Information Assurance Project Report

My Nguyen

Professor Nukavarapu

CS 465- Information Assurance for Cybersecurity

April 27, 2025

Table of Contents

Introduction

The current interconnected digital environment requires Information Assurance (IA) protection at an unprecedented level, especially since manufacturing companies need successful data flows through their operational and financial systems. As the Chief Information Assurance Officer (CIAO) at ABC Inc., my responsibilities encompass protecting digital assets from integrity damage while maintaining business operation stability and guiding strategic responses against information security threats. A serious ransomware event caused by Zloader malware started when our IT resources fell victim to a phishing attack that led to the encryption of more than 40 internal systems and interrupted vital financial operations. The incident exposed major weaknesses throughout our information infrastructure, yet left the Operational Technology (OT) segment unharmed because of established segmentation measures. This report aims to deliver an in-depth investigation of the breach incident, demonstrate its effects on operations, and explain which security weaknesses were targeted alongside risk assessments while developing strong security policies to stop this from recurring (Blyth & Kovacich, 2006). Therefore, we aim to strengthen ABC Inc.'s defense capabilities, ensure operational reliability, and protect our company's reputation.

Incident Summary

The ABC Inc. experienced a cybersecurity incident after an administrative staff member mistakenly opened a phishing email that contained harmful Excel attachment software. Due to embedded macros, the malicious document downloaded Zloader malware, which functions as a trojan that stealthily gains remote system access. As soon as Zloader gained access to the company's internal network through a four-minute intrusion, the cyber criminals obtained enhanced privileges, enabling them to search and eventually control more systems. The malware

displayed suspicious patterns initially, but security systems failed to detect it for 21 days. The attacker used this time to move through the network segment before starting Ryuk ransomware. Ryuk encryption encrypted more than 40 internal computers through financial and administrative departments, which caused essential files to become inaccessible while halting all operational activities.

Core business operations at ABC Inc.'s IT segment faced complete stoppage because of the attack that disrupted the payroll systems, procurement, and invoicing capabilities. The separate management approach of Operational Technology (OT) environments secured vital manufacturing processes from the attack effects. When IT staff members discovered the total scope of the data breach, they started initial containment procedures and swiftly understood their requirement for outside security expertise (Stewart, 2023). The organization brought in a security firm from outside the company to take charge of incident response and recovery activities. Specialized experts performed investigative forensic work to remove malware from decrypted locked systems, bringing systems back online without causing noticeable data loss.

Organizational Background

The workforce of ABC Inc comprises 1,000 employees spread through financial, administrative, and production departments of the mid-sized manufacturing organization. ABC Inc. works in a competitive demand within the industrial sector as a company that designs and manufactures precise components primarily for commercial defense uses. Commercial responsibilities include meeting stringent client specifications for quality and delivery deadline, ensuring the business maintains compliance with industry standards (Such as ISO 9001, ITAR), and achieving cost-effective production to remain competitive (Hüsch et al., 2024). Long-term

contracts with key clients depend on ABC's revenue, and ABC has to sustain operations and vendor relationships with strong supply chain coordination, timely invoicing, and accurate financial reporting.

ABC's operations are fragmented into two technological areas, Information Technology (IT) and Operational Technology (OT). IT infrastructure is placed around servers, cloud applications, enterprise software, manages the financial systems, administrative coordination, procurement, and Business Analytics. OT segment governs the real-time manufacturing process, which comprises programmable logic controllers (PLC), supervisory control and data acquisition (SCADA) systems, and IoT-enabled machinery (Stewart, 2023). The motivating force behind these segments is that a sophisticated Enterprise Resource Planning (ERP) system integrates them, centralizing data to coordinate production schedules with inventory, procurement, and financial workflow

ABC has a large volume of intellectual property (IP), which includes proprietary manufacturing techniques, patented component designs, and sensitive customer data, such as defense contract specifications. This IP is stored in ERP databases and secure file servers, which are only accessible to authorized people. The company's strategic alliances include partnering with tier dry stock suppliers, logistics providers to distribute globally, and with defense contractors for strict secrecy.

Though these strengths remain, ABC's network infrastructure has significant shortcomings. While efficient, integrating the ERP makes the systems reliant on a single point of failure because it relies on data pathways between IT and OT systems. Recently, critical vulnerabilities were exposed after a phishing attack set free malware that spread through departments, bypassing old email filtering. There is no training on cybersecurity for employees

from a company's perspective, and it mainly consists of annual compliance sessions, which put the staff at a disadvantage of being unable to detect social engineering tactics (Stewart, 2023). Furthermore, the lack of endpoint protection on OT devices puts additional risk of production disruptions.

Consequences of the Incident

The ransomware attack generated substantial operational interruptions and financial losses for ABC Inc. as it held essential business operations at a standstill for approximately three weeks. The company's operations faced significant interruption because hackers attacked over 40 IT systems, blocking processing receivables and payables and stopping cash flow. Operating activities at ABC Inc. were interrupted by a dual disruption that included the suspension of invoicing, together with payment delays to vendors and reduced order fulfillment for customers. Moreover, the financial impact from this cybersecurity breach includes $600,000 from unprocessed billings and $300,000 for implementing third-party cyber protection measures and restoring systems and recovering data.

The attack triggered a lengthy financial impact, causing operational hitches, devastating ABC Inc's reputation, and human capital damage. The company's crucial vendors and established customers voiced concern over service delays and their skepticism about how well this company protects critical business information. Because of these events, trust breakdowns could lead to potential risks for future renewals and new business opportunities at ABC Inc. Intelligence suggests intellectual property theft could occur since ransomware operators had unauthorized access to internal systems for three weeks, potentially exposing proprietary designs and customer specifications (Bakar et al., 2023). Moreover, employee morale and productivity

levels suffered because of the impact of the internal incident (Hüsch et al., 2024). Members of the IT department became victims of information overload from the massive breach as they worked impossibly long hours in a demanding environment.

Vulnerability Assessment

A detailed vulnerability assessment of the digital ecosystem of ABC Inc. is performed, and it reveals massive critical and essential weaknesses of the vital and core pillars of Information Assurance (IA). The financial and ERP systems, central in billing and accounts payable, and integration between IT and OT operations, are categorized among IT assets as *critical*. With cash flow on hold for three weeks, the breach showed what could happen when they are unavailable. Another *vital* asset, apart from the database, was user credentials, which were compromised during the first infection by injecting Zloader and, in turn, compromising the integrity and confidentiality of the system. Since the email system acted as the attack vector, it should also be identified as *critical,* as it is the main communication channel and control gate to sensitive data. Internal messaging systems are essential, but by comparison, they are *ancillary* and do not directly affect operational continuity.

Programmable logic controllers (PLCs) and manufacturing design documents are declared as *essential* on the OT side. These assets are unaffected by the attack but will be a future target as they have value to be used to enforce production integrity and proprietary operations (Wang et al., 2023). In addition, external vendor portals are *vital* to help maintain supply chain fluidity and external trust during invoice transmission, shipment notices, and technical documentation through external vendors. Public-facing assets like marketing websites and non-

sensitive storage are considered *ancillary* because, although compromised, the compromised entity could still erode public confidence and create vectors for social engineering.

However, vulnerabilities appear in multiple domains during the incident when viewed through IA principles. The compromise of *integrity* occurred with the gain of unauthorized access to sensitive files, which brings to mind the possibility of undetected data manipulation. *Availability* had been breached, as ransomware encryption prevented everyday use of the organization's financial systems, vendor communication tools, and administrative functions. *Confidentiality* was potentially breached by the harvested user credentials and the exposure of sensitive business data such as intellectual property and client information. In addition, *nonrepudiation* was weakened since undocumented changes into systems or records could have taken place with no auditable trail under the guise of unauthorized access (Butun et al., 2019). These vulnerabilities multiply further with remote work, especially when employees access systems from home without enforced VPN protocols and are connected via unprotected home networks.

Threat Matrix and Risk Assessment

A thorough threat matrix is needed to prioritize cybersecurity threats throughout ABC Inc.'s digital environment so that mitigation efforts align with the vulnerabilities found in the assessment. Risk is defined as a function of probability × impact, with probability reflecting the likelihood that a threat may exploit a vulnerability and impact being the likely damage to valuable and necessary assets based on the fundamental pillars of Information Assurance (IA): confidentiality, integrity, availability, and non-repudiation (Piet et al., 2021). The exposures highlight systemic vulnerabilities of key systems and assets (financial, ERP, email, and user

credentials) and key assets (PLCs, manufacturing drawings, and vendor sites), feeding the threat matrix below.

Table 1

The following matrix outlines key threats:

Threat	**Assert**	**Likelihood**	**Impact**	**Risk Level**
Phishing Emails	Email System	High	High	High
Ransomware	ERP System	Medium	High	High
Credential Theft	User Accounts	High	Medium	Medium
Insider Threats	Financial Data	Low	High	Medium
Zero-day Vulnerabilities	OT Systems	Low	High	Medium

Note: The Threat Matrix classifies critical cyber threats according to asset types while assessing their potential impact, likelihood of occurrence, and eventual risk rankings.

Application of the Threat Matrix

The threat matrix uses the output from the vulnerability assessment to rank risks and guide risk mitigation work. Each threat is analyzed below regarding affected, vulnerable, and impact on IA to have a structured and actionable risk management approach.

Phishing Emails (High Risk)

The threat posed by phishing emails to ABC Inc's email system is excellent, as the spam filtering was deficient. The users were unaware of it, leading to Zloader being introduced and

then Ryuk ransomware gaining entrance. This weakness directly affected confidentiality through credential harvesting, integrity through the authority of malware to alter system behavior, and availability through downstream ransomware effects, shutting down operations (Wang et al., 2023). The immediate remedial measures to contain this high-risk threat include deploying next-generation email filtering with AI-based anomaly detection, enforcing mandatory phishing awareness training, and enforcing mandatory two-factor authentication (MFA) to safeguard credentials.

Ransomware (High Risk)

The ransomware is a significant threat to ABC Inc.'s ERP and finance systems in that malware spreading across unsegmented networks leads to over three weeks of inability to perform systems. The attack severely affected availability due to the unavailability of essential systems, caused concerns on confidentiality through possible data exfiltration, and undermined integrity through possible stealthy tampering (Stewart, 2023).

Credential Theft (Medium Risk)

For ABC Inc., credential theft is a big deal, caused by disruptive password policies where they also have no Multi Factor Authentication (MFA), and this was used to steal credentials to expand the scope of the Zloader-Ryuk attack. The attackers were able to work remotely from insecure networks. This threat exposed sensitive data, weakened the system's integrity (potential for unauthorized system changes), and compromised confidentiality (Stewart, 2023).

Insider Threats (Medium Risk)

This medium risk to ABC Inc.’s financial data and ERP systems stems from insider threats (both malicious and negligent) that could potentially gain access to sensitive assets with

user behavior analytics and robust access controls. Such incidents compromise confidentiality by being vulnerable to data leaks, integrity by manipulating records, and non-repudiation through untraceable changes (Wang et al., 2023).

Zero-day Vulnerabilities (Medium Risk)

ABC Inc.'s operational technology (OT) infrastructure is at medium risk against zero-day vulnerabilities to its programmable logic controllers (PLCs) and production designs because the absence of active patch management and intrusion detection makes the systems prone to advanced persistent threats (APTs). These vulnerabilities can also impact availability through production disruption, confidentiality exposure of confidential proprietary designs, and integrity from manipulated PLC logic, in case it is exploited (Bakar et al., 2023).

Risk Management Process

ABC Inc. risk management is founded on responding to and detecting cybersecurity breaches based on their potential, with resources proportionate to protecting primary and significant assets. Emergency measures must be taken regarding severe threats like ransomware and phishing. They do this through technical controls like email gateways and endpoint detection tools and software, with the presence of non-technical employee knowledge and policy control procedures, reducing the risk probability and its impact. Continuous monitoring, strong access controls, and proactive defenses for vulnerabilities over time are important approaches to address medium risk threats such as credential theft, insider threats, and zero-day vulnerabilities (Stewart, 2023). The threat matrix should be updated regularly to reflect new vulnerabilities, attack trends, and organizational changes.

Internal and External Company Communications Plan

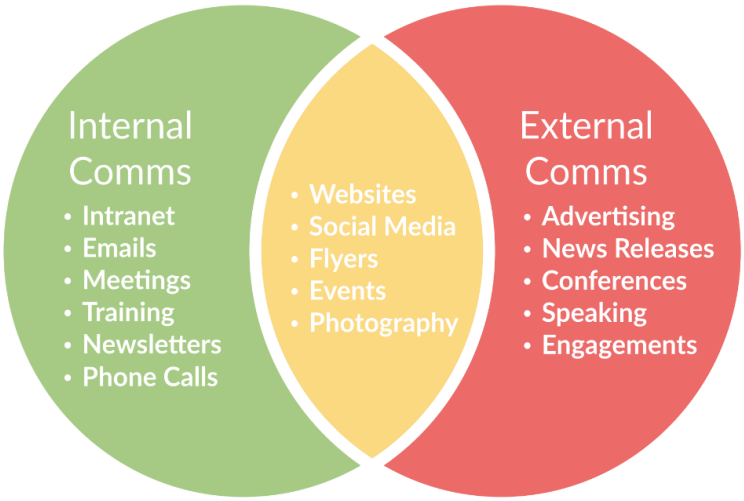
As a reaction to the recent cyberattack that began with a phishing email presenting Zloader malware and culminating in a Ryuk ransomware infection, ABC Inc. will have a focused internal communication strategy to manage the incident efficiently and minimize disruption. When it is detected, the Security Operations Center (SOC) will alert the Incident Response Team and management within 15 minutes with detailed information about the attack vector, affected systems, such as the ERP system and email infrastructure, and estimated business impact. Moreover, department-level briefings to Finance, IT, and HR will subsequently occur within the hour through internal, secure communication mediums, with personalized containment orders and short-term operational procedures, such as quarantining infected workstations or turning off specific services (Chen, 2020). A company-wide encrypted message, issued within six hours of verification, will furnish all staff members with details of the nature of the breach, how to act safely, and safe channels of reporting incidents. Furthermore, remote employees will receive tailored instructions via VPN-encrypted messaging and updated secure access protocols to limit further exposure.

Externally, ABC Inc. will implement a managed communication strategy focusing on transparency, legality, and reputation management. Primary vendors, customers, and important partners will receive encrypted, tailor-made notice within 24 hours, describing the affected systems, containment activities taken, and anticipated service disruption. Affected customers will be directed to a distinct online resource center with real-time notice and support contacts. Regulatory-compliant breach notices will be issued to authorities within 72 hours. A cross-functional crisis communications team will manage all public messaging, issuing a controlled press statement acknowledging the breach and highlighting the company's swift and effective

response, without revealing technical details that would assist further attacks (Chen, 2020). After all investigations, a senior-level summary report will be presented to stakeholders, reiterating ABC Inc.'s ongoing dedication to security development.

Image 1

External and Internal Company Communications Plan



Note: The Venn diagram establishes the boundaries between internal organizational communications and external interactions and demonstrates their areas of everyday use.

Prevention and Future Mitigation Strategies

ABC Inc. will have a multi-layered technical and policy-driven prevention mechanism to avoid repeating the same information assurance (IA) incident. Technically, the company will install next-generation email security appliances with AI-powered threat detection and sandboxing to identify phishing attacks and malicious attachments before user engagement. Endpoint Detection and Response (EDR) tools will be rolled out enterprise-wide to identify and

segregate suspicious activity in real-time (Butun et al., 2019). ABC Inc. will finalize the transition to a Zero Trust Architecture, continuously verifying user and device identity and persistent least-privilege access restrictions. Network segmentation will be in place to restrict lateral movement of threats, supplemented by regularly updated firewall policies and intrusion prevention features. Moreover, multi-factor authentication (MFA) will be mandatory for all systems handling sensitive data and remote and on-premises entry points.

On the human and policy front, ABC Inc. will enable IA through mandatory quarterly training on emergent cyber threats, phishing exercises, and engaging gamified modules, building employee vigilance and response capacity. An inclusive, policy-driven incident response process will be written down and rehearsed company-wide, outlining explicitly escalation chains, containment steps, and documentation requirements. Tight password control will be enforced using technical controls requiring complex, routinely rotated credentials and centralized credential management. (Stewart, 2023). Furthermore, hybrid workers will have a strict bring-your-own-device (BYOD) compliance regime, full device scrutiny, pre-loaded security software, and required VPN usage with end-to-end encryption (Butun et al., 2019). The Information Assurance Compliance Unit will conduct quarterly policy audits and third-party penetration testing every two years to locate and correct system vulnerabilities.

Conclusion

The ABC Inc. incident represents a classic example whereby the employment of strong Information Assurance (IA) controls to protect the company assets is paramount in allowing business functionality. Most disclosed security vulnerabilities relate to email security, user authentication, and policy-based Remote Access. At this time in the threat landscape,

organizations need much more than reactionary security measures to deal with the risk--they must have layered defenses across technical components, policy implementations, and human factor mitigation activities. The restoration of CIAO security controls across the various ABC Inc systems allows the company to establish itself as a strong, security-conscious one. Thus, by ensuring its security commitment, ABC Inc gains the confidence of all the stakeholders, and finally, operational success is its aim with the data protection initiatives.

References

Amini, M., & Abukari, A. M. (2020). ERP systems architecture for the modern age: A review of the state of the art technologies. *Journal of Applied Intelligent Systems and Information Sciences*, *1*(2), 70-90. https://journal.research.fanap.com/article_111141_81996cb945e1fb3f8c0276afca721c30.pdf

Bakar, D. A., Yahya, M. H. H., & Rahim, N. A. (2023). A Review Analysis of Earnings Management Report Disclosure. *Journal of Governance and Integrity*, *6*(1), 462-469. https://journal.ump.edu.my/jgi/article/download/9106/2775

Blyth, A., & Kovacich, G. (2006). Information Assurance, Security in the Information Environment, Springer-Verlag Ltd, London.

Butun, I., Österberg, P., & Song, H. (2019). Security of the Internet of Things: Vulnerabilities, attacks, and countermeasures. *IEEE Communications Surveys & Tutorials*, *22*(1), 616-644. https://arxiv.org/pdf/1910.13312

Chen, R. (2020). The stakeholder-communication continuum: An alternate approach to internal and external communications. *Journal of Professional Communication*, *6*(1), 7–33. https://mulpress.mcmaster.ca/jpc/article/view/4350/3658

Hüsch, P., Mott, G., MacColl, J., Nurse, J. R., Sullivan, J., Turner, S., & Pattnaik, N. (2024). 'Your Data is Stolen and Encrypted': The Ransomware Victim Experience. *RUSI Occasional Paper*. https://kar.kent.ac.uk/106978/1/RUSI-Kent-OP2024-ransomware-harms.pdf

Piet, G. J., Tamis, J. E., Volwater, J., de Vries, P., van der Wal, J. T., & Jongbloed, R. H. (2021). A roadmap towards quantitative cumulative impact assessments: every step of the way. *Science of The Total Environment*, *784*, 146847. https://www.sciencedirect.com/science/article/pii/S0048969721019173

Stewart, H. (2023). *Strengthening Cybersecurity in Digital Transformation* (Doctoral dissertation, Flinders University, College of Science and Engineering). https://flex.flinders.edu.au/file/56e99da5-1754-45e0-8cb2-d8e2b5f843c5/1/StewartThesis2023_MasterCopy.pdf

Wang, Z., Zhang, Y., Chen, Y., Liu, H., Wang, B., & Wang, C. (2023). A survey on programmable logic controller vulnerabilities, attacks, detections, and forensics. *Processes*, *11*(3), 918. https://www.mdpi.com/2227-9717/11/3/918/pdf