Cybersecurity considerations 2023

The golden thread

KPMG International

kpmg.com/cyberconsiderations

Foreword

Our future is dependent on data and digital infrastructure. The COVID-19 pandemic accelerated our shift to digital channels and brought these issues into sharp focus. As global economies, and supply chains were disrupted, organizations had to rethink their dependencies on goods, services and the digital infrastructure that underpins them.

Breakthrough technologies are expected to shape that future — artificial intelligence, blockchain, biometrics, hyperconnected systems and virtual reality, to name just a few. And all can pose new security, privacy and ethical challenges and raise fundamental questions about our trust in digital systems. Consensus on tackling those issues can be hard to arrive at with diverse national and cultural views; nonetheless, this is the environment in which global commerce needs to thrive, and we need to address concerns now as we innovate, not retrospectively when it's too late.

The list of industries we consider systemically important is also changing. In the past, we focused on utilities, telecommunications and financial services. Now we have a complex tapestry of public-private partnerships, connected ecosystems, and information infrastructures. One look at financial markets shows a hyperconnected world of financial institutions, market infrastructure, data and managed service providers — all of whom are now systemically important. As the degree of interconnectedness and dependency increases, so does the interest from those looking to attack and exploit those infrastructures.

With these changes comes a global drive toward greater cybersecurity regulation. This increases concern among organizations over the growing burden of regulation and the diversity of various reporting requirements. As a result, businesses are putting more and more emphasis on embedding privacy and security into how they operate, both in response to the changing threats and the need to comply with trans-border regulatory requirements.

Cybersecurity should be integral to every business line, function, product and service. Organizations must aim to ensure that cybersecurity is ubiquitous across the digital enterprise and woven into strategy, development and operations across the board. As Lisa Heneghan, Chief Global Digital Officer, KPMG International, says:

"Organizations need to start thinking about cybersecurity as the golden thread that runs throughout their organization. It should be put at the heart of business and used as a foundation to build digital trust. But the Chief Information Officer (CISO) and their teams cannot do this alone; it should be the responsibility of everyone. This isn't easy — first, people should understand how it relates to them — and then you must think about how you can integrate security into existing processes. Treating every business function as a customer and designing security controls with experience in mind can encourage responsible and secure behaviors and can benefit the business hugely."

CISOs will likely also play a major role in activating and shaping a broader dialogue around the resilience of business to digital disruption, helping companies better understand the evolving nature of the assets and digital services companies need to protect and providing the basis for trust in those systems.

The report explores the actions CISOs, specifically, and the broader business generally, can take in the year ahead to demonstrate to boards and senior management that digital trust can and should be a competitive advantage. See page 22 for specific people, process, data/technology, and regulatory recommendations.

Akhilesh Tuteja

Global Cyber Security Leader
KPMG International

Eight key cybersecurity considerations for 2023

Click on each consideration to learn more.

01

Digital trust: A shared responsibility

Are organizations thinking broadly enough about how to protect the interests of employees, customers, suppliers, and partners?

02

Unobtrusive security drives secure behaviors

How do security teams effectively integrate security into business processes, agile development programs, and disparate operating models?

03

Securing a perimeter-less and data-centric future

With the security perimeter all but gone, how can organizations pragmatically and realistically transition to a zero trust approach that protects every aspect of their ecosystem?

04

New partnerships, new models

How can organizations keep security, privacy and resilience at the forefront in an environment where outsourcing and managed services are a growing priority?

05

Trust in automation

What can organization do to help ensure robotic process automation (RPA), machine learning (ML) and other forms of artificial intelligence (AI) are implemented and managed effectively, sensibly, and securely?

06

Securing a smart world

What are the implications for security and privacy teams as companies shift toward a smart, hyperconnected product mindset?

07

Countering agile adversaries

How can security teams keep up with the pace of the changing threat landscape and the increasingly aggressive tactics of attackers?

08

Be resilient when — and where — it matters

Why is it important to think beyond response and proactively plan for recovery?

Consideration 1

Digital trust: A shared responsibility

Digital trust is finding its way onto Board agendas as privacy, security and ethics debates gain momentum — partly driven by regulation and partly by public opinion. The future success of any digitally enabled business is built on digital trust — cybersecurity and privacy are vital foundations for that trust. CISOs must be prepared to help the Board and C-suite create and maintain the trust of their stakeholders if they are to create a competitive advantage. Realizing this potential requires a collective commitment from all stakeholders.

Globalization has made the world borderless and interconnected — a reality made only too evident by the disruption to global supply chains brought on by the pandemic. To create lasting relationships with customers (whether B2B or B2C), organizations must establish and maintain digital trust.

> **Digital trust covers so many topics that touch every aspect of an organization and is inherently linked to corporate strategy — not just because it can create a competitive advantage, but because it is simply the right thing to do for the broader industry and society.**
>
> **John Anyanwu**
> Partner, Cyber Security Services
> KPMG in Nigeria

Value and trust

Trust is key to success — and is not just about reputation. Boosting trust can create competitive advantage and can add to the bottom line.

More than 1/3 of organizations recognize that increased trust leads to improved profitability.

But 65% report that information security requirements are shaped by compliance needs rather than long-term strategic ambitions.

65% of executives continue to view information security as a risk reduction activity rather than a business enabler.

49% believe that the Board of Directors sees security as a necessary cost rather than a way to gain competitive advantage.

Source: KPMG Cyber trust insights 2022.

Businesses are starting to care

Growing numbers of senior leaders recognize the benefits of digital trust, with 37 percent seeing improved profitability as the top commercial advantage of increased trust.[1] Digital trust encompasses a wide range of disciplines. Cybersecurity is a major part of that broad spectrum of closely linked digital trust-related issues — reliability, safety, privacy and transparency. These areas impact how companies conduct business and pursue values; the products and services provided; the technology used; how to collect and use data; and how to protect the interests of customers, employees, suppliers, and all other third-party partners and stakeholders.

By contrast, 65 percent continue to view information security as a risk reduction activity rather than a business enabler.[2] Many organizations still view cybersecurity primarily as a cost and not necessarily as an investment in the future, which is misguided. CISOs should embrace the concept of digital trust and demonstrate how security as an enabler for the business will securely support an organization's digital growth agenda.

CISOs have a significant role in helping their organizations build digital trust, but they cannot do it alone. They should invest sufficient time in encouraging other critical internal and external stakeholders with respect to their respective roles on the digital trust journey. Indeed, CISOs must demonstrate to the C-suite and Board why this is such an important topic and how digital trust depends on clearly articulated, business-focused strategies.

As the World Economic Forum (WEF) suggests, companies are beginning to acknowledge that cybersecurity is as much a strategic business element as enterprise risk, product development and data management. In its report, Earning digital trust: Decision-making for trustworthy technologies, the WEF writes, "digital trust requires a holistic approach, where cybersecurity is one dimension of trust among many."[3]

What digital trust means to customers

While the typical retail consumer may not care about the nuts and bolts of a company's formal data protection program, the moment customers learn of a breach, they want to know what action is being taken and that their interests are at the heart of the response. The organization can re-establish trust over time by responding to the incident expeditiously and transparently.

Today's consumers understand that breaches happen and, gradually, most come back if the company offers solid products and services at a competitive price point, there is a consistently positive customer experience, and the details around the response to and recovery from a cyber event are clearly communicated and reassuring.

> **Transparency means different things to different audiences. While retail consumers demand transparency when incidents occur, organizations must know in advance how the suppliers and partners they work with protect information. This is because organizations have a much higher obligation to customers and need to be certain they can deliver trust in terms of information protection.**
>
> **Henry Shek**
> Partner, Cyber Security Services
> KPMG China

[1] KPMG International, KPMG Cyber trust insights survey, "Building trust through cybersecurity and privacy," 2022.
[2] Ibid.
[3] World Economic Forum, Earning Digital Trust: Decision — Making for Trustworthy Technologies," November 2022.

Digital trust strategies that work

It's vital to embed the concept of digital trust into corporate strategy, product development, and the company's overall market presence and relationship with corporate and retail customers. Thinking broadly about what digital trust means across different stakeholder groups can help underline the importance of cybersecurity and the other disciplines that contribute to establishing and maintaining digital trust, as well as encourage a holistic approach across disciplines.

Trust is a function of specific technologies developed or deployed, and the decisions leadership makes. CISOs must continually support a narrative for the Board and C-suite to clarify why and how cybersecurity is an integral building block for digital trust.

> **Simply put, companies that are able to establish trust among all stakeholders in their products and services, and how they operate and protect the business, are more likely to see positive commercial and reputational impacts.**
>
> **Annemarie Zielstra**
> Partner, Cyber Security Services
> KPMG in the Netherlands

CISOs must help drive decisions around the right partners and suppliers. Qualifying criteria must be established covering transparency regarding information protection practices and the organization's ability to demonstrate adequate recovery and response resilience.

Make no mistake, regulatory obligations are expected to grow regarding the components of digital trust, and so can expectations over the levels of transparency and accountability regulators expect from companies in this regard. A principle-based and holistic approach to meeting the diverse and increasingly complex regulatory landscape can pay dividends and avoid creating costly compliance-driven silos.

It starts at the top and filters down — if leadership accepts and lives this narrative, so should the rest of the organization. That means making it a tangible feature of the company's annual report, in which the company's philosophy and strategy around digital trust by design are outlined in detail. With 34 percent of corporate leaders concerned about their businesses' ability to satisfy reporting requirements for greater transparency over cybersecurity and privacy, KPMG professionals advocate a proactive approach.[4]

Learn more

Cyber trust insights 2022

Building trust through cybersecurity and privacy.

Earning digital trust, together

Why trust matters more than ever in this hyperconnected world.

Reversing the digital trust deficit

The critical need to rebuild digital trust as technology proliferates.

[4] KPMG Cyber trust insights survey. Op cit.

Consideration 2

Unobtrusive security drives secure behaviors

Embedding security within the business in a way that helps people work confidently, make productive choices, and play their part in protecting the organization must be a key, albeit often elusive, CISO objective. It's all too easy for people to see security as an impediment, and only by considering security from both human and business-centric perspectives can CISOs hope to change this mindset.

Perhaps the most essential point is to be attentive to where and when security matters most and where additional security measures will likely impact the business justifiably. There is no absolute security, and if CISOs try to protect everything at every moment, they risk protecting nothing as users find ways around intrusive security measures. CISOs need to be pragmatic around the extent of security controls that are warranted and commensurate with the criticality of the specific business process and the related risk profile.

> **Ultimately, unobtrusive and intuitive security controls are a positive for users, who are your best firewall.**
>
> **Julia Spain**
> Partner, Cyber Security Services
> KPMG in the UK

Confidence in the CISO

Organizations display high levels of confidence and strong belief in the CISO's ability to deliver on crucial tasks.

79% of organizations are confident CISOs can accurately map where critical data is across the enterprise.

3/4 are confident CISOs can identify what their crown data jewels are.

78% are confident CISOs know how much of their sensitive data is with third parties and that it's appropriately secured.

Source: KPMG Cyber trust insights 2022.

Companies should move away from thinking about enterprise security in binary terms. In today's environment, it's a moving target, and the concept of 'secure' versus 'not secure' is transitory. Instead, CISOs should work to raise the organizational IQ around cybersecurity through awareness; simple, intuitive processes engineered with users in mind; and a better-informed employee base and executive team.

Customer experience applies to security too

It's crucial to focus on building realistic processes for responsible users while still having the means to detect and quickly counter malicious activity. It boils down to ease of use, customer experience, and planning around cybersecurity within the context of enterprise-wide priorities — the commercial needs of the broader business — as opposed to thinking of it purely as a regulatory imperative.

Advances in technology can help. From defensive AI, machine learning, and chatbots to cloud encryption, blockchain, and extended detection and response applications, all are vital parts of the puzzle. So too, is creating a more security-aware workforce, guided by consistent IT governance, to inspire people to approach digital communications with appropriate caution. CISOs should consider how they can help employees do the right thing instinctively and design security controls that support them in doing so.

> **Technology alone can't solve the problem. Billions of capital flow into cybersecurity and thousands of cybersecurity companies offer myriad tools, yet companies are still vulnerable. Why? Because the bad actors have access to the same tools.**
>
> **Prasad Jayaraman**
> Principal, Cyber Security Services
> KPMG in the US

As an ongoing, ever-evolving endeavor, cybersecurity presents many opportunities to 'bolt-on' new tools and controls. Still, we encourage organizations to build it in from the beginning, considering the human element. Major transformational initiatives have many components — one should be security. Building security into broad process-oriented initiatives, such as DevSecOps, operational technology and procurement, can be an effective and unobtrusive way to motivate people to behave securely and function as human firewalls without seeming overbearing.

> **Beyond technology, CISOs must look at the human aspect. From education and training to general awareness, it's important to build a solid culture of security across the organization.**
>
> **Eddie Toh**
> Partner, Cyber Security Services
> KPMG in Singapore

Security teams can learn much from the way organizations enhance the customer experience. Internal security controls should be easy to use, or employees may be motivated to bypass these processes; consider including customer experience specialists in the design of controls.

Security processes should also be personal for internal users. Require the individual to make judgment calls, explain the context, draw a parallel between the value of cautious, secure behavior in their personal and professional lives, and make them "edutaining." People can then play their part in the security and not be seen as the weakest link.

Learn more

Human firewalling

Overcoming the human risk factor in cybersecurity.

Synthetic identity fraud

A $6 billion problem.

Want better cybersecurity? Don't check that box

The greatest threat to your organization's security might not be ransomware or phishing attacks — it might be your tendency to do this.

Consideration 3

Securing a perimeter-less and data-centric future

It's no surprise that business operating models have fundamentally changed over the last decade — becoming more fluid, data-centric, connected ecosystems of internal and external partners and service providers. In this distributed computing world, to help reduce the blast radius of any potential outages or breaches, CISOs and security teams must adopt very different approaches, such as zero trust, Secure Access Service Edge (SASE) and cybersecurity mesh models.

Today, the clear business imperative is to enable employees, customers, suppliers and other third parties to connect seamlessly, remotely and securely. The accompanying security challenge is that, in a perimeter-less environment, organizations are no longer able to trust every user and device.

Zero trust for perimeter-less businesses

Zero trust approaches can help reduce the blast radius in the event of an outage or breach and limit the impact so the incident can be better managed and contained.

> **The traditional perimeter security approach is obsolete in our interconnected, digital world. CISOs have to protect a much broader attack surface across public and private infrastructure and a distributed user ecosystem. As a result, CISOs must strive to enable the business by providing security from anywhere, with any device, and in a trusted manner.**

Natasha Passley
Partner, Cyber Security Services
KPMG Australia

Data security is a key issue for stakeholders

In a perimeter-less environment, concerns over how data is protected, used and shared are the leading factors undermining stakeholders' trust in an organization's ability to use and manage its data.

28% of executives identify 'a lack of confidence in the governance mechanisms in place' as a leading factor undermining stakeholders' trust in an organization's ability to use and manage its data.

32% also identify 'a lack of clarity over why data is required for a particular service and the benefits of sharing or providing data' as another factor.

36% are concerned over how their data is protected.

35% are concerned over how their data is used or shared.

Source: KPMG Cyber trust insights 2022.

SASE and cybersecurity mesh models with a foundation in zero trust have common principles in terms of how security overall is organized, distributed and aligned across the network. Perhaps most important, however, is that as more enterprises adopt a cloud-centric mindset, it has become critical to move security mechanisms closer to the data.

As an umbrella over today's perimeter-less business environment, zero trust is a framework, a way of thinking about how the design and enablement of security and identity access needs to change over time. Zero trust complements the convergence of services under a SASE model and the holistic, analytical cybersecurity mesh architecture.

New models of identity

Decentralized identity access management is a core responsibility for CISOs and a function of network traffic. The north-south traffic concept — that is, user to resource — is all about identity, while east-west traffic — lateral movement within the environment — is about segmentation and other controls.

The link between data and identity is unmistakable. In a perimeter-less environment, there's no zero trust, SASE, or cybersecurity mesh without a clear underlying focus on identity and data governance.

For CISOs, the challenge with zero trust is verifying that devices and users are who they say they are and can be trusted. This requires CISOs to think about security from an identity verification perspective, focusing on least privilege access for users within their enterprise and the many third parties with whom they interact.

Making zero trust work in practice

Zero trust should be defined in relation to every scenario, every user and every endpoint — representing a key pillar of the company's foundational security program and core principles. CISOs must play a key role not only in codifying the zero trust model and message, but in establishing policies, setting standards, designing software solutions, and assembling an enterprise-wide security council encompassing various technology and business leaders.

Another challenge is around funding and budgeting. CISOs must be able to explain the framework around zero trust, so the board and other corporate leaders understand that the investment is not just another new technology but a new way of thinking that is designed to support a secure, perimeter-less future.

Finding a middle ground between on-and off-prem structures is a distinct challenge, particularly with cloud-native technologies. Many companies are thinking about moving multiple processes to the cloud, but often legacy infrastructures cannot fully adapt to SASE specifications because of the advanced technology requirements.

CISOs at large, complex organizations have the challenge of managing a security posture that spans an on-prem and off-prem ecosystem that can result in higher operational costs in the short term while operating in this dual environment. Clients looking toward full cloud adoption should consider the same on-prem zero trust principles for systems they deploy into the cloud. They should also factor in the impact of an operating model change. For example, a well-managed shared responsibility model with a cloud provider can be key to helping ensure a secure cloud architecture.

> **The identity ecosystem has exploded in the gig-economy world in which we operate today. Because of that, organizations can only accurately monitor humans and machines through the common denominator of identity.**
>
> **Deepak Mathur**
> Principal,Cyber Security Services
> KPMG in the US

Learn more

The convergent future of identity

What's next for identity access management.

Assume nothing, verify everything

Why zero trust is the way forward.

Safeguard your digital environments from all angles

Five steps to beginning the zero trust journey.

Consideration 4

New partnerships, new models

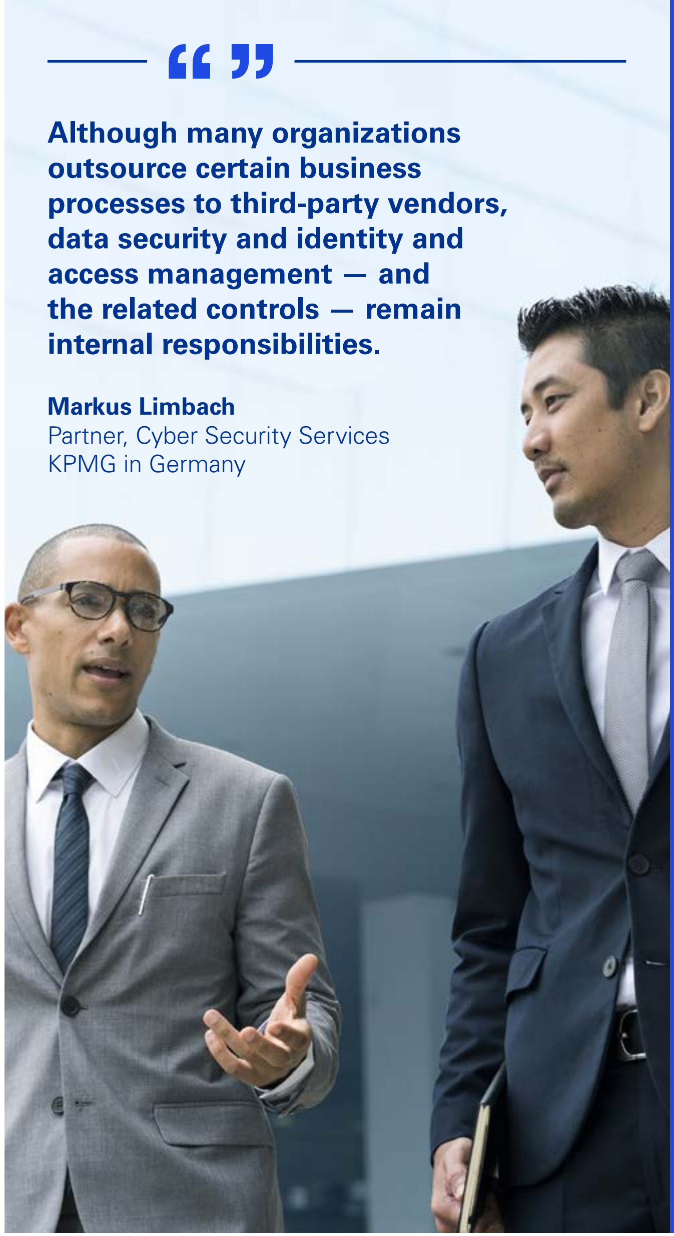
Gone are the days when security teams focused solely on the security of their organization's IT systems. CISOs need to understand when to hit the brakes, when to press go on outsourcing cybersecurity efforts and determine what skills to keep in-house today and in the future. Security has become a business priority, delivered through a shared responsibility model between the organization and service providers.

CISOs today are supporting business strategy across the organization — from operational technology and product security to complex supply chain ecosystems. Increasingly, organizations recognize that innovation is improved by collaboration between various aligned sources, from supply chain and customer service to organizational design and information security.

That combination of innovation delivered at a competitive price point to customers, wherever they might be, is how enterprises can gain competitive advantage.

However, some organizations struggle to implement robust security at scale primarily because of a lack of talent and skills, which is why they're looking to outsource, managed services, and transition to the cloud.

> **Although many organizations outsource certain business processes to third-party vendors, data security and identity and access management — and the related controls — remain internal responsibilities.**
>
> **Markus Limbach**
> Partner, Cyber Security Services
> KPMG in Germany



Trusted communities

External partnerships are expected to also be vital to success in hyperconnected ecosystems, but practical barriers stand in the way of collaboration.

79% say constructive collaboration with suppliers and clients is vital, but only **42%** report doing so.

60% admit their supply chains are leaving them vulnerable to attack.

78% of executives are confident that the CISO can secure their data across the supply chain.

Source: KPMG Cyber trust insights 2022.

Knowing what to retain

Just as companies cannot simply outsource security, they also need the right talent and skills in-house. It takes specialized knowledge to set up a repeatable control and measurement framework under which internal staff and third-party providers can operate effectively. One of the keys is understanding what to retain in-house in terms of security responsibilities and then identifying the most effective sourcing strategy for talent in those areas.

Using the cloud as an example, strategically, CISOs have to embody multiple personas — broker, orchestrator and integrator — to align the necessary staff and third-party skills and manage risk, governance and reporting. That can't be outsourced fully. Organizations might be able to outsource preparation and planning, but, ideally, someone in-house who understands the business and security environments — and the potentially broad impact of a cyber incident — should manage the organizational overlay and quality control.

> **Architecting cyber controls in a cloud ecosystem is a different skillset relative to more traditional security engineering skills. The ability to manage cyber across organizations, APIs and disparate technology sets at business speed requires a level of sophistication that many organizations lack. It's a capability CISOs should aspire to.**
>
> **Matt O'Keefe**
> Partner, Cyber Security Services
> KPMG Australia

Finding the right blend of skills

It's crucial — and easier said than done — for CISOs to understand their internal and external responsibilities, navigate the gray area between different models and disciplines, and manage those complexities by establishing the appropriate controls.

Working with outside security providers requires a unique skill set, focusing on management and governance skills rather than technical skills. Regardless of the amount of work outsourced, organizations need to retain solid in-house security knowledge and capabilities. It's also essential that dialogue between parties is clear and regular to ensure implemented controls and KPI reporting are properly managed. Furthermore, it's crucial to agree on clear incident response processes and run relevant simulations to test the system.

CISOs need to assess their skills base regularly and aim to ensure the organization is equipped to be an intelligent, collaborative customer of cloud and managed security services. Doing so requires understanding the business's future infrastructure needs and determining what the security function should look like to provide the best support. The key word is 'future' — look three to five years out and work back, rather than solely looking at the company's security needs today.

Learn more

Third-party risk management outlook 2022

Time for action.

Evolving vendor, operational and strategic risks

Third party risk management.

Third party and cloud: Regulatory challenges

Companies are forming more frequent and complex relationships with third parties, introducing new or elevated risks.

Consideration 5

Trust in automation

In the race to innovate and harness emerging technologies, concerns over security, privacy, data protection and ethics, while gaining more attention, are often ignored or forgotten. Left unchecked, this negligence could lead businesses to sabotage their potential, especially with new AI privacy regulations on the horizon.

Historically, AI has been a series of data science experiments, with a relatively small percentage of projects going into production. Now, the age of applied, real-world ML has dawned and over the next 18 to 24 months you should expect to see more of those projects go live.

There's been much trial and error, but the learnings can ultimately lead to huge success in the form of recommendation engines, decision support tools, sophisticated simulations and neural networks that may unlock hundreds of millions of dollars of value for many organizations.

Automating mundane, repetitive tasks frees time and creates efficiencies so workers can focus on initiatives requiring complex, deliberative, nuanced thought. Hence, AI is being used across many industries. In the banking sector, bots are helping to decide the most appropriate products and services for clients, and in insurance, the use of automated decision-making in an applicants creditworthiness assessment is being explored.

> **Knowing how the business is thinking about the use of machine learning is really important for the security team to add value. Once they have that understanding, the security team can look at the systems they'll use, identify the right input data, and then work to handle the adversarial risk around using their AI systems.**
>
> **Michael Gomez**
> Principal, Cyber Security Services
> KPMG in the US

Challenges of AI/ML

There are growing societal and business concerns over the ethics, security and privacy implications of adopting AI and ML solutions for big data analysis.

78% agree that AI and ML bring unique cybersecurity challenges.

3 in 4 say AI and ML raise fundamental ethics questions.

76% of executives agree that AI/ML adoption requires additional safeguards around how AI/ML systems are trained and monitored.

76% agree that AI/ML adoption requires transparency in how we use AI/ML techniques.

Source: KPMG Cyber trust insights 2022.

Building trustworthy and credible AI models

Are companies utilizing AI appropriately and getting the most productive output? With the insurance use case, there are instances where the algorithm makes decisions about applicants' who live in specific areas. Those who live in less-affluent neighborhoods were rated differently than those who live in more upper-class neighborhoods. As a result, premiums would differ based on the applicant's address. AI bias can be viewed as discriminatory and needs to be reined in.

Historically, applications were developed to run uniformly — the relationship between the inputs and corresponding outputs was not supposed to change. That was what developers tested against. The end user decided if they liked using the application and whether or not they wanted to continue doing business with the developer.

ML and AI tools are designed to learn and evolve. And that evolution represents a massive transformation in how companies must now think about these systems, how they've been trained and their fit for purpose.

People have mixed feelings and understanding of AI. And many companies simply don't have many professionals who understand AI, let alone how to secure it.

> **AI is powerful but can be harmful to individuals if the automated decision-making is inadvertently biased or discriminatory.**
>
> **Sylvia Klasovec Kingsmill**
> Partner, Privacy
> KPMG in Canada

Machines, like DevOps, are beginning to assume a role in shortening the development lifecycle and ensuring continuous delivery. And if businesses don't bring security into that machine-powered environment, it may never achieve scale because people simply won't trust it. To that end, 76 percent of executives agree that AI/ML adoption requires additional safeguards around how AI/ML systems are trained and monitored.[5]

AI and data privacy

AI elevates many core privacy principles — empowering security teams to analyze customer data more deeply, for example — but organizations need to think about proportionality with respect to the amount of data it collects relative to the data minimization requirements in certain regulations. Similarly, considering AI has the potential to embed existing biases, there must be transparency around the output.

Regulators, governments and industry must work together. AI regulation isn't just a privacy issue. It requires data scientists to work with privacy specialists to determine what requirements should be built into the technology to make it safe, trustworthy and privacy sensitive. And governments need to set the tone and establish an overarching digital agenda to inspire the industry to put budget behind innovation.

While various government bodies sometimes seem to approach AI as a competition, regulators are also starting to try to limit intrusive and high-risk applications of emerging AI capabilities.

Following the G20 adoption of principles for trustworthy AI, there have been major developments in AI risk management and regulation. Singapore was fast off the mark with its AI security standard, the National Institute of Standards and Technology (NIST) has published its AI risk management framework and the EU AI act will follow later in the year. Regulation in this space is expected to ultimately have an impact as significant as GDPR has had on privacy. Many companies need to prepare.

Learn more

Is my AI secure?

Understanding the cyber risks of artificial intelligence to your business.

Trust in artificial intelligence: Global insights 2023

Global survey exploring people's trust in AI and benefits and risks for business and society.

The path to transparency — and trust

Corporate data responsibility survey.

[5] KPMG Cyber trust insights survey. Op cit.

Consideration 6

Securing a smart world

Businesses across almost every industry are shifting to a product mindset — focusing on developing network-enabled services and managing their supporting devices. CISOs and their teams are getting pulled into discussions with engineering, development and product support teams as organizations realize product security matters too.

In today's smart-product-focused environment, some emerging drivers or enablers dominate:

5G
Offers speed, hyperconnectivity and reduced latency.

Quantum computing
Massively cuts processing and calculation time.

Trust architectures
Help to ensure that data and identities are secure and trusted from one connected device to another.

Software 2.0
Rapid, AI-written code that can reduce complexity while increasing development speed from months to weeks.

Applied AI
Real-world fundamental application of artificial intelligence as a developmental wrapper around smart products.

> **The pace of technological innovation is not slowing down, and it often forces regulators and security teams to play catch-up. CISOs should neither wait for the next wave of regulations, nor rely on regulation alone and instead take a proactive and pragmatic approach to implement security controls throughout the product lifecycle and supply chain. This is no small feat, and success will likely depend on how well CISOs engage with other functions across the business.**
>
> **Walter Risi**
> Partner, Cyber Security Services
> KPMG in Argentina

CEO cyber outlook

Growing experience of the challenges of cybersecurity is also giving CEOs a clearer picture of how prepared — or underprepared — they may be.

24% of CEOs recognize they're underprepared for a cyberattack, compared to 13 percent in 2021.

56% say they're prepared.

3/4 say their organization has a plan in place to deal with ransomware attacks.

3 in 4 CEOs say that protecting their partner ecosystem and supply chain is just as important as building their organization's cyber defenses.

Source: KPMG 2022 CEO Outlook.

There are many smart device risks, such as weak default passwords, poor or absent encryption, failure to provide timely secure software updates, malware, and lack of denial-of-service protection, to name just a few. CISOs must realize that, with these devices, security is not just based on the CIA triad (confidentiality, integrity, availability). Safety is also a key consideration because hyperconnected, tangible real-world systems are involved. Cyber professionals must apply those risks to a CIAS framework because targeted attacks at scale are a distinct possibility.

As we move to a world of ecosystems, products, devices and sensors, and they increasingly become the target of sophisticated cyberattacks, regulators are placing heightened scrutiny on how organizations embed security across the product lifecycle.

> **Numerous challenges exist with embedding security within the smart-product lifecycle, including proactively monitoring, identifying and addressing the related cyber vulnerabilities. One of the CISO's key challenges should be working with the quality control department to embed security within product design and pre-shipment inspection processes.**
>
> **Motoki Sawada**
> Partner, Technology Risk Services
> KPMG in Japan

Applying the CIAS framework in a hyperconnected world

CISOs should consider smart device-related risks across four main components spanning the lifecycle, each with specific DevSecOps-related priorities: product development, from design implementation to release; managing the expanding supply chain; maintenance and ongoing software updates; and the end user, whether it's another business or an individual consumer. These four areas help CISOs determine how to organize a security plan and gain confidence that the product is as secure as possible. It has become essential that CISOs have a line of sight in all areas of the business.

> **CISOs should work with the entire enterprise to help ensure cybersecurity is viewed as a risk management priority. Also, merely thinking about security in terms of the technical processes that can be applied within the device is too narrow an approach — the broader impact to areas such as supply chain and customer service are also important.**
>
> **Jayne Goble**
> Director, Cyber Security Services
> KPMG in the UK

Software embedded in smart devices has the added complexity of not being easily updated, which is attributable to various factors, such as connectivity and the inability to patch while in use. It depends on the criticality of the device. This poses an additional challenge to builders: having to embed early assurance mechanisms, as well as having a well-organized software bill of materials, which enables companies to detect, and eventually recall, devices in the event critical vulnerabilities are discovered once devices are in use.

Cybersecurity has become a market differentiator. Perhaps it sounds obvious, but it's important for current and prospective customers, and the broad marketplace, to know that the organization's cybersecurity program, and device controls in particular, are ever-evolving, never static, and managed with device lifecycles in mind. Expect regulators worldwide to take a growing interest in the security of these systems and the minimum standards required.

Learn more

Control systems cybersecurity report 2022

Overcoming the roadblocks to true progress as cyber threats grow.

A pathway to cyber resilience

Assessing and bracing against cyber vulnerabilities in industrial sectors.

Accelerating OT security for rapid risk reduction

Securing operational technology environments as they become increasingly digitized and connected.

Consideration 7

Countering agile adversaries

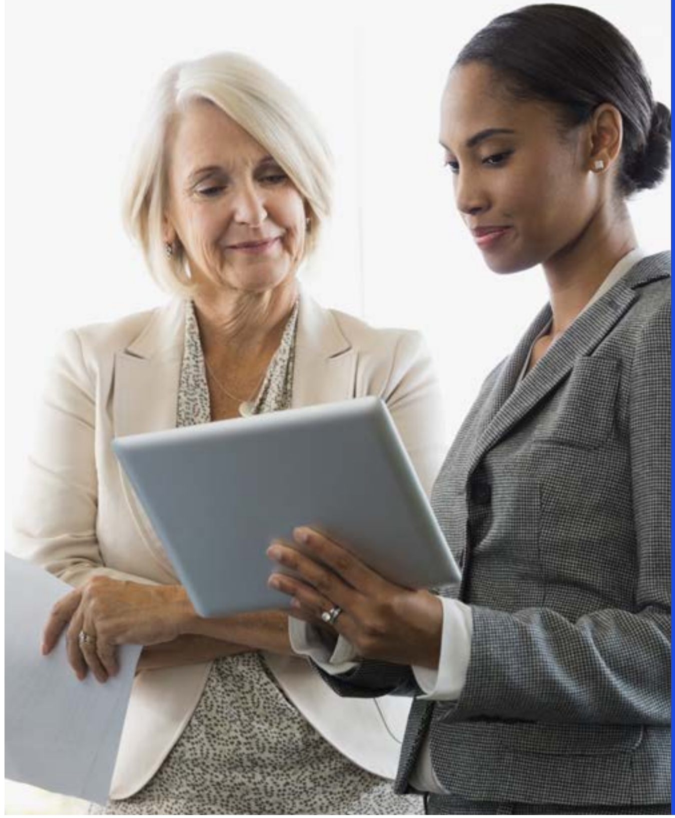
The time from initial compromise to enterprise-wide ransomware activation is shrinking. Increasingly, rogue and state-sponsored attackers can penetrate systems with automated tooling and accelerate the exploitation of systems. Security operations should be optimized and structured to fast-track the recovery of priority services when an incident occurs, which can reduce the impact on clients, customers and partners.

Cyberattackers have two apparent motives; exploitation and disruption. The exploitation of systems to steal or manipulate data, whether for intelligence or fraud, and disruption for extortion or political gain. The tactics can be quite different.

Some state-sponsored attackers focus on critical infrastructure, such as oil pipelines, electric utilities and financial systems. The mission is to cause harm or chaos and exert political or economic influence to benefit the attacker and their sponsor. They intend to monetize the misfortune of others.

The probability of success for cybersecurity incidents has increased substantially, resulting in growing ransomware attacks in recent years. And it will likely continue if security professionals don't make it harder on the attackers.

> **Attackers are going to gain access — that has to be accepted. It's about reducing dwell time. What's critical is whether their presence and actions are detected within hours, days, weeks or months.**
>
> **Charlie Jacco**
> Principal, Cyber Security Services
> KPMG in the US



Cybersecurity teams are struggling to keep up

Cybersecurity teams are under pressure to keep up with evolving threats, with talent shortages frequently undermining security efforts.

Over 1/2 of organizations admit they are behind schedule with their position on cybersecurity.

More than 50% are either very or extremely confident in combatting various cyber threats, including from organized crime groups, insiders and compromised supply chains.

59% agree that attackers are exploiting vulnerabilities in procurement and the supply chain, but they do not know whether their defenses are strong enough to stop them getting through.

#1 internal challenge to achieving cybersecurity goals is lack of key skills (40%).

Source: KPMG global tech report 2022.

To make matters worse, hybrid working has expanded the attack surface, raising the number of potentially vulnerable endpoints. Adding to the challenges, shadow IT within the business often includes business applications and software as a service use over which CISOs and CIOs have limited visibility or understanding of the possible exposures.

Sharpening your security operations strategy

Time matters. How quickly can an attacker be detected, how quickly can they be contained, how quickly can services be restored — and in doing so, how can you minimize information and system compromise? It's less about how they got in and more about what information they obtain. Was it mission-critical? Did it leak out the back door or is it being held hostage?

The time attackers take to move from initial compromise to successful exploitation of systems is reducing. Now it might take just a few days, or even less, for an attacker to deploy ransomware across an enterprise. Attackers are also increasingly creative in automating their tactics, even to the extent of exploring the potential of AI in helping them plan and orchestrate their attacks. The bottom line: CISOs and their teams have considerably less time to detect intrusions and take swift and decisive containment action.

There is a triangular structure in today's security operations centers (SOC), with a small but specialized threat-hunt team at the top, various Level 2 investigators in the center, and numerous Level 1 alert analysts on the bottom triaging an ever-multiplying volume of alerts. That triangle needs to be inverted. Today's SOCs require fewer Level 1s, more Level 2s, and considerably more threat hunters looking for potentially catastrophic events. One way to do that, and respond to the pace and volume of attacks, is to automate Level 1.

An effective SOC requires you to leverage more advanced technologies, bring the relevant data together, trust the available tools to manage the alerts, and get the partnership between human analysts, sophisticated ML, and robotic process automation right. As you do that, you can draw in new data sources that provide greater business context to the analysis of potential attacks, exploring the fusion of cybersecurity operations with physical security, fraud prevention and insider threat management.

Achieving that level of trust is a challenge for most security organizations. Suppose CISOs and their teams can harness AI to do that triage work, look across the firewall and the security information and event management (SIEM) system and assess the various threat intelligence sources and vulnerability scanning tools. They can be able to start trusting. That's where the SOC is headed, but it's not there yet.

Harnessing and retaining technical cyber expertise

As for talent, attrition and retention must be front-burner priorities. Many organizations need help to create a durable career path and model for the SOC. Teams are consumed with monitoring the system and they throw more personnel at the problem rather than properly training the professionals already on the job.

As a result, people feel stuck and ultimately move on, leaving CISOs with a perpetual revolving door in the SOC. All because they haven't prioritized training. And while attackers continuously evolve their techniques, tactics and strategies — becoming better and faster at what they do — CISOs don't have the resources to keep up.

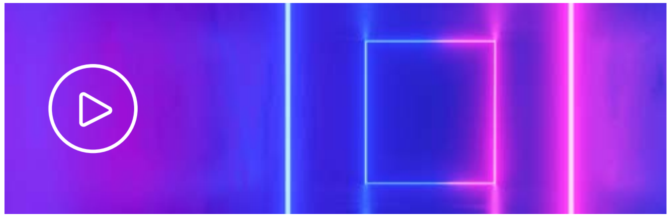
Learn more

KPMG global tech report 2022

Discover how leaders are using technology to move their business forward and strengthen ongoing digital maturity.

Really ready for a ransomware attack?

Challenging business assumptions about risk readiness, today and tomorrow.



A triple threat across the Americas: KPMG 2022 Fraud Outlook

A review of the fraud, compliance and cybersecurity risks facing the Americas.

Consideration 8

Be resilient when — and where — it matters

Every security system has its flaws. There is an air of inevitability that, at some point, an organization will suffer an incident, large or small, and likely more than one. Regulators are increasingly focusing on plausible scenarios and pushing companies — particularly those in strategically important industries like energy, finance, and health care — to be resilient and position themselves to recover.

Perhaps the most glaring issue is that organizations often don't see that the impact of — and recovery from — a cyber incident can be protracted. It's typically not a 72- or 96-hour event. They have to assume large-scale business disruption, a worst-case scenario. In too many cases, senior leaders haven't fully appreciated the enterprise-wide technology linkages or the business operational dependencies — paying staff, paying suppliers, communicating with customers and investors — on those connections.

> **It's critical for CISOs to engage with the business early and often to help ensure a clear, yet flexible resilience strategy is properly set ahead of time, rather than testing it in the middle of a crisis.**
>
> **Dani Michaux**
> Partner, Cyber Security Services
> KPMG in Ireland

The regulatory outlook

Lawmakers and regulators are paying greater attention — increasing demands for transparency and oversight. Many organizations are concerned about navigating an increasingly complex global regulatory landscape.

36% worry about their ability to meet existing or new cybersecurity regulation when activities are outsourced to digital service providers.

31% worry about the growing demands around critical infrastructure, which is the subject of increasing regulation in the UK, the EU and the US.

28% worry about existing or new regulation related to resilience of key systems.

26% worry about more stringent incident reporting requirements.

Source: KPMG Cyber trust insights 2022.

Also, many organizations have yet to truly consider what they need to do proactively to be resilient. They assume they have a backup plan and sufficient security controls. What if they don't have a plan for a particular scenario, and business operations halt? This has severe financial and reputational ramifications, let alone regulatory. There's also a psychological component. CISOs need to have ongoing conversations with their C-suite colleagues and the Board about the nature and motivations of attackers: the harder they hit you, the more likely you are to pay, and they know it. Most organizations still struggle to understand what they're really up against.

Proactive coordination is required in and out of battle

During the chaos of an active attack, the CISO's key objective is to provide the business with the insights it needs to continue operating. They must step away from the day-to-day technical details and engage proactively and strategically with the organization about the seriousness of the situation and how, collectively, the business must respond if it wants to recover expeditiously.

A big part of the CISO's job is to be a communicator and to articulate across the enterprise the potential business impact of a breach and the value of keeping cybersecurity top of mind. Beyond that, response and recovery — the components of resilience — require coordination. This can be achieved through a small 'crisis board' comprising the CISO, the CEO, CFO and the chief legal counsel.

Unfortunately, this important group doesn't formally exist at many companies because they don't think it will happen to them. And if it does, they believe their business continuity plan — which in many cases is several years old and aligned to an outdated set of use cases — is sufficient. It's not.

Recovering to your minimal viable business

It's about more than just building in good security because controls fail. It's about gaining clarity around what it takes to recover. Company leaders tend to look at the immediate horizon because most can't think any further when they're in the middle of an event. At that point, the CISO must be the voice of reason and talk pragmatically about getting back to minimum viable business processes: keeping the lights on, paying people and ensuring that operations resume.

The longer it takes to get back to minimum viable business processes, the more likely the business will have an existential crisis. The bad actors don't work on your timetable. They innovate faster because they're financially motivated. That's the challenge CISOs face — they're perpetually playing catch up.

> **There must be a structure in place and an understanding of the potential trajectory of a cyber event. Having a plan and a clear approach for marshaling resources can be the difference between a 60-day nightmare and a 30-day nightmare.**
>
> **Jason Haward-Grau**
> Principal
> Cyber Security Services
> KPMG in the US

Regulation's role in resilience

When it comes to resilience, regulations can either be seen as a foundation or a ceiling. Most organizations see it as the latter — something they must comply with; therefore, they do the bare minimum. Alternatively, it can be viewed as a foundation because there are frequently new or different actions to be taken.

Regulation plays a vital role in organizational resilience but often needs to be coordinated or aligned. This is one of the greatest challenges CISOs face as the regulatory line of sight imperatives expand to encompass a company's supply chain. It's no longer just a matter of worrying about the organization overall. CISOs have to consider the downstream implications for suppliers and other key partners and whether they're compliant with the relevant regulations, as well as the upstream implications of whether customers and investors are unclear about if the company is compliant with the European Cyber Resilience Act.

Resilience is ultimately an organization-wide issue in which cybersecurity has a vital role, alongside other recovery capabilities and disciplines such as business continuity. CISOs can play a key part in helping organizations proactively plan for disruptive cyber events, which can vary in nature, scale and response to classic technology or property incidents. Many CISOs may also find themselves taking on wider resilience responsibilities as organizations focus more and more on such scenarios and their consequences. Yet another evolution of the CISO role.

Learn more

The day after

Recovery, resistance and resilience after an industrial cyberattack.

From continuity to resilience

The growing dependence on electricity makes it more critical to build a proactive, resilient organization to help ensure continuity of service.

Incident readiness: A playbook for your worst day

Being prepared for a cyber incident can minimize critical power and utility infrastructure disruption.

Cyber strategies for 2023

What actions can CISOs and the broader business lines take in the year ahead to help ensure security is the organization's golden thread? Following is a short list of tangible steps CISOs should consider as they seek to accelerate recovery times, reduce the impact of incidents on employees, customers, and partners and aim to ensure their security plans enable — rather than expose — the business.

People

- Prioritize a robust cybersecurity culture that is interesting, engaging and, where appropriate, fun to inspire employees to do the right thing and function as human firewalls.
- Build a security team with the skills mix needed to manage a perimeter-less organization, including cloud and third-party dependencies.
- Communicate broadly and clearly. Ask leaders in other organizational functions about their pain points and how automated processes might help.
- Take a multidisciplinary, cross-culture approach. Establish a security ecosystem comprising internal business line specialists, security professionals, data scientists, privacy-oriented attorneys and external policy and industry professionals.
- Embed yourself in the organization and act as a peer, a sounding board and an advisor.

Process

- Build consistent approaches to cyber risk management with an understanding of threat scenarios and attack paths to help inform attack surface reduction and prioritize control improvements.
- Focus on fit-for-purpose security processes that feature consistent user experiences.
- Establish strict identity controls and work to achieve a mature state of identity governance and services.
- Segment legacy environments to limit the attack surface and help contain any breaches.
- Have a proactive recovery plan focusing on the organization's most critical workflows with a communication structure and stress test it often.

Data and technology

- Embrace the inevitable automation of the security function — trust the latest tools, such as robotic processes, to security orchestration, automation and response (SOAR), and extended detection and response (XDR) systems.
- Work with cloud providers to help ensure broad visibility into how products and services are configured to avoid inadvertent vulnerabilities.
- Consider cybersecurity and privacy issues up front when exploring emerging technologies, including the evolving risks associated with adopting AI systems.
- Assign responsibilities and establish accountability around how critical data is processed and managed and how it supports critical business processes.
- In the interest of speed, scalability and trust, a transition to identity as a service in the cloud needs to happen sooner than later.

Regulatory

- Be aware of changing regulatory trends and drivers and what they could mean for the company's future technology strategy, product development, and operations.
- Consider the regulatory impacts vis-à-vis AI and automation — establish a clear concept of what the business can and can't do in these arenas and be alive to public concerns and changing expectations.
- Explore automating compliance monitoring and reporting and task a team member to serve as a regulatory monitor to stay on top of privacy and security regulatory trends.
- Align security and privacy compliance strategy with the company's broad business strategy to help ensure stakeholders from across the organization are on the same page.
- Look beyond the letter of the regulation — and be prepared to ask yourself more fundamental questions about digital trust and how you make that central to your strategic thinking.

How KPMG professionals can help

KPMG firms have experience across the continuum — from the boardroom to the data center. In addition to assessing your cybersecurity and aligning it to your business priorities, KPMG professionals can help you develop advanced digital solutions, implement them, monitor ongoing risks and help you respond effectively to cyber incidents. No matter where you are in your cybersecurity journey, KPMG firms can help you reach your destination.

As a leading provider and implementer of cybersecurity, KPMG professionals knows how to apply leading security practices and build new ones that are fit for purpose. Their progressive approach to cybersecurity also includes how they can deliver services, so no matter how you engage, you can expect to work with people who understand your business and your technology.

Whether you're entering a new market, launching products and services, or interacting with customers in a new way, KPMG professionals can help you anticipate tomorrow, move faster and get an edge with secure and trusted technology. That's because they can bring an uncommon combination of technological experience, deep business knowledge, and creative professionals passionate about helping you protect and build stakeholder trust.

KPMG. The Difference Makers

Meet the authors

Akhilesh Tuteja
Global Cyber Security Leader
KPMG International
Partner, KPMG in India
E: atuteja@kpmg.com

In addition to serving as the Global Cyber Security practice leader, Akhilesh heads the IT Advisory and Risk Consulting practices for KPMG in India. He is passionate about how developments in information technology can help businesses drive smart processes and effective outcomes. Akhilesh has advised over 200 clients on cybersecurity, IT strategy and technology selection and helped them realize the business benefits of technology. He is also knowledgeable in the area of behavioral psychology and is enthusiastic about addressing the IT risk issues holistically, primarily through the application of user-behavior analytics.

Kyle Kappel
Cyber Security Services Network Leader
Principal, KPMG in the US
E: kylekappel@kpmg.com

As the US Leader of KPMG's Cyber Security practice, Kyle has more than 20 years of experience in the information systems field and a diverse background in cybersecurity, data privacy, regulatory compliance, risk management, and general technology issues. While he has strong technical skills, Kyle utilizes a business-centered approach to solving technology problems by addressing root causes rather than technical symptoms. He's a trusted advisor to numerous Fortune 500 organizations, working with senior executives, including Boards of Directors, audit committees, Chief Information Officers, Chief Financial Officers, Chief Operating Officers, Chief Technology Officers and Chief Information Security Officers.

Dani Michaux
EMA Cyber Security Leader
Partner, KPMG in Ireland
E: dani.michaux@kpmg.ie

In more than 22 years in cybersecurity, Dani has worked with government agencies on national cybersecurity strategies and with international regulatory bodies on cyber risk. She has extensive experience working with clients to improve Board-level understanding of cybersecurity matters. She has built and managed cybersecurity teams as a CISO at telecommunications and power companies in Asia. Dani advocates for inclusion and diversity and women's participation in computer science and cybersecurity. She previously led the Cyber Security and Emerging Technology Risk practices for KPMG in Malaysia and the ASPAC region and also led KPMG's global IoT working group.

Matt O'Keefe
ASPAC Cyber Security Leader
Partner, KPMG Australia
E: mokeefe@kpmg.com.au

Matt is responsible for driving KPMG's cyber strategy within the 12 KPMG member firms in Asia Pacific. He has more than 25 years of technology, finance, assurance and advisory experience, focusing on financial services industry clients. Matt specializes in technology advisory, particularly in superannuation and wealth management, banking and insurance, and provides a range of services across technology governance and risk, cybersecurity, project management, IT strategy and performance. He is deeply interested in using technology to advance organizational goals, enabling clients' digital strategies and operating models, and protecting data, assets and systems.

Prasad Jayaraman
Americas Cyber Security Leader
Principal, KPMG in the US
E: prasadjayaraman@kpmg.com

With more than 17 years of experience in identity management practice, Prasad is an intuitive and results-oriented leader with a strong track record of performance in technology-related professional services organizations. He has superior interpersonal skills and can resolve multiple complex challenges in all aspects of business, from sales, human resources and legal to finance and operations. He has directed cross-functional teams with motivational leadership and a personal touch that inspires loyalty and a willingness to give 100 percent.

Acknowledgements

This report would not be possible without the invaluable planning, analysis, writing and production contributions of colleagues around the world.

The Global cyber considerations team

Jessica Booth
David Ferbrache
John Hodson
Billy Lawrence
Leonidas Lykos
Michael Thayer

Our Global collaborators

John Anyanwu
Partner, KPMG in Nigeria
john.anyanwu@ng.kpmg.com

Jonathan Dambrot
Principal, KPMG in the US
jdambrot@kpmg.com

David Ferbrache
Head of Cyber Innovation
KPMG International
david.ferbrache@kpmg.com

Jayne Goble
Director, KPMG in the UK
jayne.goble@kpmg.co.uk

Jason Haward-Grau
Principal, KPMG in the US
jhawardgrau@kpmg.com

Lisa Henegan
Global Chief Digital Officer
KPMG in the UK
lisa.heneghan@kpmg.co.uk

Charles Jacco
Partner, KPMG in the US
cjacco@kpmg.com

Prasad Jayaraman
Principal, KPMG in the US
prasadjayaraman@kpmg.com

Sylvia Klasovec Kingsmill
Partner, KPMG in Canada
skingsmill@kpmg.ca

Markus Limbach
Partner, KPMG in the US
mlimbach@kpmg.com

Deepak Mathur
Principal, KPMG in the US
deepakmathur@kpmg.com

Dani Michaux
Partner, KPMG in Ireland
dani.michaux@kpmg.ie

Matt O'Keefe
Partner, KPMG Australia
mokeefe@kpmg.com.au

Natasha Passley
Partner, KPMG Australia
npassley@kpmg.au

Walter Risi
Partner, KPMG in Argentina
wrisi@kpmg.ar

Motoki Sawada
Partner, KPMG in Japan
motoki.sawada@jp.kpmg.com

Henry Shek
Partner, KPMG China
henry.shek@kpmg.com

Julia Spain
Partner, KPMG in the UK
julia.spain@kpmg.co.uk

Eddie Toh
Partner, KPMG in Singapore
eddietoh@kpmg.com.sg

Akhilesh Tuteja
Partner, KPMG in India
atuteja@kpmg.com

Annemarie Zielstra
Partner, KPMG in the Netherlands
zielstra.annemarie@kpmg.nl

Contact us

Akhilesh Tuteja
Global Cyber Security Leader
KPMG International and Partner
KPMG in India
atuteja@kpmg.com

Kyle Kappel
Principal, Cyber Security Services
Network Leader
KPMG in the US
kylekappel@kpmg.com

Dani Michaux
EMA Cyber Security Leader
and Partner
KPMG in Ireland
dani.michaux@kpmg.ie

Prasad Jayaraman
Americas Cyber Security Leader
and Principal
KPMG in the US
prasadjayaraman@kpmg.com

Matt O'Keefe
ASPAC Cyber Security Leader
and Partner
KPMG Australia
mokeefe@kpmg.com.au

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

kpmg.com/socialmedia

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

KPMG refers to the global organization or to one or more of the member firms of KPMG International Limited ("KPMG International"), each of which is a separate legal entity. KPMG International Limited is a private English company limited by guarantee and does not provide services to clients. For more detail about our structure please visit kpmg.com/governance.

Designed by Evalueserve | Publication name: Cybersecurity considerations 2023 | Publication number: 138614-G | Publication date: February 2023