrieved April 2, 2023, from https://www.scaler.com/topics/computer-network/subnetting/