ABC Inc: Internal Network Failure Report

Delonta Johnson

Old Dominion University

CS465 Information Assurance Project

Dr. Chuck Cartledge

04/23/2023

Table of Contents

List of Tables

ABC Inc: Internal Network Failure Report

Cyberattacks, threat detection, and threat deterrence are integral to maintaining a secure protected network. ABC Inc. has become the victim of a ransomware attack that shut down the administrative and financial systems of the company. As a result of the cyberattack, ABC Inc., has suffered significant financial loss as well as hindered business operations.

Recently, an email was sent to an employee containing an Excel spreadsheet. The employee believed the email to be from a valid source and opened the email. This caused the Zloader virus to upload onto the computer and harvest the passwords and logins of other employees.

After three weeks, administrative and financial systems were inaccessible and locked with ransomware demands. 40 computers were found to have the presence of the Ryuk ransomware files in the ABC IT network. Essentially, unauthorized users gained and maintained access to a network space that transmits and stores private and sensitive information for thousands of individuals.

Commercial Responsibilities & Intellectual Property

ABC Inc. is one the largest manufacturers of affordable cars on the entire east coast. ABC Inc. manufactures affordable cars for low-income citizens within the DMV area. ABC Inc. also provides low-cost transportation for students in after-school programs. ABC Inc. has an app that allows the ride-sharing service to be accessible to low-income students and families. ABC Inc. has provided affordable transportation for hundreds of thousands of residents within the area. ABC Inc., the logo consists of the letters “A”, “B”, and “C” in a pyramid. The letter “A” is at the top followed by the “B” at the bottom left of the pyramid and the “C” at the bottom right of the

pyramid. The letter C also has the word “INC” written in descending order. ABC Inc. also holds patents to several makes and models of cars specifically designed using low-grade steel and other biodegradable resources. These patents are what revolutionized the auto industry and allow the mass distribution of environmentally sustainable vehicles. ABC Inc. also provides car accessories as well as community resources catered to passengers within certain areas.

Strategic and Corporate Alliance

ABC Inc. uses a plethora of small and corporate businesses within the area to expand outreach and presence within the community. Safest LLC, Huge Food Store, and Food Leopard are the premier retailers of accessible fresh food to low-income residents of the DMV area. ABC Inc. sells cars to these locations to provide transportation and access to its stores. One of the most important alliances is with the company Safest LLC. ABC Inc’s partnership with Safest LLC allows families within Ward 8 of Washington, DC to access fresh and affordable groceries from their local convenience store. ABC is partnered with Huge Food Store. ABC Inc’s partnership with Giant allows the company to grant drivers the ability to deliver food to families in low-income areas in DC as well as Maryland, specifically Prince George’s County. Low-income families in Alexandria County, Virginia have the option of utilizing Safeway, Giant, and Food Lion for groceries due to the proximity of the stores to the area. One of the most important partnerships that ABC Inc., has is with Chase Bank. Bingo Bank partnered with ABC Inc., to help provide programs and incentives for low-income families to start savings accounts and develop new strategies to save money.

Strengths and Weaknesses of Network

One of the biggest strengths of ABC Inc's network is the overall availability. ABC Inc's network is exclusive to the employees that utilize the network to transmit and store company and customer information as well as those that require the network to utilize services offered by the company. The activities of the programmable loggable computers (PLC) were able to stay operational during the time of the cyberattack. Another strength of the network is its manageability. During the event of the cyberattack, IT administrators were able to remove traces of the Zloader virus from the network. Full company activity was able to be resumed once all suspicions or compromises were removed from the network.

One of the biggest weaknesses of ABC Inc's network infrastructure is its security. The Zloader virus was uploaded to the companies' network undetected for three weeks. The Zloader is regarded as a popular banking trojan virus (Tavares, 2022). Essentially, the Zloader virus is a trojan designed to steal cookies, passwords, and other sensitive information. (Tavares, 2022) The virus was not only able to harvest the logins and passwords that were in the network, but the virus was also able to infect 40 computers while remaining undetected. ABC Inc's lack of security hardware and software to detect and deter cyber threats within the network contributes to the impact of the attack.

Maintaining and ensuring the protection of data for thousands of employees and customers is essential to continuing business operations. Another weakness of the network infrastructure is employee digital literacy. An employee unknowingly opened a file from "what appeared to be a valid source". Employee digital literacy is a crucial component of information security and information assurance as it adds another layer of security to the network.

Data Breach Consequences

Ransomware attacks are considered the most costly of cyberattacks due to the financial loss it imposes on a company. Ransomware attacks are estimated to cost businesses approximately $1.85 million in 2021 (Sophos, 2021). In 2022, the number quadrupled to $4.54 million in 2022 (IBM, 2022). The recovery and downtime caused by cyberattacks will cost ABC Inc., millions of dollars if the proper safeguards are not put in place. Another consequence of this attack is a decrease in employee retention.

Cyberattacks tend to cause employees to become uneasy and doubt the safety of themselves and their data. Studies show that half of the workers agreed that they would reconsider working for a company after being notified of a recent data breach (Scroxton, 2022). With the logins and passwords harvested from the Zloader virus, hundreds of thousands of identities were stolen. Potential information acquired from the data breach could include information regarding company alliances and trade information. Intellectual properties and customer data are at risk as partnered companies share access to the same data. This means that since ABC Inc., has been breached, the partnered companies including, Safest LLC, Huge Food Store, and Food Leopard will potentially have their information obtained as well. ABC Inc. must now be aware of its reputation. Partnered companies will begin to lose trust in ABC Inc. if common cybersecurity practices are not implemented appropriately.

One of the most important impacts of the data breach is that the network is susceptible to potentially devastating attacks in the future. After being hit once, businesses are more likely to experience a data breach. Studies show that businesses have a 66% percent chance of being

repeatedly impacted by data breaches (Cymulate, 2023). ABC Inc. must ensure proper cybersecurity safeguards are in place to deter future attacks from impacting the network.

Network Vulnerability Assessment

Introduction

A vulnerability assessment has been produced to display potential exploits within the network. Components of the network including system software and hardware play a critical role in securing network security. Applications and methods for enterprise communication are examined to determine vulnerability within the network. The network infrastructure will also be examined to determine efficiency. Essentially this vulnerability assessment will provide a thorough overview of potential exploits within the network.

Methodology

An assessment of the company assets was made and categorized based on its individual importance towards business operation and impact on network function. To determine the level of impact an asset has of discontinuing network and business operation simultaneously, a threat matrix (Table 1.1) is developed to convey the value an asset has in regard to network and business operation and function. An asset with a score of two or less has little to no impact on business and network operations. An asset with a score from three to four has a medium impact on business and network operations while an asset with a score from six to nine has the highest chance of impacting network and business operations.

Findings

As a car manufacturing company, ABC Inc. utilizes tools that improve the process and efficiency of its assembly line. Operational Technology (OT) plays an important role in allowing

the company to perform services. Supervisory Control and Data Acquisition (SCADA) systems are implemented to monitor data and control equipment essential to the mass development of the cars developed by ABC Inc. The SCADA systems utilized by ABC Inc., are critical for the business operation of a company while simultaneously having a moderate impact on network operation and function. A threat score of six classifies SCADA systems as a "medium" threat meaning hackers are more likely to target this system. Doing so could bring significant damage to the network and financial loss for the business.

Furthermore, the overall segmentation of the network can be improved to minimize the impact of data breaches on the network. The network is currently segmented with the engineering and manufacturing process in one segment of the infrastructure, and engineering and manufacturing in the other segment. Hackers who gain access to administrative processes inevitably gain access to financial processes. Hardware within the administrative segment primarily includes desktops for employee use. The lack of security for desktop computers poses a great risk to the network. The intrusion of the administrative segment will lead to access to the companies' financial segment. Hardware and software within the financial segment are essential to business operations. The network infrastructure has a score of "9" on the threat matrix (Table 1.1). This means that this asset is the most likely to be targeted and if so, will have catastrophic effects on the overall network and business operation.

Employee communication is essential to business operations. The application for employee communication, specifically email, shows significant flaws. The current email communication client does not coherently notify employees of suspicious emails. Vulnerabilities in employee communication grant hackers the opportunity to gain access to the network. The

email application is given a score of "4" within the threat matrix (Table 1.1). Email communication is essential to business operations while also having a low impact on network function and capabilities. Compared to SCADA systems, email communication is less likely to be targeted and has less impact on business and network functions. This does not negate the possibility of attacks through email.

Recommendations

These systems do not show signs of utilizing an intrusion detection system (IDS). IDS implementation into SCADA systems is regarded as, "an important component of ICS/SCADA security. (Kostadinov, 2020)" SCADA Systems are critical to business and network operations and are at high risk of being targeted. network infrastructure must be revised to minimize the impact of data breaches. Splitting the networking into four segments rather than two will decrease the impact of data breaches.

Currently, the network contains administrative and financial processes in one section and engineering and manufacturing in another. Splitting each process so that they can have their segment and infrastructure will minimize data breach impact. Utilizing a new email client can decrease human risk and data breaches altogether.

Email communication is the foundation for optimizing business operations. It is important that ABC Inc., utilize an email client that can effectively notify employees of potentially suspicious emails and display the potential cost of clicking on any suspicious attachments or links.

Table 1

ABC Inc., Threat Matrix

Impact on Business Operation	3 (Critical)	Medium	High	High
	2 (Essential)	Low	Medium	High
	1 (Ancillary)	Low	Low	Medium
		1 (Very Low)	2 (Moderate)	3 (High)
	Impact on Network Function			

Table1.1: The likelihood of a company asset being attacked by hackers in order to gain access to the network is based on “Impact on Business” score multiplied by the “Impact on Network Function” score.

Reccomended ABC Inc. Communications Plan

It is vital for a company to implement a communication plan displaying potential incidents to employees, business partners, and other parties associated with ABC Inc., should begin to notice and update to appropriate personnel in order to mitigate the impact of potential cyber-attacks. An internal communication plan (Table 2.1) allows for employees, faculty, and staff within ABC Inc., to recognize potential threats and notify personnel. Incidents with high consequences will most likely require early notification to high-level personnel. The communication plan promotes awareness of suspicious activity occurring within the network.The communication also creates an additional resource for employees and faculty to detect and recognize malicious or suspicious messages. An external communication plan (Table 2.2) displays the roadmap and potential communication channels for parties outside of the organization to utilize to communicate suspicious activity. The external communication plan will improve threat dectection and mitagation. The overall objective of the communications plan is to prevent and lesse the impact of future data breaches.

Table 2.1

Internal Communication Plan

Incident	Communication Delivery Method	Required Messaging and Content	Due Date	Responsible
Suspicious Email Message (attachments, links, etc.)	Email	Date and time email were received	24hrs after viewing	IT Help Desk/Admin
Message from seemingly reliable Sender	Email	Date and time email were received	24 hrs after viewing	IT Help Desk/Admin
Inability to access company resources digitally	Verbal	Date and time of access	Immediately	CIAO
Mass computer outage	Verbal	Date and time of incident	Immediately	CIAO

Table 1.2:Displays the potential situations and roadmap for communicating incidents to the correct personnel.

Table 2.2

External Communications Plan

Incident	Communication Delivery Method	Required Messaging and Content	Due Date	Responsible
Suspicious Email Message (attachment, links, etc.)	Email	Error Number	Immediately	IT Help Desk/Administrator
Riders receiving unwanted notifications of driver location	Email	Date and time email was received	Immediately	IT Help Desk/Adminitrator
Total App failure	Email	Date and time of app access	Immediately	IT Administrator
App not responding to start request from customers	Email	Error Number	Immediately	IT Help Desk/Administrator

Table 2.2: Shows the potential roadmap, incident, and communication methods, for all external communications.

Policies and Procedures for Prevention

There are many policies and procedures that can help deter cyber threats and contribute to the assurance that information stored within the network is protected. One of the most important policies necessary for implementation is collaborating with an Information Sharing and Analysis Organization (ISAO). The objective of ISAO's to promote collaboration between public and private sector organizations and improve information sharing regarding cyberattacks and other cyber-based threats. (Exec. Order No. 13691, 2015). Studies have recognized ISAOs as an "important approach to increasing organizational efficiency and performance. (Yang & Maxwell, 2011). According to the ISAO website, ABC Inc. recommended partner would be the Multi-State Information Sharing and Analysis Center. The mission of the organization is to, "improve the nation's cybersecurity posture for state, local, tribal, and territorial governments. (CIS, 2023)" Collaboration with this organization will allow ABC Inc. to gain private sector knowledge on cyber attacks and other potential threats.

Implementing information technology standards prioritizing network security and assurance is critical to deterring threats. ISO/IEC 27000, developed by the International Organization for Standardization (ISO), is one of the most prominent IT standards utilized by businesses (ISO, 2023) ISO/IEC 27000 is said to provide, "guidance for establishing, implementing, maintaining, and continually improving an information security management system. (ISO, 2023)" Research even suggest that new security methods should derive from ISO 27000 (Meriah & Rabai, 2019).

Signature-based Intrusion Detection systems are foundational to networking monitoring and detecting suspicious activity within the network. Intrusion Detection Systems (IDS) is

software that analyzes packets and network traffic to identify and record suspicious activity (NIST, 2023). Studies have concluded that IDS can not only improve detection but inevitably enhances deterrence. (Cavusoglu et al, 2005). For ABC Inc., a Signature-based Intrusion Detection System would further increase deterrence. Researchers described Signature-based IDS as a system that, “rely on pattern recognition techniques where they maintain the database of signatures of previously known attacks and compare them with analyzed data. (Jyothsna, 2011)” Signature-based intrusion detection systems (SBS) will improve detection and deterrence within the network.

Lastly, ABC Inc. should implement cyber-based competency training employees. This training will give employees and faculty the necessary skills to detect suspicious and potentially malicious messaging. Reports show that poor or absent cybersecurity training makes up over 85% of cybersecurity attacks (Deo, 2013). Studies recommend cybersecurity training across all levels of leadership in order to reduce financial loss and data breach impact. (Adams & Makramalla, 2015)” Overall cybersecurity training can greatly improve detection and lessen the damage and possibility of a data breach within company servers.

References

Adams, M., & Makramalla, M. (2015). Cybersecurity skills training: An attacker-centric gamified approach. *Technology Innovation Management Review*, *5*(1).

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2005). The value of intrusion detection systems in information technology security architecture. *Information Systems Research*, *16*(1), 28-46.

Cost of a data breach 2022. (n.d.). IBM. https://www.ibm.com/reports/data-breach

CSRC Content Editor. (n.d.-a). *Network Intrusion Detection System - Glossary | CSRC*. https://csrc.nist.gov/glossary/term/network_intrusion_detection_system

Executive Order -- Promoting Private Sector Cybersecurity Information. (2015, June 11). whitehouse.gov. https://obamawhitehouse.archives.gov/the-press-office/2015/02/13/executive-order-promoting-private-sector-cybersecurity-information-shari

ISO/IEC 27000 – key International Standard for information security revised. (2018, March 1). ISO. https://www.iso.org/news/ref2266.html

Meriah, I., & Rabai, L. B. A. (2019). Comparative study of ontologies based iso 27000 series security standards. *Procedia Computer Science*, *160*, 85-92.

Moyal, M. (n.d.). *Survey reveals companies hit with cyber attacks likely to face repeated onslaughts*. Cymulate. Retrieved April 21, 2023, from https://cymulate.com/news/breach-survey-pr-2022/#:~:text=New%20York%2C%20and%20Tel%20Aviv

Scroxton, A. (2022, October 24). Half of the staff might quit after a cyber attack, the report says. *ComputerWeekly.com*. https://www.computerweekly.com/news/252526433/Half-of-staff-might-quit-after-a-cyber-attack-report-says

Sophos. (n.d.). *Cybersecurity Delivered - Sophos Security Solutions*. SOPHOS. https://www.sophos.com/en-us/press/press-releases/2021/04/ransomware-recovery-cost-reaches-nearly-dollar-2-million-more-than-doubling-in-a-year

Tavares, P. (2022, May 25). *ZLoader: What it is, how it works and how to prevent it | Malware spotlight [2022 update] | Infosec Resources*. Infosec Resources. https://resources.infosecinstitute.com/topic/zloader-what-it-is-how-it-works-and-how-to-prevent-it-malware-spotlight/

Yang, T. M., & Maxwell, T. A. (2011). Information-sharing in public organizations: A literature review of interpersonal, intra-organizational and inter-organizational success factors. *Government information quarterly*, *28*(2), 164-175.