The Global CISO: Why U.S. Leaders Must Think Beyond Borders

To compete for the top cybersecurity jobs on a world stage, home-grown CISOs need to take a more international approach to professional development.

Being the head of the cybersecurity practice for one of the global executive search firms gives me an ideal vantage point to see what companies are looking for in their next CISO -- and what the CISO talent pool is offering. Having those two constituencies in sync means a good fit between job candidates and positions, which in turn strengthens the collective security environment in which we all operate. When expectations start to diverge, not only do you have a great many frustrated people on both sides of the table, but cracks more readily appear in the world's cyber-armor.

That's why I can't help but be a little concerned when I look at the three searches I am doing right now for multinationals headquartered outside the United States, each in a different industry. As I talk with them about what they are looking for in their next CISO, I am surprised to hear a wariness of hiring an American for the role.

Given the fact that the United States is still the world's leading "producer" of CISOs, this is no small reservation. But the concerns are real. "We do business everywhere from the U.K to Central Europe," one told me. "Different jurisdictions, different cultures. We can't have an American walking in with a binary mentality and just shutting everything down."

"Binary mentality." When I heard that, I understood exactly what my clients were concerned about. To borrow terms from the accounting industry (which has a lot in common with cybersecurity), Americans are *rule-based* whereas Europeans are *principle-based*. Americans like things clearly defined, so that every possible case can be neatly fit into a predetermined category. Europeans are more comfortable with establishing general guidelines and working out the specifics as they go along. It's not that their standards

are lower; they just take a more flexible approach to getting where they are going. That's one reason that by one estimate, the U.S. tax code is eight times longer than the French tax code.

Translated to the world of cybersecurity, rule-based vs. principle-based might mean a different approach to structuring permissions or vetting new technologies. The important point isn't that my European-based clients are advocating for one over the other; it's that they want a CISO who can work in both environments and draw from each toolbox according to what's best for the organization within the local context. Unfortunately, few American born-and-trained CISO candidates have the global perspective and adaptability that is increasingly becoming a must-have in today's borderless economy.

Other business functions, as well as business operating units, have responded to globalization by including foreign postings as part of a rising executive's training. Ideally, global companies need to do the same thing for cybersecurity leaders. In the meantime, however, there are three things cybersecurity leaders in America can do to stay in step with a wider world:

Keep your bags packed. American cybersecurity leaders aren't only reluctant to consider job offers outside of the country; many won't even look beyond their metropolitan area. Increasingly, American CISO candidates will be taking themselves out of consideration for prime appointments unless they are prepared to relocate in the same way that other senior executives are expected to in the course of their careers.

Get mentored. If you are at a company with international reach, a good way to develop a global sensibility is to be mentored by someone for whom it is an essential part

of their job. That might be the head of a business unit, or someone like the CFO, general counsel or head of compliance, who has to operate across a range of regulatory regimes and sensibilities.

Look outside the office. If your company doesn't have the global footprint that can provide exposure to different cultural and regulatory systems (and even if it does), consider a volunteer leadership role for a non-profit or professional organization with an international mission. In addition to broadening your perspective, you will be expanding your network in ways that may bring unexpected benefits down the line.

The expectation that cybersecurity leaders can work across borders as do their counterparts in other functions is just emerging, but it will surely gather momentum as economies become truly global. Although developing a global perspective is a long-term undertaking, current and future CISOs who start now can help ensure that their professional development keeps pace with the needs of the talent market—an alignment that makes for better security for everyone.

Kal Bittianda, based in New York, focuses on technology and communications, specifically the systems, software & services, and digital segments. He also serves in Egon Zehnder's Private Equity and Financial Services Practices. Kal conducts executive search and provides leadership development services to help companies leverage technology to drive growth, transformation and innovation, while managing emerging leadership opportunities/challenges, such as Cyber Security and Big Data.

Prior to joining Egon Zehnder, Kal served in leadership positions at several privately capitalized, multinational, tech-enabled businesses. He built teams and led growth in North America for Kyriba (enterprise cloud solutions), EXL (knowledge and business process outsourcing), and Inductis (analytics consulting and services).

Kal earned an MA in Industrial Engineering from Purdue University, and an MBA from Harvard Business School. He actively serves New York area non-profits and early stage companies with pro-bono advisory and consulting support.