Supply Chain Risk and the Evolving CISO Leadership Role

The Accenture APAC Cybersecurity Forum (ACF) convened a virtual roundtable titled, "Supply Chain Risk and the Evolving CISO Leadership Role," on February 10, 2020.

The SolarWinds breach is just the latest in a series of high-profile threats over the last 12 months—from COVID-19-related working-from-home disruptions to increased phishing attacks, ransomware and now supply chain risk. Are enterprises prepared for emerging supply chain risks? How should we expect suppliers to contribute to enterprise security? What leading practices can help CISOs become more valued business leaders?

APAC Forum members examined the changing threat landscape across the extended enterprise and how new challenges are driving the evolution of CISO leadership. Our speakers included Accenture Security subject-matter experts and peer CISOs. The session was hosted by Kris Burkhardt, Accenture CISO and ACF chair and Andrew McLauchlan, Managing Director—Accenture Security, Asia Pacific Lead.

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 or participants is revealed.

The evolution of CISO leadership

APAC CISOs recognize the value of being as comfortable in the boardroom as the computer room. As one CISO said, "We're pivoting from discussions about tools and technology to deeper conversations about helping the enterprise manage business risk." A subject-matter expert said, "Along with an emphasis on governance and compliance, CISOs are now expected to be business-oriented, non-technical communicators."

A subject-matter expert noted, "There's been a lot of talk about CISOs having a seat at the executive table and engaging in business discussions—and many of us are already there. But you'll lose that seat at the table if you turn everything into a technology discussion."

CISOs point to several reasons for the evolution from technical to business-oriented communications. Recent high-profile supply chain security breaches, such as the SolarWinds

attack, have attracted the attention of the CEO and the board. CISOs find themselves having to translate news coverage into non-technical intelligence that is relevant to the enterprise. “Understand where your CEO is getting their news, whether it’s *The Wall Street Journal* or elsewhere, and help separate the truth from the hype,” one CISO said.

In addition, the trend toward digital transformation puts data at the center of enterprise strategy. In some cases, CISOs need to be more directly engaged with the broader risk management function or even take on a risk management leadership role.

Even with these changes, APAC CISOs recognize the value of being comfortable in any environment within the business. One CISO said, “We still have to get mud on our boots. We have to demonstrate practical competence and capability in terms of technology, as well as master the business linguistics.” Another member added, “We need to act as if you’re in the boardroom and the computer room.”

Third-party risks

A reliance on third-party networks, hardware and software adds complexity to the CISO’s responsibilities. Threat actors are attacking indirect targets, such as vendors and other third parties in the supply chain, creating new demands on cybersecurity defenses.

Forum members acknowledge that getting visibility into supply chain risks can be difficult, particularly when vendors are reluctant to share information. One subject-matter expert said that while many vendors are concerned about reputational risks, other firms, including FireEye, have done a good job at releasing detection rules.

CISOs raised a number of questions about managing third-party risks, including:

- How do we monitor our supply chain for vulnerabilities and risks? Should we expect more from third parties in terms of monitoring their risks and sharing information about their vulnerabilities?
- Do we need to increase our early detection capabilities?
- Are we overlooking opportunities to decrease our attack surface?
- Are our table top and scenario-planning exercises keeping pace with increasingly sophisticated threats?
- Is our team prepared for and attuned to new threats? How can we increase our team’s capabilities when cyber talent is in short supply?

According to one subject-matter expert, there is cause for optimism, said. Near real-time visibility into vendor risks is already within reach. “Democratized data is now allowing us to look outside our networks and into third-party networks—and we should be sharing that data with our peers,” he said. This kind of innovation can be transformative.

A call for collaboration

By collaborating more broadly with others with the common goal of securing the enterprise and its ecosystem, CISOs can play a responsible role in helping their smaller partners to beat cybercrime, while strengthening their own enterprise.

"Collaborative conversations with regulators can help," a CISO said. Engaging with user groups can also be worthwhile, although it was noted that not every vendor offers the transparency customers would want. Another CISO said the software industry should be encouraged to set standards to deliver data-driven insights about risks and threats.

Accenture made a commitment to the ACF to work with its vendors to increase visibility into their risk postures. The goal is to work through legal constraints and other barriers to share information that can help all enterprises increase their supply chain security.

Suggested leading practices

CISOs and subject-matter experts offered a variety of suggestions for strengthening CISO leadership capabilities and protecting the enterprise from third-party risks, including:

- Establish collaborative security efforts. Supply chain partners must work together more closely to identify, protect, detect, respond and recover from increasingly sophisticated supply chain attacks. However, it is important to keep realistic expectations of partners' security capabilities. For example, one CISO said the Malaysian government is encouraging collaboration, but it is often met with reluctance by partners.
- Strike a balance between technology and leadership skills that fits the needs of your enterprise. "If I had to pick," said a subject-matter expert, "I'd suggest leaning toward leadership and having great technologists on your team."
- Partner with the rest of the business to build security into business strategy from the start and strengthen enterprise resiliency. Align cybersecurity with enterprise risk management practices. Enlist the rest of the organization in increasing cyber resilience and keep the focus on business outcomes. "The CISO faces a unique challenge in getting the rest of the organization oriented toward the security measures that are necessary in a changing threat landscape," said a subject-matter expert.
- Focus on building trust. Give senior management specific options with pros and cons to drive executive buy-in.
- Reevaluate supply chain partner relationships. This may require asking more pointed questions about their cybersecurity capabilities; renegotiating shorter-term contracts and audits; and avoiding serving the role of security provider to partners, given that CISOs don't have clear visibility into partner environments.
- Stop leading executive cybersecurity discussions with talk of tools and technology. CISOs should take on a greater leadership role by having a deep understanding of the business and speaking in terms that resonate with senior leadership and the board.

- Abandon any “arrogant expectations” about funding that have arisen in times of expanding budgets. Focus instead on delivering business value.
- Start aligning more closely with the corporate risk management function. Since technology is a key enabler of digital transformation, the CISO needs to emerge as an enterprise risk leader. Start sharing threat intelligence with partners, peers and law enforcement. Collaborative transparency is a key to supply chain protection.

Conclusion

APAC CISOs agree with Accenture’s *Third Annual State of Cyber Resilience* report that concludes: “With two out of five cyberattacks now indirect, organizations must look beyond their own four walls to their broader ecosystems.” CISOs are right to expect greater assurances from their supply chain partners about how they are contributing to enterprise security. But they also see value in collaborating to create those assurances.

In addition to exerting leadership in strengthening the supply chain, APAC CISOs also need to feel comfortable demonstrating leadership in the boardroom and the computer room. The role today is as much about business resilience as it is asset protection. In this new threat landscape, building executive trust requires delivering value and communicating effectively.

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 514,000 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 www.accenture.com.

About Accenture Security

Accenture Security is a leading provider of end-to-end cybersecurity services, including advanced cyber defense, 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.