Joshua Freeman

Santosh Nukavarapu

Information Assurance CS465

23 April 2024

Information Assurance Project

Table of Contents

Introduction

The purpose of this report is to provide a closer look into the incident that occurred on January 18th, 2024. As the newly appointed Chief Information Assurance Officer (CIAO) of ABC Inc., it is imperative to conduct a thorough investigation of the incident, analyze its consequences, and develop detailed policies and procedures to prevent recurrence. This report will cover what happened, ABC's responsibilities, the consequences, a vulnerability assessment, creating a set of information assurance (IA) policies, and recommendations for how the company can improve. Throughout this report, a focus will be placed on objectivity, thoroughness, and adherence to best practices in information assurance. The recommendations outlined herein are designed to address the vulnerabilities exposed by the recent cybersecurity incident and promote a culture of cybersecurity awareness and resilience within ABC Inc. The successful implementation of these recommendations will not only enhance the company's ability to withstand future cybersecurity threats but also demonstrate its commitment to safeguarding the interests of employees, customers, and stakeholders.

Incident Summary

On January 18th, 2024, ABC Inc. suffered a cybersecurity attack. The company's internal network was compromised by a ransomware attack, resulting in the disruption of administrative and financial operations for three weeks. The attack originated from an email received by an administrative support employee, which contained a seemingly legitimate Excel spreadsheet attachment. Upon opening the attachment, a version of the Zloader malware was installed, allowing unauthorized access to login credentials and passwords. Three weeks later, the Ryuk ransomware was deployed, encrypted the data, and rendered the financial and administrative systems inaccessible. Although the incident primarily affected the IT segment of the company, which oversees accounts receivable and payable functions, the engineering and manufacturing segments remain largely unaffected. Immediate action was taken to allow external cybersecurity experts to assist in mitigating the attack. Through collaborative efforts with cybersecurity specialists, all suspicious and compromised files were identified and removed from ABC's network, computers, servers, and backups. The incident revealed vulnerabilities in ABC's network infrastructure and highlighted the need for enhanced IA policies and procedures to prevent future breaches

Background

ABC Inc. is a manufacturing company employing approximately 1,000 individuals, with a segmented network infrastructure. The company's network consists of two main segments: the information technology (IT) segment, which is responsible for administrative and financial operations, and the operational technology (OT) segment, which oversees the engineering and

manufacturing processes. Both segments share a common infrastructure interconnected by a custom enterprise resource planning (ERP) system. In terms of commercial responsibilities, ABC Inc. is tasked with manufacturing goods and managing financial transactions. The IT segment handles critical functions such as accounts receivable and accounts payable, which are integral to the company's cash flow management. Employees are provided with personalized email addresses for internal and external communication purposes.

While the segmentation of IT and OT networks is designed to enhance security and efficiency, vulnerabilities in email security and employee awareness were exploited during the recent ransomware attack. Previous security incidents may have also contributed to existing weaknesses within the network. ABC Inc. relies on strategic and corporate alliances to facilitate its operations, these alliances reduce risks while allowing the company to assess the potential of new market opportunities. The company's intellectual properties, including proprietary manufacturing processes and product designs, represent valuable assets that require protection from cybersecurity threats.

Aftermath

The ransomware attack on ABC Inc. resulted in significant consequences, impacting various aspects of the company's operations, reputation, and financial stability. The inability to access financial and administrative systems for three weeks led to substantial financial losses. ABC Inc. was unable to bill its customers or pay its vendors during this time, disrupting cash flow and revenue generation. Loss of revenue due to halted operations and the inability to fulfill customer orders resulted in immediate financial setbacks. The costs associated with engaging external cybersecurity experts for remediation further added to the financial burden. The incident

also tarnished ABC Inc.'s reputation, raising concerns among customers and stakeholders about the company's ability to protect sensitive information and maintain operational integrity. Due to trust and confidence in ABC Inc.'s cybersecurity measures being reduced, other business opportunities may have been lost. This could also have caused the company's relationships with other customers and partners to become strained.

The ransomware attack may have violated data protection regulations and industry compliance standards, exposing ABC Inc. to potential regulatory fines and legal liabilities. Failure to adequately protect sensitive customer data and intellectual property could result in legal action from affected parties, further exacerbating the financial and reputational impact of the incident. The disruption caused by the ransomware attack also impeded day-to-day operations, hindering productivity and efficiency across the organization. Employees were unable to access critical systems and data needed to perform their duties, leading to delays in decision-making, communication, and workflow processes. The incident may have also had a psychological impact on employees, causing stress, anxiety, and uncertainty about the security of their work environment and the company's future.

Vulnerability Assessment

ABC Inc. underwent a comprehensive vulnerability assessment following the ransomware attack to identify weaknesses in its information systems and processes. The assessment focused on evaluating the company's assets and ability to function, with a specific emphasis on critical, essential, and ancillary components essential to its operations. The goal was to ensure the integrity, availability, confidentiality, and non-repudiation of services provided by ABC Inc.

In terms of critical assets: The accounts receivable and accounts payable functions within the IT segment are critical to managing cash flow and sustaining business operations. Any disruption to these systems can have significant financial repercussions for the company. The custom ERP system serves as the backbone of ABC Inc.'s operations, facilitating communication and coordination between the IT and OT segments. Its integrity and availability are paramount to maintaining seamless business processes.

In terms of essential assets: confidential customer information stored within ABC.'s databases is essential for maintaining customer relationships and fulfilling orders. Ensuring the confidentiality and integrity of this data is crucial to preserving trust and loyalty among customers. ABC Inc.'s proprietary manufacturing processes, product designs, and trade secrets represent valuable assets that require protection from theft or compromise. Safeguarding intellectual property is essential to maintaining competitive advantage and market differentiation. Employee email accounts also play a vital role in internal and external communication. Ensuring the confidentiality and integrity of email communications is necessary to prevent unauthorized access and data breaches.

Threat Matrix

A risk analysis was conducted to assess the likelihood and potential impact of various threats to ABC Inc.'s information assets and operational continuity. The analysis aimed to prioritize risks based on their severity and the level of threat they pose to the company's integrity, availability, confidentiality, and non-repudiation services. The threats were also categorized and evaluated according to their relevance to the company's critical, essential, and

ancillary assets, as identified in the vulnerability assessment. The matrix below outlines key threats and their associated risk levels:

Phishing Attacks:

- **Likelihood: High**
- **Impact: Moderate to High**
- **Risk Level: High**

Phishing attacks targeting employees' email accounts pose a significant threat to the confidentiality and integrity of sensitive information, including login credentials and financial data. These attacks can lead to unauthorized access to critical systems and data breaches.

Ransomware Attacks:

- **Likelihood: Moderate to High**
- **Impact: High**
- **Risk Level: High**

Ransomware attacks, such as the recent incident involving Ryuk malware, can result in the encryption of data and the disruption of business operations. The inability to access financial and administrative systems for an extended period can lead to significant financial losses and reputational damage.

Insider Threats:

- **Likelihood: Low to Moderate**
- **Impact: High**
- **Risk Level: Moderate to High**

Insider threats, including malicious or negligent actions by employees or contractors, pose a significant risk to the confidentiality and integrity of sensitive data. Unauthorized access to critical systems or the inadvertent disclosure of sensitive information can result in financial and reputational harm to the company.

Supply Chain Compromises:

- **Likelihood: Moderate**
- **Impact: Moderate to High**
- **Risk Level: Moderate to High**

Supply chain compromises, such as the infiltration of third-party vendors or suppliers, can introduce vulnerabilities into ABC Inc.'s network infrastructure. Breaches within the supply chain can lead to data breaches, such as disruptions, and financial losses.

Zero-Day Exploits:

- **Likelihood: Low to Moderate**
- **Impact: High**
- **Risk Level: Moderate to High**

Zero-day exploits targeting unpatched software vulnerabilities pose a significant risk to ABC Inc.'s network security. The exploitation of unknown vulnerabilities can result in unauthorized access to critical systems and the theft or manipulation of sensitive data.

This risk matrix proves that ABC Inc. faces a range of cybersecurity threats with varying levels of likelihood and impact. Mitigating these risks will require a proactive approach, including implementing robust security controls, employee training, and ongoing threat monitoring and response capabilities.

Communication Plan

To effectively manage communications during and after a cybersecurity incident, ABC Inc. should implement a comprehensive communications plan that addresses its internal and external stakeholders.

In terms of internal communications: ABC Inc. should develop templates for internal communication to notify employees about the cybersecurity incident, including the nature of the incident, its impact on operations, and the expected timeline for resolution. Provide regular updates and status reports to keep employees informed about the progress of remediation efforts and any changes to business operations. Establish clear procedures for employees to follow in the event of a cybersecurity incident, including reporting protocols and escalation paths. Finally, designate a crisis management team responsible for coordinating communication efforts and management of employee inquiries and concerns.

In terms of external communications: ABC Inc. should develop templates for external communications to notify customers about the cybersecurity incident, including the potential impact on services. Provide timely updates and transparent communication to maintain trust and confidence among customers and minimize the impact on business relationships. Designate a spokesperson for the communications team to manage external communication with the media outlets, and other stakeholders. Develop key messages and talking points to address inquiries from the media and public regarding the incident and ABC Inc.'s response.

Prevention

To prevent something of this magnitude from happening again and to mitigate the risk of future cybersecurity incidents, there are a few things we can implement: First, is enhanced email security. Implementing email filtering and scanning solutions to detect and block phishing attempts and malicious attachments. Providing regular training and awareness programs for employees to recognize, report suspicious emails and enforcing strict password policies. Implementing multi-factor authentication for accessing critical systems and sensitive data. Requiring employees to authenticate their identities using a combination of passwords, biometrics, or security tokens could be the best way to enhance security. Conducting regular security audits and penetration testing to identify vulnerabilities in the network infrastructure and applications. Also, identify vulnerabilities quickly and implement measures to prevent future exploitation. Developing and maintaining an incident response plan, outlining roles, responsibilities, and procedures for responding to threats.

Training ABC Inc. employees should be one of the major focuses when evaluating this incident. So, providing ongoing cybersecurity training and awareness programs for all employees to educate them about common threats and best practices would be most effective. Fostering a culture of cybersecurity awareness and accountability throughout the organization would also be a priority.

Conclusion

In conclusion, the ransomware attack experienced by ABC Inc. served as a stark reminder of the critical importance of information assurance in safeguarding against

cybersecurity threats and ensuring the integrity, availability, confidentiality, and non-repudiation of business operations. The incident highlighted vulnerabilities in ABC Inc.'s network infrastructure and cybersecurity defenses, resulting in significant financial losses, reputational damage, and operational disruptions. To address these challenges and prevent future incidents, ABC Inc. must take proactive measures to strengthen its information assurance posture and enhance cybersecurity resilience. This includes implementing robust policies and procedures, such as enhanced email security measures, multi-factor authentication, regular security audits, and incident response planning. By implementing these recommendations and fostering a culture of cybersecurity awareness and resilience, ABC Inc. can mitigate the risk of future cybersecurity incidents, protect its critical assets and operations, and safeguard its reputation in an increasingly interconnected and digitally driven business environment. Ultimately, investing in information assurance is not only a business imperative but also a moral and ethical responsibility to protect the interests of employees, customers, and other stakeholders.

Citations

1) "Cybersecurity Training and Certifications." *Infosec*, www.infosecinstitute.com/. Accessed 10 Feb. 2024.

2) Michelle Steves, Kristen Greene, Mary Theofanos, Categorizing human phishing difficulty: a Phish Scale, *Journal of Cybersecurity*, Volume 6, Issue 1, 2020, tyaa009, https://doi.org/10.1093/cybsec/tyaa009

3) "What Is Cybersecurity?" *Cisco*, Cisco, 22 Feb. 2024, www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html.

4) Rezabek, Jeff. "How Much Does Phishing Cost Businesses?" *IRONSCALES*, IRONSCALES, 24 Jan. 2024, ironscales.com/blog/how-much-does-phishing-cost-businesses.

5) Sepulveda, Sebastian. "NIST CSF 2.0 Framework Update – A Comprehensive Guide." *StandardFusion*, 3 Apr. 2024, www.standardfusion.com/blog/nist-csf-2-0-update/.