Project: ABC Inc Ransomware Attack Analysis Report

Old Dominion University

CS465: Information Assurance

Professor Zehra

Isaiah Bagwell-Goines

Summary

Recently, ABC Inc. was affected by a ransomware attack that disrupted the company's financial and administrative operations for a total of three consecutive weeks. The breach was the result of an administrative employee who unintentionally opened a malicious Excel file attached to what seemed to be a legitimate email; however, the file contained malware known as the Zloader trojan, which was ultimately used by its malicious actors to gather login information, including passwords. Once inside the network, it gave the cybercriminals the access they needed to spread the malware further and deploy Ryuk ransomware across at least 40 systems within the infrastructure. On the bright side, the operational technology or OT environment, including the programmable logic controllers (PLCs) and other manufacturing processes, was not affected. Conversely, the consequences for the business side of ABC Inc. were significant, resulting in accounts receivable and accounts payable being inoperative, which caused the inability to bill customers or pay vendors; ultimately, this ceased business continuity. This event shows various major weaknesses in the company's IA knowledge and structure; specifically, in email phishing attempts, end user protection, and containment of cyber-attacks. This report will examine the technical and procedural issues that contributed to the breach, the risks presented to business operations, and offer future recommendations for strengthening ABC Inc.'s cybersecurity. In addition, these critiques and advice will not only help to prevent similar situations from occurring in the future but also help the company effectively address the new forthcoming threats as technology continues to evolve.

Background

Firstly, in order to better understand the effects of the recent ransomware incident, I have reviewed ABC Inc.'s infrastructure, commercial responsibilities, and strategic relationships as the company's new Chief Information Assurance Officer (CIAO). With about 1,000 workers, ABC Inc. is a small manufacturing company that uses both automated and manual processes to produce a range of goods. Meeting production targets and delivering goods to customers on schedule are both crucial to the business. From an information assurance standpoint, the operational and financial data are essential to making sure the company functions properly. Therefore, I will also be addressing the various strengths and weaknesses of the network structure in reflection of the recent cyber-attack, to which, in a future section, I will provide recommendations for improvements to mitigate similar and future attacks from occurring.

To start, the commercial responsibilities consist of manufacturing, invoicing, and supplier payments. The administrative and financial teams are tasked with billing customers, processing incoming payments, and paying vendors for the materials and services that keep production moving. Any issue or malfunction in these areas has a direct impact on inbound/outbound transactions, supplier relationships, and the ability to meet production goals. In addition, ABC's intellectual property includes its proprietary manufacturing processes, production deadlines/schedules, and client order information. While the company does not handle highly classified materials, the loss or exposure of the prior mentioned resources could give competitors an advantage or damage client trust. Moreover, ABC also maintains strategic and corporate alliances that are critical to daily operations. The company works with long-term suppliers to secure materials and rely on external shipping and logistics partners for delivery. These partnerships, along with client relationships, depend on reliable communication and coordination across the internal systems.

Concerning the network, ABC Inc. maintains two logically divided environments: the Information Technology (IT) segment and the Operational Technology (OT) segment. The IT environment handles administrative tasks such as finance, payroll, HR, and email communications, while the OT segment manages engineering workstations, manufacturing processes, and the PLCs. Both segments are connected through a custom Enterprise Resource Planning or ERP system that allows for coordination between production and business operations. While this integration improves efficiency, it also introduces potential security risks by creating routes for the spread of malware if the IT environment is compromised; luckily, regarding the recent attack, the OT area was unaffected.

Lastly, ABC's network possesses several positive aspects, such as a competent IT team and a divided network. However, these were outweighed by significant weaknesses like having no multi-factor authentication, limited endpoint monitoring, and a lack of sufficient phishing awareness training; not to mention, the backups were not fully isolated from primary systems. Although the infrastructure facilitated daily operations, it was unable to address the complexity of a modern cyber threat. Thus, this ransomware attack demonstrated how a phishing email could turn into a major disruption for the entire company and emphasized the need for a stronger and more proactive security strategy.

Consequences

The ransomware attack on ABC Inc. had immediate and severe consequences regarding business operations. For three weeks, the company's financial and administrative systems were effectively inoperative. From my perspective, the most pressing issue was the complete cessation of ABC's ability to process accounts receivable and accounts payable. Without access to these

systems, the business is unable to issue invoices to customers, collect payments, or pay our vendors. This interruption hindered cash flow and created a domino effect across multiple aspects of the business, as a result.

Operationally, the manufacturing or production areas were fortunate to remain functional because the OT segment was not directly affected. The PLCs and other factory floor systems stayed online, allowing the continuation of producing goods; however, due to the financial operations being frozen, the company could not generate new purchase orders or pay suppliers on time. This created delays in acquiring materials for the company and risked disrupting production if the situation lasted any longer (or was more severe).

Financially, the company experienced a growing accumulation of invoices that could not be processed, along with delayed payments to vendors. These delays increased the risk of late fees and negatively affected the finances of the business. Though production lines were still running, the inability to move funds in or out of the company created financial pressure and could have led to bigger problems if the outage continued. Consequently, the attack may have also damaged the company's reputation. Vendors and partners expect timely payments and clear communication, and having our financial operations offline for weeks would naturally raise concerns about our reliability.

Another consequence was the cost of recovery. The company had to employ an external cybersecurity team to lead the remediation and restore business operations. Though our in-house technical staff was experienced, leadership made the correct decision to bring in specialists to ensure a thorough cleanup and to rebuild trust in our systems. The process of removing infected

files, restoring backups, and verifying data integrity took significant time and resources, contributing to the overall business disruption.

Lastly, the incident demonstrated the inadequate degree of security awareness among employees. The employees were not sufficiently trained to identify malicious content, as reflected by the fact that the initial breach was caused by a single phishing email. From a leadership perspective, this incident not only caused operational disruptions and potentially harmed partnerships, but it also exposed information assurance weaknesses that need to be fixed quickly to avoid similar incidents in the future.

Vulnerability Assessment

Due to the circumstances, I examined ABC Inc.'s primary resources and assessed the company's ability to sustain its core operations, including providing services, customer billing, receiving payments, and making vendor payments, as part of my evaluation of the business's information assurance posture. Based on their significance to regular operations and their conformity to the fundamental information assurance principles of integrity, availability, confidentiality, and non-repudiation, I categorized these assets as critical, essential, or ancillary.

The critical assets include our Enterprise Resource Planning (ERP) system, financial systems, and employee authentication credentials. The ERP system serves as the backbone of ABC’s operations, integrating finance, supply chain, and production activities. Any compromise to its availability or integrity would directly disrupt our ability to track orders, issue invoices, and maintain production schedules (all of which are vital to operation). Similarly, the financial systems, specifically accounts receivable and accounts payable, are vital for maintaining financial assets and processing payments. The confidentiality of these systems is also a priority,

as financial data is a valuable target for attackers. Finally, employee authentication or login credentials are critical because a compromise here can give threat actors access to internal systems, allowing them to move freely and disrupt or damage essential business functions or assets.

Essential assets include email and internal communication platforms, along with the OT systems and PLCs. These assets are necessary to coordinate operations, communicate with vendors, and maintain efficient production. Even though the OT systems can continue functioning independently for short periods, they rely on ERP data to operate at full capacity.

Lastly, ancillary assets consist of shared file servers, non-essential data, and standard employee workstations. These assets support daily operations but do not directly affect primary business functions; however, they still need proper security to prevent them from becoming entry points for cyberattacks.

Therefore, ABC's ability to operate effectively relies most heavily on the availability and integrity of the ERP and financial systems, supported by secure authentication and dependable communication tools. The current infrastructure enables the company to operate under normal conditions; however, it has gaps in both prevention and containment, making ABC vulnerable to future incidents if these weaknesses are not addressed.

Threat Matrix Based on Vulnerability Assessment

		Impact				
		Negligible	Minor	Moderate	Significant	Severe
	Very Likely				Communications	Accounts Payable/Receivable

Likelihood	Likely			Employee Workstations		Login credentials
	Possible		Shared Drives/Data		Backups	ERP System
	Unlikely				OT Equipment/System	
	Very Unlikely					

Communication Plan

During a cybersecurity incident, managing communication effectively is equally important as resolving the technical issue. The situation may worsen if employees or vendors are misinformed or receive conflicting messages. The objective for ABC Inc. is to have a plan that is structured and practical for the size of the business, not something that could only be accomplished by a large corporation. With that being said, my proposed plan for the communications plan of ABC Inc. addresses internal and external recommendations as well as training procedures in preparation for possible breaches or cyber incidents.

First, the internal communication needs to focus on **s**peed, clarity, and security. Currently, employees rely on personalized email addresses for work, which creates several risks, including phishing, inconsistent messaging, and the potential for compromised home devices. This setup is exactly how the attacker reached an employee with a malicious Excel file. To address this, I recommend using a centralized, secure domain (like @abcinc.com) with multi-factor authentication, including advanced spam and phishing filters, and strict policy enforcement.

In addition, all event-related updates will come from the incident response team (IRT) and will be approved by senior leadership before going out. The use of secure and reliable channels, like an internal messaging platform and encrypted email, ensures that everyone gets messages quickly and safely. In the event that those systems are down or compromised, phone calls or text alerts (like Blackberry AtHoc) could be used as a backup. To add, this would prove useful for employees working remotely and in hybrid positions to which became more popular/common during the COVID-19 pandemic. Not to mention, the addition of pre-made message templates for scenarios such as ransomware incidents, phishing warnings, or system outages helps to ensure communication is faster, more consistent, and less confusing during a cyber event, which can significantly improve response times (NIST, 2025).

External communication must be carefully controlled to protect ABC Inc.'s reputation and prevent sensitive information from leaking. To accomplish this, the company can establish a dedicated communications account "communications@abcinc.com", for example, to handle all external messaging to which will be managed by a small communications team in coordination with senior leadership. Individuals will only receive updates through this account, and the information shared will focus on relevant topics like billing delays, system recovery progress, and any actions partners may need to take. Technical details and internal instructions should not be disclosed externally, and any public statements should first be reviewed by leadership and legal counsel to ensure accuracy. Also, in the event that employees are unable to muster on-site (or employees are working remotely), any updates from the external side could be accessed through the use of a cloud-based email platform (like MicroSoft Teams) to ensure consistent communication and business continuity. By keeping external communications separate from internal channels, ABC Inc. can provide updates that rebuild and sustain trust; also, reduce the

risk of attackers exploiting employee emails, as transparent and consistent communication during cybersecurity incidents is paramount to minimizing reputational damage (Knight & Nurse, 2020).

Finally, to test the viability of this plan, regular training exercises or simulated drills with the IRT, leadership, and the communications team will test the speed of internal alerts, the coordination of external updates, and everyone's ability to operate if primary email systems are unavailable. According to Knight and Nurse (2020), regular practice strengthens coordination, improves response times, and reduces errors during real incidents. As such, this plan will be implemented to strengthen the current lackluster network/communication system in place.

Preventing Recurrence

As the Chief Information Assurance Officer for ABC Inc., my responsibility is to make sure the organization emerges from this incident stronger and more resilient against future threats. Preventing a recurrence is indeed important and requires a combination of controls, procedural improvements, and testing/monitoring.

Since the original breach began with a malicious Excel attachment, the first step would be to implement email protections, including attachment sandboxing, link scanning, and enhanced spam filtering, to detect and block malicious content before it reaches the personnel. Employees will have to migrate to a centralized company email domain with MFA to prevent unauthorized access, especially for remote users. Also, deploying EDR (Endpoint Detection and Response) across all systems will allow for rapid detection and containment of threats, reducing the dwell time of attackers (Yusof, 2024). Moreover, the network will also be further segmented between IT and OT systems, with firewalls and access control lists to prevent malware spread.

Finally, immutable and offline backups will be maintained and regularly tested to ensure we can restore operations quickly if ransomware strikes again (#StopRansomware Guide: CISA, n.d.).

It is well known that human error remains the primary cause of cyber-related incidents. To address this, we will resort to employing mandatory cybersecurity awareness training and simulated phishing tests to improve employee training. In fact, per KnowBe4 (2025), simulated phishing tests have been shown to reduce phishing susceptibility significantly, for example, producing average reductions from 32% to under 20% within three months and continuing to improve over time. Then, the incident response plan will also be revised to incorporate offline copies, specified communication presets, and clear incident processes. Additionally, vulnerability scans and patching will be scheduled to address known flaws before they can be exploited.

Finally, security depends on preparation. I will conduct regular exercises simulating ransomware and remote work scenarios, ensuring that leadership, the IRT, and the communications team can coordinate effectively under pressure. Studies show that organizations performing regular cyber exercises respond faster and minimize both financial and reputational damage during actual incidents (Stoppel & Cornett, 2023). Plus, penetration tests and assessments could help identify weaknesses that the IT team may miss.

Thus, these efforts will align ABC Inc. with best practices recommended in the NIST Cybersecurity Framework (NIST, 2025).By implementing this combination of technical, procedural, and training measures, ABC Inc. will significantly reduce the likelihood of a repeat incident and ensure a quicker recovery if/when future threats emerge.

References

Knight, R., & Nurse, J. R. C. (2020). A Framework for effective corporate communication after cyber security incidents. Retrieved from https://www.researchgate.net/publication/344365101_A_Framework_for_Effective_Corporate_Communication_after_Cyber_Security_Incidents

National Institute of Standards and Technology. (2025). *Computer Security Incident Handling Guide* (SP 800-61 Rev. 3). NIST. https://csrc.nist.gov/publications/detail/sp/800-61/rev-3/final

Stoppel, M., & Cornett, H. (2023). *Game-On: Why tabletop exercises are key to cybersecurity resilience*. *Corporate Compliance Insights*. https://www.corporatecomplianceinsights.com/cybersecurity-tabletop-exercises/

Tampa Bay, F. (2025). KNOWBE4 report reveals security training reduces global phishing click rates by 86%. Retrieved from https://www.knowbe4.com/press/knowbe4-report-reveals-security-training-reduces-global-phishing-click-rates-by-86#:~:text=This%20highlights%20the%20critical%20role,to%20quantify%20the%20program's%20effectiveness.

Yusof, Z. B. (2024). *Effectiveness of endpoint detection and response solutions in combating modern cyber threats*. *Journal of Advances in Cybersecurity Science, Threat Intelligence, and Countermeasures*. https://polarpublications.com/index.php/JACSTIC/article/view/1