The CISO and audit committee chair: A discussion of best practices

On June 24, the Accenture Cybersecurity Forum (ACF) convened a virtual roundtable, "**The CISO and audit committee chair: A discussion of best practices**."

The COVID-19 disruption is presenting new challenges for CISOs and boards of directors, including the audit committee chair. What is the board's perspective on cyber risk and the cybersecurity function in the current environment? Are we seeing greater collaboration between the CISO and board? How can CISOs foster and maintain an effective relationship with their boards?

Paula A. Price, chair of the audit committee of the board at Accenture, served as our subject-matter expert. The session was hosted by Andy Vautier, 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.

The pandemic's impact on CISO/board relationships

Cybersecurity has gained increasing board attention in recent years. The COVID-19 disruption has added a new layer of complexity to the board's cyber risk concerns. For example, having employees work from home has raised serious questions. What are the implications and risks, and how does leadership regard these risks relative to its risk tolerance?

Board members recognize that changes brought on by the pandemic are also presenting opportunities, such as new lines of business and revenue streams. Boards are asking about the risks and how the enterprise is managing them. The role of all risk constituents, including the CISO, is to figure out how they can best manage that risk to an appropriate risk tolerance.

What does the board expect from the CISO? It starts with trust and confidence in the CISO's ability to lead the organization. While the entire enterprise has responsibility for cybersecurity, boards rely on the CISO to be the subject-matter expert and leader, and to stay abreast of emerging risk management best practices. Board members expect accountability, knowledgeable forecasts and information that is relevant to strategic context.

However, it is appropriate for CISOs to look to the board to help promote a security-first mindset across the entire management team. In Accenture's case, board buy-in was facilitated by a comprehensive half-day cybersecurity discussion. The board has helped embed cybersecurity accountability across the entire enterprise.

Effective communication with the board

A major CISO responsibility is to educate the board on the cybersecurity landscape and its implications for the enterprise. But frequent communications should occur in both directions: The CISO must keep the board well-informed while the audit committee shares its perspectives with the CISO. Effective communication practices include:

1. The simpler, the better when it comes to educating the board, one of the CISO's primary responsibilities. Avoid jargon; use straightforward business language. Keep strategy front and center.
2. CISOs can build trust by demonstrating subject-matter expertise and transparency. Be willing to discuss how risks are being managed and risks the enterprise may not be prepared for. The CISO's responsibility to the board and the enterprise is to help manage risks as effectively as possible.
3. Engage in regular, structured and intellectually rigorous conversations with the board.
4. A similar cadence of conversations with other members of the executive team (such as COO, CFO and director of internal audit) can help the CISO prepare for board meetings and build alignment on key messages to the board.
5. One-on-one conversations with the audit chair, outside of the traditional board setting, can strengthen the relationship. Even a 30-minute discussion can be tremendously valuable.
6. Help the board ask the right questions. Seek opinions on one or two questions at every board meeting. Asking other leaders for their perspectives is an effective way to build relationships.
7. Be proactive in addressing board concerns when cybersecurity issues and events are covered in the news. Most board members are avid readers and will likely be aware of major cyber events. Help them put news coverage into context and understand the "so what?" that makes a news story relevant to the enterprise.
8. Target board presentations to the level of the board member who knows the least about cybersecurity issues.
9. Storytelling can be a particularly productive means of communication. It can help board members learn 1) how cybersecurity issues in the news relate to the enterprise; 2) how external issues might affect peer companies; and 3) how those issues will impact the enterprise specifically.
10. Boards typically prefer quantifiable data, but they understand that quantification is not always possible, particularly when evaluating reputational risk. Offer information that helps to contextualize the "so what?" of an issue or event. How important is it? Help board members think about the topic in context.

Charting a path to board membership

As cybersecurity has ascended on every board's agenda, CISOs now have more opportunities to be invited to join a board. It is helpful to have someone on the board who understands cybersecurity issues. Some boards may even establish a cybersecurity committee.

Suggested actions for aspiring board members include:

1. Prepare a one-page board member resume or curriculum vitae detailing the skills and experience you can contribute to a board and a particular committee.
2. Let executive recruiters, other board members and colleagues know of your interest in serving on a board.
3. Check with your enterprise about any policies related to outside board membership.
4. Be patient. Board member searches often take more time than those for corporate positions.

Conclusion

Given changes in operating practices, financial condition, the threat landscape and strategy, cybersecurity is a top board concern. CISOs can help the board and management team "get on the same side of the table" when it comes to cybersecurity by communicating simply and regularly, with empathy, intellectual rigor and a commitment to transparency—all in the context of the business and risk. Help board members put change into perspective when it comes to cybersecurity, risk and business strategy. Enable the board to fulfill its role of expecting everyone in the enterprise—not just the CISO—to be accountable for cybersecurity and risk management.

CONTACT

Andy Vautier

Accenture Chief Information Security Officer

Accenture Cybersecurity Forum Chair

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.