Managing Insider Risk

The Accenture Cybersecurity Forum (ACF) convened a virtual roundtable titled, "Managing Insider Risk," on December 10, 2020.

CISOs are concerned that both malicious and non-malicious employee behavior can threaten enterprise cybersecurity. How are CISOs successfully addressing insider threats? What are the priorities, both technologically and managerially? What's the right balance between the needs of the enterprise and the rights of the employee when addressing privacy?

Industry research suggests that while insider threats don't appear to be increasing, they aren't declining, either. What is different is that many CISOs are trying to develop more mature insider threat programs in response to the impact of digital transformations, remote working practices, different employee operating styles and customer expectations. Accenture Security subject-matter experts and peer CISOs discussed how leading security executives are addressing the challenges of optimizing insider threat programs.

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.

Where to invest: Process change or tech implementation?

CISOs believe that driving behavioral change can deliver the greatest value in defending against insider threats, particularly those threats resulting from non-malicious but negligent employee behavior. As one cyber expert said, "If I had an extra million dollars to spend on insider threats, I'd put it all on process."

One CISO proposed that, "insider threat programs should be rebranded as something more positive—that enables good people to do things even better." CISOs agreed that fear was an ineffective driver of behavioral change. A cyber expert stressed the importance of understanding why people are negligent. "This is not malicious behavior. People are stressed, they're tired. We have to take that into account."

One CISO outlined a more positive approach using a program to drive behavioral change that motivates leaders to turn security liabilities into assets. The core of the program is a "cyberscore" that measures the cybersecurity compliance of each team and employee across the enterprise. Because managers and employees don’t want to score lower than their peers, they take ownership of reducing their own cyber risks. “We’ve had 10,000 employees take the training, not because it was mandatory, but because they wanted to improve their cyber scores,” the CISO said.

Another CISO said they are exploring use of Professor Richard Thaler’s (University of Chicago; Nobel Medal Prize winner) Nudge Theory for behavior modification.

Conversely, CISOs expressed some frustration with technology intended to help automate insider threat defenses. ”Several CISOs said they were dissatisfied with the current state of tools such as User and Entity Behavior Analysis (UEBA). “The technology just hasn’t caught up yet,” one CISO said. Member CISOs expect that technology tools can continue to improve over time. It's worthwhile to monitor vendor innovations.

Balancing privacy and compliance priorities

Insider threats range from non-malicious activities such as misaddressed e-mails and sharing information inappropriately to malicious acts of fraud, espionage, sabotage and intellectual property theft. But balancing the risks of these threats with the risk of undermining privacy policies and culture is a challenging task.

CISOs are adopting a variety of policies to maintain levels of privacy right for their enterprise. For example:

- “We didn't get push back from privacy (about our surveillance practices) since the information is shared with just the individual and their respective leadership chain. We are careful to not share the information broadly unless it's aggregated.”
- “Our policies permit the use of monitoring user activities for the purpose of keeping our environments secure. For more sensitive monitoring (such as, data loss prevention), we limit it to a few users on our team.”
- “We ask for consent for monitoring but we use anonymized identities and have a workflow process to actually look at the real identity, only if the insider risk score crosses a threshold.”
- “We are working with a human behavior specialist in identifying red flags for early warning signs of high risk behavior, especially for intellectual property theft.”
- “I have been asked to alert management about suicide searches but have refused on privacy grounds.”

A cyber security expert said striking the right balance starts with asking some fundamental questions:

- What triggers an insider to do something bad?
- How do we see threats coming?
- What is our HR/privacy stance?

- Which areas should we focus on (such as, accounts payable, sales, Research & Development)?

Governance

Governing insider threat programs typically requires a multi-disciplinary approach, engaging the CISO, Legal, Fraud/Corporate Security, HR and business leaders. A CISO said, “Ongoing, active governance with privacy, legal, HR, and ethics, to help balance surveillance activities in pursuit of valuable outcomes is key to a successful insider threat program.” Another CISO said that managing insider threats is a strategic issue. “The discussion can drive how we think about the present and the future of the organization and culture. Maybe this points to ownership at a higher level of responsibility for organizational and culture change.”

Governance is still a relatively immature discipline. Several CISOs said their enterprises are presently working out the best approach for their situation. “It takes years to build a program,” said a CJSO. “And the organization needs to be ready for it. It took me two years to convince management we needed to start. But after a two-year journey, HR and Legal are my best friends.”

Recommended Leading Practices:

- **Increase “the will of the organization”** to elevate the importance of insider risk management. Leadership from a multi-disciplinary team and a positive approach to driving behavioral change can help the CISO establish a higher level of cybersecurity protection against both malicious and non-malicious threats. “Getting the rest of the organization to buy in is critical," said a cybersecurity expert. “The business needs to own the solution.”
- **Establish a governance framework.** “There can be tension about who “owns” the insider risk management program–the CISO, Legal, HR or Security,” said a CISO. ACF participants agreed that a multi-disciplinary approach is best.
- **Prioritize risks and establish a threat profile.** How much tolerance can the enterprise accept for non-malicious behavior? What assets are most valuable and require the greatest attention? What controls should be in place around the kinds of work people do? It’s important to prioritize controls in the biggest risk areas.
- **Be transparent and open to audits.** Consider red team testing of insider threat defenses.
- **Account for culture.** Robust insider threat management is more prevalent in industries such as defense and financial services; here, employees are familiar with background checks and other strict controls. In other industries, establishing an insider risk management program may take more time and more creative approaches.
- **Balance privacy and compliance.** Countries often have different regulations that affect the enterprise’s ability to drive employee behavior. Companies have to decide on the boundaries by which employee behavior will be judged (such as, social media activity, publicly available criminal records). Legal and HR need to help guide risk management program parameters and have policies in place for addressing risky behavior when it occurs. As a cybersecurity expert said, “Be prepared to deal with what you’re going to uncover.”

- **Suggested reading: "The CERT Guide to Insider Threats: How to Prevent, Detect and Respond to Information Technology Crimes"** written by members of the Carnegie-Mellon Software Engineering Institute. One CISO recommended it highly.

Conclusion

Threat actors are becoming more creative in exploiting insider vulnerabilities; for example, using ransomware and blackmail to convert employees into threat vectors. Work-from-home networks and mobile devices are contributing to a threat landscape that outside threat actors are trying to exploit and that often employees don't adequately secure. In this environment, CISOs are managing a difficult balancing act. They need to invest wisely in both process change and technology. Faced with finite resources, they need to focus on protecting the most important assets. They need to enlist other leadership allies to establish and maintain governance that is right for their particular enterprise. And they need to manage insider risks in transparent ways that respect employee privacy. CISOs agree, these challenges will remain top-of-mind for the foreseeable future.

CONTACT

Kris Burkhardt

Accenture Chief Information Security Officer

Accenture Cybersecurity Forum Chair

LinkedIn profile — here

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 506,000 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.