Flexing the human component of cybersecurity

by

Slavomír Cyprich, Commercial Director, Aon Risk Solutions

David Dalva, Vice President, Security Risk Consulting, Stroz Friedberg, an Aon Company

Cybersecurity isn't just a technology risk, it's an enterprise risk—as such, it's everyone's business. But perhaps no one has more pressure to mitigate this risk than the Chief Information Security Officer (CISO).

We want to outline everyone with whom CISOs should develop relationships to improve an organization's cybersecurity. We will focus on the Chief Risk Officer (CRO), who is quickly becoming one of the CISO's most important partners in an organization.

CISOs that Partner with CROs Reduce Organizational Risk

It's imperative for a CISO to develop a tight partnership with the CRO, as both are managing aspects of the organization's risk. The first step is for CISOs and CROs to describe risk from their perspectives in a way that is meaningful to the other party. Only then can they effectively talk to each other about their needs and concerns and work in sync.

If a CRO and CISO aren't communicating effectively, the organization's risk profile can be unduly raised. Here's why: Cyber risk contains governance, operational, and technical components, which ultimately translate to financial risk. The impact to the organization, after all, can include business interruption costs, damage to brand, law suits, regulatory fines, and other expenses. CISOs are cyber security experts defending the company's business against evolving threats, as the organization's digital footprint expands to grow the business; CROs are experts at managing financial risk, with a deeper understanding of how to transfer that risk off the balance sheet to protect the organization from potential losses while enabling it to grow.

By closely aligning, the CISO and CRO can better help the organization manage its risk because their partnership can help leverage risk management resources more efficiently. For example, the CRO may be attracted to invest in a specific GRC tool (Governancne, Risk, Compliance tool) as means of managing risk, but the CISO may have a more detailed understanding of the costs involved in set-up and maintenance, how it aligns with the overall security risk management program, and may have a different perspective on the utility of such a tool to the organization. Both of their perspectives are important for making the right risk and reward calculation.

> "A proactive, pre-implementation approach is best to reduce risk.

CROs and CISOs also need to work together to draw up a strong cybersecurity insurance policy. It takes both of their perspectives to determine, among other things, what events could trigger a data breach, what triggers and losses can be covered, and what coverage limits would be appropriate for these triggers.

CISOs and CROs Best Reach the Board and Executive Leadership Together

Perhaps the biggest benefit of CISO and CRO partnership, though, is the education of senior leaders on the total risk of the organization. When CISOs and CROs work together, they can construct a holistic, realistic picture of company risk so that the board and executive leadership can better understand the focus of the teams managing the various components of risk. If the board must work to reconcile two different risk pictures—one technically-oriented and potentially difficult for them to understand and the other financially-oriented—the leadership is less likely to be able to help and respond to the true nature of the company's risk.

CISOs Should Support Innovators to Avoid the Reactivity Trap

Marketers, R&D leadership, and product managers are the company's drivers of innovation. They are likely to be the most active in terms of bringing new business-building technologies to the firm, and they're likely developing new offerings as well. For a CISO, understanding these innovations and why they're pursuing these advancements can help prevent the CISO from falling into reactive mode. When a CISO learns about a new offering after it's implemented, he or she must rush to plug the new exposure areas, often at higher cost. A proactive, pre-implementation approach is best to reduce risk.

CISOs Can Reduce Litigation Risk by Partnering with the Legal Team

A relationship with the legal team gives CISOs the opportunity to help reduce litigation risks by ensuring their security operations are set up to support any existing or expected legal obligations. For example, are the company's cloud-based services configured to produce responsive information in the case of a breach? Are contracts with third-party vendors updated on a regular basis to require updates to their information security? In addition, similar to the CISO's relationship with executive-level leadership, this relationship can help the CISO identify changes to what data should be treated as valuable.

A CISO's Strong Relationship with Compliance Executives Can Mitigate Regulatory Risk

Through a relationship with compliance executives, CISOs can discuss concerns about possible gaps in compliance, and can also learn about upcoming changes to regulations relevant to information security that might not otherwise rise to their awareness, such as shifts in financial or other regulations that could impact their work. This relationship also presents the opportunity to discuss the company's cyber security policy and training.

Three Benefits to CISOs Collaborating with Human Resources

A relationship with human resources pays off in three ways. One, it gives CISOs more awareness of possible insider threats lurking in the company and an edge in managing these politically sensitive issues. Two, CISOs can learn about new HR technologies and partnerships in the pipeline. Three, it can give them more feedback about the efficacy of new hire and staff training on information security issues.

It's ambitious for a CISO to develop meaningful and useful relationships with all of these individuals. But after putting in the effort to develop these partnerships, CISOs can better build an organization's cyber resilience and can identify opportunities where security can help the business grow.