Information Assurance Project

Aaron Jones

CS465

4/23/2024

Information Assurance Project

Executive Summary

As the incoming Chief Information Assurance Officer (CIAO) for ABC Inc., a manufacturing company with approximately 1,000 employees, I have been assigned to investigate a recent cybersecurity event and offer comprehensive commendations that can help prevent the event from occurring again (Cartledge,2022). ABC's internal network was negotiated, which distracted administrative and financial processes for about a week in late 2022(Cartledge,2022). After the investigation was conducted, it was stated that one personnel had accidentally opened a malicious Excel spreadsheet attachment, which enabled the Zloader malware to be in a position to access the login identifications and eventually install Ryuk ransomware all over the IT network.

1. Background

ABC Inc. is a manufacturing organization comprising around 1,000 personnel (Cartledge,2022). The company has a rationally segmented network that entails financial and administrative functions on one side and engineering and manufacturing processes in a different operational technology (OT) section. A custom enterprise resource planning (ERP) system links the segments entirely. The IT section is responsible for cashing in and out and conducting other tasks that need money to operate in and outside the organization. To enable internal and external communication, the workforce has personal emails that make communication easy.

ABC's network infrastructure possesses strengths and weaknesses. One strength is that the logical segmentation between IT and OT networks reduces the possible spread of risks between those surroundings. The custom ERP system also enabled specialization functionality to help facilitate ABC's organizational needs (Cartledge,2022).On the negative

side, the shared infrastructure between IT and OT and the dependence on email to facilitate communications leads to vulnerabilities. The lack of robust security controls and workers' security awareness also led to the current cybersecurity event.

ABC's Commercial Responsibilities and Intellectual Property Strategies and Corporate Alliance

As a manufacturing company, ABC has commercial responsibilities that entail manufacturing and selling its goods to clients. The company also gets necessary raw materials and supplies from sellers and controls its financial processes (Cartledge,2022). The business's intellectual property consists mainly of its proprietary manufacturing courses, quality designs, and the custom ERP system that mixes its business functions. ABC's success dramatically depends on its manufacturing processes, which enable the organization to produce and distribute its goods to clients. Billing, payments, and payroll are some examples of vital financial activities, as they enable money to come in and out of the firm, allowing ABC to continue operating and maintaining its cash liquidity. The company's intellectual property, which offers ABC a competitive edge in the market, is another critical factor. An example entails its manufacturing procedures and product designs.

Aside from its primary duties related to production and finance, ABC also upholds strategic alliances with several significant suppliers and distributors and participates in joint research and development with academic institutions and other manufacturing institutions (Cartledge,2022). These partnerships offer ABC access to particular employees, markets, and technology, yet they also attract crucial third-party risk considerations that should be handled carefully.

Strengths and Weaknesses of ABC's Network Infrastructure

One of ABC's network infrastructure's core advantages is the logical separation of its IT and OT surroundings. This division aids in avoiding the potential spreading of threats since the Ryuk ransomware mainly impacted the IT network, not the manufacturing processes. Furthermore, ABC's custom ERP system provides specific functionality and incorporation throughout the organization's business processes, allowing it to control its operations flexibly, which may appear impossible with off-the-shelf alternatives (Cartledge,2022). By customizing its systems, ABC can better meet its exclusive requirements and lessen the possibility of any vulnerabilities in more general corporate software.

However, several threats are attracted by the joint underlying infrastructure between the IT and OT divisions and by using email to facilitate external communication (Cartledge,2022). The environment appeared vulnerable to the extent of attracting a social engineering attack that led to the Zloader malware infection since there were insufficient strong security control measures, for instance, advanced email filtering, access management, and endpoint safety, and also the personnel lacked understanding of the importance of security measures. ABC's account management and access control protocols' shortcomings, as well as the lack of in-depth information backup and recovery procedures, tampered with the ransomware attack's effectiveness (Cartledge,2022). The situation took three weeks, showing that ABC's ability to recognize, investigate, and address cybersecurity proceedings was inadequate, aggravating the repercussions.

2. Incident Summary

In late 2022, ABC's internal network was compromised, disrupting administrative and financial operations for approximately three weeks. (Cartledge, 2022). The investigation

revealed that the incident began when an administrative support employee received an email with an Excel spreadsheet attachment that appeared to be from a valid source.

Within 4 minutes of opening the spreadsheet, the Zloader malware was installed, allowing the attackers to harvest login credentials. (Cartledge, 2022). Over the following three weeks, the Ryuk ransomware was deployed across over 40 computers on the ABC IT network, effectively locking down the financial and administrative systems. During this time, ABC could not bill customers or pay vendors, severely impacting its ability to conduct business. The engineering and manufacturing segments of the network, including the programmable logic controllers (PLCs), were not directly affected by the incident.

With the assistance of external cybersecurity experts, ABC was able to remove the suspicious and compromised files from its network, computers, servers, and backups and ultimately restore entire company operations. (Cartledge, 2022). However, the prolonged disruption and the consequences of the incident have highlighted the need for a comprehensive review of ABC's information assurance measures and the implementation of robust controls to prevent similar occurrences in the future.

3. Consequences of the Incident

The consequences of ABC's cybersecurity incident were enormous, affecting the firm's operations and financial position.

How the Critical Business operations were impacted

The IT network breach and the complementary Ryuk ransomware release directly impacted the ability of ABC to conduct some essential corporate operations, such as;

Billing customers: ABC was not in a position to create and send bills to its clients for three weeks, which disrupted cash flow and possibly harmed its relationship with its clients. This had the business's ability to acquire payments and maintain its financial maintainability, which was scary for conducting its operations. Paying vendors: After the incident, ABC could not pay its vendors and suppliers, which might have strained business relations and caused supply chain interruptions for the firm. This might have made it extremely challenging for ABC to meet consumer demands by causing delays in acquiring raw materials and other vital components necessary for manufacturing.

Retrieving financial information: ABC was not able to acquire critical financial records, such as cash received and cash paid, or any necessary data to carry out operations due to the encryption of files on the IT network. This hindered the firm’s ability to manage its cash flow, make wise decisions, and maintain appropriate financial controls.

Essential Business Functions Impacted

Apart from the critical functions, the incident also interrupted some crucial business activities:

Internal and External Communication: The compromise of personnel email accounts significantly compromised ABC's internal and external communication, thus affecting coordination between employees and customers, vendors, and other stakeholders within the organization (Kala, 2023). This disrupted effective lines of communication in a manner that the company could not ease, address the incident effectively, and maintain adequate information flow to the stakeholders.

Access to customer and vendor data: The IT network was compromised by broken file encryption, meaning that ABC lost a significant part of important information in regards to

their customers and vendors, specifically contact information and history of orders, among other records that businesses have to keep up with business relations. This made it very hard to manage the accounts of customers effectively, and the company's supply chain was, therefore, possibly undermined, given the strain.

Operational reporting and decision-making: The lack of access to the management's financial and any other operational data hampered its capability to effectively make sound decisions and manage the company during the occurrence. In this, responding to the crisis, the distribution of resources, and planning for returning to normal operations became further complicated, enhancing the consequences.

Ancillary Business Functions Impacted

While the above is not critical to ABC's operations, the incident has disrupted several ancillary business functions.

Human resource activities: Some Activities that affected human resources are processing payroll and records of their employees after the incident, which added difficulty to the HR Department of ABC Inc. This might also affect employee morale and satisfaction, thus affecting the company's ability to continue operations and possibly affecting employee retention.

Support and maintenance of IT: The IT department seemed to concentrate on responding to the incident to the extent that they neglected their daily tasks, which entailed maintaining the system and ensuring tasks ran smoothly (Kala, 2023). This might have introduced further weaknesses or delayed a timely security update, furthering the increased risk to the company.

Regulatory compliance: The disruption of ABC's operational and financial information may have an effect on the company's capacity to adhere to financial reporting. Failure to these might result in fines and might also ruin the company's reputation and financial position.

Overall, the cybersecurity issue affected ABC's ability to continue as a business; fallouts span more than just financial or operational disruptions (Cremer et al., 2022). The company's name and relations with its customers, vendors, and other stakeholders may also have been tarnished, thus reinforcing the importance of solid measures for information assurance to avoid the recurrence of incidents in the future.

4. Vulnerability Assessment and Threat Matrix

I undertook an in-depth vulnerability assessment and threat matrix analysis to clarify the threats ABC faces and how to develop suitable mitigations.

Vulnerability Assessment

Based on the incident details and ABC's business operations and network infrastructure, I can clearly identify the following vulnerabilities.

Critical Vulnerabilities

Poor email security controls: Ransomware used to spread the campaign's malware from an attachment of a malicious email shows that better email security is needed to recognize and stop such threats (Ursillo &Arnold, 2023). This includes advanced email filtering, attachment scanning, and impersonation so that you do not end up unsuspectingly making the company prone to malware infections.

Lack of comprehensive data backup and recovery mechanism: The fact that ransomware named Ryuk encrypted the files on the IT network would automatically imply that ABC's backup and recovery methods did not restore the operations as soon as possible.

Weak access control and credential management: The successful gaining of personnel login credentials by the Zloader malware shows dimness in ABC's user authentication. Some of the areas that needed bettering included multi-factor authentication, just-in-time access, and continued round-the-clock monitoring of users' activities (Ursillo &Arnold, 2023). This helps to avoid undue use of the credentials and damage caused by the breach.

Essential Vulnerabilities

Inadequate network segmentation: Even though the logical separation between the IT and OT networks somehow restricted the impact to a great extent, the common shared underpinning infrastructure still allowed malware movement between the two segments. This further isolate critical systems and reduces the chances of threats moving laterally across the network, with even more increased network segmentation and access controls.

Poor security awareness and training: The employee opening the attachment may appear to be accidental and unintentional; however, this only shows how there is inferior and ineffective security awareness and training of employees so as to enable them to understand better when they are being targeted and how to respond to such threats (Akter et al., 2022). Regular phishing simulations and educational security campaigns are highly needed so that a change can be introduced to improve employees' security behavior and achieve an organizational security culture.

Weak monitoring and response capabilities: The fact that the incident had been ongoing for such a prolonged duration (3 weeks) indicates weak detection, investigation, and response

capabilities on the part of ABC. Along with a formal incident response plan, centralized logging, monitoring, and implementation of the Security Information and Event Management (SIEM) capabilities will highly increase ABC's ability to effectively detect, contain, and recover from security incidents (Ursillo &Arnold, 2023).

Ancillary Vulnerabilities

Outdated or unpatched software: Insecure software harbors weaknesses that attackers could exploit, leading to larger compromise scenarios. This continuously identifies, ranks, and remediates the identified vulnerabilities across the organization and even further reduces the attack surface area.

Poor documentation and planning of the incident response: ABC business operations were interrupted due to a lack of adequately documented incident response procedures and communication plans. Regular exercise of comprehensive incident response and communications plans can help ensure a more coordinated and effective response in the future for security events with a minimum impact on the company's operations and its constituencies (Cremer et al., 2022).

Threat Matrix

Regarding the acknowledged vulnerabilities and the details of the incident, I have come up with the following threat matrix to evaluate the risks facing ABC:

Threat	Likelihood	Impact	Risk
Phishing/social engineering attacks	High	High	Extreme
Ransomware/malware infections	High	High	Extreme
Unauthorized access to sensitive data	Medium	High	High
Disruption of critical business functions	High	High	Extreme
Supply chain/vendor-related incidents	Medium	Medium	Medium
Regulatory non-compliance	Medium	Medium	Medium

The likelihood and impact of phishing/social engineering attacks and ransomware/malware infections could bring extreme risk to the organization's critical ICT infrastructure. This has become evident very recently from the successful execution of both these threats, which have brought down the catastrophic effect on ABC's overreaching operations and critical business functions.

The other significant risk is the unauthorized access of sensitive data, including financial and customer records, because any such compromise exposes these to further damage in terms of money and reputation. Hence, more importantly, measures toward more robust access controls and privileged account management are taken up.

Disruption of key business activities, such as billing, payments, and communications, is also rated as extreme risk due to the direct impact associated with ABC's immediate function. Better data backup and recovery capabilities and enhanced monitoring and incident response will improve the company's resilience and rapid recovery from such disruptions (Ursillo & Arnold, 2023). This will also lower the risk of losses suffered by the company.

While still posing risks, supply chain-related incidents and regulatory non-compliances were assessed at medium likelihood and impact levels, which aggregated to medium. This allows ABC to mitigate the risk imposed on the company—this kind of risk at a medium level. This is ensured through implementing a formal vendor and third-party risk management program to ensure that ABC enforces relevant regulations to mitigate it.

5. Recommended Communications Plan

ABC's communication in response to the recent cybersecurity incident and ongoing information assurance will need an effective communication plan, specifically for internal and external stakeholders, to ensure transparency, coordination, and a unifying response.

Internal Communications

Employees: Brief all employees about what has really transpired, its repercussions, and the actual steps being taken to set things right, along with precautionary ones to avoid a repeat. Highlight new policies and procedures for more sensitization and compliance (Jorgensen, 2018). This message will be reiterated in regular security awareness, training, and communication campaigns to help create a culture of security in the organization. IT and security teams should establish regular and structured channels of communication that enable incident response coordination, sharing threat intelligence, and coordinating the implementation of new security controls. This may include but is not limited to, weekly or

monthly meetings, shared collaboration spaces, and a central repository for incident response documentation and procedures.

Management and executive leadership: Regular communication with senior management decision-makers, both at the general operations level and the IT support from an operational perspective, to inform them of the breach's financial and operational impact and strategic decisions to be made to strengthen information assurance posture. Communication with these executives should include suggestions on resource commitment, policy change, and high-level prioritization of security-related initiatives.

External Communications

Customer: Communicate the incident and its impacts on customers' business operations, information security, and ABC's abilities to serve customers. Provide timely restoration service updates and assure customers regarding ABC's information security and business operation continuity. Open and proactive communication with customers will help mitigate any loss or damage to customer trust and confidence in the company (Kala, 2023).

Vendors and Suppliers: Key suppliers must be advised of the incident, any disruption caused to the supply chain or payment processes, and actions in place to restart the business as usual to protect the relationship from breakdown. Motivate partners to seriously examine their own security posture and cooperate in exchanging information on how to mitigate those risks.

Regulatory bodies: Proactively inform and coordinate with relevant regulatory authorities about the incident and the potential impact on ABC's ability to meet its compliance obligations when appropriate to the nature of the business and the compliance

applicable (Borky &Bradley, 2018). This can help the company demonstrate its commitment to transparency and its efforts to address the situation.

Media and public: Develop a clear, consistent, public-facing communication strategy to address the incident and demonstrate ABC's commitment to information assurance that protects the company's reputation. This could be issuing press releases, media statements, and a page on the company's website wholly to update and assure, 2023). It should be prepared in consultation with ABC Legal and Public Relations teams so that it is in full accord with whatever legal or regulatory requirement exists, and at the same time, it effectively manages the company's public image and its relations with stakeholders.

6. Recommendations to Prevent Recurrence

The following measures can further harden ABC's information assurance posture to prevent such cyber incidents from repeating.

Policy and Governance

Develop and implement throughout the organization appropriate information security policies and comprehensive procedures that describe in detail the organization's required roles, responsibilities, and expectations from all organization employees, contractors, and third-party partners (Borky &Bradley, 2018). These areas will include, but are not limited to, acceptable use, access management, incident response, data protection, and working from home.

Develop an information security governance structure with the CISO or equivalent that would report to the executive leadership team and be responsible for the development, implementation, and continuous improvement of ABC's information assurance program

(Borky& Bradley, 2018). This governance body will ensure the alignment of the security initiatives to strategic company objectives and resource allocation and drive a culture of security across all organization departments.

Put in place a formal risk management framework, which will periodically assess, prioritize, and guide the treatment of the organization's information security risks (Borky &Bradley, 2018). The process should involve cross-functional stakeholders and consider strategic and operational risks while contributing to developing mitigation strategies and security controls.

References

Akter, S., Uddin, M. R., Sajib, S., Lee, W. J. T., Michael, K., & Hossain, M. A. (2022). Reconceptualizing cybersecurity awareness capability in the data-driven digital economy. Annals of Operations Research. https://doi.org/10.1007/s10479-022-04844-8

Borky, J. M., & Bradley, T. H. (2018). Protecting Information with Cybersecurity. Effective Model-Based Systems Engineering, pp. 345–404. NCBI. https://doi.org/10.1007/978-3-319-95669-5_10

Cremer, F., Sheehan, B., Fortmann, M., Kia, A. N., Mullins, M., Murphy, F., & Materne, S. (2022). Cyber risk and cybersecurity: A systematic review of data availability. The Geneva Papers on Risk and Insurance - Issues and Practice, 47(3). https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8853293/

Cartledge. C (2022). CS-465/565 Information Assurance Project.

Jørgensen, E. U. (2018). The stakeholder attributions of corporate crisis responsibility following a cyber attack. https://research-api.cbs.dk/ws/portalfiles/portal/59754091/427671_Elisabeth_Jorgensen_digital.pdf

Kala, E. M. (2023). The Impact of Cyber Security on Business: How to Protect Your Business. Open Journal of Safety Science and Technology, 13(02), 51–65. https://doi.org/10.4236/ojsst.2023.132003

Ursillo, S., & Arnold, C. (2023, October 23). Cybersecurity Is Critical for all Organizations – Large and Small. IFAC. https://www.ifac.org/knowledge-gateway/preparing-future-ready-professionals/discussion/cybersecurity-critical-all-organizations-large-and-small