The CISO and audit committee: A discussion of best practices

The Accenture Cybersecurity Forum (ACF) convened a virtual roundtable on July 15 to discuss "**The CISO and audit committee: A discussion of best practices**." We explored how Asia Pacific security leaders are collaborating with their management and governance teams to respond to the COVID-19 disruption—and how they plan to move forward in the next 12 months.

What is the board's perspective on cyber risk and the cybersecurity function in the current environment? What makes for an effective CISO/audit committee relationship? If we could define two or three best practices for a productive relationship with the board and audit committee, what would they be?

Our subject-matter expert was an executive with an extensive career in enterprise technology who has served on several boards and is currently on the audit committee of the board of two publicly traded companies. The session was co-hosted by Andy Vautier, Accenture CISO and ACF chair; and Andrew McLauchlan, Accenture Security managing director and 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 disruptive nature of the pandemic

The COVID-19 pandemic has accelerated the need for changes in security practices. Enterprises have been forced to enable working from home, consider new business models, and respond to escalating threats and supply chain disruptions. Employees are often challenged to comply with new security requirements. As a result, the operational effectiveness of cybersecurity defenses has been stretched thin in many enterprises.

Boards of directors are acutely aware of heightened cyber risks and are relying on CISOs for leadership. Because the impacts of the disruption may extend for some time, many boards will also expect to hear about a long-term approach to keeping cyber defenses strong.

Board expectations

Transparency is one hallmark of productive CISO/board relationships. The board wants to know where the enterprise stands in managing cyber risks. Explain the steps being taken to address risks across the dimensions of people, process and technology. Present key information clearly and honestly. Try to anticipate questions and prepare in advance. When responding to questions you can't answer, indicate that you will get back to the board with answers.

Engagement is also important. Board members want to engage in a dialogue and ask questions about the cybersecurity status of the enterprise. They want regular updates, typically orally. And they don't want to be read the materials. Board members have a fiduciary responsibility to pre-read materials and don't want to cover the same ground in a presentation that will usually be limited to 10-20 minutes in a four-hour committee meeting. Be precise and cover the items of most importance to the business agenda.

Reinforce the confidence that your board has in you. Assure the board and audit committee that you are addressing risks by clearly summarizing how cybersecurity investments are protecting the enterprise and how you are keeping current on the threat landscape. Focus on the challenges you are facing, what you are doing about them and how you are making progress. Talk in terms of financial and reputational risk. Meet deadlines or risk losing the confidence of the board. Avoid jargon; consider listing acronyms in an appendix to the printed materials that are distributed before a meeting.

External validation can elevate the board's understanding. Benchmarking can help the board understand how the CISO is building resilience to address risks. Benchmarks can be based on direct competitors, industry peers or companies of similar maturity.

Build an ally on the board. One-on-one conversations with the audit chair, outside of the formal board setting, can strengthen relationships. Having conversations outside the board meeting can be very productive because you can go deeper on complex issues than you can during the meeting.

CISOs shared a variety of opinions about reporting relationships. In many enterprises, reporting to the audit committee is most appropriate. Where digitization is integral to every aspect of the enterprise, the CISO could report to the COO or chief security officer (CSO) rather than the CIO.

Rationalizing cyber investments

Answering the board's questions about the right level of investment in cybersecurity cannot be reduced to a simple formula or standard percentage of the overall IT budget. The answer is contingent on a variety of factors, including industry, level of maturity, an analysis of risks, and a validation of the consequences of those risks. To promote understanding and demonstrate that cyber investment improves resilience, consider offering data such as:

1. External validation, including peer benchmark data
2. Analysis of the current and emerging threat landscape
3. Tabletop exercises and use cases
4. Definition of key performance indicators in ways that are relevant to the board—in terms of finances and reputational risk

Governance of cybersecurity responsibilities, including budget, is an important issue. Some CISOs advocated managing the IT and security budgets separately. CISOs need to control their own destiny, ask for the investment they need to protect the company—not for a percentage of the IT budget—and be accountable for the maturity of the security organization. Avoid "splintering" responsibility too thinly across multiple budget owners.

The CISO's path to board membership

CISOs who aspire to board service must understand the oversight and governance role and responsibilities of a board member. Board members are responsible for overseeing the business, not for managing it. In addition, learn more about your own company's board. Ask questions of the CEO and CFO to understand what goes on in your company.

Best practices

CISOs discussed several effective ways to interact with board members and the audit committee:

1. **The power of soft skills**—Be transparent about risks and remediation. Encourage questions. Recruit board member allies by engaging them outside formal meetings.
2. **Use metrics that matter in budgeting**—Speed and agility are among the metrics that matter during the pandemic; think of achieving results in days and weeks rather than months or years. Focus on the business impacts of investments and discuss financial and reputational risks.
3. **Understand the board's charter**—Learn how your board works and how their oversight obligations differ from the management responsibilities of C-level executives. That understanding can also be useful in pursuing your own board aspirations.
4. **Establish independence of action—**CISOs should strive to have the credibility and authority to promote what's necessary to protect the enterprise, regardless of specific reporting relationships.

Conclusion

Cybersecurity is a major board concern, and CISOs are on center stage. Boards view cybersecurity as a significant source of risk, particularly in the current environment of sweeping changes in operating procedures, financial condition, threat landscape and business strategy. CISOs can help the board meet its risk management and oversight responsibilities by being transparent, promoting dialogue, meeting deadlines, and guiding investment decisions that impact the metrics that are most important to the organization. Despite, or perhaps because of, all the challenges, it's a great time to be a CISO.

CONTACT US

Andrew McLauchlan
Managing Director and Asia Pacific Lead
Accenture Security
andrew.mclauchlan@accenture.com

Joseph Failla
Managing Director and Australia/New Zealand Lead
Accenture Security
j.failla@accenture.com

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 509,000 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.

Visit us at www.accenture.com

Follow us @AccentureSecure
Connect with us