KPMG

Cyber security considerations 2024

Technology innovations demand strategic pragmatism.

Foreword

As 2024 unfolds, organisational leaders, from the CEO down, have much on their plates. They are contending with diverse challenges around achieving sustained growth, navigating the impact and risks of emerging technology, and attracting and retaining talent, to name just a few. For their part, Chief Information Security Officers (CISOs) are increasingly being viewed as proactive co-stewards of these ongoing business imperatives – not merely the cavalry leader riding in to save the day during a crisis.

In our annual *Cyber security considerations* report, a diverse cross-section of global KPMG cyber security specialists explores eight considerations that CISOs and their teams are encouraged to prioritise in the coming year to support the organisation's business growth objectives by mitigating the impact of specific cyber incidents and reducing overall cyber risk exposure.

Organisations worldwide face many cyber security challenges requiring the implementation of controls to build and embed resilience, meet regulatory mandates, and reduce overall risk. However, the rapid emergence of artificial intelligence (AI) as a strategic tool for both legitimate and nefarious purposes is rapidly moving up the list. The democratisation of AI – these advanced technology solutions and models are now largely accessible to anyone with a credit card via the cloud – has at once revealed new paths to value creation and exposed significant potential risks. AI is proving to be a true organisational game-changer, including for security teams.

This evolving threat landscape requires organisations and their CISOs to view security through a new, more pragmatic lens. More than ever before, they must balance data security and privacy with the broader objectives of the business.

From a cyber security perspective, the impacts of societal, economic, political, and regulatory developments are more consistently felt globally today. The simple reason is the world is more connected. The most acute effect of the connected business ecosystem continues to be within global supply chains – for all practical purposes, there are virtually no regions of the world that are isolated anymore.

However, there remain local nuances. For example, there are regulatory requirements to which businesses must adhere that remain uniquely regional, such as certain markets being more sensitive to the protection of personal data and new rules around responsible AI, critical infrastructure and supply chains.

There's a global focus within the cyber security universe on compliance in general, with a refined eye toward the overall burden of regulation, as well as the diversity of various reporting requirements. As a result, companies are putting more emphasis on embedding privacy and security within the way they comply with a broad range of trans-border regulatory requirements and regimes.

This is of particular interest when it comes to building and governing responsible AI systems, ensuring customer privacy, and enacting guidelines around critical infrastructure, supply chains, smart products, and resilience.

At the same time, cyber security budgets may have to be more objectively justified moving forward as organisations deal with economic uncertainty. Many CISOs are seeing flat budgets, not necessarily reduced, as some of that spend is diverted to organisational innovation, particularly AI and automation solutions. This noteworthy development requires security teams to engage in technology rationalisation and budget optimisation – essentially, doing more with less.

While economic headwinds drive budget pressures, there is a growing view that cyber security has matured to the point that organisations can trim investment. Further, security functionality is now embedded within other IT and transformation budgets rather than being a central budget provision. Also, the shift to a cloud-based security-as-a-service approach embeds security costs into companies' broader operating expenses in a way we haven't seen previously.

In this environment, I encourage CISOs to sharpen their cyber risk quantification (CRQ) process, which helps express the impact of cyber security risk in financial terms using mathematical modelling to illustrate risk through measurable variables.[1] Looking at risk through a CRQ lens can effectively demonstrate return on investment and investment priorities to leadership and the Board, ensuring the organisation understands the threat from both technology and financial perspectives.

Fundamentally, this report explores from various angles what is perhaps the central aspiration for executives across the enterprise: keeping their organisations resilient. Bottom line, if an organisation is crippled as a result of an attack, how quickly can the organisation resume regular operations, and how can the impact on customers be minimised?

This is emblematic of the resilience agenda that can be seen within many of the most recently proposed regulations, particularly those focusing on critical infrastructure sectors. In many cases, the emphasis is now on response and recovery, as well as mitigating harm to customers. Specifically, what are our minimal viable processes, technology data and people that we need to be able to deliver our critical services? This is a different lens through which to view security relative to the traditional perspective.

Cyber security must be viewed as an ever-evolving ongoing endeavour. The more organisations accept cyber incidents as inevitable yet manageable, the better their chances of achieving that balance between preparation and resilience.

Martijn Verbree
Head of Cyber Security
KPMG Australia

[1] Forrester, *The Cyber Risk Quantification Landscape, Q4 2022*, November 29, 2022.

Eight key cyber security considerations for 2024

Click on each consideration to learn more.

01

Meet customer expectations, improve trust

With cyber threats and data privacy concerns growing, CISOs should be seeking to work closely with stakeholders across the organisation to maintain trust by ensuring operations are resilient in the event of an incident.

02

Embed cyber security and privacy, for good

The act of embedding security across the organisation should be viewed as an exercise in driving operational excellence.

03

Navigate blurring global boundaries

A central consideration that organisations should examine how to most effectively navigate the increasingly complex global business landscape to ensure resilience and business continuity.

04

Modernise supply chain security

Despite the challenges and competing priorities, ensuring the supplier and partner ecosystem is secure should not be a bottleneck; it should be a business enabler.

05

Unlock the potential of AI – carefully

Security and privacy leaders should be supporting the business objectives reliant on AI and determine how to harness this game-changing technology effectively and responsibly.

06

Supercharge security with automation

As operating models digitise, security teams should automate and upgrade their processes to keep pace.

07

Make identity individual, not institutional

Driven by expanding business models, it's vital that organisations now view identity not in isolation but from a broad perspective.

08

Align cyber security with organisational resilience

Organisations should find a way to create a broad-ranging culture of resilient security throughout the enterprise and seek to ensure all stakeholders are on the same page.

Consideration 1

Meet customer expectations, improve trust

Consumers, employees, suppliers – every corporate stakeholder – expect businesses to pursue growth and profits. But increasingly, companies are expected to operate in a socially responsible manner, as well. Organisations should strengthen the connection between security and privacy and environmental, social, and governance (ESG) factors. This bond is being increasingly recognised across the business ecosystem, particularly by ESG rating services as they search for greater transparency in measuring and comparing organisations.

Increasing trust should be high on the cyber agenda in relation to how video and audio files are used in the creation of deepfakes, the impact of which can be grave for privacy and perhaps even democracy.

Mika Laaksonen
Partner
Global Cyber Security ESG Leader
KPMG in Finland

The importance of ESG and how security and privacy fit into the bigger picture

According to the KPMG 2023 CEO Outlook, 69 percent of CEOs have embedded ESG into their business as a means of creating value, and 50 percent anticipate significant returns from those efforts over the next three to five years.

While environmental aspects of the ESG agenda have garnered the most attention, governance elements such as cyber security and privacy are less well-developed. With cyber threats and data privacy concerns growing, CISOs need to work closely with their ESG counterparts to ensure that, in the event of an incident, operations are resilient and continuity plans are ready for activation.

By embedding cyber and privacy considerations into social responsibility programs and protecting customer data, organisations can increase the chances of maintaining their reputations and trust among customers, even in the event of a major breach.

For consumers who share personal information with public and private service providers, there is an expectation that their data will be protected and that it will not be used for purposes other than what they've supplied it for.

At the same time, there's an expectation that, in the pursuit of their business objectives, organisations will act in a socially responsible manner to reduce their carbon footprint, support their local communities, improve labour policies, and ensure workplace diversity and equality, to name just a few items.

Addressing cyber security and privacy specifically and ESG broadly have become top corporate and, by extension, CISO, priorities. There are different regulations for specific regions and industries, and those guidelines need to engender trust. This is important from a compliance perspective but also noteworthy because B2B customers and B2C consumers have discrete expectations directly impacted by the various rules.

Individual consumers can purchase alternative products or services if they're not happy with the provider's actions regarding their personal data, privacy and response to breaches. In fact, 82 percent prefer a brand's values to align with their own, and 75 percent said they would abandon a brand over a conflict in values.[2] Given a choice, most consumers prefer companies that prioritise security, privacy, and sustainability by adhering to ESG standards.

This is especially true on the B2B side, where corporate customers value safeguarding their confidential data and intellectual property. More and more industries have regulatory requirements for cyber security and data privacy, and organisations that comply with these regulations are preferred by stakeholders.[3] For many organisations operating in B2B industries, this is more than a "nice to have," with regulatory obligations flowing directly from firms in regulated industries to their suppliers, who could be tarnished by association if the brand experiences a significant cyber event.

Indeed, roughly two-thirds of consumers will pay more for sustainable products, although two-thirds of retail executives are skeptical that they actually will pay more.[4] However, while consumers may be okay with paying extra for security, privacy and social responsibility, these factors are, for the moment, "table stakes," the cost of doing business, although they are likely to hit the bottom line sooner rather than later.

In cases involving private equity or venture capital, the ethical lens through which these firms view their investments is worth noting. Many now look for assurances of the appropriate level of cyber security and privacy management. Ultimately, they're concerned about the brand damage cyber events can bring to the organisations where they infuse funds.

> **Increasingly, there's a big role for cyber to play regarding AI and data ethics. Determining that the data used to train AI algorithms is accurate, hasn't been corrupted, and is free from bias is a herculean and, perhaps ultimately, impossible task, but well worth the effort.**

Caroline Rivett
Partner
Global Cyber Security Life Sciences Leader
KPMG in the UK

[2] Google Cloud, "New research shows consumers more interested in brands' values than ever," April 27, 2022.
[3] *KPMG, Cybersecurity in ESG*, 2023.
[4] First Insight/Wharton School of the University of Pennsylvania, "The Sustainability Disconnect Between Consumers and Retail Executives," January 2022.

The social benefits of actively embedding cyber security into the ESG agenda

The scope of the ESG dialogue needs to be broadened – at many organisations, it's not yet common to be talking about cyber security and privacy in the context of ESG.

In today's environment, there are deep issues with the social contract between organisations, employees and consumers relating to data protection. Increasing trust should be high on the cyber agenda when it comes to how video and audio files are used in the creation of deepfakes – imagery, video, or audio featuring a specific individual that is replaced with another person's face or voice or manipulated to give the impression the individual did or said something they did not.

Deepfakes are difficult to combat since, in many instances, it's up to the audience to interpret whether the video or audio is real or fraudulent. Organisations must be vigilant about identifying and removing these files and should participate in educating the broader public on the subject. Increasingly, there's a big role for cyber to play regarding AI and data ethics. Determining that the data used to train AI algorithms is accurate, hasn't been corrupted, and is free from bias is a herculean and, perhaps ultimately, impossible task, but well worth the effort.

Privacy and cyber security also play vital roles in protecting freedom of speech and securing today's proliferating digital communications channels. Privacy controls can also play a key role in limiting the exploitation and misuse of personal information without consent or knowledge. This is vital in maintaining the public trust in organisations.

Many decarbonisation and CO_2 reduction programs rely on digital technologies and automated systems to monitor and manage energy production, distribution, and consumption. As efficient as these tools can be, they can also create unforeseen cyber security vulnerabilities and require a high level of data protection. Strategically embedding cyber can help mitigate threats, reduce the risk of data breaches and ensure regulatory compliance.

Finally, there's a substantial social responsibility dimension to both cyber security and privacy where organisations should work with B2C and B2B customers to help them be more cyber aware. Banks do it routinely, and retailers are doing it more and more. There's also a connection to supply chain and ecosystem security, where improving the security of the vendor ecosystem is critical.

Do people really care whether a business has a cyber incident if it's managed?

Theoretically, most people would probably say that they don't want a company whose products or services they use to suffer a data breach. But those same people don't want to pay more and want touchpoints to be quick and frictionless. People largely don't care until something bad materialises, and it seems as though they want the work of security to happen "behind the curtain."

A big part of the equation is demonstrating to customers that cyber security is an organisational imperative – it simply is the right thing to do. Organisations should approach this as though they are training their customers and clients to understand and care about the implications of cyber awareness and prove that what they're doing isn't just another to-do item but a vital service.

Training people outside your organisation is itself an exercise in ESG maintenance. Cyber security Awareness Month is an example of how government and businesses work together to ensure that employees and consumers appreciate the basics of cyber security to avoid the most obvious risks.

There is no such thing as 100 percent security. Despite all the precautions, incidents do happen. In the event of a cyber incident, make a quick decision about whether you need to disclose what happened and, if so, how much information you're prepared – or compelled – to share.[5] It's vital to be open and honest; good communication can lead customers to trust an organisation even more than they may have before the incident.

[5] KPMG International, "Maintaining cyber vigilance and staying resilient," 2023.

Suggested actions

Connect with your organisation's ESG team to determine whether they consider cyber a key aspect of their mandate. If not, work to build awareness of how and why it's important to all three areas of ESG.

Be practical. Effective cyber security is not as much about getting business partners to do things differently as it's about reframing the conversation across the enterprise to inspire other areas of the organisation to infuse security into what they already do.

Sharpen your global regulatory intelligence around cyber in general and ESG and privacy in particular to ensure timely compliance and reporting; keep track of and remain familiar with ever-increasing regulations and their effects on your cyber efforts.

Learn more

Cyber security in ESG

It's time to view ESG and cyber security through the same lens.

KPMG global tech report: ESG

How businesses can use technology as an opportunity to tackle their ESG ambitions.

Road to readiness

KPMG ESG Assurance Maturity Index 2023.

Consideration 2

Embed cyber security and privacy, for good

Security, from the CISO down through their entire team, is a very different role today. Cyber is becoming more embedded in core business processes. That reality is being reflected in a move away from a centralisation of cyber security in the CISO role to a federated model, in which the CISO is the conductor of the orchestra, establishing the frameworks, assessing risk, and providing implementation support. Security is integral to every function across the organisation, from front office to back, and many leaders now acknowledge the value of integrating a security mindset into their very different business cultures and processes.

Business models and technology are changing and impacting security

Whether you make a widget, deliver a service, or create information, operating models are increasingly cloud-based, which, in concert with other new technologies, is being used to increase scalability, reduce costs, generate revenue, and widen profit margins.

The automotive industry is a good example of transforming business models. Cars today have become huge tablets on wheels. People are ordering pizza from the road and not even using the phone. So much technology has been added to gas-powered cars, not to mention electric vehicles, that they have become arguably the most sophisticated product available to retail consumers.

The downside of technology is it widens the attack surface, creating new potential vulnerabilities and increasing the complexity of the ecosystem with which CISOs must contend. At the same time, the cost of cyber security is skyrocketing, leading organisations to consider better strategies for delivering those services.

In this new world, organisations can't deploy hundreds of people; security teams must be lean – particularly those embedded within business lines. Organisations must find the right combination of people and technology, using AI in general and machine learning in particular to cover the ground humans can't cover efficiently.

Performing timely solution reviews on thousands of applications is simply impossible for humans. Organisations must decide where to start incorporating security within application development processes and move to continuous monitoring to understand the impact of potential attacks and vulnerabilities.

The irony is it doesn't take the CISO to do that. Managing these risks requires a cultural shift across the business to embrace security as part of the organisation's standard operating procedures. CISOs don't install patches, and they don't manage operations. Security teams should determine how and where to embed certain security tasks in the business and monitor those tasks to ensure they are carried out properly. This is how we see security teams evolving.

It's going to be a matter of "insourcing" to nudge security closer to the customer or outsourcing to a third-party service provider to efficiently leverage specialised skills that may not exist within the organisation. Many organisations struggle with the idea of security as a core competency, particularly as they attempt to master the sheer volume of new technologies.

Work with business leaders to embed security effectively

There's a lot of talk about "shifting left," but while we acknowledge the importance of considering security early, we also believe organisations must look end-to-end – from concept to build and including continuous monitoring – and approach security as an ongoing requirement. Throughout that journey, the number one element of security is visibility.

Security professionals are becoming more like air traffic controllers, and the runways must be kept clear. CISOs must make sure "traffic" – that is, applications – are coming in and going out efficiently and safely. Security shouldn't hold up the release of products and services, but there should be early visibility into the processes the business is employing.

Embedding security into broader business should be viewed as an exercise in driving operational excellence. Security teams should describe and demonstrate what "good" looks like and inspire embedded security professionals across the enterprise to manage toward that vision. It's a matter of establishing appropriate guardrails to enable a secure-by-design approach to be embedded, and then integrating the right tooling and templates into development environments.

CISOs and their teams – as well as security personnel who are embedded in the business – should take a holistic approach to operational excellence and shared responsibility. This means giving equal consideration to people, process, technology, and regulatory requirements. By focusing on risk management, incident

> **"Ten or 15 years ago, the 80/20 rule for security professionals was 80 percent technical skills and 20 percent soft skills. If CISOs want to ensure they are not perceived as support staff, they must get comfortable with the new 80/20 rule under which imperatives such as communication, building trust, problem-solving and conflict management are as vital as ensuring an efficient security operations centre.**

Brian Geffert
Principal
Cyber Security Services
KPMG in the US

management, governance and compliance, technology solutions, and employee training and awareness, organisations can develop a sustainable security culture.

This is particularly pertinent as organisations prepare for the SEC's new cyber security rules[6] and the EU's NIS2 Directive, which requires member states to implement laws to protect essential businesses from cyber threats by October 2024.[7]

What CISOs need to do to remain relevant

Most CISOs grasp the security implications around data, applications and the overall attack surface, but they can truly differentiate themselves in connection with talent, budgets and cross-organisational politics. CISOs who understand how to work across the organisation to embed security into the business while maintaining a partner role are seeing the most success. Security teams must have insight into the initiatives business units are planning and the potential new threat vectors that can be revealed.

CISOs should work to speak the language of their business partners rather than esoteric cyber speak. For example, don't talk about zero-day vulnerabilities, advanced persistent threats or security orchestration, automation and response (SOAR) strategies. Those terms mean nothing to most non-security colleagues. Instead, say, "If this plan doesn't work, you will get cut off from this or that market. If we can't successfully protect the product line, you can't generate sufficient revenue because people won't be using the products."

Security teams don't need to employ scare tactics. Rather, they need to adopt a new point of view based on business enablement and risk reduction. CISOs have to inspire people to trust that their guidance and strategic vision are in the organisation's best interest. Their commodity is trust.

New essential skills and competencies

Security professionals must improve their soft skills, including interpersonal skills such as negotiations, time management, listening, and networking. Ten or 15 years ago, the 80/20 rule for security professionals was 80 percent technical skills and 20 percent soft skills.

Today, that equation has flipped. If CISOs can't work with executive leadership to tell a story that the organisation can understand and coherently position ideas to influence action across the business, they're simply not going to be successful.

In addition to these softer skills, security leaders should consider leveraging cyber risk quantification methodologies to more effectively manage overall risk exposure. This will enable better communication and articulation of the financial risks, as well as where the organisation should prioritise its cyber security investment.

The security team must acknowledge that they are communicating mainly with non-technical colleagues to get them to understand risk and act accordingly. If CISOs want to ensure they are not perceived merely as support staff, they must get comfortable with the revised 80/20 rule under which imperatives such as communication, building trust, problem-solving and conflict management are as vital as ensuring an efficient security operations centre.

[6] Securities and Exchange Commission (SEC), "SEC Adopts rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies," July 26, 2023.

[7] European Parliament, "The NIS2 Directive: A high common level of cybersecurity in the EU," August 2, 2023.

Suggested actions

Bring a new perspective to the board on what could disrupt the business and what should be done to manage those risks without impacting operations and customer experience.

Security teams should determine how and where to embed certain security tasks within the business vs. outsourced to a third-party service provider and monitor those tasks to ensure they are carried out properly.

Run the cyber team like a business, which means you must give up a degree of control over what other parts of the organisation are doing from a security perspective

Learn more

KPMG 2023 CEO Outlook

More than 1,300 global CEOs share their views on geopolitics, return-to-office, ESG and generative AI.

KPMG global tech report 2023

Discover how leaders are securing value by navigating uncertainty with confidence.

The future of IT

Discover the strategies to advance the IT function and prepare organisations to thrive in a cloud and AI-enabled era.

Consideration 3

Navigate blurring global boundaries

Global businesses are operating within an increasingly complex cyber and privacy regulatory space. National interests are playing out, leading to diverse regulatory requirements over information sovereignty, supply chain security, transparency of cyber controls compliance, incident reporting, and, of course, privacy. Businesses need to calibrate their regulatory reporting for an increasingly borderless world but also maintain security controls that can be tailored to local requirements. Organisations need to be prepared to respond quickly to changing geopolitics and diverse sanctions requirements.

The big question for security professionals is around striking the right balance between business enablement and business value while ensuring they are staying on the right side of the regulators.

Orson Lucas
Principal
Cyber Security Services
KPMG in the US

Global business landscape: Common cyber and privacy goals, but divergent in practice

For years, the global regulatory landscape has been very disjointed. While some markets prioritised aggressive regulations over the past few years, many did not. As a result, organisations were left with a decision to implement elevated governance, processes and controls responsively on a market-by-market basis or to treat emerging regulations as a bellwether for things to come and invest in proactive, mature, and automated privacy and security programs. While some opted for the latter, budget, resources and other competing business priorities caused many organisations to opt for the former.

However, that's a slowly evolving scenario. Markets like Europe, China and the US are setting the tone, and many others are following suit. Patterns and principles are emerging in the security, privacy and AI domains. This provides an opportunity for leading organisations to coalesce, locally and globally around a principles-based approach to proactively protect and manage sensitive information. Ideally, this will manifest in single global privacy and security programs that account for nuances in regulation and local practices in specific markets. Still, there are several challenges that truly global organisations will need to navigate to make that vision a reality.

For example, data localisation and transfer considerations require a solid understanding of data inventory and flows/transfers, both internally and with third-party business and supply chain partners. Often, there are multiple paths, though all require significant planning and intentionality to help ensure efficient, cost-effective, and compliant practices.

Considered through a business lens, organisations will continue to require a global audience and global footprint to scale their operations, regardless of jurisdiction and where they're based. The big question for security professionals involves striking the right balance between business enablement and business value while ensuring they stay on the right side of the regulators. It's a fine line and a clear challenge for CISOs, CPOs, and their teams.

Global businesses face challenges adhering to evolving regulatory requirements

Organisations should navigate the regulatory waters carefully, knowing that the rules are perpetually evolving. As customer relationship management and marketing technology (MarTech) tools mature, organisations are realising the value of data through the insights and ROI it provides to the business.

Regulators have responded with targeted privacy rules in many jurisdictions globally, requiring CISOs, CMOs, CDOs, and CPOs to ensure they have a sound second line of defence to navigate and comply with current and planned regulatory requirements. In terms of consequences, many countries and territories now impose strict financial penalties – as well as suspensions of business licences – for privacy infractions.

The siloing of privacy is dissipating quickly. As the focus of regulators evolves, areas such as the purchase and sale of data, consent and preference management, data ethics, and responsible use of AI are flattening the siloes between stakeholders and business functions and causing boards and executive leadership to take an objectives-based view centred on both regulatory compliance and consumer trust. The latter is something that leading organisations are using to differentiate themselves as they seek to build, sustain, and transform relationships with consumers.

> **In today's world, as cybercrime objectives and tactics have grown more nefarious and sophisticated, customers, companies, and regulators alike should follow a much more holistic approach to data management and information protection.**

Henry Shek
Partner
Cyber Security Services
KPMG China

Shifting geopolitical dynamics influencing response speed and adaptability

Doing business in multiple regions is challenging in the current environment because the tools and technologies organisations use in one market may not be accessible in others. For example, in parts of China, some companies may not have access to certain key tools because availability may be restricted due to vendor decisions to deliver in the Chinese market. This is both a supply chain and operational resilience issue and can severely impact organisational productivity.

A central consideration that organisations must examine is how to most effectively navigate the increasingly complex global business landscape to ensure resilience and business continuity. Attempting to navigate privacy and data challenges requires a well-defined governance plan that reaches a minimum maturity level quickly when the organisation operates in jurisdictions with strict sanctions regimes.

Indeed, Chinese regulations take a different approach to those in the EU, which are different than those in other parts of the world. They have different scopes, definitions of personal data, collection limitations, accountability rules and basic legal frameworks. Without a strong principles-based vision, strategy, governance and tactical plan, organisations will increasingly be challenged to innovate or risk falling behind.

The politicisation of business and its impact on security is another dynamic to bear in mind. In the US, for example, some companies skew one way or the other politically, sometimes based on the internal values of their leadership but often in response to their target customer base. This development came to a well-publicised head with the conflict in Ukraine as companies that continued to operate in or do business with Russia had sanctions applied against them.

From a security and IT perspective, the concept of segmentation or micro-segmentation – whereby companies can manage workloads in a data centre or cloud environment with granular policy controls and restrict the spread of lateral threats – is instructive. Organisations with holistic networks can create these connected segments yet separated by firewalls. We're finding that companies with segmentation models in place are better able to effectively cut off regional operations quickly as needed.

Global companies should look at national jurisdiction through different lenses. For example, offering services to EU citizens outside Europe activates GDPR requirements. In general, firms need to be clear about where their operations are located, who they depend on to conduct business (i.e., suppliers), the markets

where they offer products and services, and where they are incorporated as a legal entity. The interplay between these four sovereignty concepts gives rise to a complex regulatory picture most effectively navigated by a flexible, policy-based operational approach.

Another consideration is redundancy. For example, suppose a company maintains its entire call centre operation in a jurisdiction that becomes restricted for one reason or another, and all business in that country needs to be shut down. What becomes of the customer service apparatus? Having some level of business, security and redundancy in place if the organisation needs to temporarily step away from business in a certain part of the world to navigate the prevailing geopolitical challenges can help alleviate the risk of constraining the broader business in the process.

In the end, CISOs and their teams should always apply a lens of resilience and preparedness. This helps companies remain a step ahead of the next black-swan event and solidify the ability to make those "break-glass" decisions quickly and confidently, rather than being forced to hastily cobble together a strategic hyper-localisation cyber strategy.

Suggested actions

Maintain an understanding of the global regulatory landscape, specifically an understanding of the relevant rules at a granular, jurisdictional level.

Know where critical data – both structured and unstructured – resides across the organisation, as well as where it's shared with third-party partners.

Enhance transparency to build trust across global supply chains; rather than treating third-, fourth-, and even fifth-party supplier relationships solely as transactional and contractual (which they are), approach them as an extension of your ecosystem.

Learn more

Privacy risk study 2023

Staying on top of the evolving privacy risk challenges.

The hostile limelight

The future of cyber in geopolitics.

Global Economic Outlook

KPMG International Global Economic Outlook – H2 2023.

Consideration 4

Modernise supply chain security

Many organisations' current approach to third-party and supply chain security does not align with the reality of today's complex and interdependent ecosystem of partner organisations. Traditional models were built around the assumption that third parties provide services on a transactional basis. That view does not reflect today's intricate network of APIs and processes tethered by a complex set of software-as-a-service dependencies. Organisations are encouraged to establish more strategic supplier partnerships focused on continuously monitoring and managing the evolving risk profiles of these suppliers to strengthen operational resilience.

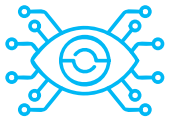
Despite the challenges and competing priorities, ensuring the third-party ecosystem is secure should not be a bottleneck; it should be a business enabler. But there can be no shortcuts. This elevates the pressing need for modernisation. How can you do it faster, more efficiently, and with minimal resources without compromising quality? That's where a risk-based mindset, paired with a data-driven approach powered by intelligent automation, can make a tangible difference.

Mitushi Pitti
Managing Director
Cyber Security Services
KPMG in the US

The evolving supply chain landscape is affecting traditional security models

Historically, the third-party security model has focused on point-in-time assessments. Continuously monitoring and taking inventory of frequently used supplier software components can help CISOs better understand the security structure of these providers and identify potential risks. With this dynamic in mind, CISOs should develop a more modern standard for "containerising" risk exposure in real-time.

To achieve that posture, we see three key challenges for CISOs and their teams:



Visibility

A longstanding problem has been organisations' inability to cover the entire vendor population. Large organisations can have thousands of suppliers, and often they cannot accurately assess their activities with traditional methods. It would require an army of security personnel to do all the physical endpoint assessments, which is humanly impossible. It would cost tens of millions of dollars, making it unrealistic logistically as well as budget-wise.

Scalability

Beyond understanding the risk profile of the broad vendor population, the ability to scale enables organisations to keep pace with the challenges of a constantly expanding and changing landscape. From new technologies and processes to the possibility that a vendor doesn't explicitly follow your security protocols, the third-party environment is an ever-fluid threat vector.

The evolving risk profile of third-party partners

The old transactional model did not have a mechanism for tracking how the relationship is changing and how that might be creating new vulnerabilities. As a result, depending on the maturity of the vendor, organisations need to do more (institute monthly reviews) or perhaps less (allow more autonomy with quarterly reviews) to ensure these relationships operate efficiently and adhere to all compliance requirements.

With the rapid pace of technological change and the reality that customers are more demanding, organisations are looking to remain innovative. And, of course, third- and fourth-party suppliers – and cybercriminals – are doing the same.

For example, many vendors are deploying AI to improve processes and complete tasks faster. But fascinating and powerful as it is, AI poses a variety of potential new risks, from questions around data integrity, statistical validity, and model accuracy to transparency and reliability issues. This human-thought simulation by machines must be used securely and responsibly at the organisational level and by third-party partners. Extrapolate those risks across the supply chain, and it reveals a new threat landscape for CISOs and their teams to monitor.

Despite the challenges and competing priorities, ensuring the supply chain ecosystem is secure should not be a bottleneck; it should be a business enabler. But there can be no shortcuts. This elevates the pressing need for modernisation. How can you do it faster, more efficiently, and with minimal resources without compromising quality? That is where a risk-based mindset, paired with a data-driven approach powered by intelligent automation, can make a tangible difference.

The role of government

Heavily regulated organisations that must keep pace with the regulatory environment and work with suppliers that don't have the same regulatory constraints must find a way to get them to cooperate and employ the right security controls. That's an ongoing battle that organisations are facing. They're looking to see where regulations will help in compelling third parties to be more secure overall.

The recent US Securities and Exchange Commission (SEC) rules around cyber security have a position on third parties. The regulators know that this is a top-of-mind concern and a growing challenge for all organisations. A little bit of a nudge from the regulators should help convince those less-than-mature vendors to participate in the program a little better and help prop up the cyber posture.

Similarly, the EU's revised Network and Information Security Directive (NIS-2) emphasises that organisations should proactively manage risks introduced by third parties. Also, the Digital Operational Resilience Act (DORA), which facilitates effective monitoring of the risks posed by third-party information and communication technology providers, focuses on getting a better handle on supply chain security.

Regulators, through DORA, are looking to determine which third parties they view as critical to the overall resilience of the broad supplier ecosystem. These players may not be regulated directly, but since they are considered systemically important, the regulated entities will also pass their requirements onto them.

Collaborative intelligence sharing: A nascent but worthy strategy

As a practical matter, information sharing between corporations and suppliers may be years away, but conceivably, it can solidify best practices and ultimately enhance supply chain relationships.

With the threat posed by bad actors growing exponentially, organisations across various industries, particularly critical infrastructure, must do significantly more sharing of threat and risk intelligence – internally, with the market, and with suppliers and partners.

AI poses a variety of potential risks, from questions around data integrity, statistical validity, and model accuracy to transparency and reliability issues. This human-thought simulation by machines must be used securely and responsibly at the organisational level and by third-party partners. Extrapolate those risks across the supply chain, and it reveals a new threat landscape for CISOs and their teams to monitor.

Elizabeth Huthman
Director
Cyber Security Services
KPMG in the UK

Organisations should seek to break down the silo mentality and encourage business stakeholders – procurement, legal, business units, risk, third parties – to communicate and collaborate.

Collaboration and information sharing also help organisations manage vendor concentration risk. This is a major consideration for extended supply chains – third, fourth, and fifth parties – where multiple organisations rely on the same suppliers. In these instances, it makes sense to join forces while maintaining confidentiality across certain aspects of the competitive landscape to ensure third parties are not a weak link across the ecosystem.

Many organisations are reticent to engage in this form of collaboration. With that reality in mind, the European Union Agency for Cybersecurity (ENISA), via Information Sharing and Analysis Centres (ISACs), and the Cybersecurity and Infrastructure Security Agency (CISA) in the US, are spearheading a variety of centralised programs aimed at gathering and rapidly disseminating information regarding threats and vulnerabilities.

It's not just about whether a vendor can access customer- or business-sensitive data. Suppose a specific supplier is critical to maintaining operational resilience – meaning it impacts the organisation's ability to assemble and distribute products – but is inadequately mature from a security perspective. In that case, steps must be taken to ramp up the vendor's security sophistication or a tough decision to move on to an alternate partner may be necessary.

By establishing a corporate culture grounded in risk awareness and security, no individual or process will be viewed as a weak link or business speed bump. And that mindset will emanate across all aspects of the enterprise – including third-party affiliates.

Suggested actions

Take a risk-based approach to assessing third-party processes rather than a blanket approach to different suppliers that provide diverse services.

Leverage intelligent automation to gain higher visibility into the changing supplier risk profiles and build a sustainable and scalable forward-looking third-party program.

Encourage crowdsourcing of intelligence and sharing both within your organisation and with trusted third parties.

Learn more

Staying ahead of cyber risk in the supply chain

With complex global supplier networks and more pathways for threat actors to find a way in, understanding and preventing cyber risk must be a priority.

Supply chain trends 2024: The digital shake-up

With digital opportunities sweeping the supply chain landscape, readiness and line of sight will be paramount to success.

The future of supply chain

From ESG to robots and the metaverse, supply chain leaders have new challenges to prepare for.

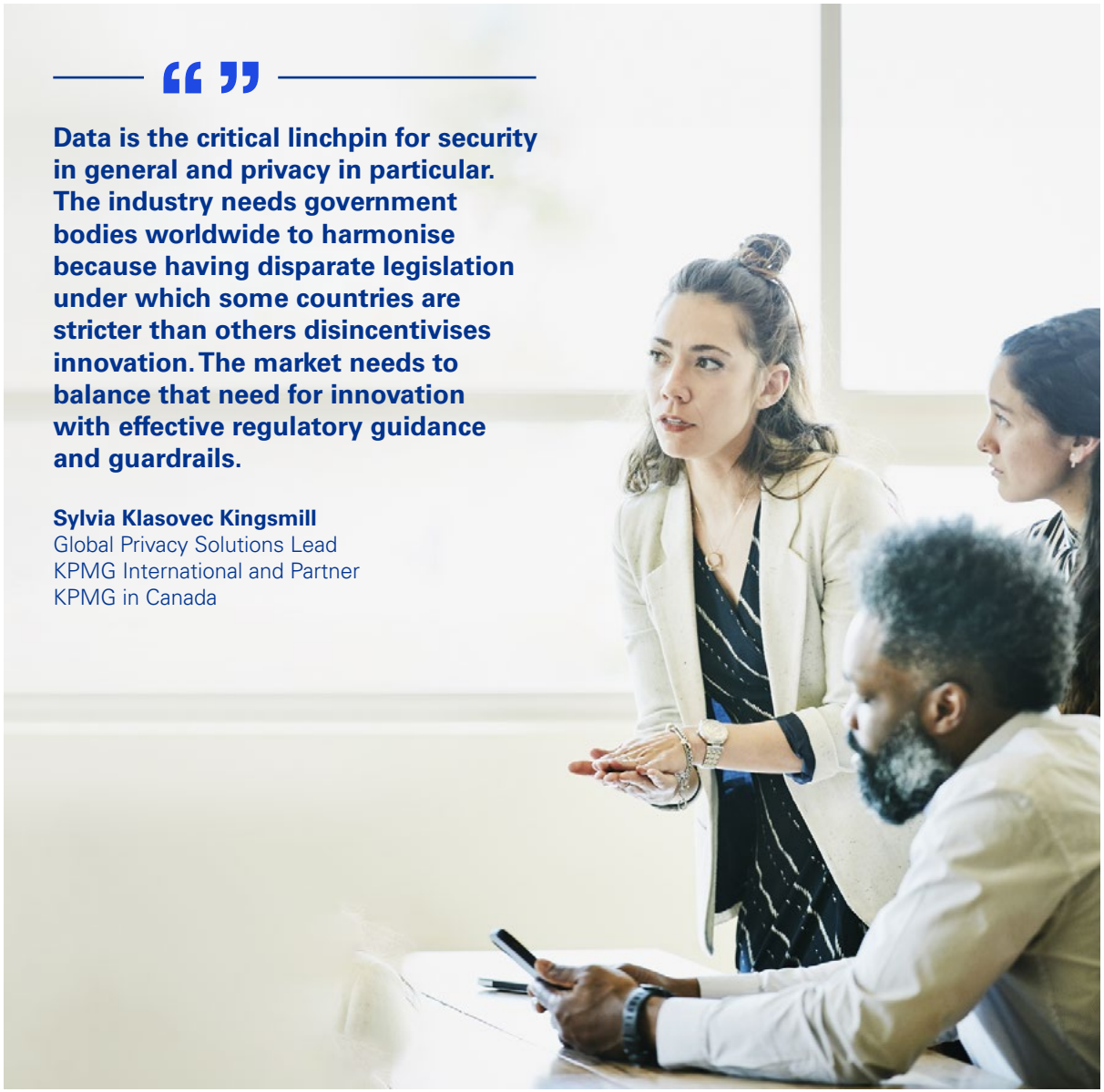
Consideration 5

Unlock the potential of AI – carefully

With careful planning and execution, AI will transform how, when, and by whom work gets done. All the talk is currently about generative AI, but many other branches of AI, from robotics to machine learning, continue to transform business. Calibrating the security, privacy, and ethical implications inherent in these technologies is challenging, and organisations are looking to establish frameworks that provide both risk management and governance when implementing AI.

Data is the critical linchpin for security in general and privacy in particular. The industry needs government bodies worldwide to harmonise because having disparate legislation under which some countries are stricter than others disincentivises innovation. The market needs to balance that need for innovation with effective regulatory guidance and guardrails.

Sylvia Klasovec Kingsmill
Global Privacy Solutions Lead
KPMG International and Partner
KPMG in Canada



AI's current path: Limited guardrails, but opportunities abound

The concern over business outcomes and the need to foster trust among employees and customers, specifically, and society, in general, has sparked a broad ethical debate around how AI can be controlled and deployed responsibly, transparently, and with integrity. To that end, regulation in this space is ramping up. The public and private sectors must work together to offer practical solutions for support during innovation and development to ensure security and privacy are embedded from the outset.

There is some trepidation in the market to innovate because of the cautionary headlines, the lack of regulatory guardrails, and the absence of a universal standardised global approach to AI. But that unease is being met with an equal measure of passion for AI's potential to spur innovation.

Even local approaches to how AI models and algorithms should be managed, deployed, and legislated are murky. Some countries and regions are further ahead than others. Organisations should maintain awareness of the key foundational elements needed to establish and maintain trust while also being mindful of the direction regulations are moving in. This will go a long way toward minimising the work needed to ensure compliance with these regimes in the future.

While we encourage organisations to move forward with the exciting and vital work they're doing with AI, at the same time, they should ensure they have a thorough understanding of the complexities involved and how to de-risk their models effectively. As the market develops, it's important to allow global regulators and legislators the time to establish meaningful guidelines for AI development. The EU AI Act is a leading example. This landmark legislation is poised to do for AI what the EU's General Data Protection Regulation (GDPR) has done for privacy, paving the way for exciting and responsible advancements in this field.

Although the absence of legislation is a clear speed bump, the good news is existing privacy legislation has similar principles that can and should be applied to new AI algorithms. Privacy factors such as notice, consent, explainability, transparency, and risk of harm are all codified in existing law.

To remain competitive in the market, CISOs should partner with Chief Data Officers and Data Protection Officers to support the business objectives that are reliant on AI and determine how to harness this game-changing technology effectively and responsibly. At the same time, they need to wrap sufficient governance and controls around processes that may have operated largely without oversight for some time. This harmony between enablement and governance is where successful adoption lies.

Primary challenges in balancing AI innovation with security and privacy concerns

To facilitate their adoption of AI, organisations must make crucial choices that will shape their approach, such as determining whether to create in-house models or rely on third parties. While it may seem that one option is less uncertain, the truth is that both come with inherent risks that organisations must recognise and effectively manage.

Organisations must educate themselves about the safeguards around transparency, accountability, fairness, privacy, and security so they can innovate and deploy with confidence. For example, look to large technology companies and jurisdictions that are further along in their AI journey for guidance around responsible development.

From a privacy and security perspective, many organisations are having their hands forced in a sense. With so many business units moving full steam ahead

CISOs and other senior leaders and their teams need to support the business objectives that are reliant on AI and determine how to harness this game-changing technology effectively and responsibly. At the same time, they need to wrap sufficient governance and controls around processes that may have operated largely without oversight for some time. This harmony between enablement and governance is where successful adoption lies.

Katie Boswell
Managing Director
Cyber Security Services
KPMG in the US

with AI, CISOs and Chief Product Officers (CPOs) must follow along and ensure the necessary controls are installed. Establishing and maintaining trust in those AI solutions from the outset is critical, for the brand and the ability to meet its business objectives.

This requires cross-functional cooperation, especially from a funding perspective. But to thoroughly embrace and pursue the innovation opportunities, organisations need to agree on a unified security, privacy, data science and legal strategy. Taking a cue from the EU AI Act, the US government recently made its commitment to this collective imperative clear by issuing a sweeping Executive Order on Safe, Secure and Trustworthy Artificial Intelligence that codifies safety and security, privacy, equity and civil rights, and innovation and competition in relation to AI.[8]

Strike a balance between rapid AI innovation and implementing robust privacy and security measures

Data is the critical linchpin for security in general and privacy in particular. The industry needs government bodies worldwide to harmonise because having disparate legislation under which some countries are stricter than others disincentivises innovation. The market needs to balance that need for innovation with effective regulatory guidance and guardrails.

This is a cultural mindset shift as well as a technological shift, with change management as a critical success factor. To integrate privacy- and security-by-design thinking with AI and other emerging technologies, the professionals that manage them – not just the technologies – must advance privacy- and security-first mindsets. If the organisation considers privacy and security from the beginning, they will become natural components of the operating model.

If the world stays the course in adopting AI to meet innovation needs, it will eventually be business as usual, like with cloud adoption.

There was a time not long ago when moving to the cloud was a monumental undertaking. Now, it's just part of regular business practice – there's no aspect of security that doesn't have a cloud element. We see that as the likely progression for AI as well. There won't be "AI security" because it will be part of overall security.

[8] Whitehouse.gov, Briefing Room, Presidential Actions, "Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence," October 30, 2023.

Suggested actions

Align your AI framework with current standards and develop solid AI governance by aligning the priorities of the various business leaders in the organisation and gaining cross-functional support from those with a vested interest in the success of AI.

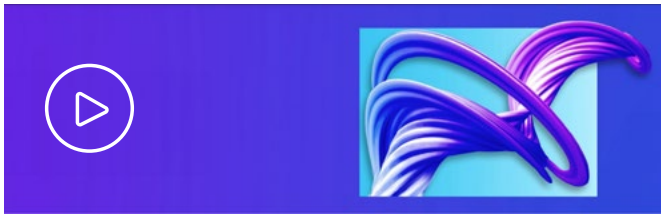
Ensure the purpose of AI algorithms, whether developed in-house or externally, is clearly defined and documented and training data is relevant, appropriate for the business objective, and secure consent.

Acquaint yourself with the stipulations of the EU AI Act and the Biden administration's Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence.

Learn more

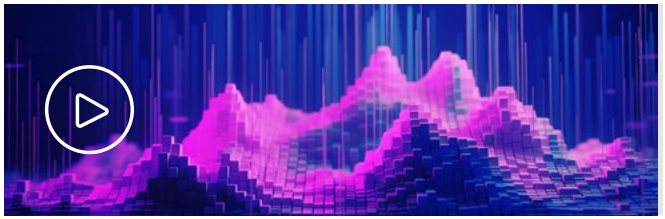
Privacy in the new world of AI

How to build trust in AI through privacy.



Generative AI models – the risks and potential rewards in business

What the rise of ChatGPT, DALL•E 2, Bard et al. could mean for your organisation.



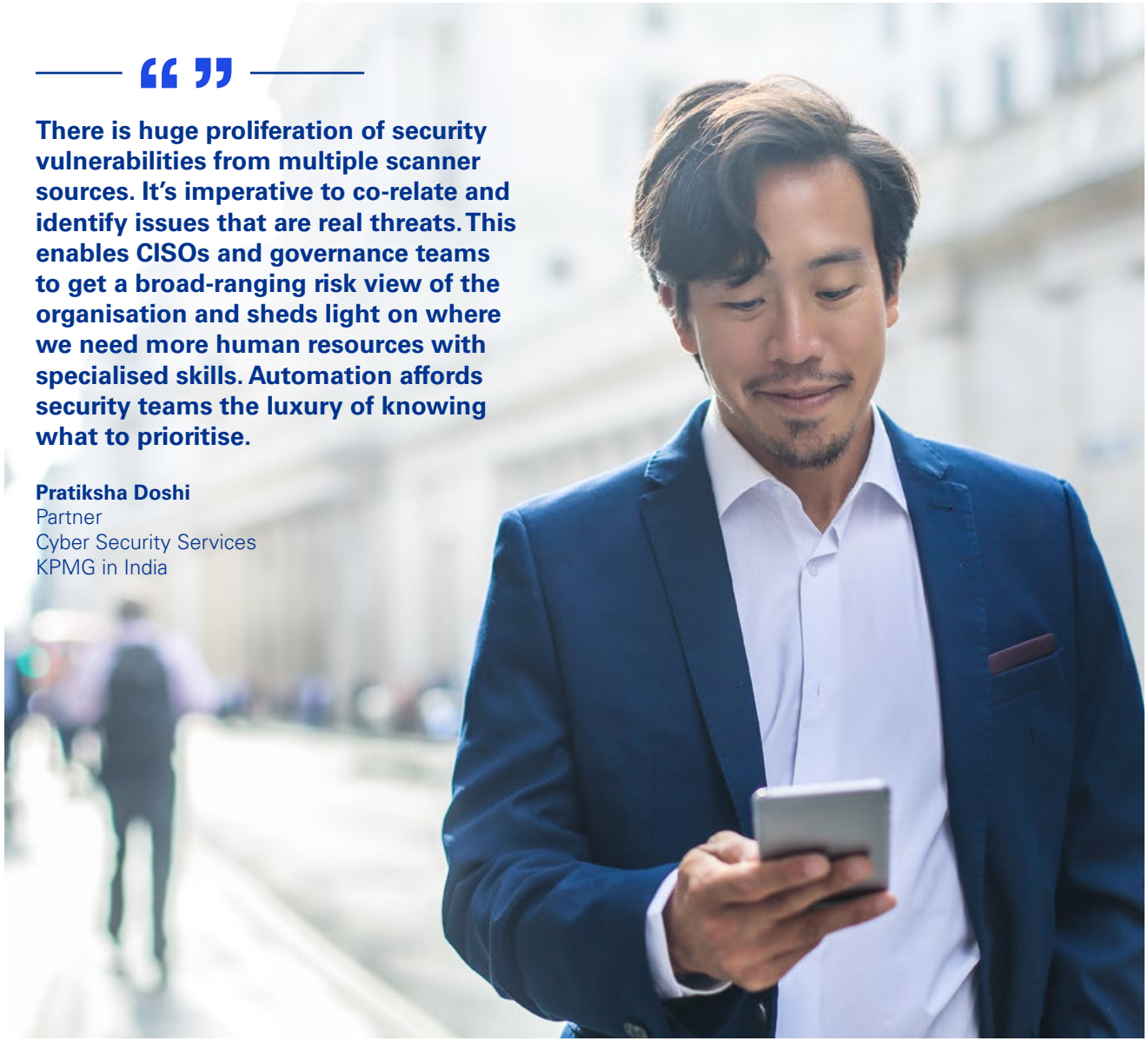
KPMG generative AI survey report: Cybersecurity

An exclusive KPMG survey examines four areas where this remarkable technology shows great promise.

Consideration 6

Supercharge security with automation

Businesses are increasingly moving systems to the cloud, the volume of data that needs protection is skyrocketing, and more people are working remotely and accessing corporate networks with their own devices. As a result, the cyberattack surface is expanding, creating more alerts, false positives and triage events for CISOs to manage. There's a lot of noise in security operation centres (SOCs), and there aren't enough panes of glass or humans to deal with the volume. How can CISOs keep detecting threat after threat and feel they're not missing something? They need to collect, correlate and escalate the signals that require a response – and it must be done rapidly. The only way to do that is through automation.



There is huge proliferation of security vulnerabilities from multiple scanner sources. It's imperative to co-relate and identify issues that are real threats. This enables CISOs and governance teams to get a broad-ranging risk view of the organisation and sheds light on where we need more human resources with specialised skills. Automation affords security teams the luxury of knowing what to prioritise.

Pratiksha Doshi
Partner
Cyber Security Services
KPMG in India

Why automate security at this moment?

Digital agendas are proliferating at a massive rate. At the same time, many organisations see themselves as tech companies, regardless of their core business, because of the explosion of new digital technologies so many must adopt and master. For example, financial institutions are now nearly completely digital in terms of customer interaction, and many health service providers are utilising telemedicine, AI-powered medical devices, and blockchain-based record keeping.

As operating models digitise, security teams need to automate and upgrade their processes to keep pace. Indeed, targeted attackers are also using new technology and growing more sophisticated seemingly by the week. And they're not merely attempting to gain access to the environment but also using AI to commit fraud once there. Cybercriminals are using deepfakes – synthetic media files manipulated to mimic another person's face, voice, or actions – to contact call centres and initiate more credible phishing campaigns.

CISOs must be as sophisticated as would-be attackers to wade through the chatter and identify legitimate incidents quickly – the most efficient way to do that is to embrace automation and AI in the SOC. Automating simple security functions such as log management, threat scanning and access controls will enable security teams to pursue more agile and efficient response times.

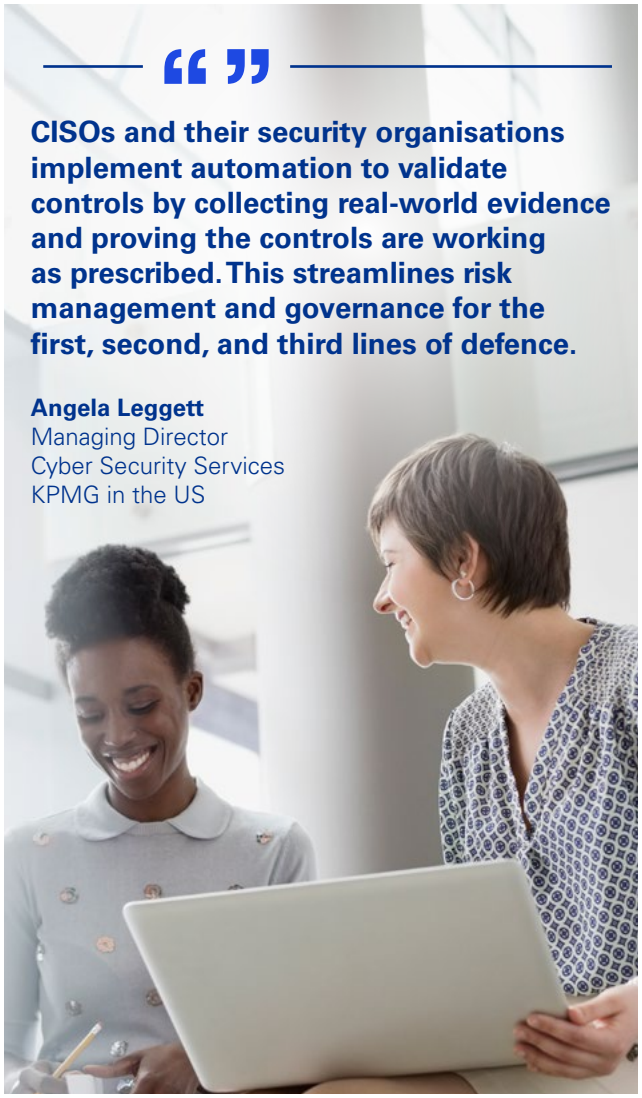
Many organisations across numerous industries are successfully automating the security function and freeing up human resources by automating routine, repetitive, albeit vital tasks. Work that was previously performed by highly trained professionals, such as vulnerability scanning, log analysis and compliance, can be standardised and executed automatically.

Automation is transforming the broad security landscape

Security automation is becoming a critical tool across every cyber security function, the first being prevention. Automating scheduled procedures and updates can play a key role in ensuring corporate and sovereign defences are resilient and trusted as organised and rogue bad actors expand their scale and accelerate their attacks. Automation can also help secure the third-party ecosystem, assessing vulnerabilities and exposing weak links within vendor and supplier ecosystems.

On the detection and response side, automation can be valuable in helping CISOs create a level of self-service security, which can be instrumental in completing assessments and testing and rolling the results into the production network. This significantly reduces the workforce that would otherwise be required. Further, if specific IP addresses are already blacklisted, there is no need for human intervention and ticket analysis can be automated.

Bad actors use automation to scale and increase the speed of their attacks. The most effective way to defend against an automated attack is with automated detection and response. In the event of a breach, automated monitoring processes can identify security incidents in near real-time and commence remediation by altering access policy rules or placing questionable devices or users in quarantine.



"CISOs and their security organisations implement automation to validate controls by collecting real-world evidence and proving the controls are working as prescribed. This streamlines risk management and governance for the first, second, and third lines of defence."

Angela Leggett
Managing Director
Cyber Security Services
KPMG in the US

Some security organisations implement automation to collect digital forensic evidence and validate that the controls are working as prescribed. This streamlines risk management and governance for the first, second and third lines of defence.

Regulatory compliance is another prime example of the value of automation. For instance, in July 2023, the SEC adopted rules for public companies on cyber security risk management, strategy and governance. Under the rules, material security incidents must be reported within four business days. To comply with this requirement, companies must detect the incident, assess its significance, and then file the report. Establishing a workflow that automatically generates and submits the required Form 6-K filing can be a particularly useful way to support compliance efforts.[9]

[9] SEC.gov, *SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies*, July 26, 2023.

For global organisations, this goes even further than filing 6-Ks. A range of regulatory reporting requirements must be met in different formats and timeframes – sometimes measured in hours. Automating these processes could be the difference between compliance and violations.

Automation impacts security teams and the business from a people and skills perspective

Automation augments the security processes and enables CISOs to prioritise where human workers are best deployed. There appears to be a huge proliferation of security vulnerabilities from multiple scanner sources, and it's imperative to co-relate and identify issues that are real threats. This enables CISOs and governance teams to get a comprehensive risk view of the organisation and sheds light on where the world needs more human resources with specialised skills. Automation affords security teams the luxury of knowing what to prioritise.

Clearly, there will be changes in the work security teams perform. Increasingly, humans will focus on more strategic issues involving threat assessment, awareness training, and business alignment, to name just a few, rather than performing the type of repetitive tasks that can be done by AI or predictive analytics engines.

And this work will require new skill sets. For example, CISOs and their teams must start to understand how large language models work, how they can be trained, how to program them, etc. There is also a need to build awareness of and proficiency in security concepts in connection with the cloud, the Internet of Things, and AI.

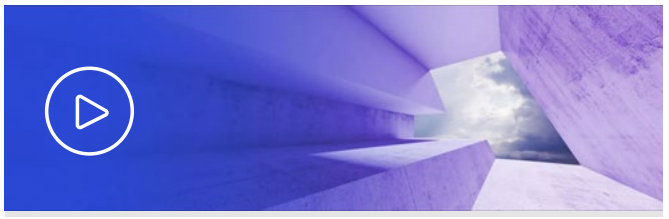
Suggested actions

Define your initial vision and strategy for automation. Consider your short- and long-term security objectives, ensure how those goals align with the organisation's business priorities, and determine the type of protections those shared objectives require.

Identify what data the organisation has centrally accessible and define an automated continuous controls monitoring plan to drive efficiencies across all three lines of defence.

Determine what tools to build versus acquire and understand how supply chain partners are automating to strengthen trust between the organisations and leverage that learning where appropriate.

Learn more



Empowering security

Security orchestration and automated response to help secure the future.

Building trust in cloud environments

2023 KPMG Cloud Transformation Survey

Mastering a multi-cloud environment

The evolution of cloud capabilities.

Consideration 7

Make identity individual, not institutional

Every organisation with which consumers interact assigns them a unique digital identity, and just as usernames and passwords vary, authentication methods do as well. From a cyber security perspective, the identity model is evolving. Most identity and access management (IAM) models were originally devised to manage digital identities and user access for single organisations. Many are now being reconceptualised to encompass a level of resilience suitable for federated, private, public or multi-cloud computing environments. This should eliminate the need for individuals to ensure the exhaustive, time-consuming and intrusive process of identity-proofing every time they interact with a new institution, either as a customer or employee.

Traditional identity models taking on a federated approach

In the current environment, being confident in the identity of people with whom businesses interact is a top concern for security leaders – and very much a moving target. Over the past 10 or 20 years, most organisations designed and implemented their identity management programs. The thinking among security professionals was, 'If I implement it myself, I have full control.' Control notwithstanding, this approach created a very isolated point of view and increased the number of unique identities to be managed. From a customer perspective, we ended up with tens or hundreds of identities, one for each business we connected with.

Today, the line between business-to-consumer (B2C) and business-to-business (B2B) security has blurred considerably. Leaving aside the fact that B2B users typically have deeper access to network resources than B2C users, they are both external users, which has led organisations in many cases to largely merge the two in terms of their identity management approaches.

Driven by expanding business models, it's vital that organisations now view identity not in isolation but from a holistic perspective. That's an important driver toward an identity model where suppliers and end-customers can nimbly interact with multiple organisations without being forced to endure a complicated identity-proofing process each time.

Consumers should control their digital identities, which should be portable between their consumer and employee personas. There has been improvement in recent years around the level of cyber assurance

"As assurance levels associated with those identities increases, we are beginning to see a trend toward a federated identity model – that is, fewer distinct digital IDs that can be securely leveraged across different domains."

Marko Vogel
Partner
Cyber Security Services
KPMG in Germany

provided by many prominent technology and social players, with IDs being leveraged across the digital commerce ecosystem. As confidence in those identities increases, we are beginning to see a trend toward a federated identity model – fewer distinct digital IDs that can be securely leveraged across different domains.

Evolving to a model where digital identities with high levels of assurance are the standard will enable businesses to collect, store and process less personally identifiable information (PII), which would be a decidedly positive outcome for consumers.

The value of blockchain in identity management bears mentioning here. Increasingly, distributed ledger systems are being used to develop effective federated identity models. Integrating security infrastructure with blockchain technology provides trust through visibility, verifiable consent, encryption and audit trails. This helps organisations address privacy and fraud issues by delegating data rights management and access control to the subject rather than a centralised third party.

The higher the level of assurance a digital identity has, the more portable it will be. And when IDs are portable, we can expect to see a trend toward fewer overall consumer logins – fewer digital identities. Ultimately, we need to not only make identities portable – indeed, digital wallet use is expected to exceed five billion users globally in 2026, an increase of more than 50 percent from 3.4 billion in 2022[10] – but consistently tamper-proof and verifiable. This is where biometrics – using unique biological, physical and behavioural identifiers – can come into play.

A related consideration is when, or if, organisations may jettison passwords, one of the top points of failure for all identity systems. Moving away from the password model and broadening the use of multiple factors of authentication (device, location, biometric, behaviour) for secure identity validation, particularly across the business ecosystem, seems productive. Will passwords actually disappear? It's likely still years away, but we appear to be moving in that direction.

Deepfake technology is changing the identity game

The threat posed by deepfakes – synthetic image, video or audio files in which an individual's face, voice, or actions are manipulated and replaced – is very real, as are the accompanying financial, reputational and service implications. CISOs must accelerate security innovation to keep pace.

With technology evolving at a breathtaking pace, deepfake-related concerns are scaling more rapidly than they did in connection with phishing 25 years ago. Today, bad actors are looking for bigger targets than individual consumers or public figures. Creative, ambitious cybercriminals with access to the latest technology have set their sights on more profitable targets – corporations, institutions and sovereigns – many of which are ill-prepared to defend against this threat.

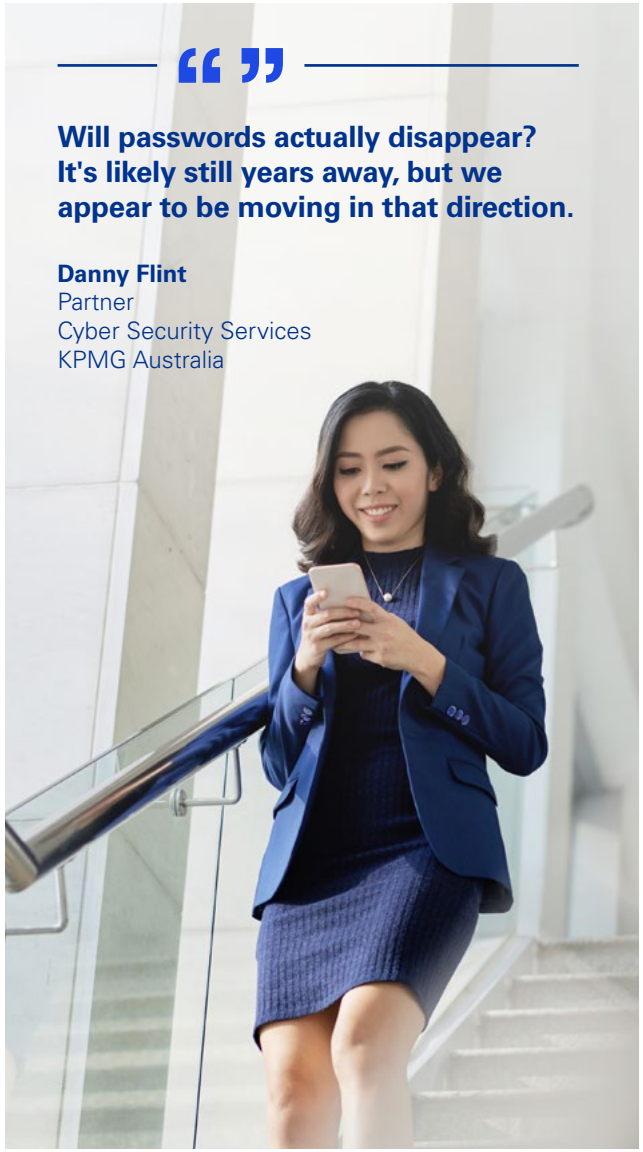
The key question is what it will take to train technology to make audio and video deepfakes that can consistently defeat biometric-based authentication.

> **Evolving to a model where a digital identity with a high level of assurance is a reality will enable businesses to collect, store and process less personally identifiable information – that is a decidedly positive outcome for consumers.**
>
> **Jim Wilhelm**
> Principal
> Cyber Security Services
> KPMG in the US

The cost considerations alone suggest it will require increasingly sophisticated attackers, but as access to the technology broadens, it will get less expensive, making it easier for bad actors to employ deepfakes as a fraudulent tactic.

A key concern regarding deepfakes is the funding required for detection, from maintaining the appropriate computing power, forensic algorithms, and audit processes to the talent needed to employ these tools. CISOs are encouraged to initiate conversations with senior decision-makers to ensure budgets match the emerging threats and keep technology up to date by ensuring software updates are installed as soon as they are released.[11]

[10] Juniper Research, *Digital Wallets: Market Forecasts, Key Opportunities and Vendor Analysis 2022–2026*. August 2022
[11] KPMG in the US, "Deepfakes: Real threat," 2023.



Will passwords actually disappear? It's likely still years away, but we appear to be moving in that direction.

Danny Flint
Partner
Cyber Security Services
KPMG Australia

Government's role in the new identity ecosystem

The government and corporate sectors appear to be coming together on the issue of identity. For example, one government is in the process of introducing the Trusted Digital Identity Framework (TDIF). This regime specifies the minimum requirements that identity service providers must meet to achieve and maintain TDIF accreditation allowing their customers access to digital government services.

The ultimate objective is to maintain a user-friendly platform that facilitates digital identities that are accessible, secure and private. Importantly, individuals will be able to use multiple identity service providers to maintain distinct or combined personal and business digital identities.

The TDIF empowers individuals to select which digital identity to use, for which purpose and duration, and have assurance around it. Government can't do this alone – it's simply not cost-effective. What's more, corporations are likely more trusted than government entities in the current environment.

In some countries, the backdrop is more fragmented because the regulatory activity is happening primarily territory-by-territory. But that's merely the tip of the iceberg, as digital identity unearths a new set of considerations around acceptance. People routinely travel across territory borders to do business. Will their digital credentials be accepted by officials across territory lines? Thinking about the public-private partnership aspect, if an individual has digital identification connected to a financial institution, as well as a government-issued digital credential, which one do they use in different circumstances?

Further, when people present a government-issued digital ID, should they be forced to share all of it? There are certain details that financial, healthcare or law enforcement officials want or need to see. Still, people should be able to maintain full control over what they disclose about themselves. For example, people should have the autonomy to disclose their citizenship status, college degree(s), professional qualifications/licensure, etc., but they should not be forced to offer the underlying personal data.

Another critical question for security professionals is who owns the risk? If someone's digital identity is compromised and used for fraudulent purposes, is the issuer or the holder responsible? Depending on a digital identity's intended use, strict but manageable regulations should be imposed on corporations. This is an issue over which there must be regulation and generally accepted standards to ensure the providers of digital identities can operate collaboratively and securely.

One of the foundational tenets of the EU's General Data Protection Regulation (GDPR) is that individuals must provide consent for organisations to use their personal data in specific contexts and for specific transactions.

But if a company wants to use personal identifiable information (PII) for another purpose or sell it, they must reacquire consent. That basic imperative should be a global standard.

Similarly, the EU Digital Identity – a personal digital wallet for EU citizens and residents – will soon enable individuals to identify themselves or confirm certain personal information. This e-identity will be able to be used both online and offline for public and private services across the EU.[12]

The global regulatory position around identity is fragmented and inconsistent. To some extent, the marketplace has become numb to the steady drumbeat of data breaches. Individual and institutional customers must be vigilant about the sensitive data they disclose and where they disclose it. CISOs and their teams should keep customer demands for the responsible use of and control over data as a core factor in developing identity management policies and strategies.

[12] European Commission, "Digital Identity for all Europeans," 2021.

Suggested actions

Keep your approach to identity flexible to comply with the evolving regulatory environment and ensure your architecture can integrate emerging technologies into the security process much faster than the two-, three- or four-year journeys we see today.

Explore more agile and interoperable identity systems to facilitate a federated identity ecosystem.

Consider your role, now and in the future, as an identity/credential issuer, relying party, digital wallet provider or all three in this evolving identity ecosystem.

Learn more

Deepfakes rewrite the cyber security playbook

Fakes aren't just for April Fool's anymore. They're coming to a boardroom near you, with the potential to destabilise your businesses.

Fake content is becoming a real problem

Widespread availability of sophisticated computing technology and AI enables virtually anyone to create highly realistic fake content.

How Identity and Access Management can enhance resilience and DORA compliance

With new EU regulations demanding vigilance around security, a robust identity and access framework is a vital tool in the kit.

Consideration 8

Align cyber security with organisational resilience

During a cyber incident, organisations need a response measured in minutes and hours, not days and weeks. In today's volatile environment, resilience has become a common theme for organisations across critical infrastructure sectors such as energy, communications and transportation, with executives focused on recovery if preventative controls fail. Resilience should seamlessly align with cyber security, emphasising protection, detection, and rapid response and recovery. Cyber resilience is vital for maintaining business operational capabilities, safeguarding customer trust, and reducing the impact of future attacks. These disciplines should work in tandem to help organisations manage risk.

"Resilience means being better equipped to manage incidents quickly, comprehensively, and with less impact on the business. It doesn't mean there will never be another incident. CISOs can't control external threats but can control the organisation's preparedness.

Dani Michaux
EMA Cyber Security Leader and Partner
KPMG in Ireland

Rebuilding trust is key after an incident

When a data breach or ransomware attack occurs, trust is the first asset to be impacted. And trust is absolutely a corporate asset. How well organisations are prepared and how quickly they can respond, and recover are key determinants in restoring customer and, for public companies, investor trust.

When organisations commit to earning – and re-earning – the trust of these vital stakeholders, they place themselves firmly on the path to operational resilience. In some cases, rebuilding trust is about rapid technical recovery; in others, it's about identifying alternate ways of delivering services. In every instance, it's about identifying vulnerable and/or impacted stakeholders, expeditiously addressing their needs and minimising disruption.

Regulators across all regions are now putting a greater emphasis on resilience and trust. For example, rules adopted in 2021 by the UK's Financial Conduct Authority are intended to ensure that important business services in the UK's financial services sector operate with sufficient resilience in the event of operational disruptions. Companies are required to demonstrate that they take a resilience-by-design approach. This framework is based on the notion of avoiding "wide-reaching harm to consumers and risk to market integrity" as a result of a cyber event.[13]

Mission criticality: Focus on what matters with advance planning

Every organisation is unique in what they do and how they do it, but from a security perspective, it's universally instructive to conduct structured, scenario-based tabletop exercises in advance of a cyber incident to ensure people, processes and technology are aligned.

Scenario planning shouldn't simply be a box that gets checked. These exercises reveal the strategic choices around how organisations deal with a major disruptive event like a ransomware attack and build confidence that leadership is prepared to coordinate response efforts and manage and ultimately lessen the impact on customers and clients. It's also imperative for organisations to determine in advance which business processes truly are mission-critical and need to be brought back online as soon as possible.

Cyber resilience, the ability to adapt to and weather a cyber incident, defers from business continuity, the procedures an organisation follows to operate during an incident. Resilience is strategic, while continuity is process oriented. In that sense, it's much less stressful to carry out a resilience exercise before a recovery situation than in the middle, when multiple business areas may be in panic mode.

Continuously assessing the state of the organisation's cyber resilience as a primary pillar of its overall preparedness and going through prioritisation exercises is critical to maintaining a cyber security plan that is both fit for purpose and fit for the-moment. It provides a response and recovery road map.

Every day, advanced persistent threat actors leverage different attack vectors in new ways. This evolution is a reality that CISOs must consider. Having a written and vetted resilience plan as a springboard to tangible action is much more effective than brainstorming during an attack.

Avoid complacency amid a changing threat landscape

Organisations' baseline security is getting better. At the same time, the business and supply chain landscapes are evolving, with increased dependency on a web of suppliers for IT, software and other services, and organisations experimenting with new technologies such as AI, Web 3.0 and smart products.

In response, attackers – organised/state-supported and lone actors – are becoming more sophisticated, exploring new vectors and manipulating reality through identity hacking and deepfakes. Today's attacks have shifted to include supply chain compromises and double or triple extortion ransomware backed by a complex "crime-as-a-service" ecosystem.[14]

> **Continuously assessing the state of the organisation's cyber resilience as a primary pillar of its overall preparedness and going through prioritisation exercises is critical to maintaining a cyber security plan that is both fit for purpose and fit for the moment. It provides a response road map.**

Jason Haward-Grau
Global Cyber Recovery Services Leader
KPMG International and Principal
KPMG in the US

[13] Financial Conduct Authority, Policy Statement PS21/3, "Building operational resilience," March 2021.

[14] KPMG International, "Maintaining cyber vigilance and staying resilient," 2023.

Bottom line, organisations need to follow a dynamic approach to resilience. They can't be complacent because not only is the threat changing, but the way bad actors seek to disrupt both internal processes and supply chains is also changing.

Organisations need to continually improve and adapt. Resilience means being better equipped to address an incident quickly, comprehensively, and with minimal business impact. It doesn't mean there will never be another incident. CISOs can't control external threats but can control the organisation's preparedness.

The investments of time, people and budget should not be focused solely on incident avoidance but instead on cultivating an enduring state of resilience that becomes an integral, embedded component of the overarching cyber security plan.

There's an ongoing arms race between organisations and bad actors, and the latter are constantly evolving and innovating faster – because it's all they think about. If CISOs understand and manage the organisation's security drift, they can chip away at attackers' ability to identify and exploit vulnerabilities.

As organisations navigate today's evolving and volatile cyber security landscape, resilience should not be viewed as a series of one-off or intermittent projects. Rather, it should be an adaptive strategy that complements the organisation's cyber security agenda, protects customer interests, aligns with the objectives of the business, and focuses on delivering long-term value.

Suggested actions

Assess how the organisation can respond better and faster if attacked again next week and next month/year to identify 'quick wins,' like expediting payments, ensuring liquidity, improving communication and enhancing response speed.

Foster organisation-wide behaviours and cultural alignment to prioritise what truly matters to the organisation in terms of data, services and infrastructure.

Regularly update plans and playbooks to align with the evolving threat landscape and IT and supply chain dependency changes.

Learn more

Maintaining cyber vigilance and staying resilient

How to recover from a cyberattack, rebuild effectively and avoid complacency.

Cyber and digital operational resilience

Targeting strategic resilience.

Mid-market: a holistic approach to boost cyber resilience

A more connected world has increased risk and expectation. In response, the mid-market can implement holistic cyber security strategies.

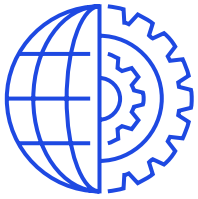
Cyber strategies for 2024

What actions can CISOs, and the broader business lines take in the year ahead to help ensure security is the organisation's golden thread? Following is a short list of recommendations 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

- Connect with your organisation's ESG team to determine whether they consider cyber a key aspect of their mandate. If not, work to build awareness of how and why it's important to all three areas of ESG.
- Bring a new perspective to the board on what could disrupt the business and what should be done to manage those risks without impacting operations and customer experience.
- Foster organisation-wide behaviours and cultural alignment to prioritise what truly matters to the organisation in terms of data, services and infrastructure.
- Determine how and where to embed certain security tasks within the business vs. outsourced to a third-party service provider and monitor those tasks to ensure they are carried out properly.
- Be practical. Effective cyber security is not as much about getting business partners to do things differently as it is about reframing the conversation across the enterprise to inspire other areas of the organisation to infuse security into what they already do.

Process

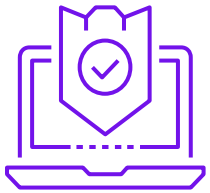


- Run the cyber team like a business, which means you must give up a degree of control over what other parts of the organisation are doing from a security perspective.
- Define your initial vision and strategy for automation. Consider your short- and long-term security objectives, ensure how those goals align with the organisation's business priorities, and determine the type of protections those shared objectives require.
- Enhance transparency to build trust across global supply chains; rather than treating third-, fourth-, and even fifth-party supplier relationships solely as transactional and contractual (which they are), approach them as an extension of your ecosystem.
- Regularly update plans and playbooks to align with the evolving threat landscape and IT and supply chain dependency changes.
- Take a risk-based approach to assessing third-party processes rather than a blanket approach to different suppliers that provide diverse services.
- Encourage crowdsourcing of intelligence and sharing both within your organisation and with trusted third parties.
- Assess how the organisation can respond better and faster if attacked again next week and next month/year to identify 'quick wins,' like expediting payments, ensuring liquidity, improving communication and enhancing response speed.

Data and technology

- Identify what data the organisation has centrally accessible and define an automated continuous controls monitoring plan to drive efficiencies across all three lines of defence.
- Know where critical data – both structured and unstructured – resides across the organisation, as well as where it is shared with third-party partners.
- Ensure the purpose of AI algorithms, whether developed in-house or externally, is clearly defined and documented and training data is relevant, appropriate for the business objective, and secure consent.
- Leverage intelligent automation to gain higher visibility into the changing supplier risk profiles and build a sustainable and scalable forward-looking third-party program.
- Determine what tools to build versus acquire and understand how supply chain partners are automating to strengthen trust between the organisations and leverage that learning where appropriate.
- Explore more agile and interoperable identity systems to facilitate a federated identity ecosystem.
- Consider your role, now and in the future, as an identity/credential issuer, relying party, digital wallet provider or all three in this evolving identity ecosystem.

Regulatory



- Sharpen your global regulatory intelligence around cyber in general and ESG and privacy in particular to ensure timely compliance and reporting; keep track of and remain familiar with ever-increasing regulations and their effects on your cyber efforts.
- Align your AI framework with current standards and develop solid AI governance by aligning the priorities of the various business leaders in the organisation and gaining cross-functional support from those with a vested interest in the success of AI.
- Acquaint yourself with the stipulations of the EU AI Act and the Biden administration's Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence.
- Maintain an understanding of the global regulatory landscape, specifically an understanding of the relevant rules at a granular, jurisdictional level.
- Keep your approach to identity flexible to comply with the evolving regulatory environment and ensure your architecture can integrate emerging technologies into the security process much faster than the two-, three- or four-year journeys we see today.

How KPMG professionals can help

KPMG firms have experience across the continuum – from the boardroom to the data centre. In addition to assessing your cyber security and aligning it to your business priorities, KPMG professionals can help you develop advanced digital solutions, advise on the implementation and monitoring of ongoing risks and help you respond effectively to cyber incidents. No matter where you are in your cyber security journey, KPMG firms can help you reach your destination.

As leading providers and implementers of cyber security, KPMG professionals know how to apply leading security practices and build new ones that are fit for purpose. Their progressive approach to cyber security also includes how they can deliver services, so 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, and move more efficiently with secure and trusted technology. That's because they can bring a combination of technological experience, deep business knowledge, and creative professionals passionate about helping you protect and build stakeholder trust.

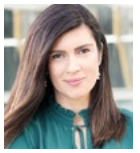
KPMG. Make the Difference.

Contacts

Martijn Verbree
Head of Cyber Security
KPMG Australia
mverbree@kpmg.com.au

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

Danny Flint
Partner, Cyber Security – Digital Trust and Identity & Access Management Lead
KPMG Australia
dflint@kpmg.com.au



Gergana Winzer
Partner, Cyber Security – Mid Market Lead
KPMG Australia
gwinzer@kpmg.com.au

Acknowledgements

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

Katie Boswell, Pratiksha Doshi, Brian Geffert, Prasanna Govindankutty, Jason Haward-Grau, Elizabeth Huthman, Kyle Kappel, Sylvia Klasovec Kingsmill, Mika Laaksonen, Angela Leggett, Orson Lucas, Dani Michaux, Mitushi Pitti, Caroline Rivett, Henry Shek, Akhilesh Tuteja, Marko Vogel and Jim Wilhelm.

KPMG.com.au

February 2024.1267206204CON