CMMI® Institute
AN ISACA ENTERPRISE

Withstanding the Shock of Continuous CISO Turnover

Amid a chronic skills shortage and high rates of turnover among security professionals at all levels—but among CISOs in particular—how can an enterprise maintain a consistent and resilient approach to cybersecurity?

Given the ongoing drumbeat of security breaches at major corporations and other institutions, the job of chief information security officer has become one of the toughest slots on the org chart to fill. This is, in part, because many CISOs don't have a long shelf life: The average tenure for the position is only about 24 to 48 months, with many packing their bags even sooner.[1]

The revolving door makes it much harder for businesses to protect their critical IT assets, according to a study by the Information Systems Security Association and analyst firm Enterprise Strategy Group. They describe the skills shortage as an "existential threat" to those companies that can't retain adequate cybersecurity talent.[2]

The government is worried too. At a recent industry conference, Mark Kneidinger, deputy director of the Department of Homeland Security's National Risk Management Center, termed turnover rates among agency CIOs and CISOs a "huge challenge" for government agencies. Six years ago, he noted, the average term of service was around three years, but currently it stands at 18 months or even less.[3]

A 'Personal Touch' Makes CISO Turnover More Painful

What makes the situation so painful, says Doug Grindstaff, SVP of cybersecurity solutions for the CMMI Institute, is that each new person who assumes the CISO position has his or her own way of doing things. Inevitably, a new CISO tends to introduce a whole new set of priorities, along with different opinions about what security model to put in place, the best tools and platforms to use, which technology providers are the most reliable, and so forth.

But, as Grindstaff observes, "CEOs cannot afford a 'flavor of the week' approach to their company's cybersecurity. The risks faced by the enterprise and its assorted business units don't change just because someone new steps into the top security role, and the organization's security strategy needs to reflect this no matter who's in charge.“

The only way to resolve this problem, Grindstaff adds, is to look beyond the role of the CISO and integrate a strong awareness of cyber risk into the corporate culture. This prompts the entire organization to assess and remain focused on the biggest risks facing the enterprise, regardless of who takes the helm.

Risk-Based Cybersecurity Strategy Should Transcend CISO Role

"As a CEO, you want to institutionalize your risk-based cybersecurity strategy," Grindstaff explains. "You want to treat it like a standard control model—a simple checklist that everyone throughout the organization adheres to." Such a model, he says, can be influenced by a new CISO, but not fundamentally altered.

To help companies determine their chief cyber risks and lay the foundation for a culture that's more security-aware, Grindstaff spearheaded the development of the CMMI Cybermaturity Platform. This cybersecurity self-assessment tool imposes a strict set of guidelines requiring every group and business unit within the enterprise to review potential cyber vulnerabilities, but granting each unit the freedom to manage those risks in the way best suited to its business requirements.

Cultivating a Security-Oriented Culture

Adopting this kind of framework breeds a security-oriented culture by formalizing and habituating risk-based cybersecurity thinking across the enterprise. It also helps the company withstand the shock of putting a new CISO in charge—and helps the new CISO get his or her bearings.

"You have to establish this type of culture in order to cope with revolving door personnel changes," Grindstaff argues. "If a new CISO is hired next week, that individual is now free to add value to the company without completely redefining its security strategy."

"This is a really important conversation to have with a CEO," he says, "because if the CEO thinks that a new CISO can just step into the role and elevate the company's security—well, that simply isn't the case. There's no magic bullet. The key is not, 'hey, this person knows these controls and is going to make sure we get our networks right.' It's about having cultural awareness and capabilities in place to protect the business."

But developing and institutionalizing such a culture takes time and persistence, and a new CISO "rarely has the time to map out a new 90-day plan and seed it through the organization," Grindstaff notes. Already having a standardized framework in place would give a new CISO the running start he or she needs.

Retaining Positive Outcomes, Not CISOs

CEOs need long-term plans for developing and sustaining their companies' cybersecurity programs that aren't based on any single individual. A successful and resilient cybersecurity program has to be culturally-driven, not personality-driven.

Given the realities of the job market, companies may not be able to retain their CISOs for the long term. But by leveraging the CMMI Cybermaturity Platform to help put risk-based cybersecurity cultures in place, companies can retain positive cyber outcomes.

[1] 'Why do CISO's change jobs so frequently?' *CSO,* https://www.csoonline.com/article/3245170/why-do-cisos-change-jobs-so-frequently.html

[2] 'ESA and ISSA Research Reveals Cyber Security Profession at Risk,' ISSA, https://www.issa.org/esg-and-issa-research-reveals-cyber-security-profession-at-risk/

[3] 'Federal CIO/CISO Turnover Rates Worries DHS Officials,' *MeriTalk,* https://www.meritalk.com/articles/federal-cio-ciso-turnover-rate-worries-dhs-officials/