Cyber security considerations 2022

Trust through security

KPMG in the UK

home.kpmg/cyberconsiderations

Foreword

Cyber security is about what you can do — not what you can't

The threat landscape is expanding. Cybercriminals are as entrepreneurial as ever and using increasingly sophisticated tools and technologies. In this fluid environment, we believe Chief Information Security Officers (CISOs) and their teams should adopt a mindset of enablement — cyber security is no longer just about prevention. It's not a matter of telling colleagues what they can't do, it's showing them what they can do — securely.

CISO paradigm shift: From enforcer to influencer

While one of the key lessons of the pandemic is that some of the best cyber teams are able to pivot quickly to enable their organisations to work safely, remotely and effectively, the broader, more strategic takeaway is that this period has caused organisations to rethink how they engage with and serve their customers in a digital-first environment. This shift in mindset to customer centricity has led to rapid digital transformation, which has helped customers move at the pace of business, securely.

Under this dynamic environment, cyber professionals are transforming from organisational enforcer to influencer. The C-suite is taking note. According to KPMG 2021 CEO Outlook, a sizeable majority of CEOs (75 percent) believe a strong cyber strategy is critical to engender trust with key stakeholders.

But within the context of accelerated digital transformation — which augments the risks of an ever-expanding third-party ecosystem — cyber teams also recognise the challenge of protecting their partner ecosystem and supply chains, with 79 percent indicating it's just as important as building their own organisation's cyber defenses.

The majority of CEOs (58 percent) feel they are well prepared for a cyberattack. Indeed, for nearly every organisation, some type of cyber event is seen as increasingly inevitable. Security teams must be prepared for the increasing inevitability of some type of cyber event and be ready to respond, recover and re-establish trust as quickly as possible to mitigate the damage. At the same time, they must recognise that risk in this environment is a moving and evolving target. From the board to the C-suite and from front office to back, controls should be in place to protect the organisation's and clients' high-value assets, the proverbial 'crown jewels.'

Over the years — and particularly as a result of the pandemic — it has been found that a lack of preparation and being overly reactionary can be as detrimental as the actual event. That's why it's so important to have a plan, test your responses according to different scenarios, and understand the depth and breadth of potential cyber incidents. This is an opportunity for organisations across virtually every sector to reimagine their response and recovery strategies and truly shift security left.

On the horizon: Eight CISO priorities

CISOs must wear multiple hats simultaneously, but they can't be everywhere at all times. While it's important to remember the oft-heard maxim, "security is everyone's job," it's even more critical to recognise that security is key to building and maintaining customer, client and stakeholder trust.

Looking toward 2022 and beyond, we're focusing on eight core topics that we believe CISOs should prioritise at the C-suite and boardroom levels. These themes, along with a focus on the always-fluid regulatory environment, can help executives better understand how cyber can support the business with a security plan based on shared accountability.

Whether it's advanced persistent threats, ransomware, backdoor attacks, or something we've yet to see, there will likely always be new perils with which to contend. But if CISOs and their teams adhere to a disciplined set of principles designed with the organisation's key objectives in mind, and if the plan is up to date and flexible, they can position the organisation to mitigate the impact of cyber events.

Akhilesh Tuteja
Global Cyber Security Leader
KPMG International

Martin Tyley
Partner, Head of UK Cyber
KPMG in the UK

KPMG has identified

Eight key cyber security considerations for 2022

Click on the topics to learn more.

Expanding the strategic security conversation

Change the conversation from cost and speed to effective security to help deliver enhanced business value and user experience.

Achieving the x-factor: Critical talent and skillsets

Transform the posture of CISOs and their teams from cyber security enforcers to influencers.

Adapting security for the cloud

Enhance cloud security through automation — from deployment and monitoring to remediation.

Placing identity at the heart of zero trust

Put IAM and zero trust to work in today's hyperconnected workplace.

Exploiting security automation

Use smart deployment of security automation to help realise business value.

Protecting the privacy frontier

Move to a multidisciplinary approach to privacy risk management that embeds privacy and security by design.

Securing beyond the boundaries

Transform supply chain security approaches — from manual and time consuming to automated and collaborative.

Reframing the cyber resilience conversation

Broaden the ability to sustain operations, recover rapidly and mitigate the consequences when a cyberattack occurs.

Consideration 1

Expanding the strategic security conversation

Align business goals with security needs.

The last 2 years have redefined how we live, govern and conduct business. Securing and protecting critical assets, systems and, most importantly, sensitive proprietary and customer data is no longer exclusively an issue for security and IT professionals. Rather, handling and mitigating risk to help the strategic viability and operational sustainability of the entire organisation is a shared responsibility that starts with the business.

Elevating boardroom visibility

Digital technology now powers and empowers enterprises much like electricity did during the industrial revolution. It also has the ability, if insufficiently secured or resilient, to interrupt communications and disrupt supply chains. A single data breach or malware attack has the insidious capacity to incapacitate real-time transactions and network interactions, and ultimately disrupt business and impact revenue growth for days, if not weeks and months.

Senior leaders have begun to understand that managing cyber risk for competitive advantage and long-term success starts in the boardroom and the C-suite. Offloading the strategic decision-making and management of risk, especially the risk inherent in digitisation, is no longer just good enough. Modern security solutions can only accomplish so much in terms of risk reduction if business objectives don't include an embedded robust security framework.

Today's global business environment is continually impacted by geopolitical, environmental, societal and technological uncertainty. The resulting cyber risk landscape is fueled by an ever-growing volume of sensitive data moving across interconnected and integrated networks. CISOs — who are increasingly expected to speak the language of the board and the business in addition to the language of security — should collaborate to build resilience through pragmatic security investments in support of organisational growth objectives. Toward that end, cyber teams are pursuing a number of strategies, including targeting automation and enhancing their security technology portfolios, developing depth in critical skillsets to hedge against a growing talent shortage, and creating delivery models that embed security and de-risk partner ecosystems.

What's your move?

To better align security with the organisation's strategic business objectives, CISOs and their teams should help leadership across the business gain an appreciation for what goes into security and privacy by design. Change the conversation from cost and speed to a more effective security architecture aimed at delivering enhanced business value and user experience. The costs of disruption of consumer-facing systems or compromised data outweigh what cyber teams typically quantify operationally and are magnified by degraded consumer and investor confidence, which can have lasting impact.

Digitally native or digitally mature businesses are determinedly focused on moving quickly from a development perspective and don't consistently place emphasis on the fundamentals of risk and security. Businesses need to strike a balance. Clearly, speed-to-market is essential for competitive advantage today,

> "Translation is a big CISO challenge: explaining risk dynamics to the board and operating committees in terms of collaboration and cooperation. They should articulate that they're not trying to stop the business, and instead supporting to enhance the trust of their consumers, investors and partners. Security should be a shared responsibility model, owned by everyone."

Rik Parker
Principal, Cyber Security Services
KPMG in the US

but it's equally important to embed security into business processes in a way that enables the organisation to maintain pace, rather than create a bottleneck at the CISO's office. The cost — in the form of lost customers, lost investors, and tarnished reputation — of not adequately focusing on security can be substantially higher than taking the time to do it right.

Talent retention and acquisition is another gap area where organisations need to assess whether automation and partner leverage can supplement and complement a skilled and increasingly diverse security workforce. There are too many companies competing for a limited talent pool. While the cyber community can work with universities to enhance the talent pipeline and build more attractive roles to attract and retain talent, the industry should also look to embed technology across business processes and planning in an effort to help reduce the resource-capacity impact of commoditised or repetitive tasks. This will likely require intelligent automation, where possible, and creativity in delivery models and talent acquisition where it is not.

Artificial intelligence (AI), machine learning (ML) in particular, in concert with smart, orchestrated security tools, should be considered not only to isolate exposures and vulnerabilities, but also to automate the fixes and remediation. In an ideal scenario, organisations should take it out of the hands of development professionals by automating appropriate work as development is in progress.

In addition to helping maintain speed over the software development life cycle, AI can help companies avoid delivering bad code to customers who might then distribute it through their networks. In practice, this may require transferring some controls and risk to outside partners. That's still a difficult concept for both CISOs and their business-line counterparts to grasp, but it's expected to be the overarching trend over the next several years as development volume and risk continue to grow.

> "The modern CISO should think in multiple dimensions: technologist, evangelist, investigator, psychologist, investor and negotiator. They need to align security with business strategy, approach incidents as opportunities and re-frame the way their team works."

Akhilesh Tuteja
Global Cyber Security Leader
KPMG International

Some key actions to consider for 2022

1. Transition from traditional security thinking around confidentiality and availability of data and begin thinking about striving to ensure integrity and resilience
2. Engage key organisational stakeholders to commit to a security strategy that can protect organisational and customer data, manage risk, and is sensitive to short- and long-term business priorities
3. Reformulate thinking in the executive suite as it relates to security by focusing on practical enterprise risk rather than expense and speed
4. Think less about operational key performance indicators (KPIs) and key risk indicators (KRIs) and focus on themes and trends in the underlying data: types of incidents, internal and external programme gaps, and data-related activities that are in progress, planned or awaiting approval
5. Build relationships with key business areas by increasing awareness of how quickly they can achieve objectives by embedding security versus what they may lose in the event of a breach

Learn more

Weave cyber security into the company's DNA
CISOs should embed cyber security into the business — making it everyone's responsibility.

Securing the new business reality
Global CEOs face their fears and confront cyber security risks.

Breaking the illusion of cyber security
Why trust matters more than ever.

Consideration 2

Achieving the x-factor: Critical talent and skillsets

Transform the cyber security team from enforcer to influencer.

It is becoming increasingly apparent that modern security programmes, led by forward-thinking security teams, empower organisations to move with agility, pursue growth and serve customers better. Cyber security strategies and tools represent the ever-present check that enables developers and business leaders to operate at pace with the knowledge that their security partners have their backs — sometimes in person, but increasingly through automated means.

As the threat landscape evolves, the cyber team's approach is changing

Perhaps the biggest change we've seen, in terms of the security team's relationship with the rest of the organisation — certainly in the age of COVID, but even going back several years before the onset of the pandemic — is an increased need for speed-to-market, albeit with an acknowledgment of the risks involved.

With the pandemic ongoing, organisations are reaching a point where they are expected to manage an increased digital footprint and change cycle, while continuing to enhance security capabilities. This in turn has fueled the transition to a secure-by-design approach, the need to operationalise development, security, and operations (DevSecOps), and the critical 'shift left' of security along the software development life cycle (SDLC).

Thinking about the makeup of an effective cyber programme, there's a leadership element and a team element. In terms of leadership, the most effective CISOs are not spending a lot of time talking about technology. Rather, they spend more time thinking and talking about the forward direction of the business, striving to ensure that executives in the C-suite and the board room are aware of and aligned with the security plan and vice versa.

Talking about firewalls, patch management, and data loss prevention — although all critical considerations — makes non-security heads spin. More and more, CISOs and their teams are understanding and speaking the language of the business. They should communicate how the organisation's cyber security programme supports and contributes to the growth of the bottom line.

As for the broader team, today we are seeing essentially negative unemployment in cyber. Not only is there a dearth of experienced professionals to fill all the necessary roles, people tend to move around in this industry because they are looking for different experiences to strengthen existing skills and acquire new competencies.

More broadly, there's an exploding gig economy where it seems as though everyone's a subcontractor. Over the coming years, cyber teams may have access to a pool of trusted resources as workloads and capacity dictate. That would enable CISOs to staff teams to operate with a smaller, more strategic core and surge up and down as needed. The nuance in that model is trust. There should be a clearinghouse of cyber specialists who have been vetted by other trustworthy professionals, either inside or outside the organisation, who can be trusted to take on sensitive cyber security projects.

This mindset shift is what is transforming the posture of CISOs and their teams from organisation enforcers to influencers.

> "As Mike Tyson famously said, 'Everybody has a plan until they get punched in the mouth.'[1] A cyber event can feel like that. Cyber teams need to be ready to get up off the mat, and respond in ways that are informed, strategic and measured."
>
> **Fred Rica**
> Principal, Cyber Security Services
> KPMG in the US

[1] Mike Berardino, "Mike Tyson explains one of his most famous quotes," *South Florida Sun-Sentinel*, November 09, 2012.

What's your move?

The evolution of the security team is as much about messaging as it is about programme design. CISOs need to change the narrative so developers and the business lines buy into the fact that cyber exists to support rather than hinder. That's a simple, yet important message that often gets overlooked or not told well.

From passwords and PINs to two-factor authentication and security awareness training, employees are going to have complaints and cyber teams should take the time to listen, be empathetic and inspirational. Clearly communicate the importance of operating safely and securely in every aspect of work and connect adherence — and non-adherence — to the organisation's financial results and future vision.

Work to change the perception of these requirements from punishment to responsibility. Look for ways to make cyber awareness more engaging, interactive, fun, even game-like, perhaps through augmented reality (AR) or virtual reality (VR). Make it clear that cyber is not here to be a speed bump but to keep everybody safe and cyber teams can do it concurrently.

CISOs should critically analyse where they and the cyber team spend their time, challenging the balance between strategy, plan, build and run (including react). In cyber, it's easy to get distracted by technology, however, when teams focus on their plan and their principles, technology decisions tend to become a little more obvious.

The opportunity is in the combination of automation, data analytics and AI, specifically ML, in a continuous controls monitoring model. That structure informs the data science aspects of decision-support systems and aligns real-time cyber outcomes with the organisation's risk profile and response activities. The goal is to capture and analyse data in real time with a standardised and dynamic security posture that is able to detect and respond to a change in the live threat landscape.

CISOs and their teams should be prepared for ongoing disruption. From a technology perspective, cyber security is the guardian of a broader digital ecosystem of interconnected vendors, suppliers, and partners. Managing that ecosystem and striving to ensure that it's secure is one of the greatest challenges that cyber security teams face.

Cyber professionals in general should continue to evolve their skills in a more system-based, strategic business direction. They need to adopt a multi-modal philosophy focused on standardisation, automation and data analytics. As an industry, cyber teams should not only seek to attract more talent in an absolute sense but be open to a broader range and diversity of talent, breaking down barriers to inclusion.

> Organisations have entered an automation arms race of sorts in the cyber estate. To get ahead of it, cyber teams should build-in realistic scenario-based thinking, testing and planning for threats that might come out of a variety of industries and geographies.

Matt O'Keefe
Partner, ASPAC Cyber Security Leader
KPMG Australia

Some key actions to consider for 2022

1. Change the narrative. Stop talking about technology and start talking about business
2. Don't limit yourself to the traditional definition of cyber security; continue to build relationships with other areas of the organisation and build a network of internal business partners
3. Embed scenario thinking, testing and responsiveness into the regular activities of the cyber function of an organisation
4. Make compliance an important outcome of your security programme, rather than the reason for its existence
5. Be an evangelist; be passionate about what you do and motivate people around the importance of security
6. Adopt a stance that cyber is a major part of what the company does, it's in the company's DNA. Help the organisation change its thinking about the role of security

Learn more

Shape the future cyber security workforce
Combine outsourcing, gig workers and automation to transform how capabilities are accessed.

Human firewalling
Overcoming the human risk factor in cyber security.

Exploiting the agile team culture
Four strategies for building an accountable security culture.

Consideration 3

Adapting security for the cloud

Enhance cloud security through automation — from deployment and monitoring to remediation.

Cyber security and cloud security are becoming synonymous. The only difference is the deployment environment. All the principles CISOs have talked about for years — data protection, identity and access management, infrastructure and vulnerability management — are all applicable to cloud security. What's different is the technology stack. The environment in which these security controls are deployed requires extreme automation, from deployment through monitoring and remediation. The 'what' and the 'why' haven't changed much, but the 'where' and the 'how' most certainly have.

Cloud security in the digital transformation age

While digital transformation propels cloud adoption and usage forward, it also puts institutions and businesses at greater cyber risk. Lack of cloud security skills means the business of protecting the organisations operates at a distinct trust deficit. Cloud may be everywhere, but so are hackers and other criminal actors.

As cloud adoption has proliferated, the stack has changed. The cloud environment requires increased reliance on automation. It necessitates automation from deployment to monitoring to remediation. Manual intervention creates higher degrees of incident reports based on internal misconfigurations; in fact, according to research by Aqua Security, 90 percent of organisations are vulnerable to security breaches attributable to cloud misconfigurations.[2]

At many firms, the expectation that the cloud development team should also function as the security engineering team can be seen. That's not realistic or sustainable in an effective way. Ideally, the security engineers are deep subject matter experts on that critical discipline and have relevant perspective on the basic structure and needs of the cloud environment. Similarly, cloud developers should be conversant with the role of security, but spend the majority of their time designing systems, coding, and analysing and maintaining the virtual environment. Certainly, organisations should expect cloud developers to embed security in their products to a much greater degree, but development teams should never be the security backstop.

Additionally, the skillset consistent with a traditional security road map is not necessarily right for cloud and cloud security deployments. It is easier for a cloud-native developer to get up-to-speed on security practices than for a traditionally trained security professional to understand the nuances of cloud development. In today's world, open source, 'infrastructure as code' and the corresponding tools for provisioning cloud infrastructure are essential for all types of cloud environments.

What's your move?

When it comes to security, cloud transformations must prioritise a broad array of regulatory and contractual factors. In terms of regulation, the veritable 'alphabet soup' of regimes — General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act (HIPAA), Directive on Security of Network and Information Systems (NIS Directive), Payment Card Industry Data Security Standards (PCI DSS), etc. —

> "The key skillset for cloud and cloud security is the developer skillset — the ability to write code and script and understand how DevOps works. Teaching professionals with that perspective the tenets of security, rather than security professionals how to write code, is a more effective strategy."
>
> **Steve Barlock**
> Principal, Cyber Security Services
> KPMG in the US

[2] Aqua Security, "2021 Cloud Security Report: Cloud Configuration Risks Exposed."

continue to drive compliance complexity, especially around security, and should be top of mind. In this environment, security teams are encouraged to add cloud security posture management (CSPM) to their toolbox. These automated class of tools offer pre-configured policy checks mapped to specific regulatory regimes to help identify cloud-related misconfiguration issues and compliance risks. With the click of a button, potential misconfigurations can be scanned and identified.

On the contractual front, both cloud providers and the companies that use their services are entering into shared responsibility agreements that often are misunderstood, especially on the client side. As a result, ownership of security of the cloud versus security *within* the cloud can be a murky concept. It becomes even more vexing when analysing platform, infrastructure, and software as a service. Organisational security teams should promote the view that all data that sits in the cloud is the responsibility of the organisation. On that basis, data needs to be encrypted (where appropriate, of course) and protected with the relevant controls.

CISOs and their teams are encouraged to work with business partners to help ensure everyone understands cloud-specific security requirements and collaborate with the provider to avoid misconfigurations. Organisations that take this approach and seek to remain informed cloud customers can position themselves for success.

You can also think of it as a subtractive model. This means that as you move from infrastructure as a service (IaaS) to software as a service (SaaS), the security team is responsible for less and less of the security estate. Either way, with the accelerated march to the cloud, enterprises should be ready to secure their own cloud-based data, especially through automation tools and protocols, within every type of contractual relationships.

To help ensure that cloud deployments feature the right level of security that is fit for your organisation and its risk profile, rich features and functionality, a strong recommendation is to build a dedicated cloud security team that is centralised from a governance perspective and distributed across the organisation when appropriate. Once structure and skills are securely in place, this team can be distributed into, or aligned with, specific business units. Continue to automate everything you can, where appropriate, particularly in the areas of deployment, monitoring and remediation.

> “Security architecture and knowledge of your cloud provider’s technology and security stack will likely be key in automating your security controls and strengthening your overall security posture. The cloud doesn’t protect and heal itself but knowing your options and security obligations can make it much easier to efficiently deploy leading security controls.”

Andreas Tomek
Global Cloud Security Leader
KPMG International
Partner, KPMG in Austria

Some key actions to consider for 2022

1. Automate your cloud security, especially around deployment, monitoring and recovery, eliminating manual processes
2. Build a centralised cloud security team that comes from the development ranks versus leading with traditional security skills
3. Lock in the operational responsibilities in a shared model, defining which entity is responsible for security in the cloud and which entity has responsibility for security of the cloud
4. Look to security posture management tools that have pre-configured policy checks mapped to different regulatory regimes
5. Construct an incident response process that is in sync with your broad cloud strategy

Learn more

Securing the cloud — the next chapter
How today's cloud-based solutions are unlocking potential business benefits and threats.

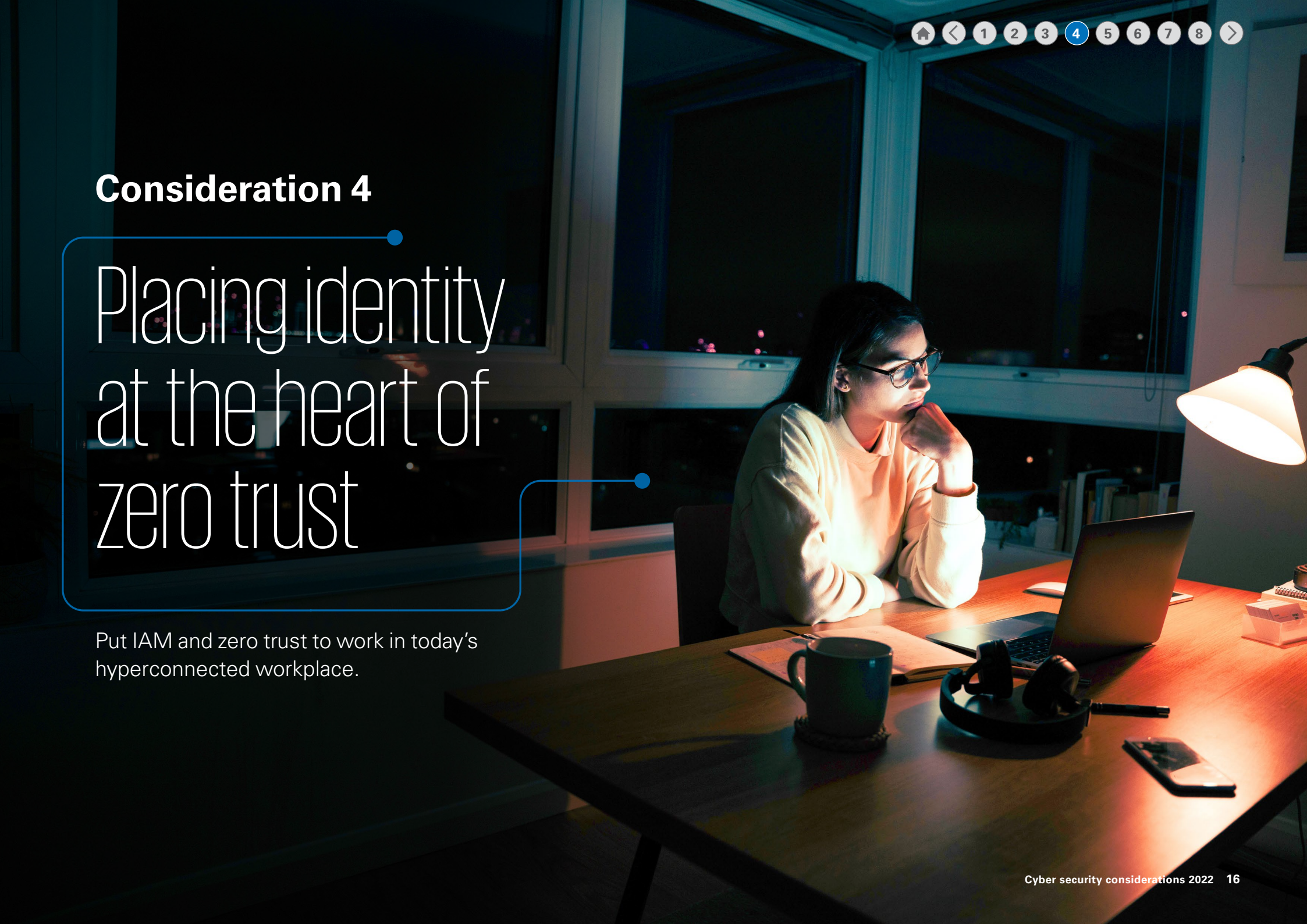
Are you a cyber pragmatist?
Adopting a new approach to business protection in the post-pandemic world.

Cloud data protection
Enabling scalable data protection capabilities.

Consideration 4

Placing identity at the heart of zero trust

Put IAM and zero trust to work in today's hyperconnected workplace.



With tens of millions of employees working at their kitchen tables and in their home offices, and billions of consumers purchasing goods on their phones from anywhere and everywhere, protecting mission-critical and other sensitive data within a complex ecosystem of suppliers and partners has never been more essential. In an environment where cybercriminals are often just a click away, organisations should adopt a zero-trust mindset and architecture, with identity and access management at the heart of it.

The demand for frictionless experiences

The explosive pace of digital transformation among both public organisations and private enterprises — especially during the pandemic — in addition to a rapidly normalising work-from-home structure, has provided bad actors with a window of opportunity. As a result, there have been an unparalleled number of cyberattacks in recent months, particularly ransomware events and supply-chain attacks. Current identity and access management (IAM) models, originally built to manage digital identities and user access for single organisations, are now being re-conceptualised to offer the right level of resilience, as well as deliver critical authentication features suitable for federated, private, public or multi-cloud computing environments.

More and more, customers, suppliers and corporate users expect frictionless experiences, unencumbered by ever-changing passwords and multiple layers of digital identification. Extended ecosystems of third-party partners, contractors and gig workers — all extensions of an enterprise's workforce — require access at different times to different levels of sensitive corporate data. Unfortunately, a lack of purpose-built processes for these constituencies too often results in significant breaches in the security chain.

The line between business-to-consumer (B2C) and business-to-business (B2B) security continues to blur, with enterprises moving away from separate security disciplines. Rather, organisations are in many cases merging the two in terms of their authentication management approaches. As security technology matures, there may be a broad move to identity proofing and passwordless authentication, not just for consumers, but also for enterprises. Scalability is likely to be an issue when it comes to the sheer numbers of B2C and B2B clients relative to corporate cyber professionals.

As an automated approach that can help eliminate costly and cumbersome manual processes, reduce an environment's attack surface and establish fit-for-purpose cyber policies and principles — the zero-trust security model is increasingly being viewed as a viable security approach in the post-pandemic world. With identity at its core, zero trust enables organisations to evaluate whether a user is properly authenticated; isolate the resource the user is attempting to access; determine if the request is from a trusted, stolen or third-party device; and confidently decide whether access should or should not be granted.

The emergence of zero trust represents a mindset shift in which the cyber team assumes compromise in connection with system access, and makes security decisions on the basis of identity, device, data, and context. With users demanding ever-faster access, and cloud-centric structures expanding the attack surface, existing security solutions and resources may not be formidable enough to adequately protect data as it moves through the network.

> "The zero-trust model and architecture can't succeed without placing identity at the centre. Develop your zero-trust road map around identity to facilitate adoption and strengthen ROI."

Deepak Mathur
Managing Director,
Cyber Security Services
KPMG in the US

What's your move?

To address the growing access and identity risks that continue to destabilise organisations financially and operationally, as well as respond to an expanded regulatory environment, enterprises and institutions should consider new standards, tools and strategies to better secure their systems, data and infrastructure.

In a post-pandemic business setting in which many, if not most, workers are remote, interim fixes and temporary Band-Aids will likely prove to be unable to keep up with the pace and virulence of cyberattacks and threats that are already bombarding businesses and government agencies. Soon, users will likely no longer need to be 'on network' (i.e. through a persistent virtual private network [VPN] connection). Conditional access is expected to come from the trust and assurance that is engendered by the devices people use, and the authentication and decisioning processes organisations implement.

The concept of zero trust is a growing point of interest, but many CISOs — and even more so, CIOs and Heads of Infrastructure — should continue to work toward the most effective means of implementing an organisation-wide zero-trust architecture, as well as a set of principles that aligns with business and operating priorities. And, of course, all of this should be considered within the context of the organisation's overall cyber security, risk management and technology programmes.

The principle of least privilege is perhaps one of the simplest ideas relating to the way data is protected, yet, it's also one of the most important. The general idea is that users, processes, workloads, and applications should only be granted the lowest degree of system resource access rights necessary to carry out their role. For example, web designers don't need access to financial records, and individuals responsible for updating the product listings, don't need admin rights. Organisations should continue to view the least-privilege access principle as a core element of the zero-trust model.

> "Zero trust is not a feature, it's not a technology, it's not a standard. It's an approach to and a framework for security, with identity as a key component."

Jim Wilhelm
Global IAM Leader
KPMG International
Principal, KPMG in the US

Some key actions to consider for 2022

1. Experiment or begin to have a strategy around passwordless authentication for selected use cases
2. Be sure your identity change to programme has a sound data and analytics foundation
3. Embed a zero-trust mindset into your overall cyber strategy
4. Commit to creating a frictionless experience to enhance user and customer experience by streamlining authentication and identity management
5. Automate security functionality to enable highly skilled professionals to focus on more strategic activities
6. Accept that adopting a zero-trust approach is a journey — it takes time to implement

Learn more

Is authentication a future enabler?
Why we need seamless authentication for digital infrastructure.

Everyone can embrace 'zero trust'
The perimeter-less cyber security model is a promising design for the evolving threat environment.

Achieving cost efficiencies in identity and access management
A strategic approach to handling IAM, with automation and right-sizing of your organisation, can help reduce operational costs.

Consideration 5

Exploiting security automation

Gain a competitive advantage through smart deployment of security automation.

While many see automation as a universal panacea, experience shows that the best outcomes derive from a pragmatic approach to application. Some of the greatest potential automation benefits come when there's a focus on implementations designed to help solve business problems: augmenting available human talent by more efficiently orchestrating mundane tasks; gaining a competitive edge in areas where speed is important; and analysing large, often unstructured data sets. In a hyperconnected world with a myriad of tools available, organisations should be future-ready as the threat landscape continues to expand and increase in complexity.

Realise the business value

Companies are successfully automating the security function and freeing up resources by applying automation to routine, repetitive tasks. Work that was previously performed by highly trained professionals, such as vulnerability scanning, log analysis and compliance is being standardised and automatically executed. This can boost the analyst's productivity, speed up incident detection and reaction times and can provide an opportunity for scalability. Automating lower level threats and routine transactions augments the security operations centre by enabling it to prioritise tasks more effectively and respond more quickly to threats that require human intervention.

In situations where data sets are too large or complex for direct analysis, automation has been tested to be tremendously valuable and is being applied in many sectors to discover hard-to-identify links and patterns. Automation is also being effectively employed to tasks that benefit from increased speed, such as identifying security incidents in voluminous log data, and performing high-volume data discovery, where analysing individual files is often inefficient.

From a DevOps perspective, security automation should be built into every critical intersection point in the SDLC from user stories and secure-code reviews to threat modeling and secure-design reviews with the help of both static and dynamic application security testing (SAST and DAST) products. With that in mind, DevSecOps is gaining momentum in response to the need for rigorous security that moves at the speed of cloud delivery.

With the shift to the cloud, organisations don't have consistent control over software versioning and the general features available in the cloud environment. Automation has been integral in securely assessing risk and adopting new baseline features, as needed. In multi-cloud environments, unintended data exposure, mismanaged account permissions, unsecure network connections, ransomware attacks and other risks are major concerns for organisations. Automated security frameworks can provide better visibility and control.

> "The growing maturity of cyber automation capabilities makes them a critical component of cyber security strategy. organisations should seek opportunities to leverage automation to displace repeated manual tasks, augment intelligence for analysts, reduce latency from complex processes and help achieve the scale and speed necessary to protect critical assets."

Matthew Miller
Principal, Cyber Security Services
KPMG in the US

What's your move?

Start small and identify the use cases for automation that your organisation truly needs and with which it will be able to generate business value. While it is prudent to implement integrated corporate security architecture, keep it simple and do not over-engineer solutions. Fearing they may miss the latest trend, companies may go on a buying spree, acquiring various tools that often go unused for lack of knowledgeable employees. Resist that impulse.

Leverage your current technology stack first. There is an enormous amount of advanced automation capabilities that exist within current tooling and often it is not necessary to look outside of your organisation. Similarly, seek out colleagues with existing automation experience and consider making them part of the cyber team. It's easier to take someone that has previous experience using robotic processing automation (RPA) in other areas of the business, or with a previous employer, and teach them how to apply it within cyber than to take someone that has basic cyber credentials and teach them RPA.

Cyber security teams are increasingly overwhelmed by ever-growing workloads. It's a smart move to use tools sensibly in terms of automating some of your Level 1 or low-level incident management, so you have enough time to devote to problems that require more nuanced or creative thinking.

Rather than having a separate security team for identifying vulnerabilities and breaches, security automation should shift left and be present at every critical intersection point in the SDLC, from user stories and secure code reviews to threat modeling and secure design reviews. Use products like static and dynamic application security testing that seamlessly integrate into the continuous integration/continuous delivery (CICD) pipeline, making it less challenging to incorporate security into the entire SDLC.

> Certain technologies, like security orchestration automation response (SOAR), are inherently complementary, meant not to replace human analysts, but to augment their skills and workflows for a better employee experience.

Shreyashi Sengupta
Partner, Digital Trust
KPMG in India

Some key actions to consider for 2022

1. Take a proactive approach to security automation by focusing on threats instead of incidents
2. Automate mundane tasks to free up human capital and cognitive ability for more important activities
3. Leverage existing technology and automation experts within your organisation
4. Build security automation into every critical intersection point within the SDLC
5. Push the limits of what's already known to be possible — be willing to fail but learn quickly and implement that insight
6. Keep it simple and don't over-engineer solutions or acquire automation tools that don't fit the problem or lead to business value for the firm

Learn more

Embrace automation as the rising star
Bringing a host of expected efficiency and workforce benefits.

Agile security in cloud DevOps
A future approach to security and building software.

Security monitoring for software build pipelines
First steps to increase confidence in your build environment's integrity.

Consideration 6

Protecting the privacy frontier

Move to a multidisciplinary approach to privacy risk management that embeds privacy and security by design.

At many companies, cyber security and data privacy are seen as different disciplines that often operate in silos. In an environment where so much sensitive data is captured and utilised, the review of third parties, new systems and new applications requires a multidisciplinary approach to privacy risk management — one that includes both privacy and security from the design phase through to organisational change management.

Keep individual rights top of mind

Today more global awareness and recognition exists for individual rights in relation to their personal information. With the cascade of global regulations, from the GDPR in Europe to various individual regimes across Asia, North and South America — notably the Brazilian General Data Protection Law (LGPD), the California Consumer Privacy Act (CCPA) and other emerging US state laws, and federal and provincial laws being enacted in Canada — the focus on data rights, privacy and security is sharper than ever.

In near-real time you can see the evolution of the regulatory environment regarding data privacy. Governments and regulators are acknowledging that privacy incidents resulting from breaches are just a subset of the broader universe of cyber incidents. In addition, they're demanding organisations disclose breaches much sooner, and in a much more transparent way, regardless of whether it's had an impact on privacy.

Most jurisdictions globally now have in place breach-reporting obligations, so there's no flying under the radar, with industry and non-privacy-specific regulators now taking a real interest and implementing similar obligations. This is a huge change from just a few years ago, pre-GDPR, when there was little more than a patchwork of rules and regulations worldwide.

There is nearly universal harmony in the sense that so many countries/territories have implemented rights-based privacy rules and regulations aimed at empowering the individual and giving them back the control they relinquish when they share their personal information. With so many different regulations, however, the regulatory landscape is becoming increasingly difficult to navigate and comply with, particularly for global businesses operating in multiple jurisdictions.

Automation is the key, especially for organisations that don't have the bandwidth and resources to manage areas such as privacy risk identification and reporting. Organisations put themselves at a disadvantage if they don't have, for example, automated IAM processes supported by effective metadata management. In a virtualised world, without automated controls embedded across day-to-day processes — including automation of subject access requests — most organisations simply will not have enough personnel to manually oversee new servers, data stores and applications in a manner that is efficient and effective.

> Privacy programmes of the future must incorporate privacy-by-design thinking, which isn't just a philosophy, it's a cultural mindset and an organisational shift. Because privacy is not a stand-alone legal discipline, but instead a multi-faceted approach to data protection that includes privacy engineering, cyber security, technology and risk management.

Sylvia Klasovec Kingsmill
Global Privacy Leader
KPMG International
Partner, KPMG in Canada

> It's paramount to secure explicit consent from any individual or entity at or prior to data collection. In turn, customers need to signal they understand the purpose of collection and what will be done with their information. Being fully transparent at all times should foster trust and help avert any ethical data-mining issues.

Matthew Quick
Director, Technology
Risk and Cyber Security
KPMG Australia

What's your move?

Keeping individuals' data secure and taking data privacy seriously is more than just implementing new processes to satisfy regulatory requirements — it's a cultural shift. Like security, organisations should adopt a privacy-first or privacy-by-design mindset. Embedding privacy and security into organisations change, culture, processes, technology and products is a good starting point and will likely help companies avoid costly retrofits and regulatory investigations, and foster trust inside and outside the organisations.

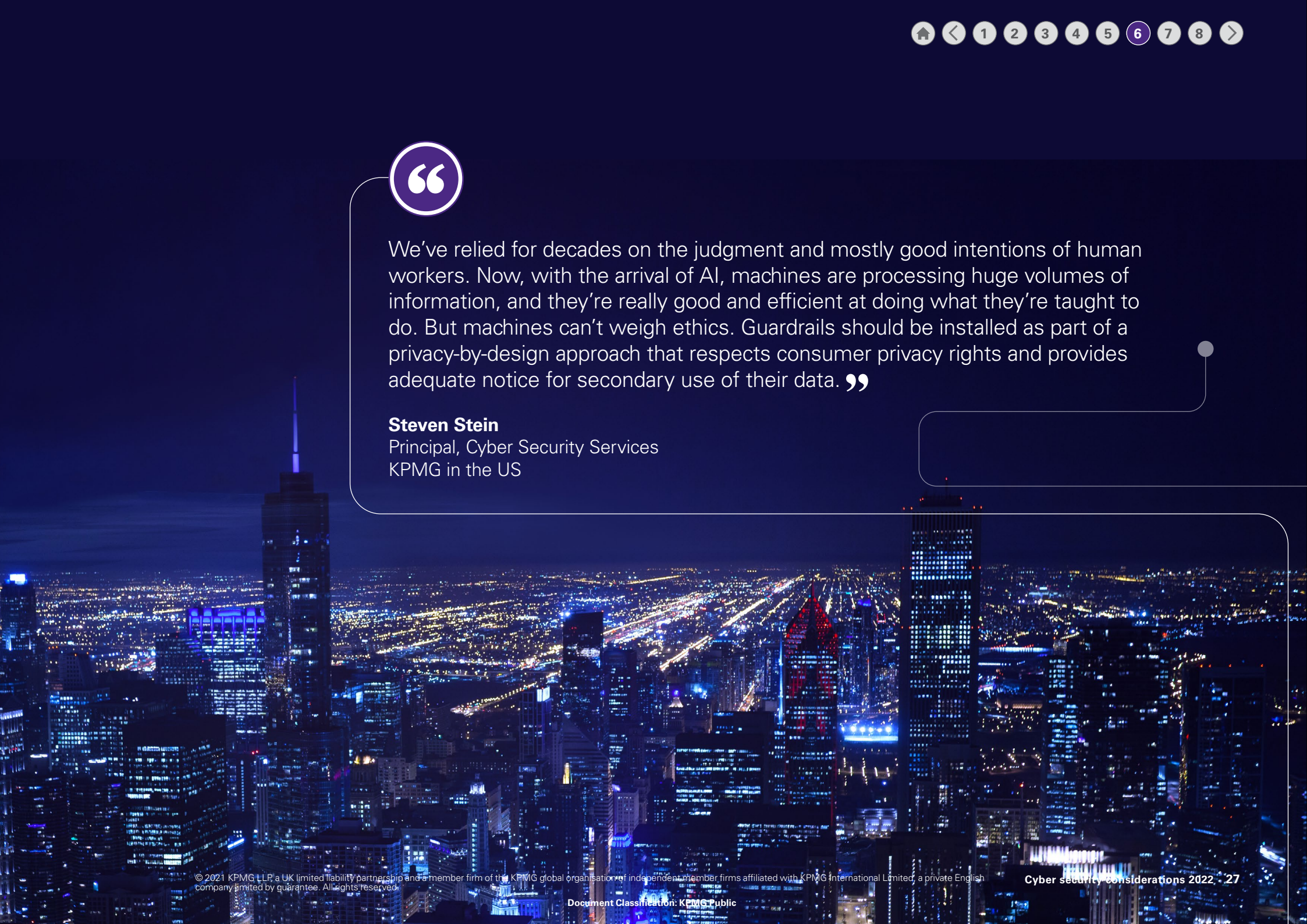
This cultural shift should start at the top, with the C-suite recognising that data belongs to their customers, clients and partners; and they have a responsibility to collect and employ it legally and ethically. With that goal in mind, companies are encouraged to develop complementary relationships between business lines, the privacy office and the security team. Similarly, there should be clarity regarding the responsibility for identifying and reporting on privacy risks, as well as owning and demonstrating a position of accountability that can be defended in front of a regulatory body.

Automation is critical for the effective management and enhanced efficiency of privacy processes, particularly privacy impact assessments and data subject access requests. This can enable the organisation to leverage the governance, risk and compliance technologies in which they've invested — content and workflow management, and risk analytics, for example — which, in turn, can operationalise privacy modules that can make a tangible impact on data and access mapping.

Automation can also help break down the silos between the cyber security and privacy functions. These are very complementary disciplines, and organisations can align them operationally and essentially 'share' bigger budgets, which at many companies the cyber team enjoys while the privacy team doesn't.

With metadata and data mapping, for example, cyber and privacy teams rely on the same assets. Both teams should understand the data to which the organisations has access and their rights to use and process this information. They can then work together to implement appropriate security and privacy controls, while keeping in mind the zero-trust philosophy. Automation can enable them to better understand where their core data assets are located and how to use them more effectively. Then they're pivoting toward leveraging the same financial resources in service of achieving the same outcome: protecting the 'crown jewels.'

Becoming familiar and conversant with emerging technologies such as automation and AI is important and recommended, but the basic principles from security and privacy perspectives are largely constant. That is, secure consent from individuals whose data you collect; only gather the data that is relevant; retain it only as long as it is needed; dispose of it when it's no longer needed; and protect it properly.



> We've relied for decades on the judgment and mostly good intentions of human workers. Now, with the arrival of AI, machines are processing huge volumes of information, and they're really good and efficient at doing what they're taught to do. But machines can't weigh ethics. Guardrails should be installed as part of a privacy-by-design approach that respects consumer privacy rights and provides adequate notice for secondary use of their data.

Steven Stein
Principal, Cyber Security Services
KPMG in the US

Some key actions to consider for 2022

1. Educate senior and business management on why striving to ensure individuals' data collection consent is so important and how failure to respect consumer rights can negatively impact the company
2. Align your data privacy programme with both C-suite and business-line leadership priorities and vision to help ensure everybody is on the same page from collection, consent and usage perspectives
3. Adopt a privacy-by-design standard to supplement and complement the rules, regulations and regulatory expectations around privacy
4. Translate paper-based policies into verifiable business practices to convince consumers and regulators of your commitment to respecting consumer rights and protecting data
5. Explore opportunities to implement a data privacy management technology tool to automate processes, comply with regulations, help increase response speed and assist with reducing human error

Learn more

Privacy technology: What's next?
The evolution of data-privacy technology in the age of automation.

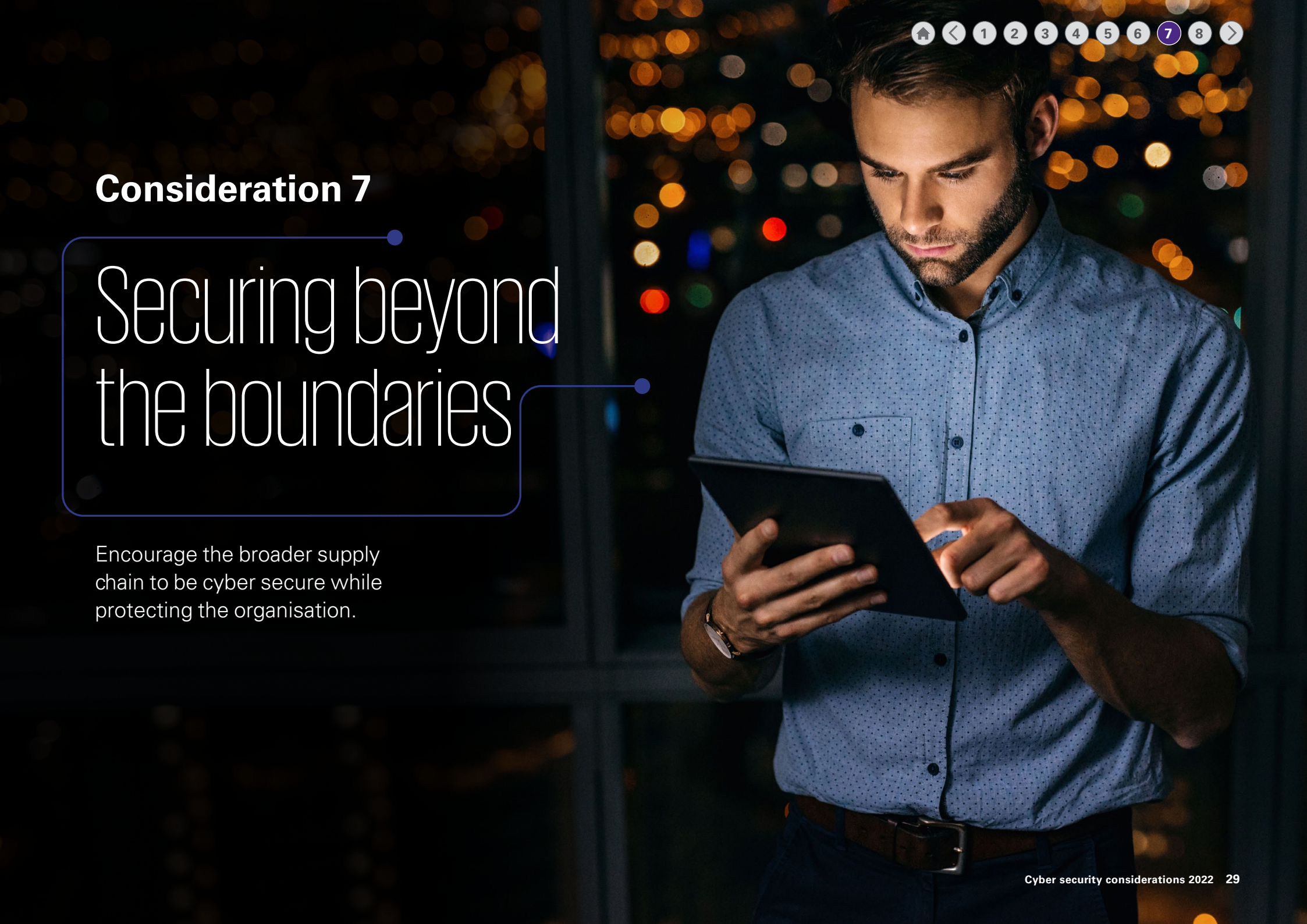
A balancing act: Privacy, security and ethics
How building the right data compound can help drive growth.

Corporate data responsibility: Bridging the consumer trust gap
As businesses collect more personal data, consumer concerns are rising. Learn how businesses can take action to reclaim consumer trust.

Consideration 7

Securing beyond the boundaries

Encourage the broader supply chain to be cyber secure while protecting the organisation.



The race to transform digitally continues to be a high priority for enterprises, large and small. Becoming a digital-first organisation implies a data-centric approach in which data is shared on a near-constant basis throughout a complex and connected ecosystem of partners and suppliers. This data fluidity between third, fourth and fifth parties creates numerous opportunities for cyberattackers to compromise systems and data. How can CISOs help secure their own organisations, while encouraging their broader ecosystem to be cyber secure?

Ecosystem security: The current state of solutions and obstacles

Most organisations are no longer the single, monolithic entities many customers have long believed them to be. They're deeply operationally dependent on a robust supply chain, as well as a myriad of traditional and non-traditional partners that often have direct access to business systems and data. Although regulatory standards and mutually agreed-upon security frameworks can help minimise the impact of third-party cyber threats, there are situations where the participants in these complex ecosystem structures — cloud providers, SaaS companies, Internet of Things (IoT) device manufacturers, etc. — may not have clear obligations for establishing adequate controls to protect their partners' data, leaving the entire network vulnerable to cyberattacks.

From a contract negotiation perspective, there should be proper vetting of all potential vendors' organisational security policies, as well as the security built into the products and services to be accessed. Currently, this requires tremendous and perhaps infeasible due diligence by each ecosystem partner. In most cases, point-in-time, periodic assessments are conducted manually by third-party security programmes managed internally or outsourced.

Some organisations, particularly in regulated industries, are also making better use of security-ratings companies, whose services supplement point-in-time assessments by providing security risk scores against a set of pre-defined parameters. This helps to determine whether an ecosystem partner's security is 'good enough' by offering detailed qualitative and quantitative analysis.

Unfortunately, this approach is no longer fit-for-purpose in today's ever-evolving digital environment. Although this form of trust — or lack-of-trust — framework can provide near-real-time risk visibility, it's simply too time-consuming and costly for the majority of organisations. As a result, many businesses, third-party vendors, and even regulators are under increased pressure to provide continuous assurance over the security of their ecosystems. This is only going to become more challenging as the complexity of the supplier ecosystem increases, and fourth parties, shadow-IT, and a lack of SaaS provider oversight demand more and more attention. As a result, CISOs are faced with the difficult task of transitioning away from the compliance-based strategy to a much more proactive approach that puts continuous monitoring, usage of AI/ML-based solutions, threat intelligence, and zero trust at the heart of their ecosystem security model.

> "With cloud and digital technologies creating hyperconnected, multi-partner ecosystems, there's new willingness to proactively address the associated risk. Automation will continue to play an important role in activating appropriate corrective measures in these environments across third, fourth and fifth parties."
>
> **Atul Gupta**
> Global Cyber Security Lead for TMT
> KPMG International
> Partner, KPMG in India

What's your move?

Regulations relating to cyber security will likely continue to tighten and expand, as exemplified by executive orders from the US White House on supply chain, as well as the European Union's continuously evolving NIS Directive, which has drawn clear lines around how member states, industries and organisations should enhance their inward and outward cyber security policies, especially in a post-pandemic world.

A strong risk management framework that looks both inward and outward is key especially for high-risk industries, such as financial services, energy and healthcare. A future-proof approach should also be applied across key industries around the world, in an effort to help ensure that all ecosystem partners follow a clear path in protecting their own organisations, as well as the broad ecosystems within which they operate.

Another key area of focus should be on automation, including the use of AI/ML across the ecosystem. AI/ML can be applied to security policies to address shadow IT issues and provide better oversight of third-party SaaS products, as well as to implement self-service chatbots and automate many aspects of the organisation's third-party risk management processes.

Continuous controls monitoring (CCM) takes this a step further, moving security assessments away from point-in-time activities that become obsolete quickly. CCM can expedite vendor cycles through the use of machine-readable assessments, which ultimately enhance risk and control oversight. To be effective within the context of a partner ecosystem, CCM requires vendor participation and acceptance of this type of assessment. This model can inspire ecosystem partners to move from a compliance-based approach to a more operational focus that allows for corrective measures in real time with or without human intervention.

Alongside a move toward continuous assurance, regulators and even large organisations may look to adopt a more active approach to building ecosystem security. In an interconnected business world, companies are realising they have a responsibility to protect their supplier ecosystem, particularly partners that don't have the same level of resources. This could mean providing a monitoring/threat intelligence service across their supply ecosystem and collaborating with partners to defend against identified threats. While in its infancy, regulators and national bodies are increasingly taking this approach, and larger, more mature organisations could follow suit.

> Many companies are looking at machine-readable assessment formats, which help cyber teams think about third-party risk assessment as part of continuous controls-monitoring. The mindset here is no longer compliance-based, it's now operations-based. Existing third-party risk programmes in virtually every industry aren't prepared for this transition.

Jonathan Dambrot
Global Third Party Security Leader
KPMG International
Principal, KPMG in the US

Some key actions to consider for 2022

1. Keep a close eye on regulatory requirements as they continue to evolve and focus on supply-chain security
2. Consider CCM as a way of moving ecosystems from compliance to a more operationally based view of security
3. Explore opportunities to automate and leverage AI/ML in supply-chain security approaches to enhance security and enable skilled security workers to focus on more strategic activities
4. Don't overlook the operational technology (OT) supply chain; as IT and OT systems continue to converge, attackers will likely seek to exploit OT systems in an effort to compromise business data
5. Larger, more resourceful organisations should seek to take a capacity-building approach by applying security measures to protect their broader ecosystem, in addition to their own environment

Learn more

The extended enterprise — securing the future
Charting the course toward a more secure third-party ecosystem.

The changing third-party ecosystem
Adapting the approach to help secure the evolving ecosystem.

Streamlining third-party risk management with AI
Introducing an AI digital worker to your third-party security efforts.

Consideration 8

Reframing the cyber resilience conversation

Broaden the ability to sustain operations, recover rapidly and manage the consequences when a cyberattack occurs.

In today's volatile digital environment, resilience should include consideration of how well companies understand, anticipate, and are prepared to recover from the potential impact of a major cyber incident. CISOs and their teams are encouraged to initiate a dialogue with senior leaders that challenges the assumption that the organisation can either absorb a cyberattack or, at worst, recover in a few days. They should explore the ability to sustain operations if the disruption lasts for multiple weeks while managing media, regulatory and public attention.

"There is a plan"

When CEOs are asked how they approach the possibility of a cyberattack, most say, "There is a plan" and "It's high on the board's agenda." Experience from the last few months suggests the more pertinent questions are: How prepared are you as a business to face a four- to six-week outage as a result of a cyberattack? How would it impact customer service? What would it mean for your call and distribution centres? Would you be able to cover the next payroll? Could you pay suppliers? How might an outage impact the company's regulatory and legal requirements?

Resilience demands an assessment of the key operational processes of the business and a strategy for protecting them.

In today's market reality, a major cyber event is almost inevitable for most companies. With that in mind, thinking about the evolving mindset of security professionals, the focus for many CISOs today is in equal parts likelihood reduction and consequence management. Clearly, it's not enough to detect a successful breach, it's equally important to act fast enough to limit the damage. Indeed, malicious code has been known to lie dormant within a breached environment for months before surreptitiously activating and re-infecting the system.

In recent years, hackers have increased their focus on two types of cyberattacks.

— **Ransomware attacks:** Clearly, there have been a number of incidents in which an attacker breaches an organisation and encrypts its data, rendering it inaccessible until the victim pays an exorbitant ransom to regain access. Except now, attackers are using double extortion tactics, throwing in the additional threat of publicly leaking the encrypted data if an additional ransom payment isn't made, while simultaneously targeting the organisation's online backups.

— **Supply chain attacks:** Increasingly, attackers are targeting companies that produce important software and are vital logistical links in much larger, broader networks. From the hacker's perspective, infiltrating a smaller target requires much less effort to inflict major damage.

While these attacks aren't overly sophisticated in terms of methodology — they still use phishing, password spraying and vulnerability scanning — they're incredibly effective. We expect these kinds of attacks to increase going forward. For ransomware specifically, as long as companies are willing to pay the ransom, this problem will likely persist.

> "The business has to play an active role in digital resilience: scenario simulations, knowing where the dependencies are, plans that make clear what they can do and what they're not able to do. So there can be a collective response."

Dani Michaux
Partner, EMA Cyber Security Leader
KPMG in Ireland

In an increasingly interconnected and interdependent digital world, these events, such as the WannaCry attacks a few years ago and the Colonial Pipeline attack earlier in 2021, can have much broader and systemic implications on an economy, motivating regulators across the globe to issue new rules and directives for a broad array of industries. Perhaps the most pertinent example is the European Union's 2016 Network and Information Systems (NIS) Directive, which aimed to create a high standard of network and information security, and its proposed replacement, NIS2, looks to address the growing range of digital infrastructure on which our societies now depend. Sector specific regulatory initiatives, such as the Digital Operational Resilience Act in Europe, will also place increasing obligations on industry around incident response, vulnerability disclosure, penetration testing, encryption and other areas.

What's your move?

The CISO and their team can't ensure cyber resilience on their own. It should be an organisation-wide effort with buy-in and active support from senior management, finance, marketing, and other stakeholders. There's an interesting dynamic developing, particularly in Europe, where a number of roles — CISOs, Chief Risk Officers (CROs), Chief Data Officers (CDOs) — are evolving toward what might be referred to as a Chief Digital Resilience Officer, which entails a broader agenda of shared security, technology risk and business continuity priorities.

CISOs should educate leadership about the risk and consequences of a breach and why cyber resilience is so important. However, avoid excessive technical jargon — talk about the threat landscape, the cost of failure, time to recover and potential impact.

Take the time to review your organisational cyber resilience plans and strive to ensure they're fit for purpose. Plans that were previously developed for physical resiliency issues are likely not suitable for a cyber event. There are several key differences between physical and cyber resilience planning: in cyber, there is often a large degree of uncertainty as to what has actually happened, when, and how; the impact is often organisation-wide, as opposed to relegated to a specific location (and it often extends beyond the organisation); and it is often assumed that IT has the capacity to help manage the incident — which may or may not be the case.

Don't wait for a cyber event to transpire to test your plans. Regularly simulating real-world cyberattacks with executives is important and helps them understand the potential impact of a cyberattack on the organisation, and what it takes to respond and recover. You cannot fully replicate a real-world event, but the better-prepared the organisation is, the better the chances of managing incidents more effectively.

Of course, cyber teams still have to focus on security fundamentals to strengthen resilience across the organisation. Indeed, many breaches are successful because the target didn't do the easy work like identifying critical assets, securing accounts with strong passwords and patch management. However, in today's fast-paced digital world, this alone is not sufficient. Organisationshould supplement the basics with solid detection capabilities, an advanced ability to respond and recover rapidly, and a focus on managing the consequences of a cyberattack.

> "What to do right now, or next? Identify the five to ten business processes and their dependencies on key suppliers that pose the greatest risk, as measured in financial impact, data corruption or regulatory triggers. This can give you a clear view of priorities, so you can implement the proper controls and strategies."

Wilhelm Dolle
Partner, Head of Cyber Security
KPMG in Germany

Some key actions to consider for 2022

1. Consider how long you can sustain the business if significant functions are down and what it would mean from a customer impact perspective
2. Think about how a significant cyber event would affect your dependency on suppliers
3. Elevate the topic of cyber security and cyber resilience to board level
4. Question whether your current resilience plans are fit for purpose for a cyberattack and take appropriate corrective measures
5. Have the humility to acknowledge that your assumptions might be wrong and an alternate plan that can be operationalised quickly
6. Help the C-suite develop their crisis management capabilities and their individual roles in the event of a cyberattack through regular, real-world simulations
7. Focus on the fundamentals, but also invest in detection, rapid response and recovery capabilities
8. Collaborate with relevant industry specialists if you don't have the in-house capacity or capability

Learn more

The changing shape of ransomware
How to defend against and respond to ransomware attacks.

Securing a hyperconnected world
How to prepare for and respond to cyberattacks targeted at critical infrastructure.

How to safeguard your OT during the 'ransomware pandemic'
The changing face of ransomware.

Conclusion

In a not-so-distant future

Going forward, the hyperconnected smart society will likely face increased cyber risks on multiple global fronts via numerous evolving threat vectors. Clearly, the technological advances powering business, communications and entertainment bring with them new perils. In this report, we've explored such timely topics as the evolving security team, automating the security function, data privacy and securing the ecosystem. Now, we take a look at several emerging cyber security challenges. While none of these topics are new, we believe they'll soon become major areas of focus for cyber professionals across virtually every industrial sector.

IIoT

As the Industrial Internet of Things (IIoT) continues to expand, millions, if not billions, of cloud-based sensors, machines, and other connected devices may potentially become vulnerable entry points for cyberattackers. The urgency from a cyber perspective is that, in the rush to innovate, the software used in these hyperconnected systems often doesn't include the appropriate risk management controls.

Clearly, IIoT is creating a new set of attack surfaces. Although manufacturers' priorities are changing, to this point, the architectural design of sensors in connection with, for example, air quality, traffic, waste management and the overall energy grid, may not have fully addressed security. There can be major operational constraints on individual devices regarding power and weight limitations that can get in the way of embedding controls, but infrastructure security simply cannot be an afterthought.

Organisations should expect to focus on how deeply security is embedded within the products that enable the IIoT and the way these devices are leveraged within the broader ecosystem. With regards to strategically deploying those products across an enterprise or smart city environment, you're talking about a much broader range of people, policies, procedures and technologies, as well as considerations such as anomaly monitoring, identity management, zero trust and more.
Going forward, we believe IIoT should be viewed as a component of a broader ecosystem of solutions that ultimately constitute an overarching security posture.

> "It's a vicious cycle, where every new technology expands the threat landscape, and it prompts rounds of cyber innovation to help improve defense capabilities. Is this race the only way to operate? I think embedding security in every aspect of IT, OT, every related process and procedure at the DNA-level of an enterprise is the inevitable future and the only way out."

Prasad Jayaraman
Principal, Americas Cyber Security Leader
KPMG in the US

> Today society lives and does business in a digital world of data, devices and dependency. Trust is placed — knowingly or unknowingly — in technology in a way that would be unthinkable a decade ago, which raises questions of security, safety, privacy and even ethics. Security professionals should navigate this new reality, helping business leaders understand the implications of placing trust in technology and its resilience, while simultaneously anticipating how that technology might be exploited by others. This can bring a different and valuable perspective, but there is also a duty to offer advice that is pragmatic and practical.

David Ferbrache
Chief Technology Officer, Cyber
KPMG in the UK

5G networks

The prospective connectivity capabilities made possible by emerging applications sitting on 5G networks is exciting. But these software-based connected ecosystems should prioritise not only technical innovation, but also the security of the devices that can facilitate these connections.

A 5G network is fundamentally different from 4G in terms of speed, bandwidth, latency and overall sophistication. Of course, 5G is going to enable massive connectivity advances, but it also brings a different set of security challenges and requires highly sophisticated security architecture, monitoring and controls. Some of those concerns play into the geopolitical supply chain tensions that exist today regarding the sourcing of key technology components and infrastructure.

It also begs a question about trust. With 5G, cyber professionals will likely be in a position where millions of devices, each with its own digital identity, may be connecting simultaneously in untrusted environments characterised by very fluid connection architectures. In our opinion, this air of unpredictability suggests organisations should assume an ongoing zero-trust mindset and an authentication architecture that is flexible and adaptable to these new dependencies and resilience issues.

AI

Already a burgeoning area, AI — ML and deep learning in particular — will likely remain a captivating topic going forward.

Clearly, securing learning AI applications is a very different challenge to securing conventional systems. There are so many questions: Is the software operating within its trained parameters? How much unconscious bias is present? Is the application being manipulated by a bad actor or adversarial AI in an effort to compromise sensitive information? Looking ahead, cyber professionals may also have to think about the integrity, predictability and acceptability of the AI application within the context of the operating environment for which it's been trained and designed. In this sphere, CISOs and their teams should expect to build strong partnerships with the Chief Technology Officer and their data science team. As a security matter, this is new territory.

In the near future, cyberattackers will likely also make use of robotic process automation, ML and deep learning. Probing and testing the vulnerabilities and defenses of a professional environment may soon be as easily automated as constructing spam campaigns or compromising email. Attackers are using AI, but they don't have boundaries. In the short term, criminals are more likely to have an upper hand in leveraging AI to industrialise attacks. It's already happening and will likely continue.

There are numerous liability issues around AI. Legal frameworks are phenomenally immature and regulatory initiatives abound. It may take time for cyber security professionals to appreciate the implications, while cybercriminals will likely be more entrepreneurial.

Contact us

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

Martin Tyley
Partner,
Head of UK Cyber
KPMG in the UK
E: martin.tyley@kpmg.co.uk

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

kpmg.com/uk