Old Dominion University

CS 465 Info Assurance for Cybersecurity

ABC Inc. Incident Report

Brian Delos Santos

UIN: 01180618

April 1, 2022

Table of Contents

Background

ABC inc. is a small tech manufacturing company with about 1,000 employees. The network infrastructure is divided into two divisions with specific organizational functions, the administrative and the manufacturing networks. The administrative department is responsible for the allocation and dispersion of organizational funds, payment to and from partnered organizations, and management of employee payments. The administrative department also handles project management, staffing, management of I.T. systems, and communication with shareholders. The manufacturing division performs the development, testing, and creation of ABC inc. goods using operational technology.

The strength in ABC inc. network is that the two divisions are logically separated. This means that if one division is infected with a virus, it is much less likely that it will spread to the other half. A weakness in this infrastructure is that if one network segment is hacked, that segment is half of the companies' resources and can reduce functionality of the other division.

Company Intellectual Properties

ABC inc. is a tech company that specializes in fully autonomous house products. ABC inc. owns the intellectual rights to the information and systems associated with their fully autonomous robots and the network infrastructure that supports business functions. We provide full customer support for our products and take pride in information and system security for our customers and our employees. As a tech provider, ABC inc. must stay a step ahead of threats and vulnerabilities with our products, but especially our in-house systems. We take pride in the fact that our customer data is held to the same security standard as our proprietary data. It is our duty

as a company to protect the confidentiality, integrity, and availability of organizational systems in order to provide continuous secure support services and a quality product for our clients.

Summary of the Incident

ABC inc. was the victim of a three-part cyber-attack that involved phishing, trojan malware, and a ransomware attack. First, an employee on the administration network was manipulated by a phishing email and willingly downloaded an attachment that turned out to be a trojan malware. Then, the trojan malware started to harvest ABC I.T. administration employee network credentials. After three weeks, The ABC I.T. administrative network was found to contain forty infected computers with ransomware which prevented authorized users from accessing pertinent network resources, system applications, and network capabilities. Because the administration network is responsible for I.T. system administration, financial responsibilities, and communication needs, the manufacturing network was negatively impacted, but not infected. Upon realization of the attack, in house staff hesitated to assess and react to the incident before it was too late. The attack ended up persisting three-weeks, until collaboration with a third-party cybersecurity organization who helped eradicate the virus from ABC I.T. network.

The Initial Phishing Attack

Post incident, we discovered that an employee on the administration network received a phishing email from a seemingly reputable source with a downloadable attachment. This employee was manipulated into believing that the CDC sent “Covid Prevention Awareness” emails out with an attachment that contained tips and tricks on how to avoid Covid-19.

Unfortunately, the attachment was a Zloader malware installation file disguised as an excel spreadsheet with Covid information.

Malware Zloader

Malware Zloader is a Trojan malware virus that is derived from the Zeus Malware which affected banks through phishing attacks, much like the one ABC I.T. suffered from. Once installed, Zloader uses web injects to steal usernames and passwords on the target network. After three weeks of the initial download of Zloader, ABC I.T. administration and financial system files were encrypted, and ransomware demands were revealed (Greg).

Ransomware Ryuk

Ryuk Ransomware is a computer virus that encrypts system files, effectively locking authorized users from accessing data stored on the infected systems. The purpose of ransomware is not to destroy systems, but to gatekeep authorized users from completing job functions until the target organization pays for the decryption key. Ryuk ransomware prevented access to ABC I.T. network resources that allowed them to access, transfer, or obtain and store monetary transactions associated with ABC inc. business operations. At peak infection, forty computers on ABC I.T. network were found with Ryuk ransomware related files (Malwarebytes).

Impact of the Incident

The initial phishing attack against an administrative employee caused 50% of ABC I.T. network employee accounts to be compromised through malware Zloader harvesting login credentials. The successful phishing attack and the installation of Zloader malware is what gave hackers the ability to access ABC I.T. network resources through an authorized user’s account.

Once hackers were able to access ABC I.T. secure network, they installed Ryuk malware that spread to forty computers on the administration network. This malware blocked access to system functions and data that is required for the operation of ABC I.T. network and reduced functionality of the engineering and manufacturing division.

Organizational Impact

The initial phishing attack has revealed a weakness in employee security situational awareness associated with job functions and allowed malware to be installed on systems without ABC I.T. knowing. The installation of malware Zloader caused several administration accounts to be compromised along with client personal data that was stored on the administration network. The organizational impact of the ransomware attack on ABC inc. is that we could not receive, send, or access financial and administration systems which caused work to stumble to a halt. For three weeks, ABC inc. could not provide full customer support, access financial systems, receive or distribute funds, and even affected the manufacturing network.

Lessons Learned

The successful phishing attack against an administrative employee is a great example of how powerful phishing attacks can be. Hundreds of administrative employees have received similar emails but did not fall for the attack. Because conducting phishing attacks are low cost, high volume, and high reward, this means that hackers can send thousands of low effort emails and only one needs to be successful to cause great damage to an organization. The undetected installation of malware Zloader is a showcase of ABC inc. inability to detect foreign installs on endpoint systems and is a flaw in how we monitor our network. Zloader granted access to authorized user’s accounts and ABC I.T. failed to detect any unauthorized access. Lastly,

ransomware Ryuk was a demonstration in how a simple phishing attack can become something much more deadly if undiscovered.

Vulnerability Assessment

Vulnerabilities of ABC Inc. network stems from potential breaches in the confidentiality, integrity, and availability of organizational systems and the data they store. ABC Inc. is a tech manufacturing company that processes, stores, and transfers sensitive data over a computer network and is subject to common internet of things and network vulnerabilities.

- Confidentiality of ABC inc. network means to collect and store sensitive data properly and in a secure manner. Making sure that only individuals who require access to sensitive data can access that data (Data Integrity).
- Maintaining system and data integrity means securing systems from unauthorized access and modification of private data. Integrity vulnerabilities of ABC Inc. network includes unauthorized access, dissemination of sensitive information, or unauthorized altering of private data. This data can be proprietary product information to employee or customer private data (Data Integrity).
- Protecting ABC inc. network systems availability involves keeping systems running and available to authorized users or customers as necessary. Much like other small businesses that provide continuous support for the products they manufacture, ABC Inc. is vulnerable to denial-of-service attacks that could interrupt support services for customers and employees (Data Integrity).

Threat Assessment

Threats to ABC Inc. network systems are closely related to the vulnerabilities identified above. Human error, malware, ransomware, social engineering, and denial of service attacks are common threats to ABC Inc. that can cause a breach in the confidentiality, integrity, and availability of organizational systems.

Risk Assessment and Vulnerability Mitigations

ABC Inc. Network Threats	
Social Engineering	Force of Nature
Malware	Theft
Ransomware	
Human Error	
Denial of Service	

ABC Inc. Network Vulnerabilities
Lack of User training and Awareness
Lax Continuous Monitoring systems
Low Incident response capability
Weak Antivirus Protection

ABC Inc. Network Risk Assessment	
Social Engineering - High Risk	Mitigation- Training and Awareness
Malware – High risk	Mitigation- Antivirus Protection
Human error – Medium risk	Mitigation- Training and Awareness
Denial of Service – Medium risk	Mitigation- Continuous Monitoring
Theft – Medium risk	Mitigation- Continuous Monitoring
Destruction of Assets- Medium risk	Mitigation- Backups and insurance
Force of Nature – Low	Mitigation- Backups and Insurance

ABC Inc. Network Security Plan
Mandatory user training and awareness specific to job functions and network usage.
Standard operating procedures for organizational system use and communication.
Implementing continuous monitoring and incident response capabilities.
Normalize a regular maintenance and antivirus scanning schedule.

Security Plan

The plan of action moving forward is to increase the security of ABC inc. network by implementing mandatory security and awareness training for all employees, upgrade antivirus software, and continuous monitoring of network resources. The main focus will be on training and awareness. This is because the event that sparked the entire incident is the initial phishing attack. If that one employee was more patient or informed, this whole incident could have been avoided. The idea behind user training and awareness is to include the user in the security scheme of ABC inc. network. This allows ABC inc. to hold its users accountable for systems and network they are associated with.

User Awareness

User training and awareness will be utilized to hold ABC Inc. employees responsible for the systems and networks they use. Without properly informing and training employees of social engineering attacks like phishing and other network vulnerabilities, I cannot hold them accountable for their negligence. Moving forward, there will be mandatory cybersecurity and awareness training for all employees. Trainings will be tracked by administrative personnel and distributed through the company employee access portal. Trainings will be distributed bi-monthly as to not overload users, but to remind and help create a more security focused environment.

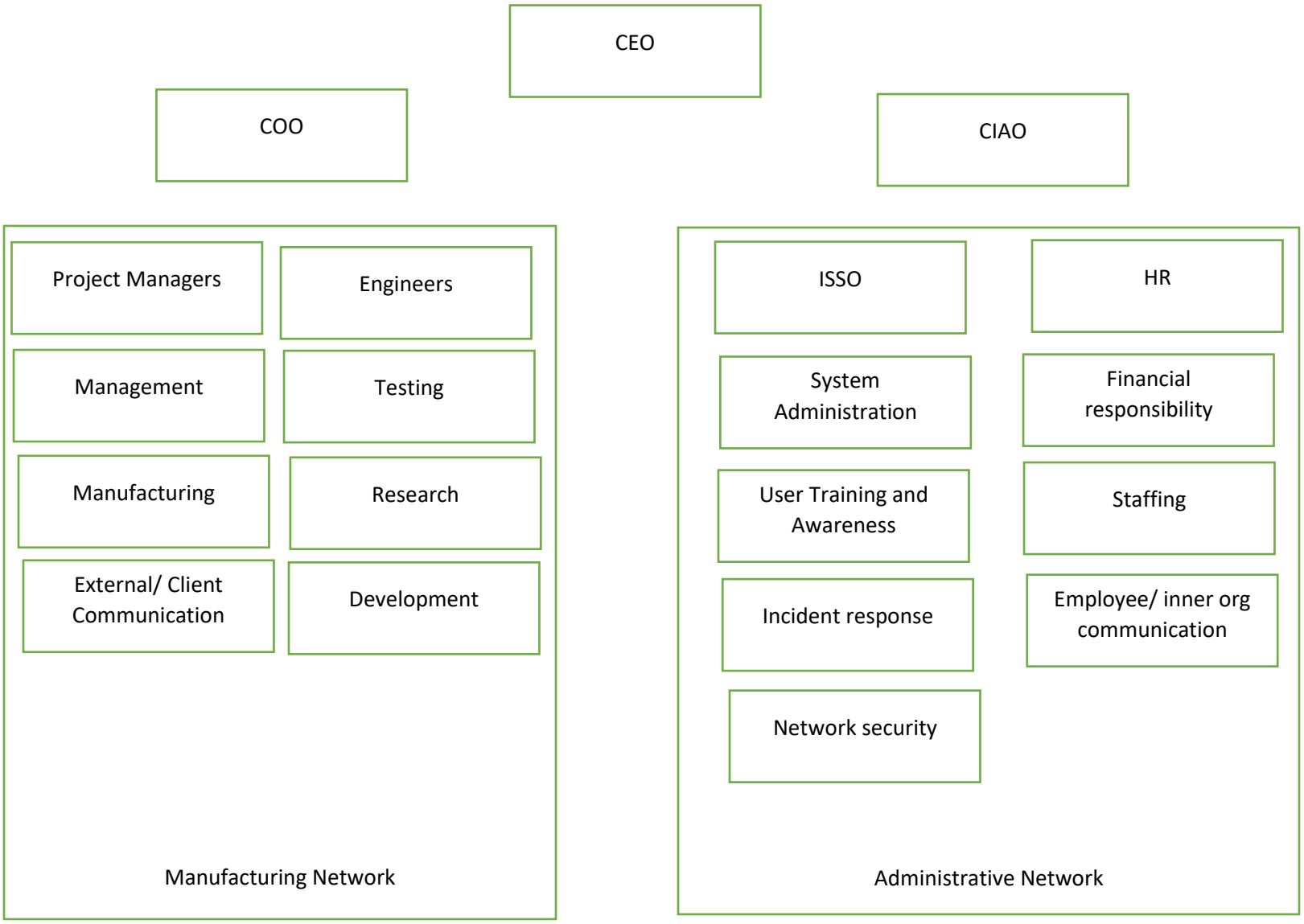
Antivirus Protection

I plan to upgrade antivirus protection capabilities in ABC Inc network by implementing operating system specific software for a more specialized capability.

Continuous Monitoring

By the time ABC I.T. identified that there was a problem, forty computers had already been infected with ransomware. I will implement end point security software to help monitor network resources and identify malicious activity before it's too late. Pair endpoint security software with a systems information and event management tool for a completely transparent and customizable view of ABC inc. network resources which will enable authorized users to identify malicious activity as soon as possible.

ABC Inc. Organizational Structure/ Communications Plan



References

Greg Belding, Zloader: What it is, how it works and how to prevent it, https://resources.infosecinstitute.com/topic/zloader-what-it-is-how-it-works-and-how-to-prevent-itmalware-spotlight/, 2020.

Data integrity: Executive Summary - NIST SP 1800-25 documentation. (n.d.). Retrieved April 14, 2022, from https://www.nccoe.nist.gov/publication/1800-25/VolA/index.html

Malwarebytes Staff, Ryuk ransomware, https://www.malwarebytes.com/ryuk-ransomware, 2021.