THOMAS MURRAY

ACG CTS 2022

Cyber Supply Chain Risk Management

9/26/2022

Thomas Murray

Highlights

- Global Risk Company, founded in 1994
- Due Diligence & Risk Assessments on c.120 markets globally for clients
- Monitoring CSD Risk for Custodian Banking Clients for 20+ years
- Today monitoring c.140 CSDs globally
- Launched Thomas Murray Cyber Risk division in 2021
- Thomas Murray now includes cyber risk analysis in every risk assessment in the post-trade world. This includes CSDs, where we provide daily risk updates to our global custodian clients; as part of their regulatory requirements to continually monitor CSD risks under 17f7 of the Investment Company Act 1940.

Key Statistics

- Financial firms are 300 times more likely to experience attacks (Boston Consulting Group)
- c.50% of cyber attacks originate through a third party (Ponemon Institute)
- Malicious activity from outside organisations accounts for 56% of data breaches, with malicious insiders accounting for just 7% (Statistica)
- 59% of UK and US companies who used a third-party service have experience a breach; just 16% thought their TPRM was effective enough in 2019 (Business Wire)
- 20% of banks reported data breaches in 2021, with 8% refusing to disclose (Thomas Murray)
- 0% of CSDs reported breaches, with 29% refusing to disclose (Thomas Murray)

Key Observations

- Attacks through the supply chain are predicted to increase and become more targeted
- Supply chain cyber risk has become a key consideration since SolarWinds and Log4J
- By attacking a supplier, a threat actor can potentially gain access to hundreds of companies, bypassing their security controls and leveraging their trusting relationship
- IBM estimates that the average cost of a cyber-attack is $3.9m – a cyber-attack can put a company out of business, particularly where it doesn't have the liquidity to absorb loss

CSD Observations

- CSDs' security strategies & roadmaps are immature compare to the Banks
- There is a clear correlation between higher-risk frontier and developing markets, and higher cyber risk in their infrastructures
- Some CSDs are unaware of digital assets they are exposing publicly – with one CSD unaware of the exposure of 75% of their public attack surface
- Both Banks and CSDs underestimate cyber risk in the securities industry, failing to see the potential impact of ransomware in particular

CSD Supply Chains (2)

- Supply chain cyber risk is the critical issue at the moment for many CSDs
- What does the CSD supply chain look like?
  - IT & Cloud Providers
  - CSD Direct Participants (Banks & Brokers)
  - Exchange Members
- CSDs also need to recognise that they are part of the FS supply chain – banks are increasingly concerned about indirect cyber exposures to market infrastructures
  - Many banks have asked if they can see CSD Cyber Risk grouped by region & custodian, so they can visualise the geopolitical exposure of client assets

Achieving Supply Chain Security

- A first-rate supply chain cyber risk management programme does not need to be expensive, but it requires knowledge of best practices
- Bank best practice we have observed:
  - Due Diligence: IT Security questionnaires issued to all supply chain organisations, analysed against a common framework & reported to management. This is the 'internal' analysis.
  - Threat Intelligence: Objective third-party threat intelligence, scanning open, deep and dark web sources for breached data, compromised infrastructure, known & unpatched vulnerabilities, and misconfigurations in a supply chain company's attack surface. This is the 'external' analysis.
  - Escalation & Remediation: Organisations with mature security strategies have implemented frameworks for identifying vulnerabilities and escalating with suppliers.

Final Thoughts

- Disruption to the supply chain is bad for business, whereas a healthy supply chain can boost trust, performance and productivity.
- Any organisation digitally touching your organisation can be a vector for malicious code.
- Monitoring & protecting your supply chain is a direct way of protecting your organisation, as well as your clients.
- No matter how well your InfoSec team believe your organisation is protected, if you have not adequately invested in mitigating supply chain risk, you have only addressed c.50% of the threat landscape.
- For CSDs, disruption is the most important consideration. A successful attack on a CSD, directly or via its supply chain, could create significant collateral damage for direct participants, damaging relationships and trust in the long term.

Roland Thomas
Manager, Corporate Development
rthomas@thomasmurray.com