Being a Cultural Influencer in Your Organization

Over time, the CISO role has evolved from one focused on protection and strengthening defenses to being a partner to the business and influencer for security. As such, the CISO must hone new skills to help shift their organization's culture toward one that embraces security at every level. Fostering this culture requires support from the Executive Management Team and Board of Directors. These leaders must establish the tone from the top and model behaviors to create and sustain a security culture.

On July 27, 2022, Accenture Cybersecurity Forum (ACF) Women's Council met for a virtual roundtable discussion on tactical practices for CISOs and their teams to gain the support of their leadership to make security a priority and ensure its persistence across the enterprise. The meeting included women cybersecurity leaders and board members, male allies, and emerging leaders from various industries. Leadership development trainer and positive psychology consultant Trish Omoqui moderated the discussion.

The roundtable was conducted under the Chatham House Rule: ACF members are free to use the information shared, provided they do not reveal the identity nor the affiliation of the speakers or participants.

The following is a high-level summary of insights shared during the 60-minute session.

Building a Strong Security Culture
The discussion started with a poll to understand what words and phrases attendees felt described a strong security culture. Agility, accountability, and partnership were the most often cited attributes.

How do you foster those qualities in an organization?

- Practice what you preach. A CISO shared that to encourage broader collaboration in her

What are the attributes of a strong security culture?

collaborative
challenge the status quo
awareness
communication
engagement
partnership
ownership
agility
accountability
change ready
embedded
responsibility
clarity
trust
agile
communicative

organization she began an effort to solicit ideas for innovation from everyone in the company. Good ideas are built and then showcased to recognize the people who brought the ideas forward. The effort has reinforced the message that everyone's contributions are important no matter their level or background in the organization.

- Ensure training is frequent and ongoing. Security training should not be an annual compliance effort but rather delivered regularly to engrain security awareness into the everyday culture. Short videos focused on topics tied to the current threat landscape or internal issues, such as phishing emails or password use, are more effective than classroom learning and long, multi-topic sessions. In addition, posters and digital signs in the workplace are helpful reminders.

- Make training interesting. Another CISO volunteered that her team participates in escape rooms with business teams to educate them on security issues creatively.

- Have a security contact. Employees should know whom to contact should they have a security question or concern.

- Broaden your engagement. A CISO of a global organization shared that she has designated security champions at the regional and country level. They host regular meetings with individual sites to discuss cyber topics and solicit feedback as they roll out cyber security initiatives. This approach helps reinforce that each person has a personal responsibility in the company's security efforts.

- Share your metrics. Another CISO offered that she hosts monthly forums with business leads to share cybersecurity trends and the organization's performance.

How Strong is Your Culture?

- Data-driven approaches, such as tracking and monitoring vulnerabilities, will show you how the organization and/or a business area thinks about security. Phishing tests can show how specific groups respond and measure what is and is not working. Application security issues can be tied back to an application's design, which can support security by design training.

Engaging With Leaders (Especially Those Who are Resistant)

- Have a data-relevant conversation. Understand what is important to their business and how security can impact that. Give them specific business examples and scenarios and position yourself as a business partner who is there to protect what matters to them.

- Leverage what is in the news. One CISO in the energy field pointed out, "Probably one of the biggest catalysts [for the business] was seeing other people in the news…it really increased their interest in going beyond what little was required."

- Approach from a different angle. If you present the business case and what you think is the right story, and it doesn't resonate, step back and consider a different angle. Your message needs to address their concerns and align with what they are trying to accomplish.

- Win over the CFO. When your CFO understands the financial impact of having poor security they can be a significant advocate for security and cultural change.

- Enlist your security champions. If you have business leads who fully support security, give them talking points and enlist their help to support your efforts.

CISO as a Cultural Change Agent

A final poll asked attendees to share what attributes they felt a CISO needed to be an effective change agent. Business acumen, risk taker, trustworthy, bold, and approachable were some of the more popular characteristics given. Attendees shared their views and techniques for garnering influence within their organizations.

What attributes does a CISO need to be a cultural change agent?

- Take time to build relationships. Particularly when your organization has had turnover or grown through M&A, CISOs/security leads need to spend time meeting with new business leads to understand their issues and where they are on the security journey. An effective way to build bridges is through coffees, cocktails, and conversations.

- Keep leaders informed. Leverage the knowledge of intelligence partners, e.g., law enforcement and ISACs, and share with leadership.

- Empower yourself. Confront any personal bias that execs are not interested in what you have to say. Don't be afraid to invite yourself to the table and be passionate about what you are sharing.

- Talk in their language. Draw in executives by inviting them to drive the discussion. One CISO shared she prepares leading questions to quick off her conversations with business leads, such as if we had a significant breach, what do you wish you would have known.

- Do not be afraid to be vulnerable. We need to be comfortable expressing that we're not always right and don't have all the answers.

- See yourself as a change agent. Understand you must shift people's mindsets, particularly if you work for a company whose culture has operated the same way for decades. These businesses are now being transformed by digital technologies and they must make security a priority.

- Engage with your board. Board agendas are getting crowded. If you aren't having frequent conversations with your board, they may become overly confident in the company's security measures. Regular exposure to the board helps build relationships, trust, and credibility. Furthermore, changes in SEC expectations support increasing engagement with the board.

Forum Contacts

Valerie Abend
Accenture Security Managing Director
ACF Women's Council Executive Sponsor

Lisa O'Connor
Accenture Security Managing Director
ACF Women's Council 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 674,000 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.