Old Dominion University

Information Assurance Policies and Recommendations for ABC Inc.

Caleb Judy

CS 465/565 Information Assurance for Cybersecurity Dr.

Santosh Kumar Nukavarapu

28 April 2025

TABLE OF CONTENTS

1. INTRODUCTION

ABC Inc was recently a victim of a ransomware attack and ABC Inc's operations were halted for three weeks, and ABC Inc was unable to perform tasks such as billing customers and paying vendors. This report will dive into the details of the ransomware attack that ABC Inc suffered from. The report will outline how the attack happened, the consequences of the attack, the vulnerabilities that were exploited in the attack, and the report will feature a threat matrix, which serves to highlight the severity of threats discussed in the vulnerability assessment. This report will also serve as a set of guidelines to enhance and protect ABC Inc's information assurance posture and prevent incidents similar to this one in the future. These guidelines will address both internal and external communications, and challenges posed by remote work environments. As the newly appointed Chief Information Assurance Officer (CIAO), I have been tasked with investigating this incident, assessing its impact, and developing a plan to prevent future

incidents that may occur. The report details the findings in this investigation and provides guidelines and recommendations to improve ABC Inc's information assurance, as mentioned.

2. BACKGROUND

2.1 ABC Inc's Operations and Structure

ABC Inc is a manufacturing company that primarily manufactures small computer parts. ABC Inc is a small company, with exactly 1,000 employees, staff, and personnel. ABC Inc is divided into two main parts: the Financial and Administrative segment and the Engineering and Manufacturing segment. The Financial and Administrative segment is the information technology (IT) side of the company, and the Engineering and Manufacturing segment is the operational technology (OT) side of the company. The Financial and Administrative segment of the company handles ABC Inc's financial operations, which includes handling the flow of money in and out of the company. The Engineering and Manufacturing segment is responsible for the company's engineering and manufacturing processes. Both the Financial and Administrative segment and the Engineering and Manufacturing segment are responsible for bank accounts receivable and payable, to a certain degree. Both the Financial and Administrative segment and the Engineering and Manufacturing segment share the same infrastructure and rely on an Enterprise Resource Planning (ERP) system.

2.2 Description of the incident

ABC Inc fell victim to a ransomware attack, which is an attack that encrypts files or data to the point where systems no longer function. A screen will demand payment in exchange for the return or decryption of files or data. Attackers can demand any kind of payment, including USD, Euro, Bitcoin, etc. It should be noted that it is possible for the victim to make a payment and still lose their files or data. Continuing, this attack originated from an administrative support employee who opened an email attachment which contained a malicious Microsoft Excel spreadsheet. Within approximately four minutes of opening the spreadsheet, a Zloader variant began cracking passwords and accessing logins. Three weeks later, the financial and administrative systems were locked down with ransomware attacks. Ryuk ransomware files were found on more than 40 computers on the IT network. The Engineering and Manufacturing segments were not directly impacted by this attack; it only affected the Financial and Administrative segments.

2.3 Strengths and Weaknesses of the Network Infrastructure

ABC Inc's network infrastructure has quite a few weaknesses which led to the eventual attack, but having said that, ABC Inc's network infrastructure isn't completely terrible. One of the strengths of ABC Inc's network infrastructure is that it features network segmentation. Network segmentation is the process of dividing a network into smaller, individual parts that enable network teams to compartmentalize the sub-networks and deliver unique security controls and services to each sub-network (VMware). The benefit of network segmentation is that since it divides your network into smaller segments, it also reduces the size of your attack surface, and it can isolate attacks to one sub-network, since the network is divided up (VMware). Another strength of ABC Inc's network infrastructure is that ABC Inc had backups for their data that could be utilized after the attack compromised some of ABC Inc's files. A backup is like a copy of your data and can be used if your data is lost or corrupted.

These strengths must not overshadow the various weaknesses of ABC Inc's network infrastructure, however. The first weakness of ABC Inc's network infrastructure is the fact that ABC Inc lacks a training program for employees on how to identify and respond to threats. On the surface this seems unrelated to network infrastructure, but this is directly linked to why the attack was able to work so well. After all, the initial point of attack was when an administrative support employee opened a malicious email attachment. If there had been employee training, or a proper training course explaining the various risks and threats a company like ABC Inc might face, this attack may have not been able to come to fruition at all. Second, ABC Inc's network infrastructure has a vulnerable email system. This was the point of the attack chosen by the malicious actors, which indicates something is wrong or vulnerable with ABC Inc's email system, possibly inadequate spam filtering or a lack of advanced threat protection. Additionally, the three-week delay between the initial Zloader infection and the ransomware attack indicates a lack of an effective security monitoring system, like an intrusion detection system or an intrusion prevention system (IDS/IPS). The attacker was able to operate within the network for multiple weeks without being detected. Lastly, while interconnected systems can better streamline and centralize company data and information, the reliance on this custom ERP system can be potentially catastrophic. Even with proper network segmentation, a compromise on one segment can lead to a compromise on another.

3. CONSEQUENCES OF THE ATTACK

The recent ransomware attack on ABC Inc. has triggered severe consequences requiring urgent attention. Core operations, including billing and payment processing, were

paralyzed for weeks, causing substantial financial losses and straining relationships with clients and vendors. The inability to invoice or pay obligations raised the risk of contractual breaches and legal issues. Internally, the overwhelmed technical support team had to enlist costly external cybersecurity experts to restore the compromised network, deepening financial strain. Beyond immediate disruptions, the attack has damaged ABC Inc.'s reputation and its network of relationships with customers, vendors, and partners. A cybersecurity breach undermines trust, prompting customers to reconsider their loyalty and partners to hesitate in future collaborations. This loss of confidence could have lasting impacts on ABC Inc.'s ability to maintain and grow its stakeholder base. Compounding the issue is the likely compromise of sensitive data. Although backups exist, they do not guarantee the integrity of the data exposed during the three-week breach. Attackers likely had ample opportunity to steal confidential customer information, proprietary business details, and financial records. The involvement of Zloader malware adds further risk, as it is specifically designed to harvest credentials and enable ongoing unauthorized access, leading to deeper security breaches. The consequences of data compromise could include regulatory investigations, hefty fines, and drawn-out legal battles, further threatening the company's stability. Additionally, the attack caused a sharp decline in productivity, especially within the Financial and Administrative departments, further amplifying operational and financial losses. Addressing these interconnected challenges will demand not only immediate action but also a fundamental overhaul of ABC Inc.'s cybersecurity infrastructure and incident response strategies to prevent future attacks.

4. RISK MANAGEMENT

ABC Inc needs to implement the following measures to prevent incidents such as this from happening again in the future. It is highly advised that ABC Inc follow the risk management process, visualized below (figure 1) (Cartledge).

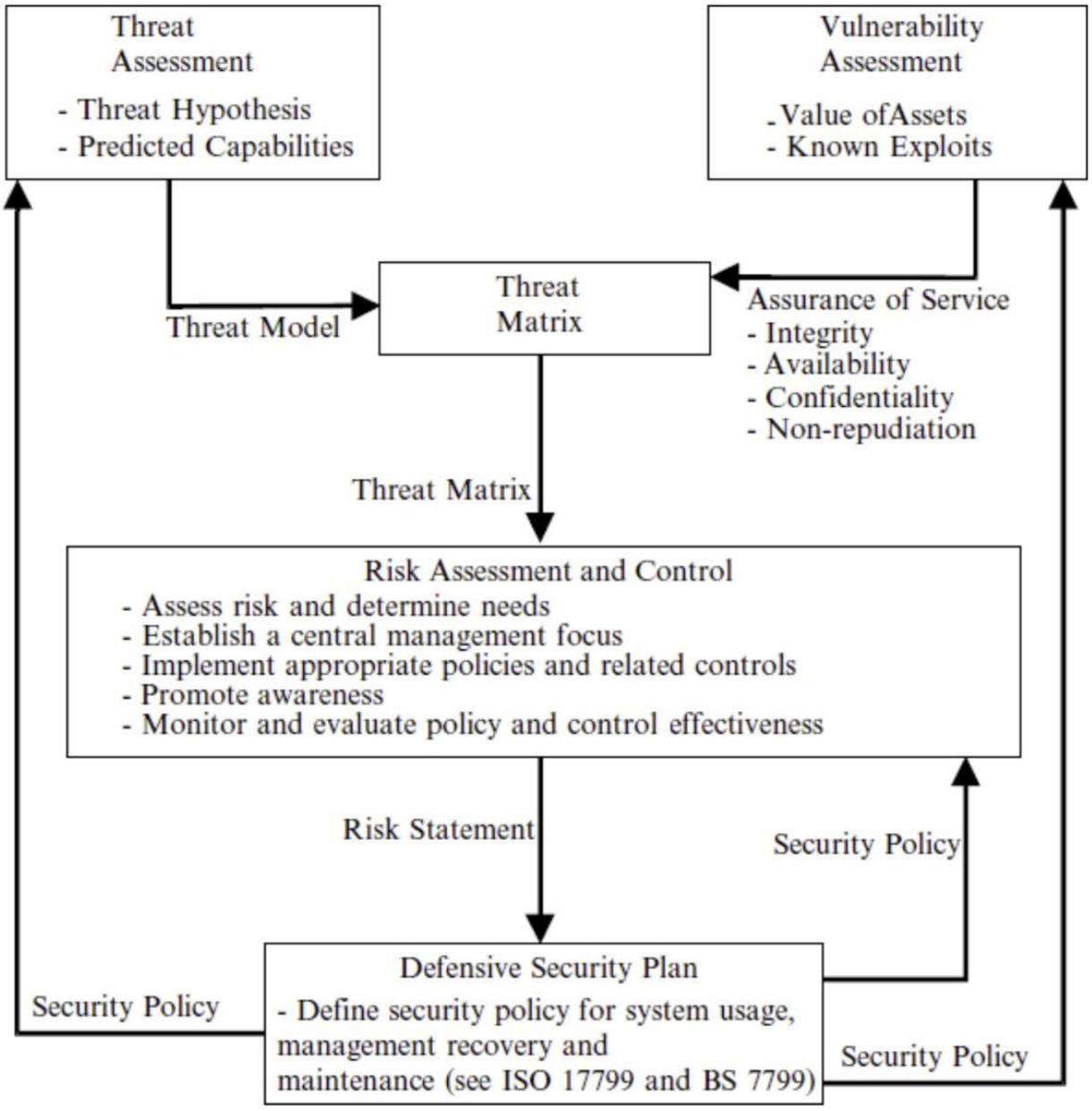

Figure 1 showcases the risk management process

The threat assessment identifies and analyzes the potential threats a company or organization might face. This step includes the threat hypothesis, which is where a company or organization predict what kind of threats they might face. Companies or organizations should ask themselves, who are the potential attackers? What might their motivations be? Who or what could be a target within our organization? These questions help companies and organizations lay a foundation to build their risk assessment off of. Predicted capabilities refers to what the threat is capable of, like what kind of technical capabilities, operational capabilities, or social engineering capabilities the threat

possesses. The vulnerability assessment examines weaknesses within the organization, through the value of assets and known exploits. The value of assets looks at all of the assets within an organization, like data, systems, and physical assets, and categorizes them to understand their criticality and sensitivity. Known exploits is exactly what it sounds like, it lists the known exploits that have affected a company or organization. The vulnerability assessment for ABC Inc is shown below (figure 2).

ASSET	DESCRIPTION	CLASSIFICATION	CIA TRIAD/NONREPUDATION	VULNERABILITIES
Financial Data	Records of accounts receivable and payable	Critical	Confidentiality, integrity, availability, non-repudiation	Lack of encryption at rest and in transit, insufficient access controls
Customer Data	Records of customer data, including contacts, order history, payment information, etc.	Critical	Confidentiality, integrity, availability	Lack of encryption at rest and in transit, vulnerable to SQL injection attacks
Employee Data	Records of Employee data, including personal information, salary information, etc.	Essential	Confidentiality, integrity, availability	Lack of encryption at rest and in transit, vulnerability to insider threats
ERP System	Custom Enterprise Resource Planning	Critical	Integrity, availability	Lack of regular security updates

	system that manages critical business processes.			
Network Infrastructure	Network devices like firewalls, etc.	Critical	availability	Misconfigurations, outdated firmware, lack of IDS/IPS system

Figure 2 visualizes the vulnerabilities that ABC Inc. faces

This vulnerability assessment classifies and describes assets of ABC Inc (ERP system, network infrastructure, etc.) and then classifies them based on necessity to ABC Inc's operation (critical, essential, ancillary) and then describes the vulnerabilities each face. You'll notice that there is a section labeled "CIA TRIAD/NON-REPUDATION". The CIA triad is essential for information assurance because it keeps information safe from adversaries or attackers. The guiding principles of the CIA triad are composed of confidentiality, integrity, and availability. Confidentiality is about ensuring that data is restricted to its intended audience and not others. The more sensitive the information is, the stricter the security measures should be. Integrity refers to maintaining the accuracy of data, ensuring it has not been tampered with or altered. Availability ensures data is available at all times so it can be accessed when needed (freecodecamp). Non-repudiation refers to the assurance that someone/something cannot deny something, such as the authenticity of a digital signature (freecodecamp).

Using the threat assessment and the vulnerability assessment, we can create a threat matrix, which is used to showcase and assess potential threats based on their likelihood and impact. The threat matrix for ABC Inc is shown below (figure 3).

THREAT	VULNERABILITIES	RISK LEVEL	THREAT LEVEL
Ransomware	Lack of employee training, vulnerable email system, insufficient security monitoring	Very high	Very high
Phishing	Lack of employee training, vulnerable email system	Very high	Very high

Insider threats	Insufficient access controls	Medium	Medium
Denial of Service (DoS)	Lack of network redundancy	Medium	Low
Malware	Lack of endpoint security, outdated systems	High	Medium

Figure 3 visualizes the threats that ABC Inc. faces

The threat matrix can help us visualize the various vulnerabilities ABC Inc faces, and we can use the threat matrix to build a better future for ABC Inc. The threat matrix can then be used to conduct a proper risk assessment, and then a strong, defensive security plan.

5. MEASURES TO PREVENT RECURRANCE

5.1 Risk Assessments and Management

The first measure that can prevent recurrence of a ransomware attack onto ABC Inc. is conducting regular risk assessments and updating the defensive security plan based on the findings of the risk assessment. It should be noted that risk assessments should be a regular occurrence, and not a one-time event. The process of risk assessment is shown above in figure 1 and should be closely followed.

Vulnerability management is also an important step in preventing recurrence. As mentioned in the “Risk Management” section, vulnerability assessment examines weaknesses within the organization, through the value of assets and known exploits. Expanding further on this, it is advised that ABC Inc. create a vulnerability management system; a program that identifies, assesses, and remediates vulnerabilities efficiently. This includes regular patching of systems and applications. If it is too much of a burden to create a vulnerability management system or program, ABC Inc could pay for the license of a third-party vulnerability management program. ABC Inc already has experience with third-party vendors, making this a viable option. ManageEngine Vulnerability Manager Plus, for example, is a robust vulnerability management program that performs various tasks such as protecting endpoints (workstations, laptops, virtual machines, etc.), automatically detecting vulnerabilities, and patching vulnerabilities and misconfigurations at the click of a button. The image below showcases ManageEngine’s Vulnerability Manager homepage (figure 4).

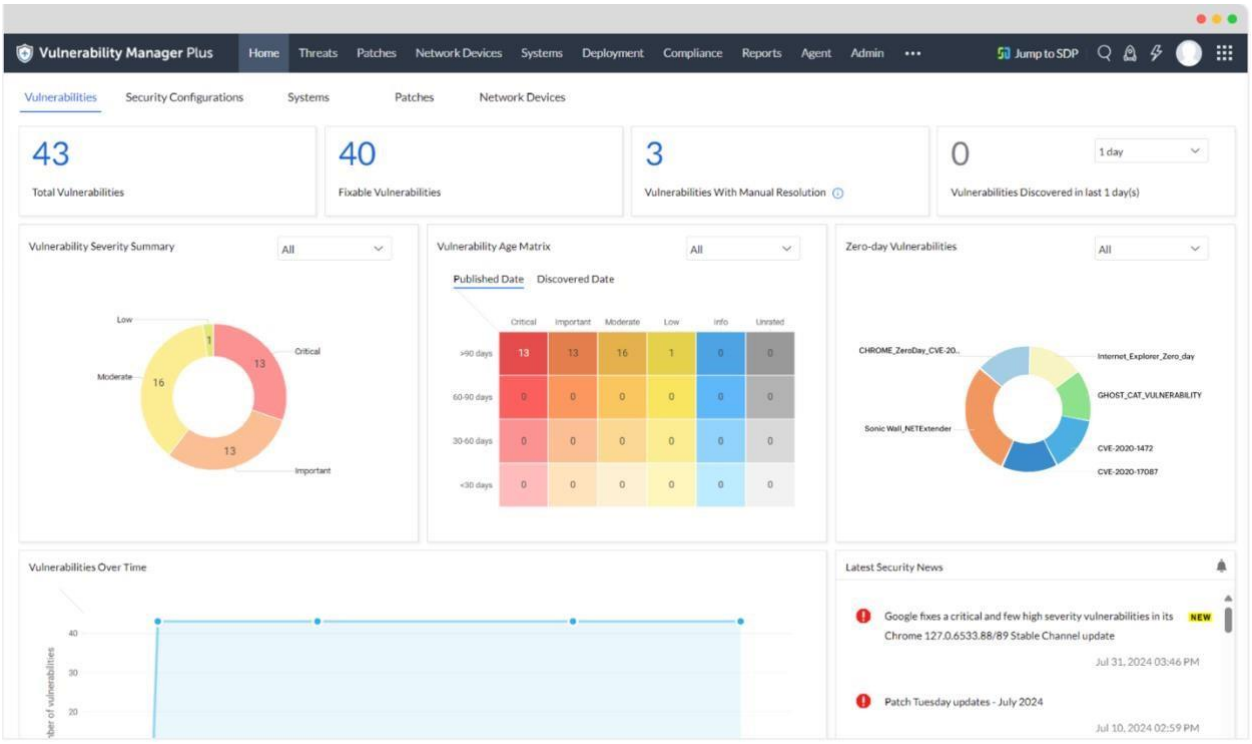

Figure 4 is an image of the homepage of ManageEngine Vulnerability Manager Plus

The homepage of ManageEngine Vulnerability Manager Plus showcases valuable information to an organization, relating to IT security. We can see that it displays total vulnerabilities (43), fixable vulnerabilities (40), vulnerabilities with manual resolution (3), vulnerabilities discovered in last 1 day(s) (0), a vulnerability severity summary, a vulnerability age matrix, and zero-day vulnerabilities. If ABC Inc wishes to create their own vulnerability management program, it should resemble or recreate the vulnerability manager created by ManageEngine.

It is also advised ABC INC preforms penetration testing to identify weaknesses in ABC Inc's network infrastructure. "Pen testing" works by launching a mock cyberattack, by ethical hackers who are trained to find weaknesses in systems. Pen tests are needed because a vulnerability assessment is not enough, and pen tests are more comprehensive than vulnerability assessments are. Vulnerabilities are exploited in a pen test, unlike in a vulnerability assessment. This can provide the security team at ABC Inc with insightful information as to how hackers could exploit these vulnerabilities to access sensitive data or disrupt operations (IBM).

5.2 Technical Controls

ABC Inc needs an upgrade to their email security. This should include enhanced spam filtering that blocks phishing emails, similar to the email that contained the malware that allowed attackers to gain access to ABC Inc's systems. Other upgrades to ABC Inc's email are advanced threat protection to detect and or block malware, training employees to understand what phishing emails are and how to recognize them, and using specific email protocols, like SPF and DKIM, to prevent email spoofing. SPF in particular allows domain owners to define a list of authorized mail servers that are permitted to send email on behalf of the domain (Perception Point).

ABC Inc is also in need of an Intrusion Prevention System and Intrusion Detection System (IPS/IDS). Intrusion detection is the practice of keeping an eye on your network traffic and examining it for indications of potential intrusions, including exploit attempts and incidents that could pose an immediate threat to your network. Intrusion prevention is the task of carrying out intrusion detection and subsequently putting an end to the occurrences that have been found, usually by discarding packets or ending sessions. IDS/IPS keeps an eye on all network traffic in order to spot any known harmful activity. Exploiting a software or device vulnerability is one method an attacker will use to try to breach a network. Before they can successfully breach any network endpoints, IDS/IPS detects and stops those exploit attempts. Because IDS/IPS can prevent attackers from obtaining information about your network, they are essential security technologies for both the network edge and the data center (Juniper).

Access control is also a need for ABC Inc. Stronger measures are needed, and the principle of least privilege should be implemented. The principle of least privilege limits user access to only the resources they need. This prevents lower-level employees from having administrator-level privileges, preventing insider threats due to the limited access. Multi-factor authentication should be implemented into all critical systems and accounts, and there should be regular review and revocation of user access rights. This is important in the event an employee is terminated and wants to take revenge on ABC Inc by compromising their systems.

5.3 Training

Employee training is also needed for the continuous success of ABC Inc. Training programs will be largely impactful in preventing attacks from happening again. The training program needs to include phishing awareness, malware prevention/recognition, data security training, social engineering awareness, and training on the important of human error.

6. ASSURANCE

As the newly appointed CIAO, I will implement the various measures recommended in the report above, with permission of the board of directors and the CEO of ABC Inc. The recommendations and measures presented in this report are essential to the future success and survival of ABC Inc, and without it I fear ABC Inc will cease to operate.

7. CONCLUSION

The ABC Inc. ransomware attack emphasizes how crucial a strong information assurance program is. ABC Inc. can greatly lower the risk of future security issues and safeguard its priceless information assets by putting the report's suggestions into practice. Given that human error is a persistent issue and that the threat landscape is ever-changing, ABC Inc. must adopt a proactive approach to security. The ability of the business to preserve the availability, confidentiality, and integrity of its information is essential to its success and ongoing operations.

Citations

Cartledge, Chuck. “Project Requirements .” *Old Dominion University*, 9 Oct. 2024, www.odu.edu/technology-services/canvas/students.

freecodecamp. “The CIA Triad - Confidentiality, Integrity, and Availability Explained.” *freeCodeCamp.Org*, freeCodeCamp.org, 1 Feb. 2020, www.freecodecamp.org/news/the-cia-triad-confidentiality-integrity-and-availabilityexplained/.

IBM. “What Is Penetration Testing?” *IBM*, 15 Apr. 2025, www.ibm.com/think/topics/penetration-testing.

Juniper. “What Is Ids and IPS?: Juniper Networks Us.” *Juniper Networks*, www.juniper.net/us/en/research-topics/what-is-ids-ips.html. Accessed 28 Apr. 2025.

ManageEngine. “Unified Vulnerability Management and Patching for Enterprises.” *Experience Perfect Harmony between Vulnerability Management and Patch Management. - ManageEngine Vulnerability Manager Plus*, www.manageengine.com/vulnerability-management/integrated-vulnerability-andpatch-management.html?network=g&device=c&keyword=vulnerability+management+software&campaignid=9145452449&creative=463439600553&matchtype=p&adposition=&placement=&adgroup=94262446004&targetid=kwd-304115066301&location=9215678&target=&gad_source=1&gad_campaignid=9145452449&gbraid=0AAAAAChA1UjvYUzOBk04AEVSr5skIj6Z9&gclid=EAIaIQobChMIlpSJJf8jAMVtkdHAR3K3TKnEAAYASAAEgIvWvD_BwE. Accessed 28 Apr. 2025.

Perception Point. “Email Security Protocols: SMTPS, STARTTLS, DMARC, and More.” *Perception Point*, 24 Sept. 2024, perception-point.io/guides/email-security/emailsecurity-protocols/.

VMware. “What Is Network Segmentation?: Vmware Glossary.” *VMware*, www.vmware.com/topics/network-segmentation. Accessed 28 Apr. 2025.