SECURITY & PRIVACY

Companies Need to Rethink What Cybersecurity Leadership Is

by Matthew Doan

November 27, 2019

Jorg Greuel/Getty Images

For businesses today, cyber risk is everywhere. Yet for all the investments they've made to secure their systems and protect customers, companies are still struggling to make cybersecurity a vibrant, proactive part of strategy, operations, and culture. The root cause is twofold: (1) Cybersecurity is treated as a back-office job and (2) most cyber leaders are ill-equipped to exert strategic influence. Given that a cyber leader's average tenure is just 18 months, it's clear that something needs to change.

Historically, companies have expected CISOs (Chief Information Security Officer) and security chiefs to focus on technical tasks — and haven't expected more of them. Cyber leaders have the monstrous and all-important goal of securing a business, but when companies make big, strategic decisions — about business models, digital strategy, product mix, M&A — cybersecurity is an afterthought. That means companies are losing out on the value that the function can provide. (It's not unlike the situation that many CMOs find themselves in.)

This approach was acceptable in the past, when threats were slower and less complex, but it is no longer sufficient. Today's cyber leaders must be able to embed security throughout the company's operations, rapidly respond to threats, and influence fellow senior leaders. In short, they must be able to *lead*. And that means companies need to hire and develop security executives who have the skills to do so.

It's time for boards and C-suite executives to reset their expectations of how cybersecurity is positioned and what a cyber leader is. Research being run by New America (where I'm a Cybersecurity Policy Fellow), paired with my observations from dozens of consulting engagements, suggests a framework for what business leaders must do to spur cybersecurity success.

1. Set your intent with cybersecurity strategy. What outcomes are you seeking? Since every business faces a unique risk portfolio, there is no one-size-fits-all approach. However, there are a few primary options that all companies should consider building their strategy around: business continuity, brand protection, compliance, and bottom-line growth. Your business context will drive your choices; you'll want to think about factors like regulatory pressure, risk exposure, and what customers value. For example, an electric utility company may prioritize business continuity to ensure the highest service uptime in a cost-pressured market, while an internet-of-things manufacturer may focus on growth, betting on cybersecurity's ability to be a differentiator and to justify premium prices.

Business leaders must thoroughly analyze their "why" for cybersecurity and be very clear regarding their choice. The chosen strategy will cascade down to operational activities, which will then drive business outcomes. You can't afford to be aimless or

generic with your cyber strategy — there's too much at stake.

2. Position the cybersecurity function to have influence. In this sense, "positioning" breaks down into location, authority, and incentives. It's easy to default to slotting cybersecurity within the IT function (under the CIO), but putting IT operations and security under the same roof, and on the same budget, can create problems.

Before deciding where cybersecurity will sit, determine the types of influence you want it to have. Businesses operate in sprawling ecosystems, where digital infrastructure and data are not neatly contained, and cybersecurity needs to be tailored to specific elements. For example, if your cyber needs are especially high in R&D, manufacturing, and customer support, you'll need to position the function for lateral impact. Giving the cyber leader and program proper authority is also vital; they must have political sway and a top-level mandate to orchestrate change across the business.

And lastly, since cybersecurity can't operate in a vacuum, business leaders need to incentivize the right stakeholders to work closely with the function. In the supply chain management department, for example, you might want cybersecurity "checks" to be part of evaluating potential business partners, while in the manufacturing unit you want to ensure that secure machines are being installed on the plant floor. A global pharmaceutical organization that I've worked with incentivizes "better" behavior by tailoring cyber KPIs to each business unit, creating healthy peer pressure that encourages executives to partner with the cybersecurity function, and establishing bonuses for those leaders whose departments do.

3. Get the right cyber leader for your needs. It's clear that the "who" matters for critical leadership positions, so it's worth dissecting which characteristics to look for. Boards and C-suite executives should prioritize mindset over technical skills when they're considering and evaluating cyber leaders. Looking at what successful cyber leaders do, mindset characteristics jump out, such as having an expansive worldview, understanding how neuroscience can improve leadership, being eager to grow others, and having a voracious hunger for learning.

This mindset stands in stark contrast to skill set — the supreme focus of the cybersecurity community to date. While organizations do require key cyber skills such as network security, threat intelligence, and incident response, these shouldn't be the yardstick used to measure cyber leaders. Yes, cyber leaders must appreciate these technical capabilities and have people to handle them, but the leaders themselves need to be something different: an influential voice in business strategy, technology decisions, and enterprise risk management.

To make this a reality, they must build tight relationships across the business ecosystem while structuring, growing, and empowering teams. They must translate abstract technical concepts into messages that grip senior leaders both logically and emotionally, and elicit their contribution. What this means is that, just as the best person to lead a digital transformation isn't necessarily a digital expert, your best cyber leader might be a proven non-cyber executive who knows the business, has key relationships throughout the company, and has a general appreciation for technology. It's your job to find this person and ensure they serve as an energetic and enduring force within the enterprise.

From the New America research and my consulting work, I've seen how this framework can help mitigate business risk, reduce friction with regulators, lay guardrails for technology and security, and increase competitive advantage. I've also seen that making tangible progress requires substantial top-down initiative from a company's leaders — otherwise the inertia is too great, and cybersecurity remains a back-office, noninfluential activity.

We're now beyond cybersecurity's "whack-a-mole" past of addressing one-off vulnerabilities. The function can — and should — be an essential ingredient to business success. But for that to happen, executives need to embrace their role in embedding cybersecurity across a company's entire landscape and developing the right leaders to make the function thrive.

Matthew Doan is a cyber and digital strategist at BCG Platinion, where he consults to top companies across the world. He's also a Cybersecurity Policy Fellow at New America. His passion is for solving problems at the intersection of technology and human dynamics.

This article is about SECURITY & PRIVACY

⊕ Follow This Topic

Related Topics: Leadership | Technology

/