Teneo®

The Global CEO Advisory Firm

Teneo Insights:

Six Imperatives to Help Drive Security Risk Management Programs in 2019

January 2019

As we usher in a new year and the promise of change, whether stemming from new administrations and legislation or new developments in business and technology, one thing is clear – the security issues we face, whether cyber or physical, are only increasing in complexity and prevalence. The year 2018 saw an onslaught of major data breaches, questionable privacy practices and an increase in severity and frequency of workplace violence incidents. The degradation of the Islamic State's so-called caliphate in Iraq and Syria has actually increased the risk of future attempts abroad to demonstrate their continued relevance. Despite a lull in more obvious activity, corporations need to anticipate that future attacks are not only possible, but probable. To be sure, and more than ever, 2019 is the year to adopt a proactive stance and embrace the old adage that 'the best defense is a good offense'.

In the corporate world, there are more than enough significant challenges pulling at leaders as they strive to meet or exceed targets and run a successful business. Add to that a daunting and ever-changing landscape of security challenges, and it's no wonder executives can be overwhelmed in trying to prioritize and make sense of it all. Fortunately, today's security market is rich with solutions – more and more of which are predicated on AI and 5G – and research firms predict total global security spend on both physical and cyber initiatives will surpass $200B in 2019. As you plan for your security deployments in 2019, we offer six key imperatives to serve as a backdrop to help you plan your own offensive strategy:

1. Help Your Humans Embrace AI

In the security services realm, AI is all the rage as companies look to inject more sophistication and technology into security risk management programs. However, many fear the advent of the robots means the end of the road for gainful human employment. But that's just not true. For example, robots, drones and facial recognition capabilities have a very meaningful role alongside their human counterparts, and in fact offer an avenue to reduce or eliminate the more mundane tasks associated with security programs in favor of more strategic and analytical initiatives. But it's all in the delivery. As you embark on an AI security implementation, bring a cross-functional team into the planning and design efforts. Let them articulate the current state pain points and inefficiencies and then use this cross-functional team to formulate ideas which build strategic programs around the AI. AI doesn't deploy itself, and there's no replacement for human experience. Smart executives will recognize that their employees' judgment and emotional intelligence are critical components in harnessing the power of AI's superior data analytics skills for new and unanticipated insights. Look to AI to be a force multiplier that empowers you and your people to do even bigger and better things.

Courtney Adante
COO,
Risk Advisory
courtney.adante@teneo.com

2. Peel Back the Curtain on Privacy

As data breaches and ransomware consumed the US market once again in the second half of 2018, customers and employees concerned about the security of their personal information have a renewed frustration and are looking to businesses for more protection and better solutions. In response, companies must develop and adopt transparent policies and clear information campaigns regarding personal and enterprise information management. The trick however, is that the competition is watching – emphasizing the importance of balancing privacy concerns with opportunities essential to maintaining an edge. Recognizing that both regulation and technology perpetually evolve, companies that approach and address privacy as an ongoing initiative rather than a discreet venture will be better positioned to gain and retain consumer trust, protect brand and respond in this perpetually-shifting landscape.

3. Commit to Building a Strong Security Culture

As companies increasingly look to improve corporate security awareness and manage risk in 2019, they must be sure not to overlook the very asset that is required to enforce and uphold it – your people! As tempting as it may seem, you can't rely on technology alone – it starts with the people who operate it. In today's world fraught with phishing scams, advanced social engineering tactics and an upward trend in workplace violence, your people, with their early warning indicators and human intelligence are oftentimes your greatest offensive strategy. And let's not forget the basic well-being of your employees. Something as common as the flu costs the global economy billions in healthcare and lost productivity – and, in extreme cases, lives. Those who don't take necessary precautions put co-workers at risk. To enable a security culture, executive leadership should commit to protecting the health, safety and security of the organization and advocate for security as a core mission to be owned by all. Enforcing policies and procedures and rewarding those who go above and beyond as security stewards are the hallmarks of an organization that fosters a collaborative security awareness culture. Without a strong security culture inclusive of both the carrot and the stick, employees can end up inadvertently, or worse yet, maliciously exposing the organization to unanticipated risk.

4. Recognize that Risks Don't Respect Borders

The world of business travel is evolving at a rapid pace, and while your employees may be preoccupied with making their flights to get to the next client meeting, savvy executives must recognize that safety concerns continue far beyond airport security. Tensions within and between nations are rising around the globe and the potential for violence is pervasive, whether it stems from a political protest gone awry or a premeditated terrorist attack. Acknowledging that there are few 'safe' destinations, companies with traveling employees must ensure they understand and have implemented appropriate travel safety policy and procedure guidelines in the context of 'duty of care'. These guidelines need to fully consider the range of precautions essential to inherent travel hazards, including regular evaluation of a destination's political and terrorist activity profile and the ability to track and communicate with your workforce in the event of an issue. Smart executives will balance risk against benefits of business travel and take precautions by working with their insurance companies, local contacts, and travel agencies to help get their employees to their destinations and safely back home again, even in the face of potential major incidents.

5. Prioritize Cyber Risk Management with Your Board

In 2019, the success and security of a company's business operations will hinge upon alignment of board and company-level priorities, particularly as relates to data assets and data management in an increasingly cyber-centric operating environment. Boards need to focus on oversight of their company's cyber risk management program, including being well-versed on the impact of regulations like the European Union's General Data Protection Regulation (GDPR) and evolving regulation in the US (such as the California Consumer Privacy Act to come into effect in 2020) and elsewhere around the globe. You can help your board help you in this regard by ensuring they and the rest of the organization understand the components of your cyber risk management program and its alignment within the context of your overall enterprise risk management framework. Further, ensure that you are reporting with appropriate metrics aligned with business objectives. Another way to help your strategy resonate with the board is to demonstrate how your cyber risk management program is an investment in the future of the company rather than another technology cost line-item.

6. Mind the Talent Gap

Security risk management is a 24x7 complex endeavor. We see the strain on our workforce, with security operations teams under more pressure now than ever before. Companies will need to make talent retention and acquisition a top priority in 2019. An overwhelming number of organizations already report a gap in high quality, available security talent, with cybersecurity talent in particularly high demand. Job-seekers, particularly the good ones, will have their pick of opportunities. To close the gap and retain the best talent, companies must offer more than a competitive paycheck. Surveys show that security professionals' desire to work where their ideas and opinions are valued as a key driver, in some cases over compensation. For these same people, a company that prioritizes the safety and security of the company and its people is a major factor in the decision to accept a job offer. This is a healthy attitude for employees and companies. If your people value the company, it is highly likely they would be motivated to protect it.

For questions about this article or to learn more about Teneo Risk Advisory, please email us at teneoriskadvisory@teneo.com.

Teneo

Teneo is the global CEO advisory firm.

Working exclusively with the CEOs and senior executives of the world's leading companies, Teneo provides strategic counsel across their full range of key objectives and issues. Our clients include a significant number of the Fortune 100 and FTSE 100, as well as other global corporations.

Integrating the disciplines of strategic communications, investor relations, digital advisory, diversity & inclusion, management consulting, physical & cyber risk advisory, financial advisory, corporate governance advisory, political risk advisory, and talent advisory, Teneo solves for the most complex business challenges and opportunities.

teneo.com