A Constant State of Crisis: The new normal corporate security teams face and how they're adapting

Corporate security teams face a new normal, and it's called permacrisis – a state where instability and insecurity are constant.

While many security teams already operate in this mindset, the difference is that the security department is one of many teams in constant vigilance. As a result, departments across organizations are becoming aware of permacrisis and company boards are including specific security topics on their agendas to help manage risks associated with it.

"The board would pay attention to risks - broad enterprise risks - including financial and regulatory," Glenn Aga, Managing Director-Cyber at Deloitte, said. "For a security topic to rise to the board agenda, now that's something we're seeing that has been a big pivot over the last few years."

Given the volatile political environment and rising cultural tensions, company leaders want to understand specific threat topics. Understanding these threats help companies take proactive safety and security measures.

"I've got several clients who are very concerned about workplace safety, not just security of the enterprise, but for its employees," Aga said. "All of those topics come together, and they're now becoming a board agenda item, not just a risk that's traction report."

Chief Security Officers (CSOs) also respond to the new normal by tying potential security initiatives to a company's business objective. Specifically, using a section of the company's Form 10-K outlining risk factors (Part 1, Item 1A), CSOs can recommend proactive security initiatives to help stabilize the stock price, strengthen fiduciary responsibility, and increase stability in the supply chain.

It's the most difficult time to be in corporate security

Rachel Briggs, CEO of the Clarity Factory and a leading corporate security expert, said, "There has never been a more difficult time to work in corporate security."

Through her research, Briggs discovered three areas that make today the most difficult time to work in corporate security – change in external threats, digital transformation, and talent.

Change in External Threats

The threat level is at the highest it has been in recent years. Factors that contribute to the raised threat level are:

1. Geopolitics and external threats
2. A fast-moving and relentless industry
3. Bad actors are more sophisticated than ever before
4. Corporate security and the environment we work in are more complex

[INSERT CTA: STREAMLINING SECURITY OPERATIONS AMIDST GEOPOLITICAL TURMOIL WHITEPAPER]

Digital Transformation

Briggs also shared that 40% of global CEOs say that their company will not be economically viable in 10 years without a substantial change in their business model. The lack of technical skills and a generational shift in demographic contributes to this somber outlook.

Plus, some companies still need help with the post-pandemic reality of remote work. For example, corporate security teams must find innovative ways to protect intellectual property and other sensitive information outside the traditional office walls.

Obtaining and Retaining Talent

According to the World Economic Forum, the cybersecurity sector needs 3.4 million people to fill its workforce gap.

Along with finding talent, companies need to build a more diverse workplace – both in skill level and gender. For example, men make up 94% of today's global candidates. Plus, 70% of security professionals have a former government career.

Company leaders willing to radically change their talent strategy for what is suitable for tomorrow will put themselves in a different league above their competition.

Building Trust in Permacrisis

Keith White, Chief of Safety and Security for Salesforce, coaches his team to connect any security initiatives to the company's core business objectives.

"Everything that we do should have some type of relationship to something that [the board] sees as a top priority," White said. "And it promotes relevancy for your organization."

The pandemic proved an opportunity for corporate security teams, like those at Salesforce, to earn the right to be a strategic partner at the company's decision-making table.

Breaking Down Silos

Corporate security teams are taking on more roles than ever before. Once viewed as solely focused on guards, guns, and gates, security teams are now health and safety officers, security for employee travel, data and product loss prevention, and executive protection. The evolution of the role is part of this environment of permacrisis.

However, wearing more hats within a company is good news for security teams. Corporate security leaders can take advantage of this opportunity by breaking down communication silos and collaborating with other groups like HR, Legal, Marketing and Sales.

Leaders like White see measurable results after leading the charge to break down silos.

“Our connectivity is higher than it’s ever been before,” White said. “The evidence of that is, from time to time, we’ll have senior executives ping us about different markets that they want to explore, high-risk markets, and [ask] what’s our opinion and could we operate there?”

As organizations around the globe adapt to permacrisis, one trend is emerging that bodes well for corporate security – security is becoming a shared responsibility.

Accepting shared responsibility for risk and breaking down silos will be fueled by universal software technology and consolidated threat intelligence. Collaboration of these departments also enables holistic data analysis for deeper visibility, speedy decision-making and clear communications across multiple functions.

“We will begin to see more cybersecurity experts embrace physical security.” Chuck Randolph, Vice President of Security and Intelligence at Ontic, said. “This will be in the form of a rise of security practitioners who have knowledge of both the cybersecurity and physical security industries. This convergence of security-related knowledge will also lead more businesses to create a Chief Risk Officer role to address security holistically.”

What technology is your company using to see the holistic threat landscape? Are you focused on the right threats and avoiding the noise?

Looking for ways to protect your business operations during permacrisis? Download our whitepaper ‘Navigating Corporate Security Through Times of Chaos’ here.