Cybersecurity Post-Mortem Investigation: Information Assurance Project

Branden Barnes

School of Cybersecurity, Old Dominion University

CS-465 Information Assurance

Professor Nukavarapu

December 7, 2024

Contents

Introduction

ABC Inc. recently suffered a ransomware threat, which prevented it from billing customers or paying vendors for three weeks. The information technology (IT) financial and administrative segment was compromised, while no harm was reported in the operational technology (OT) engineering and manufacturing segment. An expert outside cyber-security support was brought in to perform a post-mortem cyber investigation.

It was revealed in this investigation that an administrative support employee had received an email, with no notable suspicious intent, containing an Excel spreadsheet file embedded with the Zloader malware package. Upon clicking the spreadsheet file, it was validated that within the 4-minute window, Zloader had begun harvesting logins and passwords on the IT network. Important note: No breach of security was detected at the time of the incident. Three weeks later, all financial and administrative systems were locked down with ransomware demands. After systems were compromised, reports show that over 40 computers on the ABC IT network were infected with Ryuk-related ransomware files.

After the investigation, the outside cyber-security team reports, “all suspicious, or compromised files were removed from ABC’s network, computers, servers, and backups, and full company activities resumed.”

Background

ABC Inc.’s commercial responsibilities for being a small manufacturing company, with approximately 1,000 employees, include “negotiating contracts, managing customer relationships, identifying new market opportunities, and maintaining a competitive edge in the

industry" (BuildStream, 2024). ABC Inc. also fulfills its manufacturing production requirements on an Enterprise Resource Planning (ERP) software model. This software allows the Manufacturing Production Manager the ability to carry out vital manufacturing operations, crucial to the company's success.

Intellectual Properties ABC Inc. possesses include, "patents, patent applications, inventions, trade secrets, proprietary processes, databases, software, and formulae, and all other proprietary technical information, know-how, and processes" (Law Insider, n.d.). Intellectual Properties are critical for a small manufacturing company's ability to operate within the market. They contain valuable assets that set the company apart from direct competitors.

ABC Inc.'s manufacturing company has multiple strategic and corporate alliances. DEF Corporation is a larger manufacturing company that is partnered with ABC. ABC Inc. takes on the more specialized manufacturing needs of its strategic alliances. These strategic alliances consist of multiple small personal brand retailers.

The network infrastructure constructed for ABC's operation is worth discussing. Using logically segmented networks is a good way to promote ease of access while implementing isolation and security throughout the main system. The ERP system ABC used to separate IT functions and OT functions, held a strong execution of security between the two fields. This is the reason why the ransomware couldn't leak into the engineering and manufacturing functions of ABC Inc.

Negative attributes of ABC's infrastructure include unsafe e-mail configuration and lack of threat detection software. ABC Inc. uses personalized e-mails for internal and external communication. This left a pathway for ransomware to enter externally and spread internally

within the system. With that open vulnerability, the lack of threat detection software allowed ransomware to go undetected and devoid of response action.

Consequences

The ramifications of this ransomware threat exerted immense repercussions on ABC Inc. and other affiliates and customers. To begin, the outside cyber support investigation breaks down costs as such (Ellis, 2024):

- **Merchant processor compromise fines:** $5,000 – $50,000
- **Card brand compromise fees:** $5,000 – $5,000,000+
- **Onsite QSA assessments following the breach:** $20,000 – $100,000
- **Free credit monitoring for affected individuals:** $10 – 30/card
- **Card re-issuance penalties:** $3 – $10 per card (this could be included in card brand compromise fees)
- **Security updates:** $15,000+
- **Lawyer fees:** $5,000+
- **Breach notification costs:** $1,000+
- **Technology repairs:** $5,000+
- **Loss of consumer confidence:** often businesses lose 40% of customers after a breach

ABC Inc. is classified as a level 4 merchant, so the cost for the investigation is another $30k. Both strategic alliances and corporate alliances took a hit from ABC's downtime. Reputational loss and regulatory fines are still undisclosed. It is also still unknown if the data breach will be

leaked. All 1,000 employees experienced downtime for three weeks during the ransomware attack. This downtime cost could be considered the largest loss ABC Inc. faces. Luckily, cyber support was able to recover ABC's network, computers, servers, and backups. Often ransomware will leave encryption on infected systems deeming all production lost.

Patches

To ensure that an event like this won't happen again, it is my duty as the incoming Chief Information Assurance Officer (CIAO) to enforce a security posture that upholds the preservation of ABC Inc. After rebuilding the system back to its original form, I will firstly hire a Chief Information Officer (CIO) and a Chief Information Security Officer (CISO). My CIO will oversee the IT department in patch management on all software, carry out ransomware protection software, fix the personalized e-mail configuration, and put multi-factor authentication everywhere into practice. My CISO will manage phishing, vishing, and social engineering prevention training for all employees. They will also enforce policies and procedures like end point detection and response. They will hire professionals to manage threat detection, business continuity planning, and disaster recovery planning, and identify vulnerabilities through penetration testing. Last, they will conduct frequent audits of the IT systems to determine normal activity from suspicious and have the CIO activate software specified in this early detection plan.

References

BuildStream. (2024). *Commercial Manager*. Commercial Manager Job Description. https://www.buildstream.co/job-descriptions/commercial-manager#:~:text=Key%20Responsibilities&text=This%20includes%20negotiating%20contracts%2C%20managing,for%20success%20in%20this%20role.

Ellis, D. (2024, April 29). *What does a cyber forensic investigation do and how much does it cost?*. SecurityMetrics. https://www.securitymetrics.com/blog/what-does-cyber-forensic-investigation-do-and-how-much-does-it-cost#:~:text=The%20cost%20will%20depend%20on,to%20more%20than%20%24100K.

Law Insider. (n.d.). *Manufacturing Intellectual Property Definition*. Law Insider. https://www.lawinsider.com/dictionary/manufacturing-intellectual-property#:~:text=Manufacturing%20Intellectual%20Property%20means%20all,case%20to%20the%20extent%20such