A Brief Discussion on Cybersecurity Issues in Supply Chain Management

Kevin Yang

Taiwan Depository & Clearing Corporation (TDCC)

August 2022

Outline

1. Preface
2. Cybersecurity incidents
3. Enhanced measures for supply chain security
4. Conclusion

1. Preface

- As types of cyberattacks increasingly vary, supply chain attacks have also increased in recent years. The world has become more vigilant about internet-based supply chain threats.
- As platforms that process securities clearing, settlement, custody, and transferring for investors, central securities depositories constantly produce information services and products. The data-based services need the support from IT hardware/software suppliers and internet service providers. For this cybersecurity supply chain, it is crucial that we enhance our management and monitoring of supply chains to mitigate cybersecurity risks of supply chain attacks.

2. Cybersecurity incidents

Emergency directive: Global governments issue alert after FireEye hack is linked to SolarWinds supply chain attack

Jessica Haworth 14 December 2020 at 14:42 UTC
Updated: 14 December 2020 at 16:08 UTC

US | Malware | Cyber-attacks

Authorities worldwide caution against use of IT management tool Orion

3. Enhanced measures for supply chain security

A. Supply chain security management policies

B. Principles of the Zero Trust Model

C. Joint cyber defense collaboration

3. Enhanced measures for supply chain security

A. Supply chain security management policies

- Guidelines for supply chain risk management in the securities and futures service industry
  - Help securities firms, futures firms, and investment trust companies safely and effectively manage their supply chain risks related to IT services. Draw up risk management guidelines for supply chain regarding the selection, management, and service termination of IT service providers, as well as the uninstallation of their services. The goal is to help the supply chain maintain a safe environment of risk management.

3. Enhanced measures for supply chain security

A. Supply chain security management policies (cont.)

- Article 9 of the *Cyber Security Management Act* and Article 4 of the *Enforcement Rules of Cyber Security Management Act*.
  - Relevant rules of outsourced information systems regarding the provision of setup, operation and maintenance, and information services; regulations and matters needing attention when selecting and supervising outsourced vendors
- Enhanced measures for outsourced IT service providers
  - Enhanced measures for every stage of information systems, thorough auditing of outsourced vendors, and careful inspections of outsourced vendor requirements
  - An enhanced cybersecurity management checklist of critical infrastructure providers in the securities and futures industry when dealing with outsourced IT services

B. Principles of the Zero Trust Model

- Risk assessments of suppliers and providers
  - Assess your service providers before entrusting them with your requests. Know their ways of handling cybersecurity matters, and assess what types of risks you will face.
  - Keep monitoring and evaluating providers' cybersecurity performance on a regular basis to check if the initial risk assessment changes. When the risk level increases, we can promptly formulate countermeasures to mitigate risks.

B. Principles of the Zero Trust Model

- Specify service level agreement clauses
  - Clearly tell our providers about relevant service standards, e.g., system uptime, open source software, proof of system security, vulnerability scanning results, vulnerability fixing reports.
  - Specify requirements concerning transferring, co-contracting, or subcontracting so that we can promtly control the third-party supply chain.

B. Principles of the Zero Trust Model

- Acceptance, maintenance, and warranty
  - Take relevant regulations as references, and formulate system security related rules that include concrete proof of code review inspections, vulnerability scanning, or penetration testing.
  - Examine providers' business continuity plan (BCP), response to abnormal situations and recovery exercises, spare parts, staff, and other aspects to know their capability of sustaining system uptime.
  - Examine how providers respond to cybersecurity incidents to see their capabilities of promptly containing damages, recovering uptime, and notifying us of countermeasures.

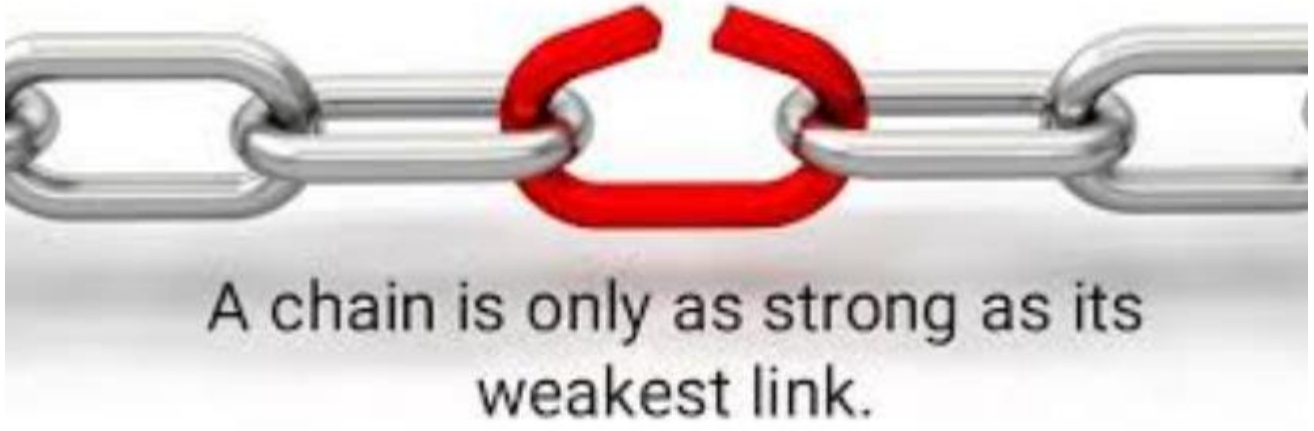
3. Enhanced measures for supply chain security

C. Joint cyber defense collaboration

– A joint financial cyber defense system was established by the Financial Information Sharing and Analysis Center (F-ISAC) and Security and Future Computer Emergency Response Team (SF-CERT). The defense system will provide information about cybersecurity events and contingency plans. Such information, within the proper scope of services, can be sent to providers, included in new contracts, or added to existing contracts. Providers will have to cope with cybersecurity issues and bolster their defense mechanisms accordingly.

4. Conclusion

- The competent authorities have developed supply chain security management policies to tighten the control of supply chain risk and auditing management. The policies are expected to effectively mitigate supply chain risks and minimize cybersecurity weak spots.
- With joint cyber defense collaboration, the cyber supply chain becomes more resilient and fast responsive when it comes to cybersecurity events. The mechanism helps mitigate impacts and improve cybersecurity readiness.



TDCC

Thank you!