How can businesses address the cybersecurity risks brought by supply chains?

14 June 2024

Building a better working world

How can businesses address the cybersecurity risks brought by supply chains?

14 June 2024

In the era of digitization, supply chain security defenses are facing unprecedented challenges, emerging as prime targets for cyber threats. The repercussions of cyber-attacks extend beyond financial losses, posing a significant risk to an organization's credibility. This article will delve into the current landscape of cyber threats targeting global supply chains, the underlying reasons for their vulnerability, and the formulation of robust security measures and strategies.

(1) Cyberattacks on supply chains pose a significant threat to the continuity of business operations

Over the past few years, several extensive supply chain attacks have had a devastating impact on global organizations. For instance, the NotPetya ransomware attack, which propagated through infecting a single segment in the supply chain - an accounting software, resulted in over 50,000 endpoints being infected within a global logistics company[1]. Even, businesses around the world faced over US$10 billion in estimated damages from the NotPetya ransomware attack[2].

Furthermore, a recent ransomware attack on the healthcare payment exchange platform systems of the IT subsidiary of a prominent U.S. health insurance provider resulted in US$872 million in losses for the organization. This attack caused significant disruptions in the U.S. healthcare system, affecting healthcare services and insurance claims processing across the country.

	NotPetya ransomware attack	Ransomware attack on a U.S. health insurance provider
Threat type	Ransomware that demands a ransom in the form of encrypted files.	
Attacked supply chain links	Ransomware spreads through the updater of an accounting software, affecting organizations and businesses that use it.	The attack targeted the healthcare payment exchange platform system of the enterprise's subsidiary, affecting healthcare providers and related insurance companies.
Defects	The update mechanism of accounting software lacks sufficient security validation and is vulnerable to being hijacked by attackers.	The subsidiary's information system security measures were inadequate and failed to effectively defend against external attacks.
Consequences	Widespread dissemination affected organizations in multiple countries around the globe, resulting in significant data and economic losses, damage to critical infrastructure.	The incident affected the U.S. healthcare system and insurance claims processing, causing US$872 million in financial losses and business interruptions. A large amount of sensitive data was compromised.

Table 1 Comparative analysis of supply chain network attack cases

[1] Ransomware: The key lesson Maersk learned from battling the NotPetya attack https://www.zdnet.com/article/ransomware-the-key-lesson-maersk-learned-from-battling-the-notpetya-attack/#google_vignette

[2] The Untold Story of NotPetya, the Most Devastating Cyberattack in History https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/

The interconnectedness and reliance between various organizations in the supply chain make it possible for such attacks to rapidly spread from a single point to the entire network, impacting companies on a global scale. Cyberattacks, including ransomware, can cause significant disruptions to business operations and have a substantial impact on reputation. These attacks often lead to delays in production and shipment, inventory issues, and operational disruptions that affect multiple industries due to the interconnected nature of supply chains. The long-term consequences may also include financial losses, delivery failures and reputational harm resulting from delays.

A study by Centrify[3] revealed that 65% of customers lose trust in an organization after a security breach or incident. The World Economic Forum[4] also states that disruptions can cause a 4-5% decrease in industrial production within one to two years. The repercussions of a supply chain security incident can be catastrophic for reputation and trust, affecting customers, stakeholders, and other companies around the globe.

Incidents can have legal regulatory consequences as well, in addition to the negative impact on the firm's image. Some companies have been subject to fines, penalties and even liquidation for failing to implement appropriate governance measures such as data protection and security.

(2) What makes supply chains most susceptible to cyberattacks?

The complexity and interconnectedness of global supply chains make them a prime target for cyberattacks. There are several key reasons why supply chains are vulnerable to attacks:

1. Cyber threats are complex and varied in nature, providing attackers with numerous opportunities to exploit vulnerabilities. This results in a wide range of cyber attacks, such as insider threats, malware, ransomware, data exposure, firmware attacks, physical theft, unauthorized access to Internet of Things (IoT) devices, breaches of supply chain intermediaries, social engineering, and more.

2. Security vulnerabilities are often hidden and dispersed throughout modern supply chains, making it challenging for organizations to identify and address them. With multiple links and participants involved, enterprises struggle to detect vulnerabilities in their upstream and downstream partners, giving attackers prolonged access to exploit these weaknesses for financial gain.

3. Many enterprises lack the necessary awareness and resources for effective vendor management to mitigate supply chain security risks. This is particularly true for small and medium-sized enterprises (SMEs) that struggle to address security challenges in their supply chains due to limited support capabilities. According to the Global Cybersecurity Outlook by the World Economic Forum 2022 [5], 39% of organizations have been affected by a third-party cyber incident. This survey shows that many organizations have not been adequately assessing third parties within their supply chain and may not be informed of their involvement in an incident.

4. Operational technology (OT) security absence as the norm: Industry 4.0 has led to a significant rise in the utilization of OT within the supply chain, as information technology (IT) IT and OT assets become increasingly interconnected. Nonetheless, findings from a 2022 survey conducted by the European Union Agency for Cybersecurity (ENISA)[6] indicate that 76% of organizations lack dedicated roles and responsibilities for OT supply chain cybersecurity, and only 47% of organizations allocated an exclusive budget for this purpose. Notably, the manufacturing sector is particularly susceptible to targeted attacks compared to other industries. According to the IBM cybersecurity experts' report[7] in 2022, the manufacturing industry accounts for 58% of all OT attacks due to the lack of default security measures on most OT devices which are heavily used in the industry.

5. Limited adoption of risk assessments: The data from ENISA's survey highlights a concerning fact that only 37% of organizations are actively engaging in risk assessments for their supply chains. The absence of comprehensive risk assessments in the supply chain domain contributes to the rising success rates of supply chain attacks.

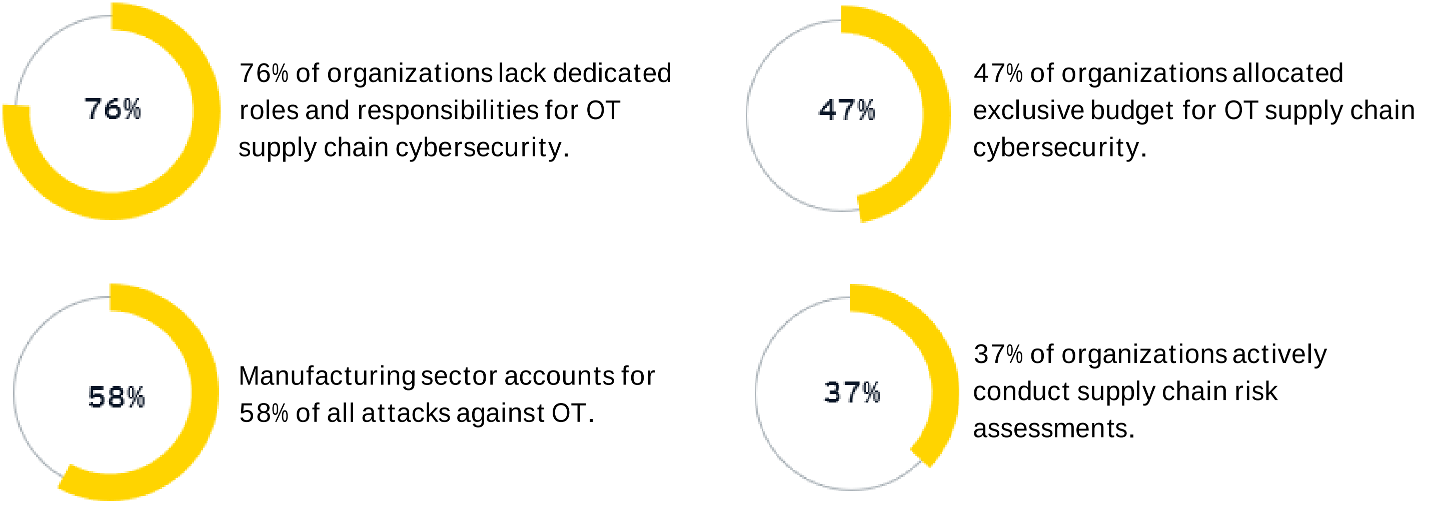
[3] Analyzing Company Reputation After a Data Breach https://www.varonis.com/blog/company-reputation-after-a-data-breach

[4] Why are supply chains facing disruptions, and how long will they last? https://www.weforum.org/agenda/2022/07/supply-chain-disruptions/

[5] Global Cybersecurity Outlook 2022 https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2022.pdf

[6] Good Practices for Supply Chain Cybersecurity https://www.enisa.europa.eu/publications/good-practices-for-supply-chain-cybersecurity

[7] IBM X-Force Threat Intelligence Index 2023 https://www.ibm.com/reports/threat-intelligence



76% of organizations lack dedicated roles and responsibilities for OT supply chain cybersecurity.

47% of organizations allocated exclusive budget for OT supply chain cybersecurity.

Manufacturing sector accounts for 58% of all attacks against OT.

37% of organizations actively conduct supply chain risk assessments.

Figure 1 Overview of key data from multiple surveys related to supply chain security

(3) How do companies build a supply chain security program and strategy?

The EY 2023 Global Cybersecurity Leadership Insights Study indicates that cybersecurity mature organizations (38%) are more focused on supply chain risks compared to cybersecurity developing organizations (20%). In contrast, cybersecurity developing organizations are primarily focused on financial risks. According to the EY 2021 Global Information Security Survey, 67 percent of CISOs (Chief Information Security Officers) do not have confidence in their supply chains' ability to defend or recover from cyber threats. Supply chain security involves protecting and managing the processes, assets and infrastructure within an organization's supply chain from potential threats. Given the serious nature of cyberattacks, security measures should be integrated throughout the entire supply chain infrastructure. Developing a comprehensive supply chain security program and strategy necessitates a holistic approach that encompasses people, processes, and technology.

People

People are the most critical, but possibly the weakest, link as part of supply chain security. People strategies for a supply chain security program can include:

- Compulsory training initiatives: Conducting routine security awareness training sessions for both internal staff and external vendors to improve their understanding of security measures and their impact on the supply chain. The training should cover topics such as protecting sensitive information, following security protocols, privilege management, OT techniques, and social engineering.
- Simulation drills: Creating practical tabletop exercises to encourage teamwork in responding to incidents and to guarantee that all employees are ready to handle any potential emergencies.
- Internal certifications: Establishing an internal certification scheme to verify that employees have the necessary skills and knowledge to carry out security-related duties effectively.

Processes

Supply chain operations rely greatly on well-defined processes. Therefore, robust management processes will help mitigate some of the supply chain security risks. Elements to focus on in terms of processes include:

- Governance and compliance: The initial phase of a supply chain security program involves harmonizing policies, regulations and a data protection framework. By incorporating established security measures and standards, integrating standardized security protocols into the supply chain, and enforcing mandatory privacy and compliance measures, the overall security position is significantly strengthened.

- Third party management: It is recommended to perform risk assessments, categorize vendors and partners, continuously monitor them, sign SLAs (service level agreements) and create a database for third party risks. Additionally, setting up a secure communication channel for vendors is crucial to promptly inform all involved parties about any newly identified vulnerabilities.
- Incident response runbook: Development of a comprehensive Incident Response Runbook, which encompasses Recovery Point Objective (RPO) and Recovery Time Objective (RTO).
- Network asset lifecycle management: Management of network assets throughout their lifecycle to guarantee adherence to corporate security standards from acquisition to retirement.

Technology

Technology serves as a means to safeguard the supply chain against cyber attacks. Methods for establishing a secure supply chain technology program encompass:

- Security control tower: Creating and executing a supply chain control tower that utilizes real-time data to furnish essential cybersecurity metrics.
- Supply chain architecture redesign: Embracing the "secure-by-design" concept to reassess and enhance the design of their Enterprise Resource Planning (ERP) and data architecture and infrastructure.
- DevSecOps in supply chain: Integrating DevSecOps to infuse security into every stage of software development and operations by continuously integrating and deploying the latest OT, IoT devices and software updates, and implementing monitoring and automation.
- Data protection: Safeguarding sensitive data through data security governance, data encryption and data leakage prevention technologies.
- Security testing: Conducting security testing of OT and IoT devices, including code review, static or dynamic application security testing, etc., to ensure there are no backdoors and critical vulnerabilities.
- Identity access management (IAM): Integrating security across the organization with IAM technologies such as Single Sign-On (SSO) and Multi-Factor Authentication (MFA), implementing role-based identity and access management solutions to protect resources.

(4) EY teams assist businesses in enhancing supply chain security measures

EY team provides a variety of services to assist organizations in developing and upholding their supply chain security. These services encompass, but are not restricted to:

Consultation on transforming supply chain security systems

- Establishing or improving supply chain security programs and strategies: Offering suitable governance, processes, and risk frameworks, including management and oversight, policies and standards, third-party inventories, risk management methodologies and models.
- Defining supply chain security management requirements: Specifying fundamental information security requirements to support the sourcing and provisioning of all products and services, such as manufacturing or assembly of products, business process sourcing, components of software and hardware, knowledge process sourcing, and cloud computing services.
- Designing supply chain security management processes: Providing implementable standard processes for the entire process of supplier relationship planning, supplier selection, supplier relationship agreement, supplier relationship management, and supplier relationship termination around the supplier relationship lifecycle.

Supply chain security risk assessment:

Assisting enterprises in comprehending the structure of the supply chain and identifying potential security risks in the supply chain (e.g., malicious tampering, counterfeiting, supply disruption, information leakage, etc.); determining the likelihood and degree of impact of the risks, categorizing and prioritizing the risks; and formulating a risk disposal plan based on the results of the risk assessment.

Supply chain security joint operations

- Supplier security assessment implementation: Utilizing enterprise-specific security requirements and frameworks, conducting on-site or remote research and review of supplier security capabilities, identifying actual security risks based on business scenarios, and formulating risk control measures to ensure compliance with enterprise security standards.
- Security training: Offering training to suppliers to enhance their awareness and capabilities in supply chain security, and enhancing their focus on the security of the company's services.
- Continuous monitoring: Setting up a monitoring system to regularly evaluate suppliers' security performance and directing them to enhance and improve their own security management level.

Technical implementation and support:

Supplying professional technical support, suggesting security technology tools and solutions that are suitable for enterprise needs, developing relevant strategies and aiding in their implementation to support enterprises to effectively prevent, monitor, and mitigate risks to enterprise supply chain security.

Furthermore, the EY team has the capability to assist organizations in enhancing supply chain security controls and establishing a more secure and robust supply chain against evolving cyber threats by offering experienced consulting services such as policy and standards development, incident response plan development, and compliance assessment.

Conclusion

It is crucial to implement security measures to identify, safeguard and address supply chain disruptions caused by cyber issues. Potential victims of a cyber attack within the supply chain may experience not only financial losses but also significant reputational harm, which can undermine trust among supply chain partners, customers and stakeholders.

To establish a resilient supply chain, organizations need to create a supply chain security program that encompasses people, processes and technology. A resilient supply chain can withstand challenges and assist organizations in achieving long-term business objectives, positioning them for sustained growth, profitability and success in a demanding business environment. However, implementing security is an ongoing process that requires continuous evaluation, proactive enhancements and long-term governance.

For more information, please contact us:

Kelvin Gao

Managing Partner, Greater China
Cybersecurity and Privacy Consulting Services
Ernst & Young (China) Advisory Limited
kelvin.gao@cn.ey.com

Nancy Zhang

Partner, Digital Risk Consulting Service
Ernst & Young (China) Advisory Limited
nancy-nc.zhang@cn.ey.com

Dylan Si

Senior Manager
Digital Risk Consulting Service
Ernst & Young (China) Advisory Limited
dylan.si@cn.ey.com

Skyler Zhang

Senior Consultant
Digital Risk Consulting Service
Ernst & Young (China) Advisory Limited
skyler.zhang1@cn.ey.com

EY | Building a better working world

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

EY embraces innovation and adopts advanced technologies, helping clients identify market trends, capture opportunities and accelerate business transformation through integrated high-quality services.

Working across assurance, consulting, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients, nor does it own or control any member firm or act as the headquarters of any member firm. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. EY member firms do not practice law where prohibited by local laws. For more information about our organization, please visit ey.com.

APAC no. 03020523
ED None.

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, legal or other professional advice. Please refer to your advisors for specific advice.

ey.com/china

Follow us on WeChat
Scan the QR code and stay up-to-date with the latest EY news.