CYBLE®

CASE STUDY

Supply Chain Company

- **Industry:** Supply Chain and Logistics
- **Size:** 10,000+ Employees
- **Revenue:** US$240 million

INTRODUCTION

Supply chain cybersecurity is an essential aspect of safety measures, focusing on managing cybersecurity for information technology systems, software, and networks. Supply chain management is highly threatened by cyber terrorism, malware, and data theft. Common cybersecurity practices to mitigate these risks include sourcing exclusively from trusted vendors and disconnecting critical machines from external networks.

BACKGROUND

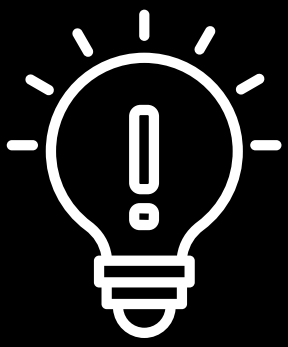
A prominent supply chain company, with a vast network of franchise partners managing their own IT infrastructure, faced significant cybersecurity challenges. Operating with numerous decentralized collection centers, the company struggled to maintain control over the security measures implemented by its partners. This setup left the company vulnerable to cyber threats, including malware and data breaches, resulting in an increase in courier scams and fraudulent calls. Threat actors exploited compromised partner systems to perpetrate these fraudulent schemes, causing financial and reputational damage.

PROBLEM STATEMENT

- **Decentralized IT Infrastructure:** The company's numerous franchise partners operated independent IT systems, leading to inconsistent security practices.
- **Vulnerability to Cyber Threats:** Collection centers became targets for malware and cyberattacks, resulting in data breaches and sensitive information extraction.
- **Increase in Fraudulent Activities:** Compromised systems facilitated courier scams and fraudulent calls, impacting the company's financial stability and reputation.

SOLUTION

To address these pressing issues, the company deployed Cyble's Advanced Threat Intelligence System.



IMPLEMENTATION DETAILS

COMPREHENSIVE INSIGHTS

Cyble's threat intelligence module is a centralized global database, which aggregates attacker information from dark web forums, cybercrime marketplaces, and security reports. This continuously collects and analyzes data relevant to the company's franchise partners and IT systems.

DETECTION OF COMPROMISED SYSTEMS

Advanced search algorithms scanned the dark web and other sources for information on the company's IT infrastructure and partner systems and the process identified and flagged over 1,000 compromised partner systems, revealing their details as exposed on the dark web.

RISK MITIGATION

Cyble's detailed threat intelligence capability allowed the company to assess the impact of the breaches and implement targeted risk mitigation strategies and effectively minimize the potential financial and reputational damage.

BENEFITS DELIVERED

1

REDUCTION IN FINANCIAL LOSSES AND REPUTATIONAL DAMAGE

The company observed a 45% reduction in new fraudulent calls within the first three months post-implementation.

2

ENHANCED SECURITY POSTURE

Early identification of compromised systems allowed the company to take swift action, thereby reducing risks.

3

RESTORED TRUST

Effective management of cybersecurity threats helped the company restore trust among customers and partners, reaffirming the company's dedication to protecting sensitive information.

4

IMPROVED PARTNER COLLABORATION

The proactive engagement with franchise partners regarding cybersecurity threats fostered better collaboration and compliance to security best practices.

CONCLUSION

By implementing Cyble's Advanced Threat Intelligence System, the supply chain company effectively tackled significant cybersecurity challenges posed by its decentralized IT infrastructure. Cyble empowered the company to better manage its cybersecurity risks, maintain its reputation, and safeguard sensitive information across its extensive network of franchise partners.