Ransomware Incident Analysis and Information Assurance Assessment

Diane Gilzow

Old Dominion University

CS 465 - Information Assurance Cybersecurity

Susan Zehra

May 4, 2026

Table of Contents

Objective

The main objective of this report is to analyze the ransomware incident that occurred within ABC Inc., its consequences, and best practices going forward to prevent incidents like this one. As the incoming CIAO, this report will include a recommended company communications plan and key steps to strengthen the organization's security posture.

Summary of the Incident

ABC Inc., a small manufacturing company, experienced a significant cybersecurity incident involving ransomware that disrupted financial and administrative operations for approximately three weeks. The incident began when an administrative support employee received an email that appeared to look legitimate and contained an Excel spreadsheet attachment. Upon opening the file, a variant of Zloader malware was executed within minutes and began harvesting user logins and passwords. Over the course of three weeks, the attacker likely used these compromised credentials to move laterally within ABC Inc.'s information technology (IT) network. This activity led to the deployment of Ryuk ransomware within the financial and administrative systems. After investigation, it was discovered that the Ryuk ransomware was found on more than 40 computers within ABC Inc.'s IT network. The operational technology (OT) network, which was composed of engineering and manufacturing systems, remained largely unaffected due to existing network segmentation.

As a result of the ransomware attack, financial and administrative systems were rendered inoperable that led to the disruption of core business functions. As a result, ABC Inc. was unable to issue invoices, receive payments, and pay vendors, which impacted its financial continuity and operational stability. In response to the incident, internal technical staff wanted to restore the

infrastructure, however upper management determined that consulting with an external cybersecurity organization will provide a more efficient recovery process. External experts were subsequently brought in to remove all compromised files from ABC Inc.'s network, computers, servers, and backups. Following remediation efforts, business operations were successfully resumed.

Organizational Background and Infrastructure Overview

ABC Inc. is a small manufacturing company employing approximately 1,000 personnel. Its core commercial responsibilities include manufacturing production, engineering design, supply chain coordination, customer billing, and financial operations such as accounts payable and payroll. ABC Inc. manages incoming payments from customers through accounts receivable and outgoing payments to vendors through accounts payable.

ABC Inc. also maintains several intellectual and operational assets that are critical to its competitive position in the manufacturing sector. These include proprietary manufacturing and engineering designs that represent core intellectual property. In addition, the organization manages sensitive financial data through its enterprise resource planning (ERP) system. This data includes accounts receivable and payable records, vendor contracts, and customer billing information. ABC Inc. also stores employee and customer personally identifiable information (PII), payroll records, and internal operational schedules that further increases the sensitivity of its data environment. These assets can be considered high-value targets to adversaries and make them more prone to being compromised in the event of a cyberattack. In addition, ABC Inc. holds strategic and corporate alliances with other organizations to meet business objectives,

primarily through vendor relationships that support manufacturing operations and supply chain activities.

The network infrastructure of ABC Inc. consists of a segmented network infrastructure to separate information technology (IT) systems from operational technology (OT) systems. The IT network supports administrative and financial operations, whereas the OT network supports engineering and manufacturing processes, including programmable logic controller (PLC)-controlled production systems. These systems are connected through a shared ERP integration layer.

There are strengths and weaknesses to consider with this network layout. A key strength to note is the logical segmentation between IT and OT networks, as this helped limit the spread of the ransomware attack into manufacturing systems. Additionally, the centralized ERP system enhances operational efficiency by enabling coordination between financial and production workflows. However, this ERP system can also serve as a high-risk convergence point between IT and OT environments if it were to be compromised. It's also important to note other weaknesses in this infrastructure, mainly pertaining to ABC Inc.'s email security and credential protection mechanisms. There were insufficient controls to prevent malicious macro execution from the Excel attachment, which allowed the initial infection to occur. In addition, the Zloader malware was able to harvest credentials and move through the IT network with limited resistance. This indicated weaknesses in endpoint protection and authentication controls.

Consequences of the Incident

This ransomware attack has led to several consequences that impacted both operational stability and the financial health of ABC Inc. One of the main consequences that impacted ABC

Inc. were disruptions to day-to-day business operations. The company's operations had to come to a halt as a result of their financial and administrative systems being shut down from the ransomware. During the three week outage, ABC Inc. was unable to issue invoices, process incoming payments, or pay vendors. This interruption directly affected the organization's ability to maintain normal financial workflows.

Not only were operations stalled, but so did the revenue of ABC Inc. With limited financial processing capability, revenue collection was delayed that caused cash flow instability across the organization. Furthermore, ABC Inc. faced the potential risk of late payment penalties and strained relationships with vendors due to missed or delayed payments. This can also extend to customers who purchase from ABC Inc., if ABC Inc. can't receive payments from their customers then it can lead to delayed order fulfillments.

Having strained relationships with both vendors and customers can ultimately lead to reputational damage and reduced trust in ABC Inc.'s reliability as a business partner. Reputational impact represents one of the most significant long-term consequences of the incident, as it may affect future commercial relationships for the company.

Vulnerability Assessment

A vulnerability assessment is the process of identifying, analyzing, and prioritizing security weaknesses in an organization's assets and functions. In the case of ABC Inc., this vulnerability assessment primarily focuses on assets that were affected by the ransomware incident and their role in maintaining business operations.

The table below breaks down ABC Inc.'s main systems and assets to show how important each one is to the business and where the main weaknesses are. It helps highlight which parts of

the company are most exposed based on how critical they are to daily operations and how easily they could be targeted.

Function/Asset	**Description**	**Criticality**	**Vulnerability**	**CIA Impact**
Daily Business Operations	Product operations	Essential	Limited monitoring of OT environment	Availability
Financial Systems	Billing and payments	Critical	High-value target, centralized access	Confidentiality, Integrity, Availability
Administrative Systems	Business operations	Critical	Excessive user privileges	Confidentiality, Integrity
Manufacturing PLC Systems	OT Network	Essential	Weak integration monitoring with IT	Availability
Accounts Receivable	Customer payment	Critical	Dependent on ERP system access	Integrity, Availability
Accounts	Vendor payment	Critical	Susceptible to	Integrity

Payable	systems		credential compromise	
ERP System	IT/OT Bridge	Critical	Single point of failure between networks	Confidentiality, Integrity, Availability
Email System	Communication vector	Essential	Phishing entry point, weak filtering	Confidentiality, Integrity
Employee Workstations	Daily operations	Essential	Malware execution via attachments	Confidentiality, Integrity
Backup Systems	Recovery capability	Critical	Potential lack of isolation (ransomware exposure)	Availability
Documentation	Non-essential records	Ancillary	Low protection priority	Confidentiality

Overall, the assessment shows that ABC Inc.'s biggest risks are concentrated in financial systems, identity-related access, and the ERP system that connects IT and OT environments. These areas are the most critical because they either directly support revenue flow or act as

central points that other systems depend on. While the manufacturing systems were mostly protected due to segmentation, their reliance on IT services still creates indirect risk that could become a problem if another attack happens.

Threat Matrix

To better understand the risks facing ABC Inc., a threat matrix was developed. A threat matrix is a way of organizing cyber threats by linking them to specific systems, their weaknesses, and the potential impact if they are exploited. This helps prioritize which risks are most important based on how likely they are and how damaging they could be.

The following threat matrix summarizes the main cyber threats relevant to ABC Inc. and how they relate to specific systems within the organization. Each threat is evaluated based on the affected asset, the underlying vulnerability, and the potential impact on business operations. Likelihood and risk ratings are included to help prioritize which issues pose the greatest concern.

Threat Event	**Asset**	**Vulnerability**	**Impact**	**Likelihood**	**Risk**
Phishing Attack	Email System	Low user awareness	High	High	High
Credential Harvesting (Zloader)	Workstations	Weak endpoint protection	High	High	High

Ransomware (Ryuk)	Financial Systems	Weak detection and monitoring	Critical	Medium	High
Unauthorized Access	ERP System	Weak authentication, excessive privileges	Critical	Medium	High
Lateral Movement through IT Network	Internal Network	Flat network structure, weak segmentation	High	High	High
Insider Threat	Administrative Systems	Excessive access rights, limited monitoring	High	Low-Medium	Medium
OT Network Compromise	Manufacturing /PLC Systems	Exposure through ERP bridge, limited monitoring	Critical	Low	Medium
Backup Compromise	Backup Systems	Lack of isolation (no	Critical	Medium	High

		air-gapped or immutable backups)			

Overall, the matrix shows that the highest-risk threats for ABC Inc. are those that involve phishing, credential theft, and ransomware, since they directly target users and provide attackers with access to critical systems. These threats are especially dangerous because they can escalate into wider network compromise through lateral movement. Though OT systems didn't show signs of impact in this incident, the connection through the ERP systems still creates a potential pathway that could be exploited if similar attacks occur in the future.

Incident Communication Plan

An effective communications plan is essential for managing information flow during a cybersecurity incident and ensuring that all stakeholders receive accurate and timely updates. In the case of ABC Inc., clear communication procedures are crucial in order to reduce confusion and maintain coordination across all departments. This helps support effective incident response and prevent additional damage.

It's important to first consider how ABC Inc. will communicate internally with employees from each department. During an active incident, internal communication must be structured and controlled to ensure that accurate information is shared without causing unnecessary confusion or panic. The first step is immediate notification to executive leadership so that the incident at hand can be addressed quickly and resources can be allocated appropriately.

Following this, updates should be communicated to department heads. For ABC Inc., this includes finance, administrative, IT, and operations, since these areas can be directly affected by system disruptions. These updates should be controlled and consistent to ensure that all departments are working with the same information. There should also be regular status briefings to track progress and communicate any new developments. This helps maintain coordination across each department. After the incident has been resolved, a formal debrief should be conducted to review what occurred, what vulnerabilities were exploited, and what could be improved.

Besides internal stakeholders, external stakeholders should also be notified if an incident occurred. External stakeholders include ABC Inc.'s business partners, vendors, and customers. External communication must be handled carefully due to potential legal and reputational impacts. It's important to be transparent as to keep trust and credibility with stakeholders, along with providing timely updates to ensure clear understanding of the situation and avoid misinformation.

Finally, it's important to assign clear roles during incidents like these. For instance, a dedicated communication lead should be assigned to ensure that all updates come from a centralized and trusted source. There should be technical teams that focus on containment and remediation, while communication teams should handle communication with external parties.

Prevention Strategy

To help ensure an incident of this scale won't happen again, several prevention strategies can be deployed within the organization. This can be achieved through a combination of technical controls, policy developments, and most importantly, user awareness. This approach

will aim to mitigate high-risk vulnerabilities and also improve overall information assurance across the organization.

A key factor that must be addressed first is human error, especially for this case as it played a major role in the initial compromise. Human error is an inherent and always present risk in any organization, and while it cannot be fully eliminated, it can be significantly reduced through regular user awareness training. Having consistent training programs that focus on recognizing phishing attempts and suspicious activity can help employees respond more effectively to potential threats before they are executed.

Email security should also be strengthened, as the initial attack vector originated from a phishing email. It is recommended that ABC Inc. implements advanced email filtering tools to detect and block malicious attachments before they reach users. Macro-enabled Office files should also be restricted by default to prevent unauthorized code execution, as what happened in this case.

There are additional controls that should be implemented to mitigate the impact of threats similar to the ransomware incident. The investigation indicated that the malware remained undetected within the network for about three weeks before the ransomware activity was triggered. This shows that there are weaknesses in threat detection and monitoring capabilities. Therefore, having stronger monitoring and detection tools, such as an intrusion detection system (IDS) and endpoint detection and response (EDR) solutions, could help identify and respond to malicious activity much earlier.

However, no amount of technical controls alone can fully eliminate the risk posed by human error, which is why continuous user awareness training and security education must remain a core part of ABC Inc.'s long-term defense strategy. Humans are often the first line of

defense, but also the most common point of failure in cybersecurity incidents. Strengthening the human element first contributes significantly to improving the overall security posture of ABC Inc. Long-term resilience against threats like ransomware ultimately stems from strengthening human awareness alongside technical defenses.

Conclusion

Ransomware continues to be an evolving threat for many organizations, and ABC Inc. is no exception. It began with a phishing email, which led to credential theft, system compromise, and the disruption of financial and administrative operations. What this case shows is that phishing remains one of the most effective entry points for attackers, mainly because it takes advantage of human error rather than breaking through technical defenses. This incident shows just how quickly a small mistake can escalate into a major operational disruption when both human and technical weaknesses are involved. While security tools and controls are important, they are not enough on their own if users are not prepared to recognize and respond to threats. Because of this, improving user awareness alongside strengthening technical defenses is key to reducing the chances of something like this happening again.

References

Guidance on effective communications in a cyber incident | National Cyber Security Centre. (2024, October 16). https://www.ncsc.gov.uk/guidance/effective-communications-in-a-cyber-incident