KPMG

The CISO's imperative

Building trust in security for 2023

The world feels very different than it did just a few years ago. COVID changed how we approach work and accelerated the shift to remote and hybrid models. Along the way, we encountered a new wave of cybersecurity risks, protecting against which has become a necessity for business survival. Just as we were catching up and securing our new IT environment, circumstances changed once more as geopolitical tensions created an increasingly polarized world. Looking ahead, we see further business, economic, technological and regulatory changes — and more disruption.

Unsurprisingly, the cyber threat landscape continues to evolve as criminals — both organized and state-backed — seek new opportunities to create chaos and extract profit. Cyber professionals, CISOs in particular, often feel as though they are running hard but making little progress.

We believe the most rational mindset for security teams is to acknowledge they'll never be able to protect against everything. This is a challenging message to communicate to executives. Organizations will likely always carry some degree of cyber risk and despite all due diligence, security controls can, and often do, fail. If companies try to protect against all potential risks, not only can the budget demand be burdensome, but the opportunity cost can be onerous given the impact of security measures on operations and business activities.

Perhaps the central aspiration for CISOs is to keep their organizations resilient as the cyber-attack risks grow. If a data leak or network breach occurs, how quickly can the company detect and contain the attack, resume regular operations, and minimize the impact on customers? This is emblematic of the resilience agenda we're seeing in the latest wave of regulation, particularly in the financial sector. Often the solution involves effective detection and response, rapid and prioritized system rebuild/restoration following disruption, and a focus on what really matters to the business. In the end, companies must strike a balance between investment in protective controls and improvements to resilience.

Our upcoming annual Cybersecurity considerations report brings a diverse cross-section of global KPMG cybersecurity specialists together to explore eight considerations that CISOs and their teams should prioritize in 2023 to help mitigate the impact of cyber incidents and protect the future of their organizations. Here's a brief preview of those considerations.

1 In times of uncertainty, trust matters

Digital trust is becoming a boardroom issue. People expect firms to act with honesty, integrity and transparency in the way they handle their personal information while providing robust digital services safely and securely. Sensing the public mood, politicians and regulators are acting to shape and challenge corporate behaviors. Leveraging our recent Cyber trust insights survey, the report will look into the practical actions CISOs and their teams can take to help frame the debate and play an integral role in building and maintaining trust.

2 Trust in automation

Our Cyber trust insights survey found that 78 percent of executives believe adopting sophisticated artificial intelligence and machine learning systems raises unique cybersecurity challenges, with many believing they also raise broader ethical issues. Creating a framework to support the security and privacy of AI-driven structures while also enabling rapid innovation and agile development will be key to harnessing the potential of these developing technologies. The report will explore how CISOs achieve these objectives in partnership with privacy and data science teams and how they help their firms prepare for a rapidly changing regulatory environment.

3 Unobtrusive security

Security is often perceived as a speed bump, adding complexity and cost to systems while simultaneously limiting functionality. Clearly, customers continue to rely on passwords, venting their frustrations as accounts are locked, causing tempers to fray. We often hear the "people are the weakest link" maxim, but is that really the case, or are our security systems unfriendly and unusable? The report will examine how security can be effectively embedded into the business, so it's not only unobtrusive, but intuitive, inspiring employees across the enterprise to be part of a human firewall.

4 Securing a perimeter-less future

To the extent a digital business perimeter still existed, COVID removed that illusion, forcing organizations to adapt to remote and hybrid working arrangements. Today's global, 24/7 businesses need help to truly define their perimeters as they've come to depend on a complex ecosystem of partners and suppliers, linked by cloud computing platforms. In this new reality, how can companies secure this highly distributed business model? The report will dig into the practicalities of implementing new trust paradigms and frameworks better aligned with the business models of tomorrow.

5 Security teams must change too

It can be easy to ignore the need for change in the security function itself, but to do so would be naive. Security teams are taking on very different roles today. The shared responsibility model brings new partnerships with cloud service providers; shifts to agile DevOps processes inspires new thinking on embedding security by design; and the security of the enterprise — and customers and business partners — now encompasses a far wider range of systems and assets, often outside the direct control of the CISO. The report will shed light on new security models, which treat security as a golden thread connecting all areas of the extended enterprise and the accompanying need for new skills.

6 Smart security for a smart world

Our world is becoming smarter as connected devices are embedded into every aspect of our lives, particularly the infrastructure that supports the digital and physical realms. From sophisticated operational technology (OT) and networked and ubiquitous sensors to autonomous systems and robotics, the development and operational environments are very different from the classic enterprise IT landscape. But, arguably, security matters even more with these new structures and the traditional divide between IT and OT is fading. The report will delve into how firms can embed a security mindset into these different environments and what regulators will expect of companies to enable infrastructure and product security going forward.

7 Countering agile adversaries

A few years ago, a week was a long time in cybersecurity. Today, a day can seem like an eternity when you are dealing with an agile and sophisticated attacker. As a security community, we have become far better at detecting and blocking new attacker tactics, working with technology partners to take down the infrastructure that supports the attack, and implementing active defense measures at the national level. But that requires security operations that can respond within minutes rather than days, quickly detecting anomalous and malicious behavior, applying containment measures and eradicating an attacker from the network. The report will provide an assessment of what the future security operations center and managed detection and response service might look like, as well as the role of machine learning, and the broader community engagement model.

8 Be resilient when and where it matters

Finally, despite all the best efforts, the worst can happen. In fact, it's likely inevitable. Resilience is fundamentally a business discussion, not just a security aspiration, and CISOs should resist the urge to assume responsibility for organizational security as their problem alone. Rather, CISOs and their teams can function as conveners, encouragers, and catalysts for that dialogue across the organization. CISOs bring a valuable perspective to these discussions as they seek to counter malicious adversaries intent on disrupting the organization. The report attempts to get inside that perspective analyzing the challenges of resilience in the face of a cyberattack and how organizations can best prepare.

As we head into 2023, our world remains fast-paced, challenging and fluid. Securing the enterprise remains as relevant as ever, but CISOs and their teams must be ready to adapt to new challenges. In doing so, the golden thread of cybersecurity is being woven throughout the business, touching every aspect of future strategic and operational planning.

Contacts

Koos Wolters

Partner

Head of Cyber Security & Data Privacy

KPMG Advisory N.V. - The Netherlands

E: wolters.koos@kpmg.nl

T: +31 20 656 40 48

Justin Black

Senior Business Development Manager

Cyber Security & Data Privacy

KPMG Advisory N.V. - The Netherlands

E: black.justin@kpmg.nl

T: +31 20 656 72 62

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

home.kpmg/socialmedia

Designed by Evalueserve.
Publication name: The CISO's imperative | Publication number: 138468-G | Publication date: December 2022