Accenture
Cybersecurity
Forum
APAC

Supply Chain Attacks: Lessons Learned from Log4j and Sanctions

On March 16, the Accenture Asia/Pacific Cybersecurity Forum (ACF) convened a virtual roundtable titled, “Supply Chain Attacks: Lessons Learned from Log4j and Sanctions—How Are We Thinking Differently About Supply Chain Attacks & Cyber Defence?”

The recent Log4j incident, geo-political driven sanctions and their implications for future supply chain attacks and cyber defence are of great interest to APAC CISOs. In this session, Forum members and subject-matter experts examined what good supply chain defences should look like and specific actions CISOs can take in reestablishing best-in-class supply chain security.

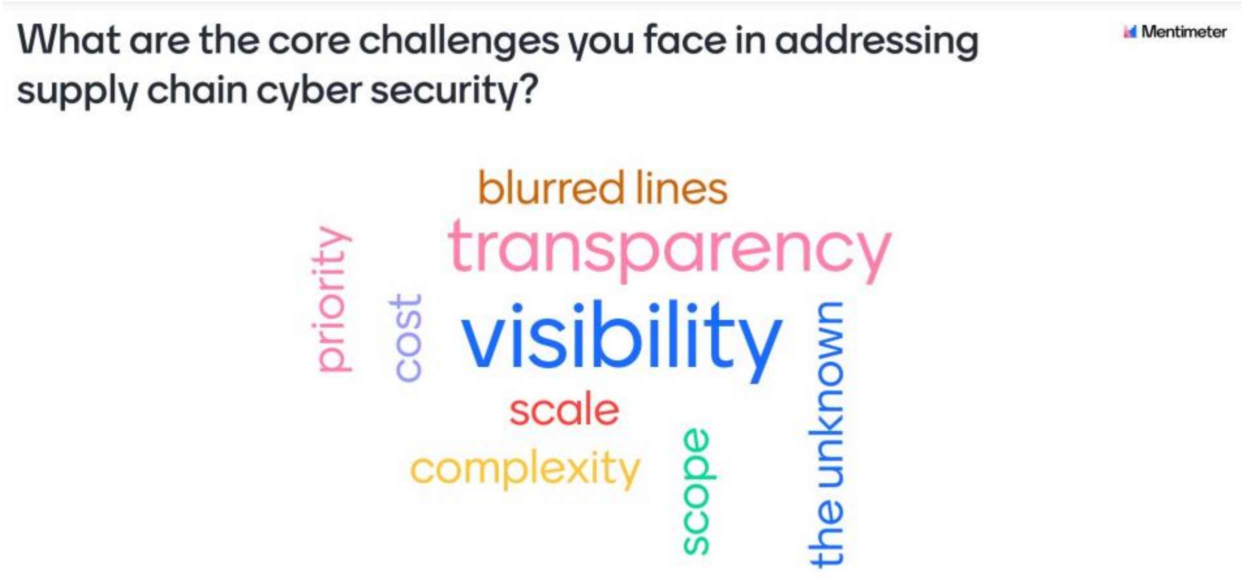
The roundtable was conducted under the Chatham House Rule: ACF members are free to use the information shared, provided that neither the identity nor the affiliation of the speakers, nor participants, is revealed.

Below is a brief summary of the call:

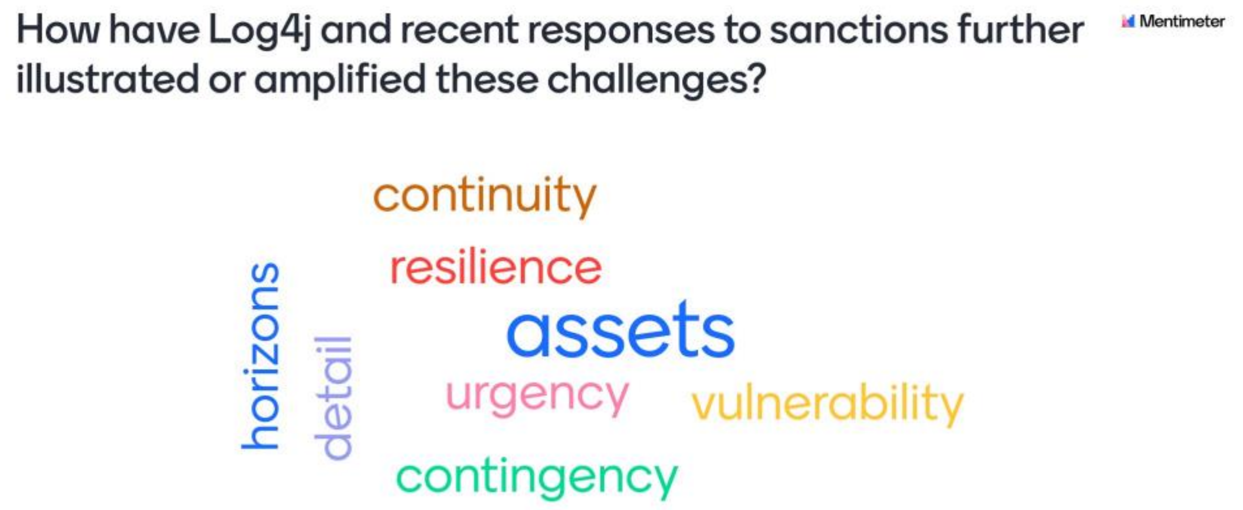
The greatest supply chain security challenge facing APAC cybersecurity leaders is a lack of visibility, as highlighted by SolarWinds and Log4j events. As one Forum member said: “If we can’t see it, we can’t secure it.”

A number of factors contribute to this lack of visibility. Technology companies haven’t fully embraced the idea of a software bill of materials (SBOM). IT vendors typically only offer a “level 1” view into their cyber defences, with no guarantee of protection. Transparency into legacy systems is often lacking. Acquisitions make traceability harder. Asset databases may be incomplete.

Concerns about asset management were underscored by the responses to two polling questions:



What are the core challenges you face in addressing supply chain cyber security?



How have Log4j and recent responses to sanctions further illustrated or amplified these challenges?

Forum members acknowledged that traditional approaches to asset management have fallen short, particularly as supply chains have become more complex, with a greater reliance on third and fourth parties. A Forum member asked: “We’re securing ourselves, but when will we get to the point where we can have the expectation that the companies we’re working with are secure?” Another Forum member called on industries to set requirements for driving vendors toward compliance. “They need to take more accountability themselves,” he said.

There’s no one right answer or roadmap to build enterprise resilience, but some are optimistic about the power of societal or peer pressure. In the energy industry, for example, multinational leaders are driving vendors to improve their cybersecurity. Some companies are adding cybersecurity requirements into their vendor contracts. But another Forum member added: “It’s not necessarily wrong to go with a vendor who isn’t cybersecure. But it is up to the security leader to help management understand and manage the risks of that decision.”

Leading practices for supply chain cyber defence

The conversation yielded many recommendations to address the supply chain security challenge:

- **Understand the risks**—Threat intelligence, penetration testing, heightened threat detection capabilities and a deeper understanding of the business all contribute to a greater understanding of supply chain risks. Several Forum members stressed the importance of a broader and deeper view into the extended supply chain.
- **Take a dynamic approach toward contingency planning**—Threat actors will continue to innovate. Enterprise interdependencies will evolve. Mergers and acquisitions may introduce new risks. CISOs need to regularly assess their attack surface and make investments to minimize the impact of attacks when they inevitably occur. "Consider more extreme scenarios," said a subject-matter expert. "And assess how a reliance on Russia and China could cause greater supply chain contagion." Another suggestion: "Ask hard questions about what you will do if you have to disconnect from a vendor."
- **Prioritize across the planning horizon**—Identify, for the board and senior management, all the supply chain security investments that need to be made immediately and which defences should be shored up over a longer time period.
- **Recognize that "not all risk is bad."**—A Forum member said: "If we have to spend $2 million to clean up a cyber problem, but the relationship generates $50 million in revenue, that's a risk the business is willing to accept. We need to get people more educated on how to understand and manage the risk." The reliance on operational technology (OT), which in many cases can only be sourced from a handful of suppliers, forces enterprises to factor in the costs and risks of substituting OT, even when the current supplier is not hyper vigilant about cybersecurity.
- **Set contractual security expectations with suppliers**—Make suppliers understand the cybersecurity priorities that are most important to your enterprise. Even a "meet/don't meet" assessment of vendor security postures can help raise the bar. Practically speaking, however, "Even if a vendor can't document its cyber strategy, the business may decide to do business with that company," said a Forum member.
- **Set baseline requirements internally**—A subject-matter expert suggested that end users be held accountable for demonstrating cybersecurity compliance before fulfilling requests for IT assets. "In order to get the services you're asking for, here's what you have to do," he suggested. The model is somewhat like Walmart's vendor inventory management practices.
- **Reassess open source**—Log4j underwent in-depth penetration testing and source code reviews but still presented cyber risks. One approach suggested by a Forum member was "Defensive architecture," whereby developers deliberately opt in to open-source features rather than accepting all features wholesale. "When you put modules like this out, you disable everything by default and then consciously turn bits of code on."
- **Promote synergy across the cybersecurity team**—Ongoing collaboration between threat hunting/monitoring and response teams can accelerate response and recovery times after an attack.

CONTACT

Kris Burkhardt
Accenture Chief Information Security Officer
Accenture Cybersecurity Forum Chair
LinkedIn

About Accenture

Accenture is a global professional services company with leading capabilities in digital, cloud and security. Combining unmatched experience and specialized skills across more than 40 industries, we offer Strategy and Consulting, Interactive, Technology and Operations services — all powered by the world's largest network of Advanced Technology and Intelligent Operations centers. Our 699,000 people deliver on the promise of technology and human ingenuity every day, serving clients in more than 120 countries. We embrace the power of change to create value and shared success for our clients, people, shareholders, partners and communities. Visit us at accenture.com.

About Accenture Security

Accenture Security is a leading provider of end-to-end cybersecurity services, including advanced cyber defence, applied cybersecurity solutions and managed security operations. We bring security innovation, coupled with global scale and a worldwide delivery capability through our network of Advanced Technology and Intelligent Operations centers. Helped by our team of highly skilled professionals, we enable clients to innovate safely, build cyber resilience and grow with confidence. Follow us on @AccentureSecure on Twitter or visit us at www.accenture.com/security.

View the entire suite of ACF roundtable summaries on our webpage – here.