

Troy Bannister

CS465

Prof. Susan Zehra

15 AUG 26

CS-465 Information Assurance Project

Table of Contents

List of Figures	2
List of Tables	2
1.Introduction.....	3
2.Summary of Incident.....	3
3.Background.....	4
4.Consequences.....	6
5.Vulnerability Assessment	7
6.Threat Matrix	9
7.Communications Plan	11
8.Recommendations and Preventive Actions	13
8.1 Establish Centralized Management.....	13
8.2 Assess Risks and Needs	15
8.3 Implement Policies and Controls	15
8.4 Remote/Work from Home Security	16
8.5 Awareness Culture	16
8.6 Monitor and Evaluate Effectiveness	16
References.....	18

List of Figures

1. The IA risk management process, adapted for ABC’s incident.....	9
2. ABC, Inc. proposed information assurance reporting structure	14

List of Tables

1. ABC, Inc. asset vulnerability assessment	8
2. Threat Matrix: Zloader/Ryuk Compromise	10
3. Recommendations Mapped to Findings and Area of Responsibility.....	17

1. Introduction

I am submitting this report as the newly appointed Chief Information Assurance Officer (CIAO), for ABC, Inc. addressing the ransomware incident that recently disrupted the company's billing and accounts functions for three weeks. Information Assurance is about keeping the right information available and with integrity and keeping it within the reach of the people who have the authorization to use it (Blyth & Kovacich, 2006, p.2). With that standard to judge against, this incident is a clear signal that ABC did not yet have an information assurance program that was able to meet it.

This report is organized around the questions I was asked to answer in taking on this role: what happened, the background conditions that allowed it to happen, the consequences to the business, a vulnerability assessment of ABC's critical assets, a threat matrix built from that assessment, a communications plan for keeping employees, customers, and vendors informed during an incident, and the organizational and technical changes, which will include a new IA reporting structure, that I recommend to lower the risk for this to happen again.

2. Summary of the Incident

On or about June 15, 2026, an employee of ABC's accounts-payable group received an email that appeared to come from a known vendor, carrying an Excel spreadsheet attachment. The employee opened the attachment as part of routine invoice processing. Within four minutes, a variant of the **Zloader** malware family activated on that workstation and began harvesting stored credentials and any other login information reachable from the machine.

Over the course of three weeks, the compromise spread through ABC's IT segment, which handles ABC's financial and administrative systems, without being detected. This extended dwell time reflects the absence of any dedicated monitoring or incident-detection

function within ABC's IT organization; day-to-day system administration staff had neither the tools nor the mandate to look for this kind of activity. At the end of that window, ransomware encrypted files and issued a ransom demand, and Ryuk-related files were identified on more than 40 IT-segment computers. ABC's billing and accounts-payable functions were effectively frozen, and the company could not send invoices to customers or pay vendors for that timeframe.

The manufacturing and engineering systems to include the programmable logic controllers (PLCs) were not affected. Those systems were separate from the IT network and that separation functioned as an incidental, but effective containment boundary.

ABC's IT staff wanted to attempt recovery internally, but executive management chose to bring in an outside cybersecurity incident response firm, judging that external expertise would restore operations faster and more thoroughly than an internal effort alone. That firm worked with ABC's staff to identify and remove suspicious or compromised files from affected computers, servers, and backups, which included files associated with Zloader and Ryuk. Full business operations resumed after the three-week disruption. With this timeline in mind, it forms a solid basis for a vulnerability assessment, threat matrix, and recommendations that follow.

3. Background

Commercial Responsibilities. ABC, Inc. manufactures precision connectors and custom wiring harness assemblies for military communications and avionics systems, employing approximately 1,000 people. ABC operates as a Tier 2/3 subcontractor to a defense prime contractor, producing components under a Department of Defense (DoD) contract. Its revenue depends on the same billing and collections cycle as any manufacturer, plus contract performance obligations tied to delivery schedules that the primary contract owner relies on to

meet its own DoD requirements. This means a whole domino effect of consequences accross an important supply chain if ABC has an outage.

Intellectual Property. ABC's IP centers on connector and harness design specifications, system diagrams, and comms-system interface schematics developed for this contract. Given the DoD program this work supports, ABC's subcontract with the contract's primary company includes some baseline security expectations for handling this data that are part of our contract and most likely fall under some regulations that can be addressed by ABC's legal staff.

Corporate Partnerships. Beyond its raw-material suppliers, ABC's most important relationship is with the defense contract's prime it subcontracts to on a DoD program of record. Some of the equipment ABC uses to test and calibrate its connector and harness assemblies is Government Furnished Equipment (GFE) to meet the Quality Assurance standards while the rest of ABC's production and IT equipment is contractor-owned and contractor-maintained. That distinction matters operationally: GFE carries its own accountability chain back to the government program office, separate from how ABC manages the equipment it owns outright.

Network Infrastructure: Strengths/Weaknesses. ABC's network remains separated into an IT side that covers administrative, financial, email and engineering design and an Operational Technology (OT) side that covers the product assembly, monitoring and testing equipment. The segmentation is the clearest strength and is the reason production was not interrupted with the 40 IT-side assets being compromised. Blyth and Kovacich (2006, p.28) define a vulnerability along with International Organization for Standardization (ISO 13335), as a weakness of an asset that can be exploited by a threat, and by that definition, ABC's IT segment had quite a few. It had no dedicated IA or security governance function or formal awareness program, no email or attachment filtering to stop a spreadsheet-delivered payload, and

no monitoring or detections set up to catch credential-harvesting activity before being escalated.

While the manufacturing portion of our engineering was protected on the OT side, the engineering design data itself was not and put important contract-specific data at risk.

4. Consequences

The most immediate consequence was operational: for three weeks, ABC could not invoice customers or pay vendors through normal channels, since the systems supporting both processes sat within the compromised IT segment. That gap put real strain on cash flow due to the down time of payment collections, which in turn, delayed paying our vendors. ABC did not pay the ransom; executive management and the incident response firm chose to rebuild the systems that were compromised and restore them from backups instead. While that prevented ABC from funding the attackers, it forced them to pay the full cost of remediation out of pocket, which was the incident response firm's fees, rebuilding or reimaging 40 assets, and the unplanned overtime for IT staff. There was not a policy or any indication that ABC had a cyber insurance policy in place to cover the ransom anyway.

Beyond the general possibility of a data-breach notification obligation, ABC's status as a subcontractor on a DoD program of record raises the stakes of this incident in ways a purely commercial manufacturer wouldn't face. Because some of ABC's test and calibration equipment is Government Furnished Equipment, any incident reaching systems connected to that equipment likely triggers a duty to notify the program office's contracting officer representative, who would have their own interest in confirming their provided equipment was not compromised as well. There are also some security expectations that need to be addressed with how the engineering design data for a defense contract should be handled and coordinating with the contracting

representatives on whether ABC met those expectations will need to be worked out for future storage of that data.

The incident also carries reputational consequences. ABC's customers depend on its components for their own production and delivery schedules; even a temporary slowdown risks being read as a reliability problem, not just a one-time incident. That risk runs up the supply chain to the primary contractor and their reputation with the DoD is reliant on ABC's performance and security capabilities.

Finally, the incident is a consequence in itself of a major gap in the background section, which is ABC's ability to detect and respond quickly to this kind of breach did not exist before this happened, and three weeks of undetected movement within its network is the plain and simple, measurable cost of that gap.

5. Vulnerability Assessment

The purpose of this assessment is to evaluate ABC's assets against its ability to perform services, charge for services, receive payment for services, and pay for services. Then, to label each of the assets as critical, essential, or ancillary to that ability. Following Blyth and Kovacich's (2006, p.6) model of the relationship between assets, vulnerabilities, threats and risk, each asset in **Table 1** is scored against the four dimensions IA is meant to assure: confidentiality, integrity, availability, and non-repudiation.

Table 1*ABC, Inc. Asset Vulnerability Assessment*

Asset	Business Function	Importance	Confidentiality	Integrity	Availability	Non-Repudiation
Identity & credential directory services	Underlies all four functions	Critical	High	High	High	Moderate
ERP / Financial & Billing system	Charge, receive payment, pay	Critical	High	High	High	Moderate
IT Backup systems	Recovery of all IT assets	Critical	Moderate	High	High	Low
IT/OT network segmentation systems	Perform services (protects production)	Critical	N/A	High	Moderate	N/A
OT network / PLC-controlled harness assembly & test equipment	Perform services	Critical	Moderate	Moderate	Moderate	Low
Engineering design data (connector/harness specs, pin configurations)	Perform services (contract deliverable)	Critical	High	Moderate	Low	Moderate
Email & collaboration system	Supports charge/receive/pay workflows	Essential	High	High	Moderate	Moderate
IT-segment endpoint workstations	Charge, receive payment, pay	Essential	High	High	Moderate	Low
Vendor/supplier banking & payment records	Pay for services	Essential	High	Moderate	Moderate	High
Customer contact / order records	Charge for services	Essential	Moderate	Low	Low	Low
Physical facility access control systems	Indirect support, all functions	Ancillary	Low	Low	Low	Low

Note. Confidentiality, integrity, availability, and non-repudiation dimensions follow Blyth and Kovacich (2006); criticality labels (critical/essential/ancillary) follow the framework specified in the assignment.

A few of these need to be addressed specifically. The identity and credential directory service is rated critical across the entire assessment because it was the actual point of failure in this incident. Zloader began harvesting credentials within four minutes, which gave the attacker a foothold that was then free to move laterally for three weeks, which points to a lack of least-privilege enforcement and account segmentation, not just a phishing problem. The ERP system is critical for the same structural reason discussed in the Background section being the one system with reach into both the IT and OT segments. Backups are rated high risk on integrity and

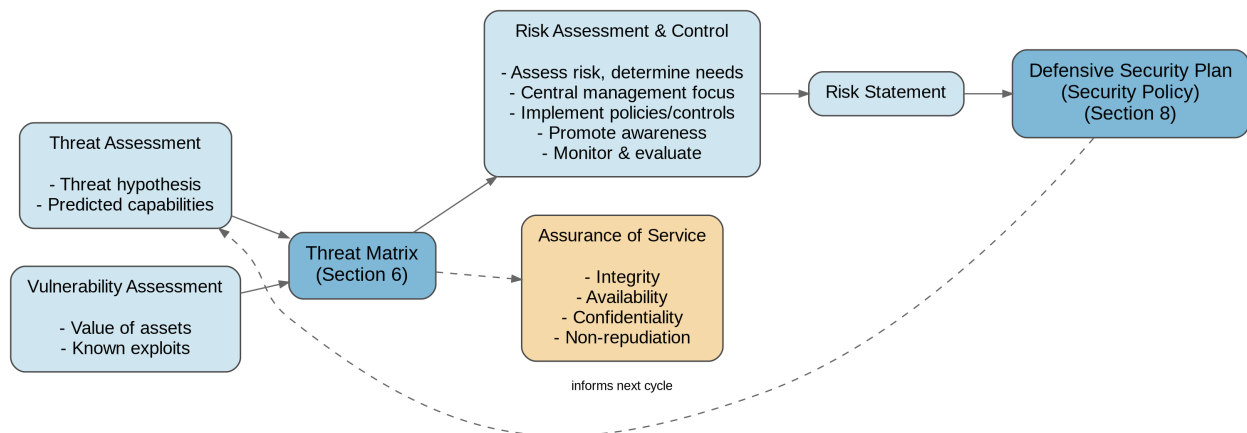
availability because incident responders found it necessary to clean suspicious or compromised files from the backups themselves, which means ABC cannot fully trust that its recovery point was clean without that verification step.

Engineering design data is rated critical specifically because it now carries a dimension beyond its ordinary business value: it was developed for a DoD program, sits on the same IT-segment systems that were compromised for three weeks, and its confidentiality is plausibly a contractual obligation to ABC's defense-prime customer, not just a competitive concern. The IT/OT segmentation boundary is rated critical despite functioning correctly during this incident because that boundary was maintained for operational convenience instead of documented and audited as a formal security control.

6. Threat Matrix

Figure 1

The IA Risk Management Process Applied to ABC, Inc.'s Incident



Note. Adapted from *Information Assurance: Security in the Information Environment* (p. 45), by A. Blyth and G. L. Kovacich, 2006, Springer-Verlag London. Copyright 2006 by Springer-Verlag London. Section labels ("Section 6" and "Section 8") were added to the Threat Matrix and Defensive Security Plan boxes to show where this report's sections fit into the original cycle.

Figure 1 shows the risk management process that this section applies which is that threat assessment and vulnerability assessment together produce the threat matrix, which then drives risk assessment, a risk statement, and at the end of the day, a security plan which will be in Section 8 (Blyth & Kovacich, 2006, p.45). **Table 2** is that threat matrix, built following Blyth and Kovacich's (2006, p. 46) threat matrix format. Threat and capability are set against vulnerability and asset. Then, the compromise is analyzed from the perspectives of performance, cost and decision-making.

The realized threat involved Zloader credential harvesting followed by ransomware activity associated with Ryuk. The compromise was opportunistic instead of targeted and it depends on a user opening a malicious attachment, then exploits whatever access and lateral movement the compromised network permits.

Table 2
Threat Matrix: Zloader/Ryuk Compromise

Asset	Threat & Capability	Vulnerability Exploited	Nature of Compromise
Identity & credential directory services.	Primary threat (Zloader/Ryuk compromise)	No least-privilege or account segmentation; one harvested credential set enabled broad lateral movement	Performance: Single credential enabled broad IT reach. Cost: Full credential reset/access audit. Decision-making: Treat all IT credentials as untrusted, slowing recovery.
Email & collaboration system	Primary threat (Zloader/Ryuk compromise)	No attachment filtering or sandboxing capable of catching a malicious spreadsheet	Performance: Malicious spreadsheet was the initial entry point. Cost: Cheap control gap relative to the damage enabled. Decision-making: Fastest control gap to fix.
ERP / financial & billing system	Primary threat (Zloader/Ryuk compromise)	Single system bridging IT and OT segments, with no compensating monitoring	Performance: Billing, payables, and payroll halted for three weeks. Cost: Delayed transactions plus remediation. Decision-making: Ransom-versus-rebuild decision without an incident response plan.
IT-segment backups	Primary threat (Zloader/Ryuk compromise)	Backups reachable from the compromised network; not verified as isolated or immutable	Performance: Recovery required cleaning/verification. Cost: Extended incident response. Decision-making: Uncertain clean recovery point complicated the rebuild.

Asset	Threat & Capability	Vulnerability Exploited	Nature of Compromise
Engineering design data (connector/harness specs, pin configurations)	Primary threat (Zloader/Ryuk compromise)	Resides on IT-segment engineering workstations/file shares, subject to the same access-control and monitoring gaps as other IT-segment assets	Performance: Reachable across 40+ compromised hosts; exfiltration unconfirmed. Cost: Targeted forensics required. Decision-making: Legal/contracts must determine defense prime or program office notification.
OT network / PLC-controlled harness assembly & test equipment	Forward-looking: an OT-aware threat actor (not the compromise in this incident)	IT/OT segmentation maintained for operational, not security, reasons. It was not independently audited or monitored.	Performance: Could halt production, with safety/program-delivery effects. Cost: Potentially greater than this incident. Decision-making: No OT-specific response plan or playbook.

Note. Cell structure (threat and capability set against vulnerability and asset, analyzed by performance, cost, and decision-making perspectives) follows Blyth and Kovacich (2006, p. 46).

The last row is meant to be a hypothetical threat scenario and is not a record of what happened, but it is important to point out like in Section 5, the segmentation boundary between OT and IT segments was not done from a security standpoint.

7. Communications Plan

This incident isn't just about ABC's ability to implement technical controls. It's also about trust moving forward. McKnight et al.'s (2002) institution-based trust model, shows us that trust in a relationship depends on "structural assurance", meaning there are safeguards and procedures in place, and "situational normality", meaning things are going as planned. Both point to the same conclusion for ABC, which is that silence or a minimal, defensive statement would do more damage than directly explaining what happened and what has changed.

Internal Communications.

Detection: Once IT staff or the CIAO's office confirms an incident is underway, the CIAO notifies the CEO immediately, with the CFO looped in given the direct impact on financial systems. The CEO briefs the Board within 24 hours. This chain did not formally exist before this incident; establishing it is itself one of the changes described in Section 8.

Employees: All employees receive a same-day notice from the CEO's office confirming that ABC experienced a cybersecurity incident affecting IT systems, that engineering and manufacturing operations are unaffected and continuing normally, and that a dedicated point of contact (the CIAO's office) is available for questions.

Ongoing Updates: Employees in affected functions (billing, accounts payable, payroll processing) receive interim manual procedures and a realistic timeline for restoration, updated weekly for the duration of the incident.

External Communications

Customers: ABC's customers depend on its components for their own production schedules, which makes prompt, specific notification more valuable than a delayed, vague one. Affected customers should be told what happened in plain terms, given a revised timeline for any delayed orders or invoicing and told clearly that the manufacturing and engineering systems producing their components were not compromised.

Primary Contractor: Given ABC's role as a subcontractor on a DoD program of record, and the potential involvement of Government Furnished Equipment, ABC's legal and contracts staff should determine promptly whether the primary contractor or the program office's contracting officer representative needs to be notified, separate from the customer and vendor communications below. This determination should not wait for the rest of the recovery to complete, since government notification expectations tend to move faster than commercial ones.

Vendors/Suppliers: Key suppliers whose payments were delayed should be contacted proactively, before they have to ask, with a specific revised payment timeline and a named point of contact in accounts payable.

Regulatory: If ABC's legal counsel determines that employee or vendor financial data was exposed in a way that triggers state breach-notification law, formal notification letters go out to affected individuals within the applicable statutory window, coordinated through outside counsel given ABC's current lack of an in-house legal/compliance function.

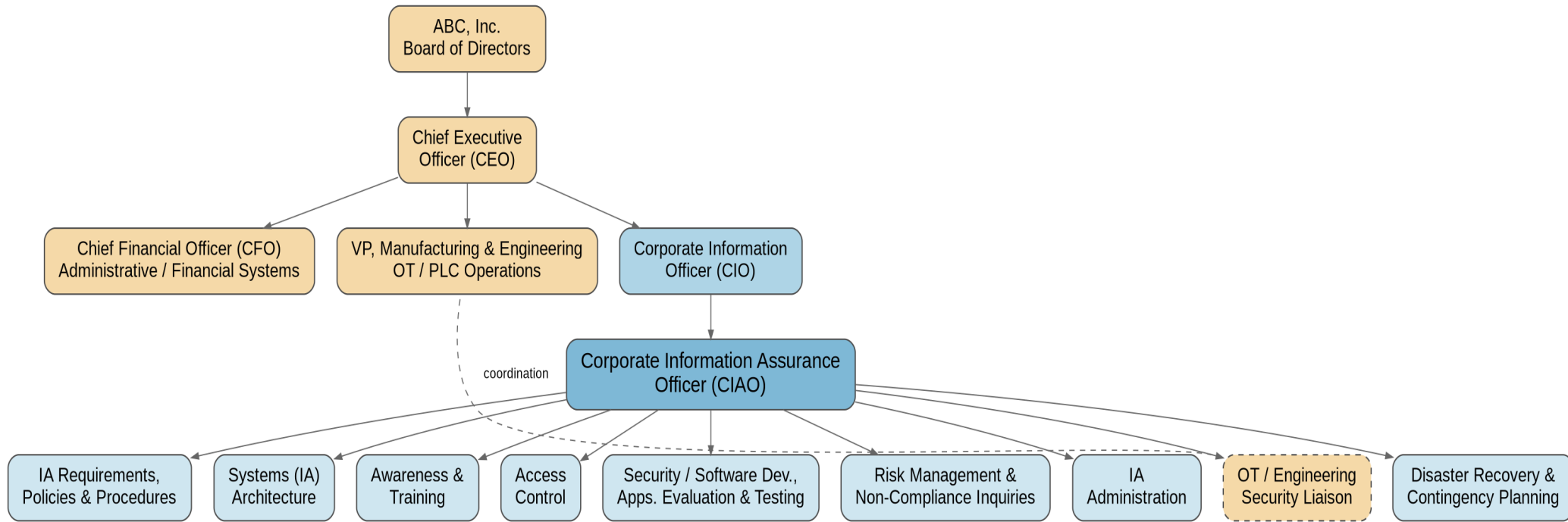
Public Statement (If needed): If the incident is leaked via ransomware, customer or press, ABC should have a short, factual holding statement ready in advance, confirming the incident, confirming manufacturing was unaffected, and directing further questions to a single named contact.

8. Recommendations and Preventive Actions

These recommendations are centered around Blyth and Kovacich's (2006, pp. 45-46) five principles of risk management, keeping the actions tied directly to what Sections 5 and 6 found. Table 3 maps each recommendation to the findings in this report and the areas of responsibility that are shown in Figure 2.

Establish Centralized Management

None of the other four principles can be sustained without someone whose job it is to own them. ABC currently has no such function. Section 3 brought up the issues about IA responsibilities being rolled into general IT administration, with no one accountable for policy, risk, or awareness. Figure 2 establishes that role with a CIAO reporting to the CIO, with the areas of responsibility underneath, based off the structure described in Blyth and Kovacich's (2006) Figure 12.1 and redone for ABC's IT/OT network segmentation, which includes a new OT/Engineering Security role who coordinates with the VP of Manufacturing and Engineering.

Figure 2*ABC, Inc. Proposed Information Assurance Reporting Structure*

Note. The CEO/CIO/CIAO reporting line and IA functional areas shown are adapted from Figure 12.1, “A Sample IA Functional Organisation,” in *Information Assurance: Security in the Information Environment* (p. 164), by A. Blyth and G. L. Kovacich, 2006, Springer-Verlag London. Copyright 2006 by Springer-Verlag London. The Board of Directors, CFO, VP Manufacturing & Engineering, and the OT/Engineering Security Liaison function were added to reflect ABC, Inc.'s organizational and IT/OT context

Assess Risk and Needs

The vulnerability assessment and threat matrix in Sections 5 and 6 were a one-time exercise for this report; they need to become a recurring function. The CIAO's Risk Management function should re-run that assessment at minimum annually, and after any material change to ABC's systems or network. As part of that recurring process, the Risk Management function should monitor CVE recommendations (MITRE Corporation, n.d.) for software and firmware used across both the IT and OT environments, so that newly disclosed vulnerabilities in ABC's actual technology stack are caught before they can be exploited rather than discovered after the fact.

Implement Policies and Controls

Each control below maps directly to a specific finding from Sections 5 and 6. Because ABC's work for a DoD program of record likely carries security expectations beyond typical commercial practice, ABC's legal and contracts staff should review the subcontract with the defense prime to confirm exactly what's required; the controls below should be treated as a reasonable floor pending that review, not as a substitute for it.

- *Identity and access*: Enforce least-privilege access and multi-factor authentication (MFA) across the IT segment.
- *Email and attachments*: Deploy attachment filtering and sandboxing and disable macro execution by default on office documents.
- *Backups*: Move to backup architecture that is isolated or immutable, so a future incident doesn't require cleaning the backups themselves before they can be trusted.

- *Network segmentation*: Formalize the IT/OT boundary as a documented, audited security control, including regular testing of the boundary itself.
- *Incident response plan*: Adopt a written incident response plan defining roles, escalation timelines, and decision authority. For the OT segment specifically, containment decisions should sit with the VP of Manufacturing & Engineering, advised by the CIAO's office, rather than with cybersecurity staff alone (Carhart, 2025).

Remote/Work from Home Security

A meaningful share of ABC's administrative and financial staff work from home at least part of the time. Recommended baseline controls: mandatory VPN with MFA for any remote access to ABC systems, minimum endpoint security standards for any device connecting remotely, and a clearly published channel for remote employees to report a suspicious email immediately.

Awareness Culture

The initial compromise succeeded because an employee treated a malicious attachment as routine which is a training gap, not a personal failure. Recommended: mandatory, recurring security awareness training for all employees, including phishing simulations built around vendor-impersonation and invoice-themed lures specifically, since that is the exact pattern that worked against ABC. The goal is not just compliance with training, it's to establish a culture that's security oriented.

Monitor and Evaluate Effectiveness

The three-week dwell time in this incident happened because nothing was watching for it. ABC needs a baseline monitoring and logging capability sufficient to flag unusual authentication activity or lateral movement within the IT segment, along with periodic access reviews. Additionally, OT-specific tabletop exercises related to ransomware should run separately from general IT exercises due to the safety considerations needed (Carhart, 2025).

Table 3

Recommendations Mapped to Findings and Area of Responsibility

Recommendation	Vulnerability / Finding Addressed	Area of Responsibility
CIAO reporting structure	No central IA ownership (Sections 3, 5)	Executive / CIAO
Least-privilege access, MFA	Credential store compromise (Section 6)	Access Control
Email filtering, macro controls	Initial phishing entry point (Section 6)	Security / Software Dev.
Isolated/immutable backups	Backup integrity risk (Section 5)	Disaster Recovery & Contingency Planning
Formalized IT/OT segmentation	Incidental, unaudited boundary (Sections 5, 6)	OT/Engineering Security Liaison
Written incident response plan, OT containment authority	Undocumented, reactive decision-making (Section 6)	IA Administration
WFH security baseline	Remote access not addressed by any prior control	Systems (IA) Architecture
Mandatory awareness training	Successful phishing lure (Sections 2, 6)	Awareness & Training
Monitoring, logging, OT tabletop exercises	Undetected 3-week dwell time (Section 2)	Risk Management & Non-Compliance Inquiries
Legal/contracts review of subcontract security terms	Undefined security obligations tied to DoD program work (Sections 3, 4)	IA Administration (with Legal)

Note. “Area of Responsibility” entries correspond to the functional areas shown in Figure 2. This

table maps each recommendation to the specific finding it addresses from Sections 3–6.

References

- Blyth, A., & Kovacich, G. L. (2006). *Information assurance: Security in the information environment* (2nd ed.). Springer-Verlag London.
- Carhart, L. (2025). *A simple framework for OT ransomware preparation*. SANS Institute. <https://www.sans.org/white-papers/a-simple-framework-for-ot-ransomware-preparation>
- McKnight, D. H., Choudhury, V., & Kacmar, C. (2002). Developing and validating trust measures for e-commerce: An integrative typology. *Information Systems Research*, 13(3), 334–359. <https://doi.org/10.1287/isre.13.3.334.81>
- MITRE Corporation. (n.d.). *CVE: Common Vulnerabilities and Exposures*. <https://www.cve.org/>