Cameron Waddy

Santosh Nukavarapu

CS 465

April 23, 2024

Information Assurance Project

As the newly appointed Chief Information Assurance Officer (CIAO) at ABC Inc., a manufacturing company employing approximately 1,000 people, I am reporting our investigation into a recent security incident. Our company's network, logically segmented into financial/administrative (IT) and engineering/manufacturing (OT) segments, was compromised. The breach was initiated through a phishing email opened by an administrative support employee, which led to the installation of Zloader malware. This malware began harvesting logins and passwords within four minutes of the email being opened. Three weeks later, our financial and administrative systems were locked down due to ransomware demands. Ryuk ransomware related files were found on more than 40 computers on our IT network.

During this period, ABC was unable to bill its customers or pay its vendors, causing significant disruption to our operations. After our initial investigation, our engineering segment and the manufacturing programmable logic controllers (PLCs) have been identified as not impacted. In response to the crisis, our in-house technical support staff attempted to restore the infrastructure. However, upper management decided to bring in external cybersecurity support for a faster and more thorough resolution. With their help, all suspicious or compromised files were removed from ABC's network, computers, servers, and backups. Consequently, full company activities resumed. As the CIAO, my role now is to ensure such an incident does not recur by implementing robust information assurance (IA) policies and procedures. This incident report serves as the first step in that direction.

The incident has highlighted the importance of robust cybersecurity measures and the potential consequences of their absence. The fact that an email attachment could lead to such a significant disruption underscores the need for improved security protocols and employee training. Additionally, the decision to bring in external cybersecurity support indicates a recognition of the seriousness of the situation and the need for expert intervention. The successful removal of the malicious files and the resumption of company activities is a positive outcome, but it does not negate the need for ongoing vigilance. As the CIAO, my role extends beyond incident response to include proactive measures to prevent future incidents. This includes a thorough review of our current policies and procedures, identifying gaps, and implementing improvements. The goal is not just to respond to incidents, but to create an environment where such incidents are less likely to occur. This incident serves as a stark reminder of the potential threats we face and the importance of our ongoing commitment to information assurance.

ABC Inc., as a manufacturing company, has significant commercial responsibilities. We are entrusted with the production of high-quality goods that meet the needs and expectations of our customers. Our operations span across various sectors, making us a key player in the market. We are responsible for maintaining the standards of our products, ensuring timely delivery, and providing excellent customer service. Our company holds numerous intellectual properties, including patents for our unique manufacturing processes, trademarks for our brand, and copyrights for our proprietary software. These intellectual properties are crucial assets, giving us a competitive edge in the market. We have strategic partnerships with several corporations ranging from suppliers and distributors to research institutions and technology firms. These alliances enable us to streamline our operations, expand our market reach, and stay up-to-date on the latest advancements in our field.

Our network infrastructure is a vital component of our operations. It supports our enterprise resource planning (ERP) system, connecting our financial and administrative segment (IT) with our engineering and manufacturing segment (OT). This interconnectedness allows for seamless data flow and operational efficiency. However, the recent ransomware attack has exposed some weaknesses in our network infrastructure. Despite having logical segmentation between the IT and OT segments, the breach in the IT segment had a significant impact on our overall operations. The incident revealed that our current security measures were insufficient to prevent sophisticated cyber-attacks, while also highlighting the need for improved employee training on cybersecurity, as the breach was initiated through a phishing email. On the other hand, the fact that our OT segment remained unaffected during the incident indicates some strengths in our network infrastructure. This segmentation of our network likely helped prevent the spread of the ransomware to our OT segment. This incident serves as a valuable lesson for us to further strengthen our network security and implement robust information assurance policies.

The consequences of the ransomware attack on ABC Inc. were significant, however it was minimized due to our network segmentation. The most immediate impact was the disruption of our financial and administrative operations. For three weeks, we were unable to bill our customers or pay our vendors, causing a halt in our cash flow and potentially damaging our relationships with these key stakeholders. Through presenting a plan on how to retroactively prevent incidents like this again, we will be able to mend these relationships. This will work to help us gain back their trust in our ongoing partnerships. Regardless, this incident has had a considerable impact on our reputation. In today’s digital age, a company’s cybersecurity posture is a critical aspect of its overall reputation. The breach may have caused our stakeholders to question our ability to protect our network and the sensitive data it holds. Moreover, the breach exposed sensitive data, posing a threat to our intellectual properties and partnerships. The harvested logins and passwords could potentially be used for further attacks or sold on the dark web. This not only puts our company at risk but also our partners who trust us with their data.

The incident also revealed weaknesses in our network infrastructure and security measures. These weaknesses are being addressed currently to fix any gaps and to create a more secure infrastructure. It's crucial that we learn from this incident and take steps to strengthen our networking security posture. Furthermore, the incident has likely resulted in significant financial costs. These include the cost of the external cybersecurity support, potential regulatory fines, and the cost of implementing new security measures. There may also be hidden costs such as lost business due to damaged reputation. This incident serves as a stark reminder of the cyber threats that we face and the importance of robust information assurance policies. I will work hard to ensure that we learn from this incident and take all necessary measures to prevent such breaches in the future. This includes a thorough review of our current policies and procedures, identifying gaps, and implementing improvements. The goal is not just to respond to incidents, but to create an environment where such incidents are less likely to occur.

Our network infrastructure, which is the backbone of our operations, was identified as a critical asset. It supports both our IT and OT segments, enabling us to perform services, charge for services, receive payment for services, and pay for services. However, the recent ransomware attack has exposed vulnerabilities in our network security, particularly in the IT segment. This incident has highlighted the need for ensuring the integrity, availability, confidentiality, and non-repudiation of our network. (Staff) Another critical asset is our enterprise resource planning

(ERP) system. This system, which connects our IT and OT segments, facilitates the flow of information across the company, supporting various functions from financial management to manufacturing processes. (Corporation) Any vulnerabilities in this system could disrupt our ability to function effectively, emphasizing the need for securing our ERP system.

Our intellectual properties, including our patents, trademarks, and copyrights, are critical assets. The breach exposed sensitive data, posing a threat to these intellectual properties. Therefore, protecting these assets from breaches is crucial for maintaining our market position and ensuring the integrity and confidentiality of our proprietary information. In terms of essential assets, our employees play a significant role in maintaining our network security. The recent incident, having been initiated through a phishing email, indicates a need for improved employee training on cybersecurity. While not directly involved in performing or charging for services, employee training is essential for preventing security breaches. Lastly, our partnerships with several corporations were identified as ancillary assets. These partnerships help us streamline our operations and expand our market reach. While these alliances do not directly affect our ability to perform services, charge for services, receive payment for services, or pay for services, they are still important to our business. Any breach in our network could potentially impact these alliances, making it important to ensure the confidentiality of our shared data.

This assessment highlights the need for robust information assurance policies and procedures. As the CIAO it is my duty to guide the implementation of these policies and procedures to prevent future incidents. This includes a thorough review of our current policies and procedures, identifying gaps, and implementing improvements. The goal is not just to respond to incidents, but to create an environment where such incidents are less likely to occur.

ABC Inc.’s lifeline in enabling seamless communication and data transfer across all departments is our networking infrastructure. Cyber threats such as DDoS and malware pose a significant risk, with potential consequences including service disruption and financial implications. Given the recent ransomware attack, the probability of such threats is high, making this a high-risk area that requires immediate attention. Therefore, it’s crucial to have robust security measures in place, including firewalls, intrusion detection systems, and regular vulnerability assessments. Additionally, a disaster recovery plan should be in place to ensure business continuity in the event of a network failure.

The enterprise resource planning system is another key asset that bridges the IT and OT segments. Data breaches could interrupt the seamless flow of information, affecting a range of functions from finance to manufacturing. While the segmented network reduces the likelihood of such breaches, the impact would be substantial, placing this in the high-risk category. Therefore, securing the ERP system is of utmost importance. This can be achieved through regular system updates, strong access control measures, and continuous monitoring for any suspicious activities.

Intellectual properties are the cornerstone of ABC Inc.'s competitive advantage. Theft or unauthorized access to these assets could erode this advantage and result in financial loss. Although the probability of such threats is low, the potential impact is high, making this a medium-risk area. Therefore, it’s crucial to have strict security measures in place to protect these assets. This includes secure storage solutions, strong access control measures, and regular audits to ensure compliance with intellectual property laws.

Employees are the first line of defense against cyber threats. Their awareness and understanding of cybersecurity best practices can significantly reduce the risk of breaches. Therefore, regular cybersecurity training should be provided to all employees, regardless of their role in the company. Additionally, a strong security culture should be fostered within the organization, encouraging employees to report any suspicious activities and to stay updated on the latest cybersecurity trends. The recent phishing incident underscores the need for improved cybersecurity training. The high probability of social engineering attacks and their potential to lead to data breaches places this in the high-risk category.

Our corporate partnerships are another potential target for attack. A data breach could impact these partnerships, potentially leading to a loss of trust and financial implications. However, both the likelihood and impact of such a breach are low, making this a low-risk area. Therefore, it’s important to have clear data sharing agreements in place with all partners, outlining the responsibilities and obligations of each party. Regular audits should also be conducted to ensure compliance with these agreements and to identify any potential vulnerabilities.

In summary, the threat matrix risk analysis underscores the need for robust information assurance policies and procedures. As a whole, ABC Inc. will work to mitigate these risks and safeguard the company’s assets. This includes enhancing our network security, bolstering data protection measures, providing employee training, and establishing data sharing protocols with strategic alliances. It’s important to remember that risk management is a dynamic process, and the threat matrix should be updated regularly to reflect the evolving threat landscape.

Effective communication is the lifeblood of any organization, and ABC Inc. is no exception. It plays a crucial role in building trust, fostering transparency, and ensuring the smooth functioning of all operations. In the context of cybersecurity, communication becomes even more vital. It helps in creating awareness about potential threats, educating employees about best practices, and ensuring a swift response during security incidents. Moreover, clear and timely communication with external stakeholders like customers, partners, and regulatory bodies helps in maintaining trust, meeting compliance requirements, and managing crises effectively. Therefore, a well-defined communication plan is an integral part of ABC Inc.'s information assurance strategy. It not only helps in mitigating risks but also contributes to the company's overall growth and reputation management.

In the wake of the recent security incident, it's crucial to openly communicate with our employees about what happened. We will hold a company-wide meeting to discuss the incident, its impact, and the steps taken to resolve it. This will not only keep everyone informed but also help in dispelling any rumors or misinformation. Following this, we will share a detailed incident report with all employees, outlining the nature of the attack, how it was detected, and the measures taken to mitigate it. Moving forward, we will establish a regular communication schedule to keep all employees updated about our cybersecurity initiatives. This will include monthly all-hands meetings and bi-weekly departmental meetings focused on cybersecurity. We will also launch a cybersecurity training program to equip our employees with the knowledge and skills to prevent such incidents in the future.

Transparency is key when communicating with our external stakeholders about the incident. We will issue a public statement detailing the incident, its impact, and the steps we have taken to resolve it. This will be shared on our website, social media channels, and through a press release. We will also set up a dedicated customer service line to address any queries or concerns related to the incident. In the future, we will continue to maintain transparency with our customers and partners about our cybersecurity measures. Regular updates will be provided on our website and social media channels. We will also collaborate with our partners to share best practices and learnings in cybersecurity. In case of a future security incident, a crisis communication plan will be activated to manage external communications.

Our first and foremost priority is network security. We will deploy state-of-the-art firewalls, through which we will establish sophisticated intrusion detection and prevention systems and execute regular vulnerability assessments. Constant vigilance over our network infrastructure allows us to promptly identify and address any suspicious activities or potential threats, staying one step ahead of cybercriminals. Shifting our attention to the security of our enterprise resource planning system, we will ensure it is always up to date with the latest patches to address any known vulnerabilities. Strict access will be implemented to allow only authorized personnel to access sensitive information. Continuous monitoring of systems is crucial to detect any signs of unauthorized access or potential data leakage. The protection of intellectual properties is another critical aspect of our security strategy. We will work to utilize secure storage solutions and robust access control measures to safeguard these valuable assets. Regular audits will be conducted to ensure compliance with intellectual property laws and to prevent any potential infringements.

Recognizing that our employees are the first line of defense against cyber threats, we are working to implement a comprehensive cybersecurity training program. This program covers essential topics such as recognizing phishing attempts, practicing secure password habits, and reporting suspicious activities. This training program will be updated regularly to keep pace with the rapidly evolving threat landscape. Furthermore, we will establish data sharing agreements with our partners. These agreements will clearly outline the responsibilities and obligations of each party regarding data handling and protection. Additionally, these agreements will be reviewed and updated regularly to accommodate changes in the partnership or regulatory environment.

In the event of a security incident, we are actively working to implement a detailed disaster recovery and business continuity plan. This plan will outline the steps to be taken to ensure minimal disruption to our operations. Regular drills will be conducted to familiarize all employees with the plan and to ensure a swift and effective response in the case of an incident. In addition to our disaster recovery plan, we will incorporate an incident response plan. This plan shall outline the procedures for identifying and containing a security breach, eradicating the threat, and recovering from the incident. It will also include a communication strategy to keep stakeholders informed about the incident and the steps taken to resolve it. We will continuously ensure compliance with all relevant laws and regulations, including data protection laws, privacy laws, and industry-specific regulations. Regular audits will be conducted to ensure compliance, identifying any areas of non-compliance, and taking corrective actions.

In conclusion, this comprehensive plan, if effectively implemented, can significantly mitigate the risk of future security incidents. However, it’s crucial to remember that cybersecurity is a continuous effort. The plan should be reviewed and updated regularly to address the evolving threat landscape. Additionally, it’s important to foster a culture of security awareness among all employees, as they are often the first line of defense against cyber threats. Lastly, we should also consider engaging with external cybersecurity experts for periodic audits and consultations to ensure our security measures are up-to-date and effective.

Works Cited

Corporation, Microsoft. *What Is Enterprise Resource Planning (ERP)?—Microsoft Dynamics 365*. dynamics.microsoft.com/en-us/erp/what-is-erp.

Staff, Coursera. “What Is the CIA Triad?” Coursera, 29 Nov. 2023, www.coursera.org/articles/cia-triad.