“Third- and fourth-party risk management: A perspective on leading practices”

The Accenture Cybersecurity Forum (ACF) convened a virtual roundtable titled, “Third- and fourth-party risk management: A perspective on leading practices,” on March 4, 2021.

During this roundtable we explored the challenges facing CISOs in securing the supply chain and the extended enterprise. Do we need better breach identification and communications methods? What should we be asking of our vendors? What about contracts and enforcement? Do we need to improve business processes, incentives and penalties?

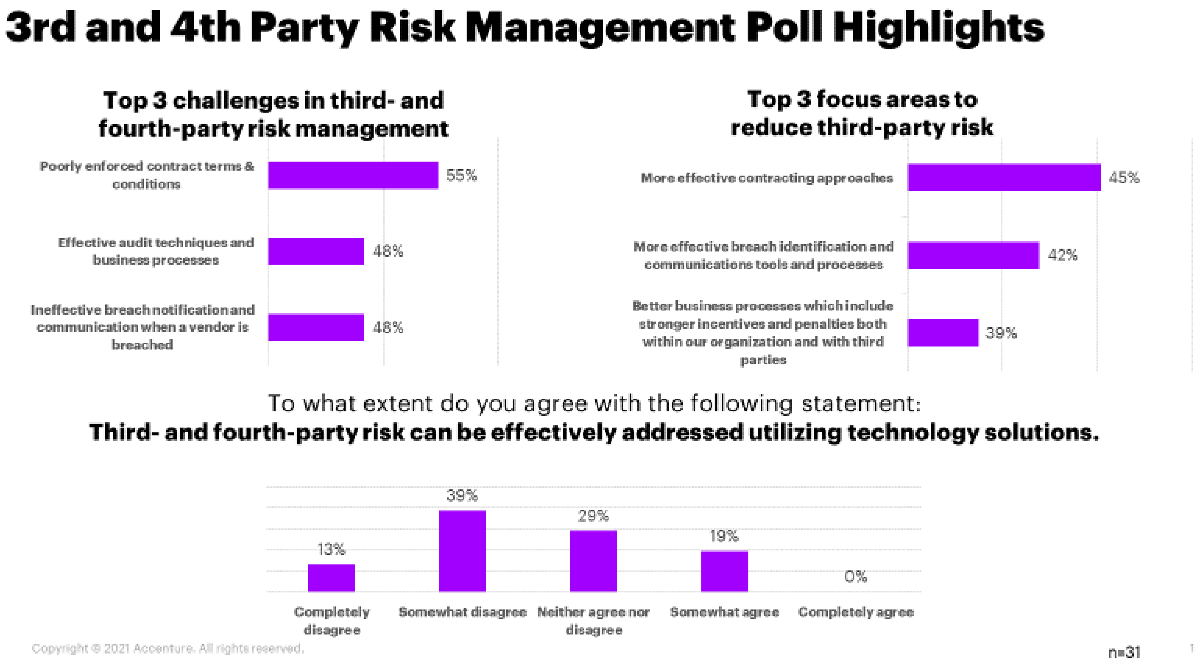
Our speakers included Accenture Security subject-matter experts, peer CISOs and board members. The session was hosted by Kris Burkhardt, Accenture CISO and ACF chair.

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.

Vendor risks a top concern

While CISOs have long been attuned to third- and fourth-party risks. As a CISO said, “It’s not a matter of if, but when third- and fourth-party risks will impact your enterprise.” Now, boards of directors are becoming more interested in this issue. Their concerns are driven by a variety of factors: significant reputational and operational risks, high profile reports of bad actor behavior in the media and unfamiliarity with the issues. As a board member said, “When you see a graph of board concerns, cyber is always in the upper-right quadrant.”

A survey of ACF members revealed that the top three focus areas to reduce third-party risk include more effective contracting approaches (45%); more effective breach identification and communications tools and processes (42%); and better business processes which include stronger incentives and penalties, both within the enterprise and with third parties (39%). A high-level overview of the survey finding is below, and the complete results can be found here.



3rd and 4th Party Risk Management Poll Highlights

Top 3 challenges in third- and fourth-party risk management

Top 3 focus areas to reduce third-party risk

To what extent do you agree with the following statement:
Third- and fourth-party risk can be effectively addressed utilizing technology solutions.

n=31

1

Evolving vendor relationships

Increasingly complex supply chain ecosystems, driven by a shift from asset-centric models to customer-centric models, are creating new points of vulnerability. Some estimate that as much as 40%of cybersecurity attacks are now occurring indirectly through the supply chain. In this environment, CISOs are driving changes in vendor relationships.

For example, a CISO recommended a multi-pronged approach that starts with tiering vendors in terms of strategic value and enterprise resiliency. That tiering should not be a static exercise, she said. Because relationships evolve as vendors move between tiers, her team conducts annual assessments and adjusts standards and compliance requirements. Using technology to map vendor relationships can be useful, she added.

The same CISO recommends trying to avoid adversarial relationships, particularly with smaller vendors. "Rather than just give them a list of requirements, invest the time to bring them along, help them understand your objectives and be open to compensating controls," she said.

She emphasized that strict, structured contracts have their place. For example, her enterprise has sued for breach of contract and terminated relationships when vendors weren't forthcoming about breaches.

"Compliance does not equal security," said a CISO. Another CISO added, "Often regulation drives the wrong behaviors. It becomes a compliance exercise rather than managing risk and being collaborative with key partners."

A subject-matter expert encouraged using incentives to drive vendor behavior. "Incentives such as early payment and premiums can change the dynamic of the relationship," he said.

Other CISOs endorsed the idea of partnering with vendors on threat intelligence. Work with them to set up effective monitoring systems. Understand that, in the throes of a stressful breach, notifying customers immediately may not be a top priority. “None of us are immune to attacks,” said a CISO. “Stigmatizing vendors isn’t productive. It’s better to make vendors feel comfortable about disclosing threat intelligence quickly.”

A subject-matter expert said, “We need a best practices framework for breach notification. While the announcements are painful, we have to reward those that do a good job on notifications and we need some level of market forces to work here because otherwise we will always defer to regulation, which is the bare minimum.”

Because the enterprise is always in a reactive mode when it comes to threats, a foundational set of controls is essential, said a CISO. You must be ready, for example, to quarantine data quickly. CISOs said that attracting and retaining the talent needed to maintain adequate controls is often a challenge.

Views are mixed about how the public sector can contribute to managing third- and fourth-party risks. Legislation can’t keep pace with nimble, resourceful threat actors, said a CISO. “The goal posts keep moving,” he said. Another called for supply chain security guidelines and principals similar to ISO/IEC 27000. The possibility of incorporating supply chain cybersecurity requirements into the European Union General Data Protection Regulation (GDPR) was also discussed.

Leading practices

- Maintain an accurate third-party vendor inventory. Other departments should contribute to this effort. A subject-matter expert said, “This is not only a responsibility of the CISO or the contracting department. It’s a responsibility across the entire enterprise.”
- Review risk tiering regularly as a vendor’s strategic importance may shift.
- Create incentives for collaboration and disincentives for non-compliance via contracts and interpersonal relationships. One CISO noted, “Potential lawsuits are not a sufficient deterrent for smaller partners when intellectual property is involved. You'll pay more in legal fees than you'll get back. The damage is already done.”
- Conduct regular vendor audits and contract reviews, at least for tier one suppliers. CISOs acknowledged that this can be time-consuming and difficult, but still important. “You need to distinguish between those companies that are forthcoming and those that are reluctant to disclose threats,” said a CISO. “We all have to acknowledge that some vendors will purposefully withhold information.”
- Ensure that vendor security priorities mirror your enterprise. A CISO has monthly conversations to monitor vendor progress on complying with security requirements. “Ultimately, the vendor sees that this effort is making their own products better,” he said. “But you need to dig deeper into the details.”

- Technology will never be the sole solution, but third-party risk management platforms and IT vendor risk management tools may be appropriate in certain situations as data points in a broader assessment process.
- Collaborate with peers. A subject-matter expert sees value in creating an independent information clearinghouse for disclosing vendor security practices.
- Building trusted relationships with board members who can act as cybersecurity supporters is critical. Anticipate the board's needs before a crisis occurs. A CISO said, "Leverage board relationships to get input and create champions that will support you when the need arises." A board member added, "When a vendor breach becomes public, the board's first reaction is 'Are we going to get rid of them?' That's the wrong question. Having deeper, offline discussions with tech-savvy board members can help a lot."
- A CISO added, "Equally as important as the board's understanding is your executive management's understanding. Does each direct report of your CEO know how much of their business outcome value chain is dependent on resilient operations by third parties? Which ones are in the top five?"

Conclusion

The points of security vulnerability for connected enterprises will keep growing and changing. That's why supply chain security is now an urgent priority for the CISO, the C-suite and the board of directors. In response, many CISOs are taking a more holistic view of supply chain security. They are applying new ways of working with third- and fourth-party supply chain partners to increase threat visibility and mitigate risks. They are applying incentives as well as traditional punitive measures to drive behavioral change. Some enterprises are actually helping their suppliers improve their security posture. While not a panacea, technologies such as intelligent automation are being tested and evaluated.

Ultimately, when it comes to managing third- and fourth-party risks, the CISO can't go it alone. Shared responsibility and accountability—within the enterprise and across the supply chain ecosystem—are required to keep the enterprise safe.

CONTACT

Kris Burkhardt

Accenture Chief Information Security Officer

Accenture Cybersecurity Forum Chair

LinkedIn

About Accenture

Accenture is a leading global professional services company, providing a broad range of services and solutions in strategy, consulting, digital, technology and operations. Combining unmatched experience and specialized skills across more than 40 industries and all business functions—underpinned by the world's largest delivery network—Accenture works at the intersection of business and technology to help clients improve their performance and create sustainable value for their stakeholders. With more than 514,000 people serving clients in more than 120 countries, Accenture drives innovation to improve the way the world works and lives. 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.