KPMG

Cybersecurity considerations 2026

Building trust and enabling innovation in a dynamic world

KPMG International

kpmg.com/cyberconsiderations

Contents

Foreword 03

Eight key cybersecurity considerations for 2026 05

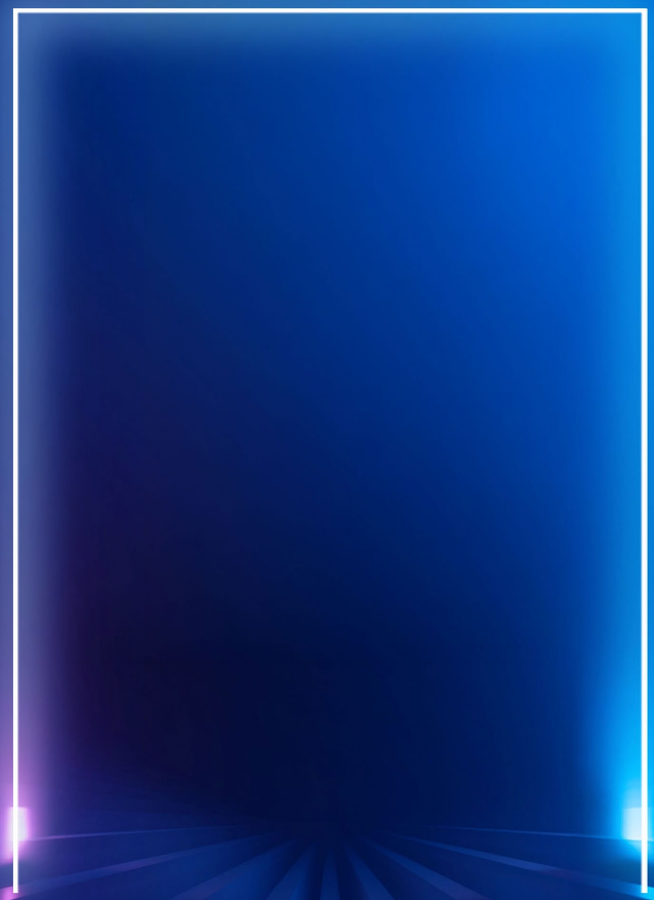
Sector insights: Emerging cybersecurity priorities 06

Cyber strategies for 2026 40

How KPMG professionals can help 41

Meet the authors 42

Acknowledgements 43



Foreword

As organizations transform for growth, the speed and intensity of technological change bring both opportunity and risk. Chief Information Security Officers (CISOs), and those responsible for balancing business agility with cyber risk, must keep pace with developments in technology, the geopolitical landscape and evolving compliance requirements that directly impact cybersecurity. They must support trusted operations and innovation in the face of an expanding cyber attack surface. The ubiquity of technology continues to expand their role across every business function, requiring CISOs to work with multiple stakeholders and present a strong case for investment in cybersecurity. This imperative is informed by several critical drivers that are currently shaping the world of cybersecurity for CISOs and enterprise leaders alike:

Opportunities and threats from AI

AI is at the center of today's disruptive period and is proving to be a double-edged sword for cybersecurity professionals. On the one hand, those charged with defense, protection and response can leverage AI to detect and address threats faster and more efficiently than humans alone. On the other hand, AI empowers threat actors, who not only automate and scale their efforts, but also use more sophisticated methods and tools to breach cyber defenses. Agentic AI and the proliferation of digital agents is also placing digital identity management under greater scrutiny as CISOs strive to protect the plethora of non-human identities and keep their activities under control.

Regulation and sovereignty add complexity

As the global regulatory environment becomes more fragmented, CISOs and Chief Risk Officers (CROs) are increasingly involved in efforts to comply with digital safety, sovereignty and resilience requirements. The range and complexity of these obligations are straining the resources and capabilities of cybersecurity teams striving to keep data secure and private.

The geopolitical landscape is increasing cyber risks

Geopolitics has become a common feature of cyber conversations, with rising tensions causing (sometimes rapid) decoupling of former trading partners. As organizations rethink where they operate and who they source from, these decisions have a cascading impact on CISOs as they manage the threats from nation states and help ensure a safe transition to new supply chains.

CISO visibility and responsibility continues to increase

Cybersecurity is now everyone's responsibility, and CISOs should continue to raise awareness of risks, instill responsible digital behaviors, and communicate cyber risk in the language of business to leadership, employees, suppliers, and partners. By adopting a principle of 'radical transparency', CISOs can help the organization and its partner ecosystem understand the importance of cybersecurity and make decisions based on signals, risk and intelligence.

Quantum presents a real threat in the medium term

The transition to post-quantum cryptography (PQC) presents a significant transformation requirement and, for sectors like finance and defense, an existential one. Proactively preparing for quantum-related cyber risks now can help secure organizations' futures by making them more resilient, supporting business continuity, and managing regulatory changes.

Stepping up to IT/OT hyperconnectivity

As digital and physical systems merge, hyperconnectivity makes the operational technology (OT) environment in sectors like Utilities, Oil and Gas, Natural Resources, Manufacturing, and Telecommunications more vulnerable to breaches via vast numbers of internet of things (IoT) devices. Data centers are now considered critical infrastructure and their immense thirst for electricity raises the pressure to safeguard power and utility facilities. Power plants are being constructed, and older ones reopened, with attendant OT security risks — especially from obsolete legacy technology.

Cyber and trust as a differentiator and business asset

Technology will continue to develop at its own pace, and, to some extent, organizations are 'building the plane as they fly it'. While there is a huge responsibility to secure AI, there is also an incredible opportunity to leverage AI as a superpower to boost cybersecurity defenses and productivity. Organizations may not be able to completely control how they adopt technology, but with the help of the cyber function, they can do so in a responsible and trusted manner.

Cybersecurity has become a priority across the enterprise and should be fully embedded. Notably, the KPMG 2025 CEO Outlook identifies cybersecurity and digital risk resilience as one of the top pressures influencing investment decisions. By creating safer, more resilient operations, CISOs can continue to build stakeholder trust, reduce the cost of capital, and enable new product development — to keep their businesses competitive.

About this paper

Cybersecurity considerations 2026 presents insights from more than 20 leading KPMG cyber experts around the world, alongside senior leaders from our cybersecurity alliance portfolio including Google, Microsoft, Palo Alto Networks, and ServiceNow. It is further informed by findings from KPMG global and regional surveys.

The paper explores eight key considerations on the agenda of CISOs and other senior leaders across the enterprise, spanning multiple sectors. At a time of heightened cyber challenges, it aims to contribute to the future direction of cybersecurity and highlights opportunities to strengthen resilience, improve organizational performance, and embed AI safely and effectively.

Laurent Gobbi
Global Cybersecurity and
Tech Risk Centre of Excellence Leader
KPMG International
E: lgobbi@kpmg.fr

Jim Wilhelm
Global Cybersecurity Investment Leader
KPMG International
E: jameswilhelm@kpmg.com

Eight key cybersecurity considerations for 2026

Click on each consideration to learn more.

01

Preparing the cyber workforce for autonomous security

As security becomes automated, agents are taking on more intelligence-driven tasks in the security operations center (SOC) as well as compliance, risk management, and identity management. Autonomous security is set to play a critical role in identifying and monitoring non-human identity activity.

02

Navigating geopolitics, building resilience and compliance

Both digital defenses and physical assets are threatened by potential attacks from hostile nations. Organizations should assess potential risks and use AI, automation, and analytics to streamline controls, speed up evidence collection, and boost regulatory compliance.

03

Safeguarding AI systems

As AI becomes deeply embedded in enterprise operations, its security is emerging as a critical priority. Safeguarding AI is no longer a technical challenge alone, but a strategic imperative that intersects with compliance, trust, and operational resilience.

04

Managing non-human identities in the age of AI

In increasingly digitized and automated environments, non-human identities — such as AI agents, service accounts, and machine credentials — now outnumber human users. Organizations must rethink identity governance to include the full lifecycle of both human and machine actors — with AI managing the complexity it helped create.

05

Enabling trusted IT/OT hyperconnectivity

Embedded sensors, IoT devices, and fully connected environments are becoming commonplace, particularly in infrastructure-intensive and service-driven industries. Aiming to secure hyperconnected systems demands a dynamic ‘mesh’ architecture, clarity of ownership, and the capability to monitor and respond across cyber-physical boundaries.

06

Transitioning to post-quantum cryptography

The transition to post-quantum cryptography (PQC) is increasingly anticipated on a global scale and is unlikely to be avoided. Around the world nations are implementing guidance and regulations to migrate encryption in order to manage quantum cyber risk. This will be a major challenge and, for sectors like finance and defense, an existential one.

07

Protecting the supply chain through detection and response

Today’s complex supply chains create a vast digital attack surface that includes AI and a myriad of IoT devices. Organizations should extend the scope of third party risk management with continuous monitoring and oversight to maintain operational resilience.

08

Broadening the role and influence of the CISO

The scope and responsibilities of the CISO continue to expand as security becomes more deeply integrated into business and operations, converging the cyber and physical domains. At the same time, CISOs must manage the opportunities and threats associated with widescale AI adoption.

Sector insights: Emerging cybersecurity priorities

Our conversations with cybersecurity leaders across industries signal that **supply chain risk, geopolitics, and non-human identity management** are rising to the top of the eight cybersecurity considerations. The chart below depicts how these priorities are emerging across sectors and where executive focus is aligning.

Government and Public sector	Financial Services	Defense	Energy, Natural Resources and Chemicals	Technology, Media and Telecommunications	Healthcare
Geopolitics	Geopolitics	Geopolitics	Geopolitics	Autonomous security	IT/OT hyperconnectivity
Safeguarding AI systems	Autonomous security	Managing non-human IDs	Managing non-human IDs	Managing non-human IDs	Managing non-human IDs
Quantum	Supply chain detection and response	Supply chain detection and response	Supply chain detection and response	Supply chain detection and response	Supply chain detection and response

Example sector perspectives and implications

Government and Public Sector:

- Failure to migrate to PQC puts sensitive government and citizen data at risk, undermining trust in digital public services. Governments and public sector organizations can prioritize PQC-ready architectures to maintain resilience and public confidence.

Financial Services:

- AI-driven fraud detection offers high accuracy but may suffer from lack of transparency, heightened data privacy risks, and biased outcomes. Organizations should embed security in design, and reinforce governance and human oversight, including continuous monitoring of AI systems.

Defense:

- Political fragmentation and sustained, grey-zone cyber activity expose defense supply chains to persistent compromise, particularly across software, OT, and critical infrastructure. Continuous supply chain detection and response help protect operational resilience, readiness, and mission assurance when systems must perform under pressure.

Energy, Natural Resources and Chemicals:

- Intricate supply chains with global components can prevent full transparency, especially at the IT/OT intersection. In response, organizations in this industry should implement robust visibility, standardized frameworks, and continuous monitoring, leveraging managed services where needed, to build a truly resilient ecosystem.
- An advanced, identity-centric security approach can improve cybersecurity in AI-driven operations and interconnected OT environments, although legacy systems and fragmented ownership can hinder implementation.

Technology, Media and Telecommunications:

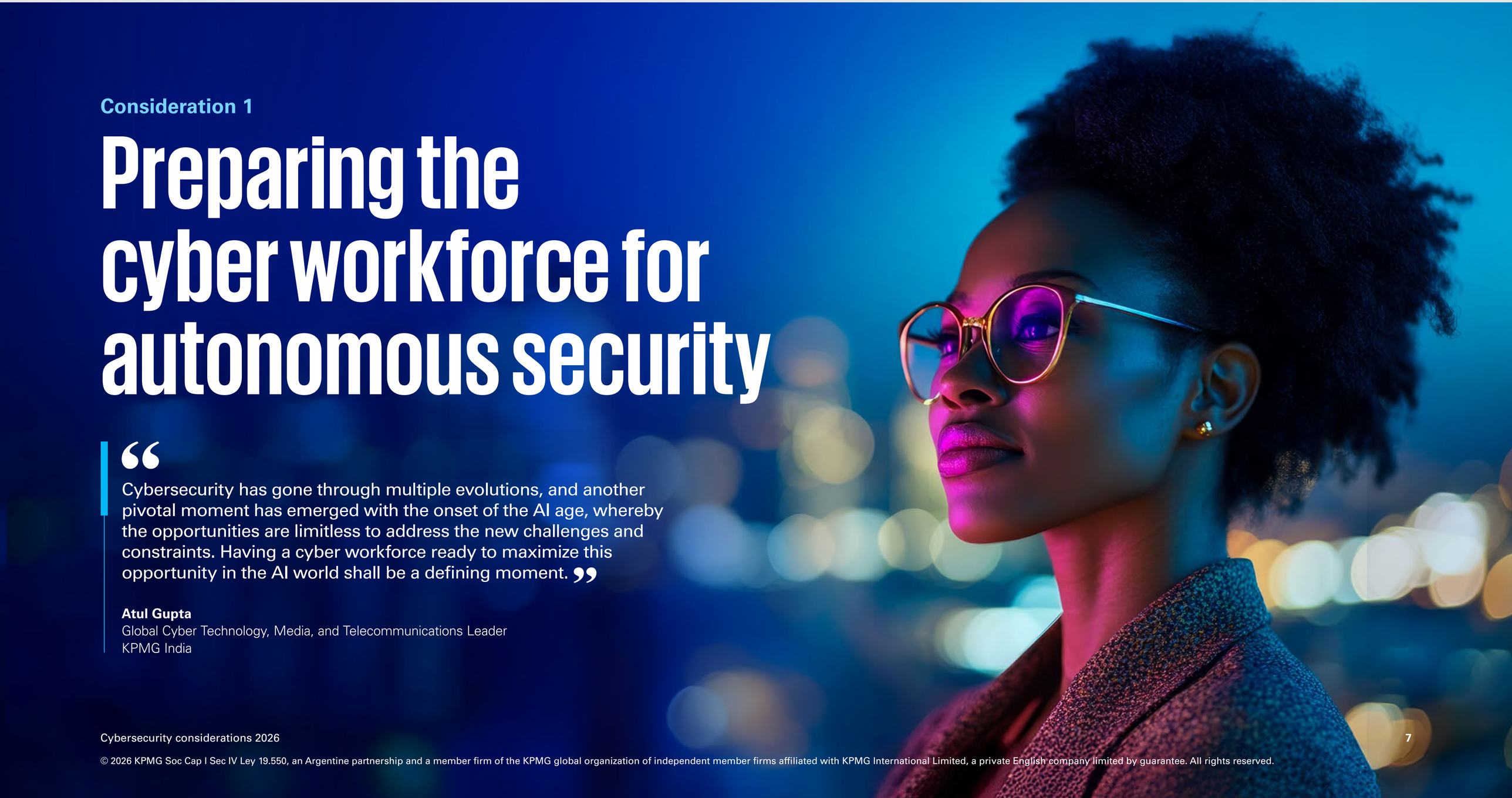
- Telecommunications carriers have deployed systems that detect international revenue fraud by verifying non-human identities and securing machine-to-machine voice traffic.

Healthcare:

- Optimizing complex clinical workflows with AI requires transparent, ethical, and secure AI agent development. As demonstrated by Oslo University Hospital's AI scheduling solution improving surgery productivity, organizations should champion AI with these characteristics, ensuring outcome alignment to build confidence and trust.
- Interconnected medical devices and clinical systems open lateral movement opportunities for attackers, complicating incident response, with outages impacting patient care. Organizations should focus on resilience and cross-domain intelligence, aligning IT/OT security with business goals.

Consideration 1

Preparing the cyber workforce for autonomous security



> “Cybersecurity has gone through multiple evolutions, and another pivotal moment has emerged with the onset of the AI age, whereby the opportunities are limitless to address the new challenges and constraints. Having a cyber workforce ready to maximize this opportunity in the AI world shall be a defining moment.”

Atul Gupta
Global Cyber Technology, Media, and Telecommunications Leader
KPMG India

Consideration 1

As security becomes automated, agents are taking on more intelligence-driven tasks, especially in the security operations center (SOC), but also in other parts of the cyber domain, including compliance, risk and identity management. In this context, what is the role of security professionals? What are the future skills of the cybersecurity workforce? Let us explore first how agents and automation are transforming the cyber function.

The rise of agents

Agents are making decisions and scanning the multitude of alerts that reach an incident desk, at a pace SOC analysts cannot match. As non-human identities proliferate — including machine credentials, service accounts, and digital agents capable of creating and deleting other agents — autonomous security will play a critical role in identifying and monitoring their activity. AI and automation can accelerate the onboarding process, which now takes place primarily in the cloud. Traditional on-premises data centers cannot cope with such large data volumes. Automation is powering other key business processes such as automated workflows, real-time support, (application) onboarding, and performance management.

To exploit vulnerabilities, cyber attackers are increasingly targeting and exploiting machine credentials through non-human identities, often via third parties such as hyperscalers and software as-a-service (SaaS) providers. This puts intense pressure on cybersecurity teams to identify a rapidly growing body of agents, monitor access permissions, and record their presence in inventories.

Robust cloud and data governance are crucial for implementation of AI systems — and deployment of agents by other agents — to ensure that data is securely stored and managed, and that AI systems are compliant with regulatory requirements. However, many organizations are dependent on a single hyperscaler, which leaves them vulnerable to any service disruption. Banks, retailers, telecommunications networks, government departments and other entities have all suffered due to temporary cloud provider shutdowns, leaving service account identities (SAIs) unable to access their services.

Building resilience with technology

CISOs are adopting a dynamic risk management approach to autonomous AI, using accepted principles of zero trust, clear policies, and access controls. Security teams are partnering with AI specialists and data science teams, and building safeguards, to demonstrate resilience to internal audit and external regulators. The key is to align the use of AI technology with their risk limits and thresholds, and CISOs can draw parallels to the shift from perimeter-based to zero trust security. The rise of agents poses questions about the adequacy of the skills across all three lines of defense. The third line, which is traditionally internal audit, now requires deep technical skills to keep up with rapid technological change.

> “An analogy is the autopilot on a plane, which doesn’t replace human pilots, but makes their job more effective and safe. By putting a whole bunch of automation workflows and safeguards and other complex systems around the human delivery, you can drive a much higher degree of efficacy than humans could ever possibly get to on their own.”
>
> **Chris Corde**
> Head of Product, Security Operations
> Google

Consideration 1

With new agents emerging continually, CISOs are concerned that they are unable to identify and catalog these agents, or to determine which ones are vulnerable. 'Shadow agents' (autonomous or semi-autonomous AI agents) are popping up everywhere, from SaaS providers to existing agents that are even creating their own agents. The management of non-human identities requires a centralized identity store and policy-based access controls. CISOs also need to introduce autonomous security architecture into the SOC — quite a transformation — to manage the high volume of events generated in the new AI-powered world, including the enhanced abilities of threat actors. This requires robust safeguards and policies to establish AI security posture management (AI-SPM), supported by continuous monitoring and improvement of AI models, data, and infrastructure. Although still nascent, AI-SPM focuses on identifying vulnerabilities and unauthorized access in line with AI security policies. As AI solutions proliferate, CISOs should establish red-teaming of these solutions, to build in AI security.

A new role for humans

As agents become ever more autonomous, organizations and the security function will need to retrain and reposition their workforce to carry out more meaningful tasks — such as advanced threat analysis, strategic cyber decision-making, and AI integration. New roles may include AI agent managers — to oversee agent activity — and data governance specialists. This is no longer a niche technical concern. In the KPMG Global tech report 2026, 92 percent of technology executives say that managing AI agents will become an essential skill within the next five years, highlighting a broader shift toward human oversight, governance, and intervention in autonomous systems. As Chris Corde, Head of Product, Security Operations at Google, notes: "As agentic approaches are embedded into every workflow, cybersecurity professionals will need to build agentic functions, test and validate efficacy, and perform additional training of models. This is highly specialized, AI-driven expertise, which is probably a very, very new thing for most security engineers." CISOs may also have to find ways to attract engineers to work in the internal audit function, to satisfy demand for greater AI capabilities.

Agentic-led cybersecurity presents a big opportunity to gain greater visibility and control over an organization's digital assets. Supported by a strong security data lake, such an approach can shift cybersecurity from manual to automated and restore the balance of power to CISOs and their teams.

92%

of technology executives say that managing AI agents will become an essential skill within the next five years

Source: KPMG Global tech report 2026

> "With the expansion of the attack surface to more endpoints and the significant growth of data to protect as a result, using AI and automation to sift through the noise and escalate the security events that matter will be imperative for all functions within the organization to embrace."
>
> **Charlie Jacco**
> Global Cyber Managed Services Leader
> KPMG International

Consideration 1

Suggested actions

Embed security with AI specialists and data science teams to co-design safeguards, align AI use with defined risk limits and thresholds, and demonstrate resilience to external regulators.

Set up an AI/agent red-team function to regularly test AI solutions and agent behavior, and channel findings into control improvements and assurance activities.

Extend AI and automation beyond the SOC into operations, the third line of defense, and other cyber domains to improve threat monitoring and response.

Proactively address the challenge of non-human identities by embedding them into enterprise-wide identity governance.

Retrain employees for higher-value, strategic tasks and establish new AI-focused roles, reinforcing ‘humans in the loop’ to maintain control over AI activity.

Consideration 2

Navigating geopolitics, building resilience and compliance

> “Given geopolitical tensions and resilience challenges, from a technology perspective, we are leaving the decade of standardization and international collaboration and entering a new era of decentralization and sovereignty, which increases complexity for CISOs.”

Dani Michaux
Cyber Security Leader, EMA region
KPMG Ireland

Consideration 2

Geopolitics is profoundly influencing cybersecurity, with both digital defenses and physical assets, such as space satellites and submarine cables, threatened by potential attacks from hostile nations. The increase in inter-country tensions is forcing CISOs to consider the resilience of their service and technology infrastructure, and how this can adversely impact their competitiveness. Threats include spying, theft of intellectual property, and system shutdowns due to backdoor incursions. With lines blurring between nation states and corporates, a form of hybrid cyber warfare has evolved.

In some cases, governments are decoupling from 'unfriendly' states and mandating where businesses can and cannot buy their technology. Tariffs are a further complication, pushing up the prices of imports from certain geographies. With globalization on the retreat, corporate leaders are seeking to localize their supply chains and are exploring new partnerships and alliances.

Companies in critical sectors like telecommunications, technology, and defense are likely to be subject to particularly rigorous sourcing restrictions. Regulations also differ from region to region, and country to country, with varying reporting requirements — for example, over the use of AI and data sovereignty — pushing up the burden of compliance.

This shift from global to local means that multinationals who have built up harmonized, centralized systems are having to decentralize to some extent, adding layers of cost and complexity. For example, it may no longer be possible to have single, global warehouse systems, global IT and security services, or identity management systems. CISOs need to increase the resilience of their security service and tool architectures, while gaining visibility across their global technology stacks. This is essential to protect against attack, minimize disruption, and meet regulatory and governmental demands. As technology grows more complex, third-party ecosystems expand, and agentic AI introduces non-human identities, achieving full transparency becomes a major challenge.

Major threats to organizations' future prosperity

79% Cybercrime and cyber insecurity

69% Regulatory demands

57% Geopolitical conflicts

Source: KPMG 2025 CEO Outlook

Some regulations are making executives more accountable for cybersecurity governance and controls, creating a material risk and placing even greater pressure to demonstrate resilience.

Emerging cybersecurity regulations:

- EU NIS2 (Network and Information Security Directive 2) aims to improve cyber resilience for critical infrastructure and essential services, including enhanced risk management, and quicker incident reporting
- EU CER (Critical Entities Resilience) requires organizations to strengthen critical infrastructure resilience, calling for national strategies, risk assessments, and prevention and response
- Presidential Policy Directive 21 (PPD-21)/NSM-22 (2024) in the US
- Cyber Security and Resilience (Network and Information Systems) Bill in the UK
- Critical Cyber Systems Protection Act (CCSPA) — Bill C-8 in Canada
- Security of Critical Infrastructure Act (SOCI Act) in Australia
- Cybersecurity Law (CSL) + 2025 Amendments (effective January 2026) with focus on resilience in China

In the aftermath of a significant data breach or suspected major incident, the organization's cyber defenses will immediately come under regulatory scrutiny, with a rising focus on AI-driven continuous control testing and automated reporting.

Consideration 2

Cybersecurity as a strategic imperative

Geopolitics and compliance have become key enterprise risks. With products, services and operations, from front-to-back office, increasingly connected, organizations need the kind of holistic oversight that only CISOs can provide. Cyber professionals should be involved with product teams, and technology procurement and implementation, to ensure that cybersecurity is embedded from the start, balancing speed and innovation with security, resilience and compliance. Regulatory compliance can be a positive force, as it requires CISOs to understand their risk landscape, and practice strong governance that can drive business continuity.

Many companies are reliant upon a single technology vendor, which can be problematic if the vendor is restricted for some countries. The technology supply chain is also likely to contain multiple smaller vendors, which raises the complexity of third party risk management (TPRM), extending the resilience, as well as the compliance checklist to fourth, fifth or even sixth parties. A single security breach in any of these parties has the potential to create a larger, systematic failure that could halt operations and lead to regulatory penalties and reputational damage.

Gaining visibility over such a wide range of assets — and spotting any weak links — is a huge task, encompassing hardware, software, and data across public and private clouds. Regulations are driving digital resilience. DORA (Digital Operational Resilience Act) in the EU, calls for financial services institutions to manage and report incidents, carry out resilience testing, and manage third-party risks. Also in financial services, Operational Resilience focuses on vital or critical business services (VBS/CBS) and setting impact tolerances for disruption. The CISO's role is to create greater transparency over supply chain risks, enabling informed decisions based upon the organizational risk appetite. By thinking in terms of scenarios, they can help executive management maintain operations in the face of cyber threats and minimize disruption to customers.

As Ben de Bont, Chief Information Security Officer, ServiceNow, says, "Threat intelligence, vendor management, supply chain management, third party, fourth party, fifth party risk management can't live in silos. Integrating live threat feeds into vendor workflows enables continuous risk correlation, linking what's happening externally with who you depend on internally."

> "Your supply chain is now your attack chain — it's so fragmented and country specific. That fragmentation, along with cloud interdependence and AI model sourcing, have turned that supply chain risk very much into a geopolitical issue, and I think that is really making every line of code geopolitical."
>
> **Ben de Bont**
> Chief Information Security Officer
> ServiceNow

From compliance to resilience

In their role as cybersecurity and resilience advocates, CISOs should integrate cybersecurity into the organization's broader goals, aligning compliance efforts with strategic risk reduction. To achieve this, CISOs need to be involved in important technology decisions — such as cloud vendor contracts, AI adoption, and new product development. They should work closely with the business and IT leadership and build a collaborative culture. CISOs can help frame technological choices in terms of their measurable, material business impact, and enable leaders to invest in products, services, and infrastructure that stay within acceptable risk thresholds. To manage this complexity efficiently, CISOs should quantify the risk and impact of related measures. Cyber Risk Insights (CRI), KPMG's leading cyber risk quantification platform, uses scenarios to assess the likelihood and impact of cyberattacks. AI, automation, and analytics can do some of the heavy lifting to streamline controls, speed up evidence collection, and boost risk analysis and regulatory compliance.

CISOs and their teams should act as continuous risk sensors for the organization, enabling leaders to assess change, understand emerging threats, and maintain resilience.

> "CISOs need to become trusted business advisors, translating technical risk into material business impact, and integrating cybersecurity with resilience."
>
> **Marko Vogel**
> Head of Cyber Security and Resilience
> KPMG Germany

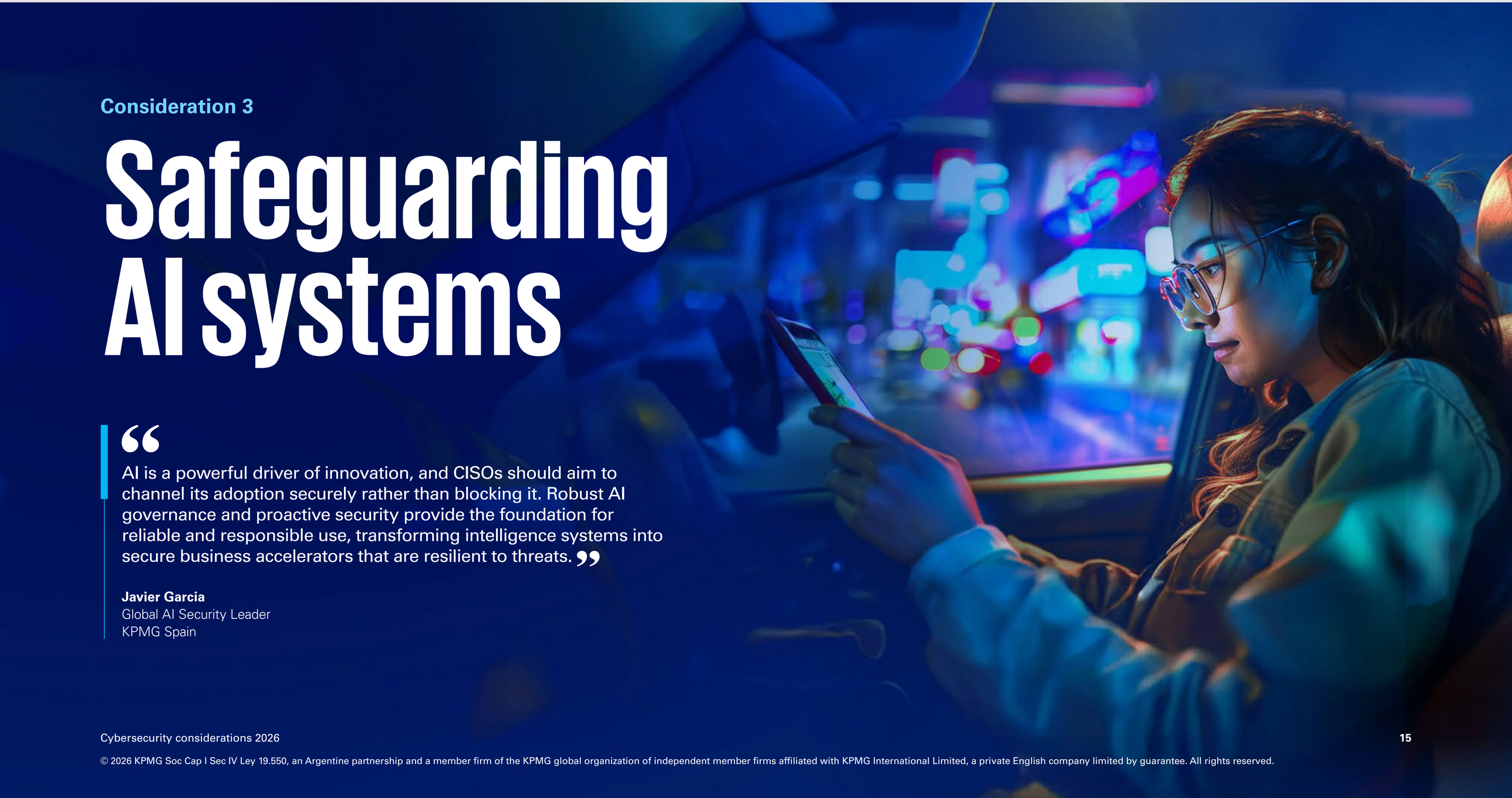
Consideration 2

Suggested actions

- Integrate geopolitical risks and emerging regulatory standards into CISO programs to strengthen foresight and resilience.
- Communicate the business impact of cyber risks and security initiatives to the board and executive leadership.
- Build a collaborative, holistic risk culture, working with the board, IT, Procurement and Risk Management.
- Proactively define and implement the data, service and technical architecture, to adapt to changing conditions.
- Gain visibility across internal and supply chain technological assets, to detect and mitigate existing or potential vulnerabilities.

Consideration 3

Safeguarding AI systems



> "AI is a powerful driver of innovation, and CISOs should aim to channel its adoption securely rather than blocking it. Robust AI governance and proactive security provide the foundation for reliable and responsible use, transforming intelligence systems into secure business accelerators that are resilient to threats."

Javier Garcia
Global AI Security Leader
KPMG Spain

Consideration 3

As organizations introduce AI, and increasingly agentic AI, they must not only safeguard the data that feeds into AI systems, but the behavior of the AI agents themselves. This means ensuring that AI models are fair and ethical, but also robust and resilient against threat actors — who are applying innovative, AI-enabled automation to improve their attack efficacy. Across sectors and regions, there are evolving regulations over AI use, putting pressure on CISOs to demonstrate appropriate governance over their systems' integrity and reliability. However, AI systems operate at speeds and scales that today's security practices struggle to match. This includes automated cyberattacks orchestrated by hundreds or thousands of agents working independently. As attackers innovate with automation, AI and AI agents, organizations require new approaches to monitoring and control.

Managing AI

AI agents are gaining greater privileges, accessing vast amounts of data, collaborating, coding, and acting autonomously at an unprecedented pace. However, they can also behave like black boxes, making it difficult for organizations to trust what they cannot see. To gain greater confidence over agent activity, CISOs must ensure that information sources are reliable, that agents have clear boundaries of authority, and that data is used appropriately. This means validating that an AI agent is not manipulated or corrupted by 'bad actors' and distinguishing whether past decisions were taken by humans or agents.

AI agent checklist

- Where are agents operating?
- What are the agents' identities?
- What can agents access?
- What are agents' permissions?
- Are agents' permissions aligned with the approved use case?
- How do we shut down actions outside of the approved use case?

As Saira Mohammed, Chief Security Advisor, Microsoft, notes, "Clear policies and defined accountability are essential for responsible agent creation and adoption. Effective agentic AI governance requires precise scope, strong guardrails, and clear ownership of what an agent can and cannot do — and how to respond when it drifts from its intended purpose. As agent sprawl and misuse grow, security operations teams must partner closely with the business to determine the right actions when deviations occur. Without clear accountability, continuous monitoring, detection, and response break down, leaving security teams unable to make informed decisions or mitigate risk effectively. It's similar to a manufacturing plant — when a machine isn't operating correctly, they shut it down."

Some AI agents are sourced directly from third-party suppliers or embedded in products — including enterprise resource planning (ERP) software. This increases accessibility but also introduces new risks. To reduce the risk of bias, or security breaches, organizations should perform continuous red-teaming and remediation exercises. AI-embedded products should be securely configured and tested before deployment. To foster trust in AI systems, CISOs should be aware of third-party AI and apply AI governance, including formal third-party contracts on AI usage, with security clauses and accountability for any breaches.

> "AI security carries immense risk and impact. We don't need to reinvent the security wheel; but the unprecedented pace and scale of AI demands a fresh approach — embedding security-by-design and leveraging automated AI throughout the process."

Kristy Hornland
Director, Cyber Threat Management
KPMG US

Consideration 3

"Developers must embed security from the start — well before AI solutions reach production," says Microsoft's Saira Mohammed. "Achieving true visibility across the digital estate demands a platform-centric model grounded in security-by-design and secure defaults. This is also a chance for security teams to modernize their operational approach by adopting an open, integrated platform stack that connects seamlessly with third-party APIs (application programming interfaces) and has security built in, not bolted on."

When organizations use hundreds or even thousands of agents, they cannot rely on a purely manual process to detect and observe their actions and check their access rights. AI helps to automate security operations, process vast amounts of data and telemetry, and analyze patterns and anomalies, to predict and prevent attacks as a form of 'predictive shielding'.

The Open Web Application Security Project (OWASP) Agent Observability Standard (AOS)[1] aims to make AI agents more transparent. It requires agents to be "instrumentable, traceable and inspectable", with hard controls over what they can and cannot do, and the ability to trace any action back to the reasoning behind it and the originating task, and highlight the tools, models and capabilities it uses. Part of this approach involves developing AI systems with security-by-design embedded into the process, with a type of 'firewall' that filters data before it can enter an AI model for processing. The next step in AI agent security is what Gartner calls 'guardian agents'[2] that continually monitor agents to spot any suspicious behavior and report incidents.

Building trust in AI through responsible governance

Understandably, given their significant investment in AI, organizations want employees to use this technology safely and routinely. This can only happen if there is faith that the model has been trained on trustworthy data — and that the training process and the data is visible. In a recent global study of almost 50,000 people from 47 countries, carried out by KPMG and the University of Melbourne, over half (54 percent) say they are wary about trusting AI.

CISOs have a key role to play in helping communicate the AI value proposition, but also the risks of regulatory penalties. In the worst case, organizations might have to shut down an agent process or even an entire AI system if it proves untrustworthy, or if it does not match regulatory expectations. With responsibility for continuity and disaster recovery planning, CISOs are critical to avoiding business interruption, and maintaining trust in systems. To communicate the importance of AI security to the board, CISOs need to speak the language of risk, by showing the business impact of breaches or model bias, and positioning security as an essential business enabler that drives operational continuity and resilience.

> "AI streamlines security operations by analyzing data, detecting attacks we might overlook, and assisting SOC teams around the clock. It can reason over data and pull apart and piece it together to see the full picture, such as an attack that we missed. So, we have a trusty helper that's sitting there in the SOC running 24/7 — often autonomously — freeing human operators to focus on thorough investigations and mitigation."
>
> **Saira Mohammed**
> Chief Security Advisor
> Microsoft

[1] The Open Web Application Security Project (OWASP), *OWASP Agent Observability Standard*, 2025.

[2] Gartner, "CIOs, *Leverage Guardian Agents for Trustworthy and Secure AI", webinar*, May 19, 2025.

Consideration 3

An AI governance committee, led by the CISO, and composed of executives from data security, technology, risk, legal, and privacy, can establish a framework and principles for adopting AI. KPMG's Trusted AI Framework provides an integrated approach to the responsible and ethical design, development, procurement and use of AI technologies. The priorities are protecting data and AI architecture and infrastructure, with recurrent and automated testing — especially red-teaming. Along with security operations (SecOps), these actions help to integrate security and IT operations teams to foster collaboration, detect threats and speed up response. Human oversight is a central feature of safe AI usage to question model outcomes and recommendations, improve data accuracy, and allow intervention.

Essential steps toward AI governance

- Embed security resources in initial agent deployments to learn processes.
- Use tools to detect and inventory agents (API-first capabilities).
- Implement runtime observability: instrumentable (to control actions), traceable (to log actions), and inspectable (to identify tools/models used).

Blending technology and people

Across the technology sector, start-ups are emerging, focused on guardrails to protect AI systems, by automating red-teaming, and redacting sensitive information. And, with major security vendors acquiring these start-ups, CISOs have an opportunity to integrate advanced AI security into existing technology stacks.

Acquiring the skills to manage AI security is quite a challenge. It is rare to find highly specialized security engineers, with a data science background, who are experts in threat-modeling AI systems and agentic workflows.

In addition to recruitment, some organizations are partnering with universities to train their current staff on specific AI techniques for cyber. Those employees with experience in threat modeling and security-by-design are the obvious targets for upskilling. Some organizations may choose to have a dedicated role for safeguarding AI, while others may ask security team members to interact with OWASP or information sharing networks, to better understand emerging risks. Others again could task AI security to a third party as a managed service.

Recruitment, training, and strategic partnerships are only the starting point. The real competitive edge comes from empowering people to secure AI at the speed of innovation.

Technological evolution is nothing new, but what makes this moment so unique is the speed of change, which gives organizations little option but to adopt AI at pace. As threat actors are enabled by AI, security teams are under pressure to innovate, using AI to detect threats earlier, manage permissions and access, and practice strict governance over the use of AI agents. By giving people the skills and understanding to work with AI, CISOs can strengthen trust in AI and data.

> "If I'm a security engineer, I need to be really thinking about how I embed agentic approaches into every workflow that I built on top of tools inside of the organization. And not only how do I build those agentic functions, but how do I test and validate efficacy, and perform additional training of models to make things work?"
>
> **Chris Corde**
> Head of Product, Security Operations
> Google

Consideration 3

Suggested actions

- Establish a cross-departmental governance committee to oversee AI adoption and set policies and controls.
- Keep humans in the loop, using AI to augment — not replace — people, especially in high-risk or critical areas, with strong oversight of models and outcomes.
- Embed security by design across AI system development, integrating security early into agent deployment and workflows.
- Continuously monitor AI systems, including red-teaming exercises.
- Strengthen third party risk management, prioritizing higher risk, lower-maturity suppliers.

Consideration 4

Managing non-human identities in the age of AI

> “Tomorrow’s identity and access management must evolve beyond static controls into an intelligent, adaptive ecosystem — where real-time decisions and automated policy orchestration appropriately govern and manage the scale of both human and non-human identities.”

Juan Manuel Zarzuelo Diaz
Global Digital Identity Leader
KPMG Spain

Consideration 4

Non-human identities — such as service accounts, workloads, and AI agents — are proliferating to the point where they already outnumber human users.[3] It is becoming increasingly difficult to spot these identities, which are dispersed across OT, on-premise, cloud and hybrid environments in the shadow-AI space, often with excessive permissions. Some may even have been created by other non-human identities. Classic 'static' identity and access management (IAM) alone cannot ensure security, and organizations instead need AI-led governance and controls able to adapt to ephemeral, dynamic and autonomous systems.

59% **of companies experienced a data breach caused by one of their third parties in the past 12 months**

Source: SailPoint Non-employee identity security lifecycle management.

What is going on under your nose?

For CISOs, identity is no longer just about humans. Unlike traditional machine identities, AI agents have extensive and changing privileges, allowing them to perform complex tasks and make decisions based on context and prompts. In contrast to scripts or robotic process automation (RPA), AI agents do not follow predictable patterns. They operate like humans to initiate access, create and use code, and create new virtual technology infrastructure — 24/7. Some agents can even create other agents for specific tasks, then delete them quickly — leaving little or no trace.

Given their transient and autonomous nature, how can CISOs trace these identities and audit their behavior, to gain greater confidence over their use, and ensure they work in the best interests of organizations and their employees, customers and other stakeholders? Traditional IAM controls aim to establish policies to ensure the right people have the right level of access to the right resources at the right time, with authorization based on verified identity, backed up by regular tracking to spot potential violations. But in many cases, organizations do not have a clear inventory of non-human agents, and cannot easily distinguish between human identities, machine identities, and AI agents. Humans are simply unable to keep up with the speed at which non-human identities are created, operate and erased — each with a unique identity and each one performing vital work.

KPMG's article, Invisible access, visible risk, notes that compromised non-human identities already feature prominently in major breaches, with issues amplified by agentic AI systems acting autonomously at machine speed — creating, modifying, and using credentials without human intervention.

61% **of US companies are not yet comfortable with autonomous agents and will require human-in-the-loop oversight**

Source: KPMG AI Quarterly Pulse, Survey: Q3 2025

Getting a handle on non-human identities

Identity is now the common fabric of security across SaaS, infrastructure and platform-as-a-service. The first step towards gaining control is to discover where agents exist and what they are doing.

By establishing a central identity store, CISOs and their teams can tag and track AI agents, so that they are recognized and managed within an identity provider and recorded in a continuously updated inventory. The scale of automated AI means that traditional, manual approvals cannot keep up, especially as agents are non-deterministic, and could complete the same activity in different ways, with different executions — requiring different permission. Organizations should implement policy-based access controls. These runtime controls enable real-time monitoring and can prevent unauthorized activities (such as using inappropriate or inaccurate data) by limiting agent privileges and/or shutting them down. Controls should also speed up threat detection and shut down an identity immediately if they notice suspicious activity. Pressing a 'kill switch' means turning off an individual agent, not a group of agents.

Controls should be based on zero trust principles (that assume no identity — human or non-human — can be trusted) across identity, network, and device layers. Other features of controls include adaptive access, just-in-time permissions, least privilege access, and continuous monitoring of data flows, to detect unauthorized source code uploads. Hyperscalers are investing in zero trust capabilities and gathering information on how different clients are using their platforms and how frequently They are asking for permissions. This support is giving CISOs valuable insights that help to enforce their policies.

Agents behave like workloads composed of APIs and tokens in the cloud, necessitating the use of existing cloud-native mechanisms for whitelisting (only permitting approved and trusted users), filtering, and enforcing policies. CISOs face a tricky balance between getting the benefits of AI and keeping the organization secure. Open-source frameworks and standards (e.g., SPIFFE, SPIRE, OAuth for delegation) are set to play a key role in enabling secure agent operations.

[3] CyberArk, "Machine Identities Outnumber Humans by More Than 80 to 1," press release, April 23, 2025.

Consideration 4

> Future IAM will likely integrate runtime enforcement, dynamic policy orchestration, and identity fabrics that aggregate data across multiple platforms.

Hemal Shah
Principal, Advisory, Cyber Security Services
KPMG US

Effective management of non-human identities increasingly relies on the secure issuance, rotation, and retirement of digital certificates, whether X.509 or JWT. These credentials underpin the authentication and trust models of ephemeral workloads, APIs, and machine-to-machine interactions. As organizations adopt highly dynamic architectures such as microservices, serverless, and container orchestration platforms, the volume and velocity of short-lived identities surge dramatically. This shift makes robust Certificate Lifecycle Management (CLM) not only a security imperative, but also an operational necessity. CLM helps automated systems maintain continuous trust, while minimizing exposure to compromised or expired credentials.

Strengthening identity governance

To meet auditor demands for information, identity governance should include automated responses to accelerate processes. These use real-time logs, SIM (subscriber identity module)/SOAR (security orchestration, automation, and response) data, and behavioral analytics, enabling managers to make informed access decisions for non-human identities. AI can accelerate the automation of labor-intensive processes such as application onboarding, entitlement reviews, and certification campaigns — the latter is a critical part of any audit, to confirm who can access what.

Despite the importance of automation, human oversight remains critical for policy definition, risk prioritization, and governance frameworks. AI should augment, not replace, strategic decision-making. Identity security platforms are adopting AI to protect human and machine identities across hybrid and multi-cloud environments. They can feed identity analysis into a centralized dashboard that shows where risk lies across the organization, from both an audit and security perspective.

Beyond these capabilities, organizations are now adopting Identity Threat Detection and Response (ITDR) to proactively identify anomalous behaviors and contain identity-centric attacks before they escalate. Complementing ITDR, Identity Security Posture Management (ISPM) continuously evaluates configuration drift, control gaps, and policy misalignments across identity systems, helping security teams maintain consistent compliance baselines. At a more strategic level, platforms incorporating Identity Visibility and Intelligence Platforms (IVIP), unify telemetry from Identity Governance Automation (IGA), Access Management (AM), Privileged Access Management (PAM), and cloud identity infrastructures to generate centralized, AI-driven insight.

Humans are at the center of security culture

When building a broader security culture, it is important to demonstrate how the organization protects human identities, so that people appreciate the risks of unauthorized access/impersonation, and the importance of strong controls. From here, it is a logical step to assessing the behavior of machine identities or agents. By developing a top-down model for AI adoption patterns, CISOs can prioritize identity risk based on privilege and impact. The top concerns are high-risk AI agents with broad permissions, and machine identities tied to critical infrastructure.

Security cannot be approached in a siloed manner, and CISOs should push for a broader, trusted AI capability framework that integrates comprehensive identity governance. This requires engaging the Chief Risk Officer, the Data Privacy Officer, the Chief Data Officer, and different parts of the organization including Legal. CISOs can also justify the need for AI security investments by quantifying potential risks and benefits, to secure funding and support from the board and executive leadership. There is a short window to embed security by design into AI/agentic AI, before scale makes it unmanageable. By designing everything from a security perspective, organizations can reap the benefits of AI while managing the risks.

> Non-human identities — workloads, devices, and AI agents — are growing at machine speed. We must apply the same discipline and principles we use for humans: strong authentication, clear authorization and enforced ownership. Killing an agent doesn't create accountability. Machine identity without human accountability is unmanaged risk.

Sitaram Iyer
Area VP Emerging Technologies
Palo Alto Networks

Consideration 4

Suggested actions

- Establish a central identity store, tagging and tracking AI agents to maintain visibility and control.
- Implement zero trust principles, using policy-based access controls, decentralized identity management, and continuous monitoring.
- Balance security and business needs by aligning security initiatives with business goals.
- Although AI increasingly drives identity governance, human oversight remains a priority to maintain strategic control.
- Strengthen collaboration across security, risk, privacy, legal, and business teams, with identity as part of a broader trusted AI framework.

Consideration 5

Enabling trusted IT/OT hyperconnectivity

> "The convergence is no longer just between IT and OT. A new pillar, AI, now demands adoption through well-governed capabilities: deep understanding of AI risks, thoughtful evaluation, and the design of a dynamic 'mesh' architecture with built-in safety and oversight. Only then can AI enhance operational reliability without compromising availability, safety, or continuity. Always keep in mind: OT zero trust, data sovereignty, localization and culture."

Hossain Alshedoki
Global Internet of Things and Operational Technology Security Lead
KPMG Saudi Arabia

Consideration 5

The merging of IT, operational technology (OT), smart connected systems, suppliers and customers is reshaping the cyber risk landscape. Digital twins, embedded internet of things (IoT) sensors — including robotics — and AI-powered environments are becoming commonplace, particularly in infrastructure-intensive sectors such as energy and industrial manufacturing. This interconnectedness introduces new vulnerabilities and expands the potential attack surface across physical and digital domains. The proliferation of IoT, for instance, creates opportunities for bad actors to steal data, compromise IT systems, infect devices with ransomware, and launch distributed denial of service (DDoS) attacks.

Organizations operating integrated IT/OT environments, including industrial and critical infrastructure, are striving to make security more effective and efficient, by streaming processes and extending capabilities from IT security to OT environments — and vice versa. They are keen to adopt advanced technologies — including AI — into their OT, but many architectures rely on rigid design principles, limiting CISO/CTO/COOs' ability to adopt advanced technologies.

The traditional Purdue Model[4] (along with other static models), which separates IT and OT, has applied to many industry frameworks. However, it is increasingly unsuited to modern industrial networks, as it lacks flexibility, real-time data analytics, and support for zero trust principles and interoperability. This can create blind spots that cyberattackers can exploit.

The consequences of a cyberattack on critical infrastructure can be devastating to the business, employees and wider society. Risks include physical harm, environmental damage, and major disruption to supply chains and essential services.

Regulators are understandably concerned about these risks and paying increasing attention to organizational resilience — resulting in an increased compliance burden. In a recent KPMG paper Critical Entities Resilience (CER) Directive, we discuss how this new EU regulation aims to strengthen the physical security and operational resilience of essential services across 11 key sectors, including energy, transport, health, and banking. Building on the NIS2 (Network Information and Security) Directive (which focuses on digital assets), the CER Directive covers risks from natural disasters, terrorist attacks, sabotage and insider threats — to name just a few. Organizations need to demonstrate strong cyber controls across their technology stack, including both IT and OT.

> "There is no perimeter anymore. Security has to move with the data, the identity and the intent. As these digital and physical systems merge, the ownership blurs and creates governance drift. Hyperconnectivity itself isn't the problem. Unmanaged convergence is."
>
> **Ben de Bont**
> Chief Information Security Officer
> ServiceNow

A shift to dynamic security architecture

Organizations operating in this space need to reshuffle static security architecture to a dynamic mesh, spanning IT and OT, rather than treating them as separate. In this architecture, zero trust principles (including least privilege access and multi-factor authentication) are distributed between IT and OT layers, enabling them to continuously adapt to shifting threat intelligence. These networks allow devices to defend themselves through point-to-point trusted communication. Along with an asset inventory, this increases visibility over all assets in OT environments — particularly important for sectors with legacy technology dispersed across multiple sites and geographies. By driving ongoing discovery and monitoring, they raise protection levels to identify and mitigate potential vulnerabilities in real-time. These architectures also help integrate new technologies with existing systems.

Any major systems change — including integrating new and legacy systems — can raise the vulnerability to cyberattack, which could result in a serious incident. Consequently, the transition towards mesh architecture should aim to enhance security controls and comply with regulations, without hindering network flow. Secure change management is essential when integrating new and existing systems, including adaptive controls like segmentation and monitoring.

Blending IT/OT teams into an integrated SOC can improve the monitoring of both environments. This is in line with a recent paper by the U.S. Cybersecurity and Infrastructure Security Agency (CISA),[5] which calls for greater IT/OT collaboration to address security concerns. However, the publication also highlights the importance of OT-specific policies and procedures.

[4] The Purdue Model provides a common language and structure for integrating business and manufacturing systems by organizing systems into different levels with clear boundaries, responsibilities and interfaces. | Claroty, ICS Security: The Purdue Model, March 2, 2023.

[5] Cybersecurity & Infrastructure Security Agency, *Cross-Sector Cybersecurity Performance Goals Version 2.0*, U.S. Cybersecurity and Infrastructure Security Agency, December 2025.

Consideration 5

Earning trust in security in the AI age

Within asset-intensive organizations, machine learning is starting to take off, using autonomous robotics to enhance threat detection. AI usage, however, is in its relative infancy, more commonly deployed for predictive maintenance — with growing use in detecting anomalies, load balancing, and quality control.

But AI has real potential, as it can operate 24/7, automate routine tasks, learn quickly, identify trends, and even, with agentic AI, make independent decisions and address threats. Manufacturing is setting the pace for AI adoption, while leaders in hazardous industries retain a degree of caution — especially over the introduction of autonomous AI.

Recent guidance from national cybersecurity agencies[6] warns that the integration of AI into OT environments introduces significant risks, including OT process models drifting over time, safety-process bypasses, and new attack surfaces. As a result, AI "should almost certainly not be used to make safety decisions for OT environments" due to concerns about reliability, plus the possibility of plausible but false responses.

To reduce AI risks, CISOs should identify OT data that trains AI models, and ensure that OT vendors use AI and data safely, applying robust data usage policies.

> "IT/OT hyperconnectivity towards zero trust architecture and full asset visibility can be done, but it needs buy-in from the leadership and clear communications to stakeholders about the benefits. OT engineers will discover that, far from taking their jobs, autonomous AI will make them more efficient and create a pioneering culture."
>
> **Ronald Heil**
> Global Cyber Security Leader for Energy and Natural Resources
> KPMG Netherlands

Collaborating to accelerate cybersecurity

Digitalization, AI innovation and geopolitical pressures are driving the need for a more collaborative approach to security, involving the CISO, CTO/COO, the business, engineering teams, and the broader network of stakeholders such as original equipment manufacturers (OEMs), governments and regulators. OEMs can provide valuable insights and innovative approaches to integrating new technologies, prioritizing security from the design phase through deployment and into operation — encompassing the full life cycle. Third-party validation of cybersecurity controls provides further assurance, emphasizing the value of monitoring and testing.

Together they can forge processes and regulations based upon trust in AI and robotics to detect cyber threats. Ownership cannot sit solely with the CISO; successful transformations require top-down sponsorship from the Chief Executive Officer (CEO) or Chief Operating Officer (COO), to achieve full commitment. CISOs need a seat at the table to ensure that cybersecurity is baked into transformations across a network of plants, factories and other assets. In one major company's IT/OT transformation program, the CISO gained influence by sitting on an advisory board that included the CISO, engineering chiefs, plant presidents, and 400 stakeholders. Ultimately, as with any major change program, stable boards and long-term vision should increase the likelihood of success.

> "Every sensor, building control, and logistics platform now feeds into shared cloud and AI systems. So, the next leap is really from isolated telemetry to correlated intelligence, using AI to connect weak signals across IT and OT that we can't see as humans."
>
> **Ben de Bont**
> Chief Information Security Officer
> ServiceNow

[6] Cybersecurity & Infrastructure Security Agency, *Principles for the Secure Integration of Artificial Intelligence in Operational Technology*, December 3, 2025.

Consideration 5

Suggested actions

Collaborate with OEMs to redesign architectures and integrate security, while managing performance and keeping abreast of regulatory change, to avoid any drag on progress.

Focus on cyber and operational resilience to meet regulatory expectations and protect the organization and wider society.

Engage leadership early by securing top-down sponsorship, offering CISOs support and investment across the business.

Drive cross-domain intelligence by correlating telemetry for IT and OT to enable predictive defense and operational insight.

Align IT/OT security initiatives with business goals to ensure that they support, rather than hinder, organizational objectives.

Consideration 6

Transitioning to post-quantum cryptography

> “Changing encryption is like suddenly speaking a new language. If your business partners don’t change with you, communication stops. Secure communication is essential for business, and this transition will be critical. There is time enough, but there is no time to waste.”

Michael Egan
Director, Quantum Technologies
KPMG Australia

Consideration 6

Quantum computing is on the brink of transforming industries, potentially solving complex problems exponentially faster than today's classical computers. Yet, this revolution poses an unprecedented cybersecurity risk. Quantum computers, once fully matured, will render current encryption algorithms[7] obsolete, compromising sensitive business, financial, healthcare, and national security data.

Public key encryption is the backbone of modern cybersecurity, ensuring the confidentiality, integrity, and authenticity of data. Without it, critical operations would come to a standstill. Organizations also face growing threats from 'harvest now, decrypt later' (HNDL) attacks, in which threat actors collect encrypted data today with the intent to decrypt it once quantum computing capabilities mature.

For CIOs, CISOs, CROs, CEOs, and board members, preparing for post quantum cryptography is a non-negotiable responsibility. Beyond cybersecurity, delayed migration risks include business disruption, financial loss, regulatory penalties, and reputational damage. Despite this, many organizations already recognize that they are behind the curve and this gap between awareness and readiness highlights why PQC must move from a future consideration to an active transformation program. To help steer this crucial transition, organizations should appoint clear responsibility for this transition so that CIOs and CISOs can proactively assess risks, develop transition strategies, and join the global race toward quantum resilience.

41%

of organizations say they are concerned they are falling behind in preparing for quantum-driven security threats and the transition to post-quantum cryptography

Source: KPMG Global tech report 2026

Regulatory landscape — driving forces behind PQC adaptation

Existing and forthcoming regulations are driving the PQC transition. The US Quantum Computing Cybersecurity Preparedness Act is a framework mandating government agencies to mitigate looming quantum threats. According to the Office of Management and Budget's (OMB) 2025 report, the projected cost for federal PQC migration between 2025 and 2035 is US$7.1 billion[8] — and that is only for prioritized systems, representing a significant cost for almost all organizations.

Internationally, the G7 Cyber Expert Group has urged financial institutions to adopt PQC, highlighting the critical risks of cross-border financial transactions exposed to quantum vulnerabilities. The group proposes harmonized adoption across borders to address substantial impacts on global financial frameworks — and have outlined a transition roadmap.

In Europe, the European Commission (EC) released a PQC transition roadmap in June 2025, with notable legislation including the EU Cyber Resilience Act, NIS (Network and Information Security) 2 Directive, Digital Operational Resilience Act (DORA), and GDPR (General Data Protection Regulation) compliance frameworks.

These initiatives already require organizations to implement security measures appropriate to the level of risk, considering the state of the art, implementation cost, and the sensitivity of the data involved. With the publication of FIPS (Federal Information Processing Standard) 203, 204 and 205, the definition of the state of the art has shifted, increasing expectations for quantum-safe readiness. Some entities must already meet the PCI DSS (Payment Card Industry Data Security Standard) V4 requirement for cryptographic bill of materials, with a need to inventory and manage cryptographic systems. The Australian Signals Directorate (ASD) has revised its guidelines, including newly approved cryptographic algorithms,[9] to reflect NIST's recent PQC standards, with a target date of 2030 for this transition.

These developments illustrate an expanding international consensus on the need to transition to PQC, as governments and businesses aim to secure data for the next decade and beyond.

Timing the post-quantum transition

PQC implementation will span multiple years, requiring strategic planning and sustained collaboration across industries. As outlined by NIST's PQC Standardization Project,[10] milestones for deploying standardized algorithms will extend into the coming decade.

[7] Examples of current encryption algorithms include RSA (Rivest–Shamir–Adleman) and ECC (elliptic-curve cryptography).
[8] Executive Office of the President of the United States, *Report on post-quantum cryptography*, July 2024.
[9] ML-KEM (Module-Lattice-Based Key-Encapsulation Mechanism) (FIPS 203) and ML-DSA Module-Lattice-Based Digital Signature Algorithm (FIPS 204).
[10] National Institute of Standards and Technology, What is Post-Quantum Cryptography?, February 27, 2026.

Consideration 6

The FS-ISAC (Financial Services Information Sharing and Analysis Center) guidance for financial institutions also reflects the tight timelines for PQC integration, as the industry strives to protect cross-border financial systems. Likewise, the G7 roadmap for the financial sector increases the pressure for a coordinated transition.

Transitioning PQC across an organization's IT estate is a multi-year commitment demanding significant stakeholder buy-in, especially to manage older hardware that cannot accommodate PQC's longer key lengths. Delays risk not only compliance breaches but also operational obsolescence if critical systems fail to support emerging cryptographic requirements.

Failure to meet key milestones could expose organizations to many vulnerabilities, hindering everything from customer transactions to communications, national security and critical infrastructure.

Third party and procurement challenges

Transitioning to quantum-safe cryptography means overhauling procurement practices to avoid introducing systems or hardware incapable of transitioning to PQC. This includes requiring third-party vendors to adopt stringent quantum-safe standards.

The TNO[11] PQC transition handbook highlights multiple challenges facing organizations:

- Third-party vulnerabilities: Many vendors are behind on PQC adoption, particularly in managing encrypted data stored on legacy systems.
- Procurement planning: Adjusting procurement security requirements promptly is essential to align with quantum-safe standards and mitigate risks from unprepared vendors.

Organizations should urgently create comprehensive plans to identify and assess suppliers' cryptographic capabilities. Prompt collaboration and consistent communications with vendors can reduce disruption, especially where supply chains rely on timely encrypted data exchanges.

Financial sector implications

The financial sector is among the most exposed to quantum vulnerabilities[12] due to its reliance on encryption for secure transactions, customer data protection, and cross-border financial stability. Delays in adopting PQC could erode customer trust, breach fiduciary duties, and disrupt global financial networks.

In an article in the *Australian Financial Review* (AFR),[13] Michelle Bullock, Governor of the Reserve Bank of Australia (RBA), calls for proactive collaboration throughout the financial sector. Leading companies are actioning quantum-safe projects to reduce risks, setting examples for others to proactively address their technological roadmaps.

Defense sector considerations: National security at risk

PQC migration is an existential risk for the defense industry. A lack of preparedness could threaten classified communications, command-and-control systems, and emerging defense technologies, leaving national and global defense ecosystems vulnerable. High-profile cyberattacks show how business operations can be paralyzed by offline digital systems.

Time is running out to secure the future

The transition to PQC represents one of the most significant cybersecurity challenges, necessitating proactive, global alignment driven by regulators and industry leaders. It is not just a technical issue, but a fundamental business priority that demands early action and sustained leadership attention.

CIOs, CISOs, and boards should seize the opportunity to address quantum risks now, safeguarding their organizations from operational vulnerabilities and long-term financial losses. As the UK National Cybersecurity Centre states: "Migration will happen, globally. It will not be possible to avoid PQC migration, so preparing and planning now will mean you can migrate securely and in an orderly fashion."[14]

The key is to start today. Assess risks, engage in education, and forge partnerships for a quantum-safe future.

> "To secure budget and resources, and build traction for the roadmap, CISOs should find allies in leadership from risk, regulation and internal audit. This can help broaden the perception of PQC from an IT and data issue, to a strategically critical capability."
>
> **Alexander Rau**
> Partner, Cybersecurity
> KPMG Canada

[11] TNO is a Dutch organization focused on applied scientific research.
[12] US Government, Department of War, "Preparing for Migration to Post Quantum Cryptography", November 20, 2025.
[13] Eyers, James, "Bullock warns banks of 'scary' quantum computing security threat," Australian Financial Review, October 24, 2025.
[14] Timelines for migration to post-quantum cryptography, *UK National Cybersecurity Centre*, 20 March 2025.

Consideration 6

Suggested actions

Conduct quantum risk assessments to define the scale of exposure and build a clear business case for transition.

Build cryptographic inventories to map and understand critical dependencies, emphasizing cryptographic agility and continuous monitoring throughout the transition.

Update procurement standards, supporting vendor compliance with early engagement. Implement procurement rules to manage third party security risk during the multi-year transition.

Upskill teams and launch educational campaigns across your stakeholder group to equip teams with necessary skills across the organization and enable a common understanding of the challenge and the impact.

Partner with experts, leveraging frameworks for structured risk assessments and detailed planning. Planning will be key to managing operational implementation risk and budget.

Consideration 7

Protecting the supply chain through detection and response

> “Supply chain detection and response improves communication and trust between suppliers and the first party, enabling data sharing. By driving positive action, it can bridge the gap between simply identifying cybersecurity problems and actually solving them.”

Raj Ahuja
Managing Director, Cyber Managed Services
KPMG US

Consideration 7

Today's supply chains depend on cloud platforms, SaaS providers, and hundreds — or even thousands — of third, fourth and fifth parties, including distributors, business partners, and retailers. Attack surfaces that historically spanned vast numbers of IoT devices have now been extended to include AI. Organizations are under threat from criminals, malicious hackers and nation state threat actors eager to steal intellectual property and disrupt operations. According to the KPMG Global tech report 2026, security, intellectual property, and data protection concerns are now among the top five barriers to collaboration across partner and supply chain ecosystems.

Supply chain resilience is the number one factor driving companies' short-term decisions.

Source: KPMG 2025 CEO Outlook

Traditional, often manual, third party risk management (TPRM) is no longer able to keep pace with the frequency and severity of cyber threats, exacerbated by AI bots and deepfakes. The focus is primarily on third-party vendors providing services directly to an organization, characterized by point-in-time assessments, resulting in blind spots and a focus on more traditional, paper-based reviews. Such an approach fails to give full, real-time supply chain visibility, allowing suspicious activity to sneak under the radar.

Security professionals may be unable to view suppliers' technology stack, which increasingly includes AI systems and applications, raising attack opportunities. Consequently, organizations may be less secure, necessitating a shift to integrating TPRM into first-party threat monitoring workflows. The onerous nature of TPRM compliance can also lead to assessment fatigue encouraging suppliers to focus on box-ticking rather than addressing real risk, leaving gaps for bad actors to exploit. Even during a real incident, static questionnaires provide little in the way of actionable intelligence.

Increasing regulatory complexity

Supply chain and TPRM threats have increased regulatory pressure across the globe, with legislation emphasizing organizational resilience and protection of critical infrastructure. Examples include SOCI (Security of Critical Infrastructure Act), NIS2 (Network and Information Security Directive), and DORA (Digital Operational Resilience Act).[15] This is particularly relevant to manufacturing supply chains, given the digitalization of OT. Data protection is a further concern for industries like healthcare, that carry large amounts of personal information. The entire supply chain must also meet data sovereignty regulations, requiring them to store certain data within national boundaries. The 2026 KPMG Global Third-Party Risk Management Survey highlights that regulatory and compliance risk has grown in importance for 45 percent of organizations, underscoring the intensifying regulatory scrutiny on supply chain cybersecurity.

In the face of tariffs, conflicts, and shifting geopolitical coalitions, organizations should scrutinize the supply chain, to avoid affiliation with companies in sanctioned or 'unfriendly' geographies. As geopolitical tensions increase, some organizations are shortening supply chains, bringing them closer to home — which introduces new parties in need of due diligence. All these factors raise the compliance burden. Reflecting this shift, according to the KPMG Global tech report 2026, 36 percent of organizations say they are planning to strengthen data sovereignty audits across partner networks. The second consideration in this paper on geopolitics, compliance and resilience, discusses this in greater detail.

45%

of organizations say that regulatory and compliance risk has grown in importance

Source: 2026 KPMG Global Third-Party Risk Management Survey

[15] Critical Infrastructure Security Centre, *Security of Critical Infrastructure Act 2018 (SOCI)*, August 27, 2024. | European Commission, *NIS2 Directive: securing network and information systems*, January 20, 2026. | European Insurance and Occupational Pensions Authority, *Digital Operational Resilience Act (DORA)*, December 15, 2025.

Consideration 7

Integrating risks across the third-party ecosystem

Supply chain detection and response (SCDR), by contrast, shifts the focus from vendor compliance to resilience. It identifies, prioritizes, and addresses vulnerabilities across the entire supplier ecosystem to prevent supply chain cyberattacks and reduce concentration risk in instances where critical providers suffer outages or security failures. It encompasses every player in the supply chain, with data-driven, continuous monitoring powered by AI and automation.

Zero trust principles — particularly in OT environments — help reduce the risk of unauthorized access. Designing systems on zero trust principles helps organizations reduce the third party risk surface area and is foundational to effective TPRM.

Ultimately, SCDR is proactive, to identify and mitigate vulnerability exposure before a cyberattack occurs.

Cyber threat intelligence should be integrated into a wider TPRM program, involving continuous monitoring, enabling organizations to better understand their risk exposure from the third-party ecosystem. By plugging in AI layers, CISOs can scale up their activities to cover multiple third-party relationships in a way that humans could not possibly manage. We are starting to see AI agents help determine third party risk profiles, synthesize third-party information, and triage potential threats — highlighting those that may require further attention. Looking forward, 39 percent to 47 percent of organizations surveyed in KPMG's study expect to integrate moderate AI use into core TPRM tasks over the next three years, signalling a clear move towards leveraging AI for enhanced threat intelligence.

By taking a risk-based approach to SCDR, organizations can apply more rigorous, automated, continuous monitoring of higher-risk partners — especially those with lower cyber maturity — which enables greater visibility. This includes monitoring for leaked credentials on the dark web, as well as for other indicators, suggesting a trusted vendor may have been compromised.

Collaborating with third parties to build resilience

Organizations can work more closely with suppliers to improve defenses and reinforce shared accountability for cybersecurity. Alternatively, they can take a risk-based approach, adopting a mentality that 'compliance alone doesn't equal security'. As ServiceNow's Ben de Bont says, "It can drive operational action and not just rubber-stamped awareness."

Contracts should detail expected levels of cybersecurity (including protection against quantum cryptography), with an obligation to communicate breaches, and a response plan in the event of security incidents, to shut down compromised assets and systems. Traditional TPRM can result in extensive assessments, which is time-consuming. SCDR, on the other hand, involves monitoring of fewer, higher-risk areas of the supplier network, using AI and automation to speed up the process and reduce errors. When a vulnerability is found, organizations can help third parties to neutralize the threat. Internally, the TPRM team should build closer relationships with the managed detection and response (MDR) team that's responsible for 24/7 monitoring — forging a stronger, risk-aware culture. Breaches affect the entire organization and sharing responsibility can help reduce threat, preserve reputation and satisfy regulatory demands.

> "With cloud-based AI in the ascendancy, organizations may struggle to view where and how AI is being used. To gain greater visibility, organizations should try to create a comprehensive AI bill of materials across their supply chain."
>
> **Srijit Menon**
> National Head for TPRM in India
> KPMG India

> "The biggest blind spot is time, with most organizations still relying on annual audits or static questionnaires which are outdated before they're even finished. Continuous monitoring should integrate live vendor telemetry and automated scoring, driving real-time signals instead of once-a-year certification. Security has got to be continuous, it's got to be automated, and it's got to be measurable — and I think AI can greatly help us with that."
>
> **Ben de Bont**
> Chief Information Security Officer
> ServiceNow

Consideration 7

Suggested actions

- Extend third party risk management beyond traditional vendors to include distributors, partners, and retailers, with a focus on operational resilience.
- Allocate resources based on risk profiles, prioritizing high-risk, low-maturity third parties that lack robust cybersecurity controls.
- Strengthen asset management resilience — particularly in OT — through business impact analysis and up-to-date continuity.
- Identify vendors with the highest risk exposure (such as helpdesk providers with internal access) and apply increased scrutiny and continuous monitoring.
- Ensure supplier contracts define risk-based compliance requirements, clear incident response plans, and controls for access management, monitoring, and privileged access.
- Foster a shared-responsibility culture with suppliers by involving them in resilience activities such as incident response, business continuity, and tabletop exercises.

Consideration 8

Broadening the role and influence of the CISO

> “Enlightened CISOs are starting to expand accountability from cyber to encompass the business. They’re articulating cyber issues to the board in a business context, helping them to understand the financial, reputational, and operational implications, rather than using compliance as the stick.”

Anna Poole
Cyber Security, Energy, Mining & Property Sector Lead
KPMG Australia

Consideration 8

The scope and responsibilities of the CISO continue to expand as security becomes more deeply integrated into business and operations, converging the cyber and physical domains. At the same time, CISOs must manage both the opportunities and threats associated with widescale AI adoption. But is this translating into influence at CIO, CTO, and, ultimately, board level? And how will these changes impact the way the cyber function operates?

CISOs often fall into two broad categories. The more traditional, operations-focused, technical type who prioritizes resilience, control effectiveness, and measurable cyber risk reduction. This role is essential, it builds and maintains the security foundation through rigorous metrics, engineering discipline, and consistent execution. While this approach may involve less routine engagement with the broader business — including the board — it ensures the organization's baseline protection and compliance are robust and reliable.

Increasingly, we are also seeing the emergence of forward-thinking CISOs, who align themselves with business strategy, and aim to embed cybersecurity into the broader enterprise. These CISOs are raising senior-level awareness of operational, financial, and reputational risks from cyber threats. They are expanding the perception of cybersecurity away from compliance, towards a strategic enabler for digital transformation, cloud and AI adoption, and new business initiatives.

As John Israel, Global Chief Information Security Officer at KPMG observes, "The CISO role is fundamentally evolving into that of a 'Chief Secure Transformation Officer'. We are no longer just securing the business; we are enabling it. Our primary goal is to embed security so seamlessly into the fabric of the organization — from business processes to technology adoption — that it accelerates innovation and velocity, rather than hindering it. This means moving beyond a purely technical or risk-advisory role to become true strategic partners with the board, the CIO, and the CTO, driving secure transformation to achieve key business objectives."

Balancing risk with regulation

Regulations on data privacy and security affect every part of an organization. Failure to comply — including reporting incidents — can result in fines and reputational damage. The regulatory focus is shifting toward resilience and availability — not just confidentiality and integrity — obliging organizations to show they can prevent and withstand cyberattacks while minimizing disruption to supply chains and operations. CISOs need to balance compliance with innovation to meet regulatory requirements without slowing the delivery of new products and services; compliance should be seen as the baseline, not the ceiling.

> "Giving the CISO greater influence signals that security is taken seriously, establishing a holistic view of enterprise risk, and raising the conversation to make cyber risk an intrinsic part of strategy — not just an afterthought."

Del Heppenstall
UK Cyber Lead
KPMG UK

Organizations also face increasingly diverging regulatory regimes across industries and geographies. Europe differs from the US, and regulatory requirements can vary even between states or regions. As the cost of compliance rises, CISOs must balance local regulatory obligations with the need for a cost efficient, globally coherent compliance model. Through tighter relationships with general counsel, especially regarding data privacy, CISOs can keep abreast of regulatory change, help their organizations protect and enhance their brands, avoid costly penalties, and most importantly, maintain resilience.

Toward a unified cyber risk leadership model

As the digital and physical worlds collide, CISOs' roles are extending to encompass IT, OT, the enterprise, and third parties, to shape organizational security. CISOs are also increasingly driving data management in concert with data security programs — especially unstructured data management. This involves bringing together functions that would normally operate under the CIO or CDO (Chief Digital Officer), managing a broader spectrum of risks. In some industries, CISOs are appointed to Chief Security Officer roles.

Some CISOs, and their teams, may not be fully equipped or empowered to handle the nuances of physical security or OT environments — not to mention AI and emerging compliance — calling for significant upskilling and/or structural changes. Ongoing training and awareness programs beyond the security team can help equip employees in the wider organization to handle security challenges. As an added challenge, IT and OT teams often operate in silos, which hinders the ability to coordinate security across these domains. CISOs should attempt to bridge the trust gap between functions.

To succeed in a converged IT/OT role, CISOs should work closely with the board to align security and business objectives, brokering relationships across functions such as operations, sales and marketing, procurement and human resources. They need to understand the threat landscape, and translate this into business language, to drive informed decisions.

The CEO and the board should add their support by strongly advocating that cybersecurity is everyone's responsibility with greater accountability at board level and throughout the organization. As part of this new culture, where security is democratized, employees should feel comfortable reporting concerns or incidents without fear of reprisal — crucial for early detection and response.

Consideration 8

Operationalizing AI

Generative AI (GenAI), and now agentic AI, represent an inflection point, a monumental tech shift on par with the introduction of the internet. The pace of AI development has compressed strategic planning horizons from 4-5 years to as little as 18 months, requiring earlier and more active CISO involvement to define the security of, with, and from AI systems. As organizations shift from compliance toward safe AI adoption, CISOs and their teams are integrating security into the front end of major AI-driven, CIO- and CTO-led programs. The key value-add is for CISOs to be in the room early, to articulate the importance of security within programs and products, and protect data to improve performance.

> “In the age of AI, data is the currency of a durable market advantage. While it represents one of the highest-velocity risks in the enterprise, it’s also the key to unlocking new revenue streams and competitive advantages. As CISOs, we must lead the conversation on data from a position of opportunity, not just danger. Our role is to build the secure framework that allows the organization to harness the full power of its data, turning a potential liability into its greatest asset.”

John Israel
Global Chief Information Security Officer
KPMG International

> “The trick to gaining influence with the CIO and CTO isn’t necessarily to be the police. It’s about enabling through security, to support velocity, efficiency and creativity.”

Gary Berletti
Deputy Global Chief Information Security Officer
KPMG International

AI also raises ethical and regulatory concerns over the avoidance of bias and compliance with data security and privacy requirements. CISOs are treading an ethical tightrope, trying to rein back unfettered, unfiltered use of AI, without being seen as a blocker to innovation. By establishing frameworks, continuous and automated testing, and AI red-teaming, CISOs can provide guardrails for trusted use of AI to drive the business forward.

As well as a challenge, AI offers an exciting learning opportunity for CISOs to stay current on the accelerating pace of innovation, and understand how AI can help at a strategic, market and operational level. By taking a lead on AI beyond cyber to strategy and operations, CISOs are expanding their roles and influence. By acting as Chief Secure Transformation Officers, CISOs should think more like private equity investors, aggressively divesting legacy, inefficient technology, and seeking capabilities that drive significant improvements and material efficiencies.

AI-powered cybersecurity

Within the cyber team, AI can save workers significant time and effort, enhancing productivity. AI automation techniques will dramatically speed up continuous monitoring and incident response, enabling security teams to scan for threats, collate data and prioritize targets. As discussed in consideration 4, agentic AI creates a challenge to identify agents, confirm their access rights, and track their behavior, to ensure they stay within agreed scope. There is an additional insider risk of employees attempting to use bespoke agents, with access to confidential data, outside of organizational boundaries.

> “AI hasn’t just created new opportunities — it has elevated the cyber function itself. As the attack surface expands, security becomes a business imperative. And because AI is powered by data, data security and governance — especially identity and access management — have taken on heightened importance and are at the center of trust.”

Saira Mohammed
Chief Security Advisor
Microsoft

Consideration 8

Suggested actions

Adopt an AI-first posture to stay ahead of adversaries through continuous monitoring, identity and access management, and heightened productivity.

Strengthen cyber resilience across the supply chain by using security telemetry to assess third-party risk and recover quickly from disruption.

Minimize disruption and pre-empt attacks through strong posture management across data, cloud and identity security.

Embrace ambiguity and make decisions with eighty percent certainty to maintain the pace of innovation.

Listen to the business to ensure cyber applies proportionate controls that enable, rather than hinder, progress.

Cyber strategies for 2026

What actions can CISOs and business leaders take in the year ahead to ensure security acts as a true enabler of enterprise objectives, as organizations unlock the value of AI and maintain trust? The following recommendations outline how CISOs can both protect and enable the business in an increasingly complex environment.

People

- Build a collaborative, holistic risk culture by working with the board, IT, and Risk Management.
- Partner with experts, leveraging frameworks like the KPMG Trusted AI and Quantum Care Framework for structured risk assessments and detailed planning.
- Keep humans in the loop, using AI to augment — not replace — people, with strong oversight of models and outcomes.
- Strengthen collaboration across security, risk, privacy, legal, and business teams, with identity as part of a broader trusted AI framework.
- Promote a supplier culture grounded in shared responsibility for cybersecurity, rather than compliance alone, creating value for all parties.

Process

- Implement zero trust principles using policy-based access controls, decentralized identity management, and continuous monitoring.
- Embed security by design across AI system development, supported by continuous monitoring and red-teaming exercises.
- Conduct quantum risk assessments to define the scale of impact and build the business case for transition.
- Extend third party risk management beyond traditional vendors to include distributors, partners, and retailers, with a focus on operational resilience.
- Focus on asset management resilience — particularly in OT — through business impact analysis and up to date continuity planning.

Technology

- Help define and implement the data, service and technical architecture, to adapt to changing conditions.
- Treat data as a survival mechanism by making classification, tagging and labeling foundational to data security.
- Establish a central identity store to tag and track AI agents, ensuring they are authenticated and operate within permitted boundaries.
- Introduce autonomous security architecture into the SOC, with continuous monitoring to triage security alerts, identify vulnerabilities and manage AI-driven threats.
- Build cryptographic inventories to map and understand critical dependencies, emphasizing cryptographic agility and continuous monitoring throughout the transition.

Regulations

- Focus on cyber and operational resilience to meet regulatory demands and protect the organization and society.
- Integrate geopolitical risks and emerging regulatory standards into CISO programs to improve foresight and decision-making.
- Ensure supplier contracts define risk-based compliance and clear incident response obligations.
- Collaborate with OEMs to redesign architectures and integrate security while managing performance and regulatory change.

How KPMG professionals can help

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

This support also extends into ongoing operations through KPMG Cyber Managed Services, a subscription-based, outcome-driven model that manages knowledge intensive business processes. By combining advanced technology with deep functional, process, and sector expertise, this approach helps you continuously evolve your business functions, strengthen cyber and operational capability, reduce cost, and limit disruption and risk.

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

Through the KPMG Velocity business transformation offering, we bring AI-enabled products and services together in one place to help you change smarter, and move faster — balancing speed, security, and value across the enterprise. Whether you are entering a new market, launching products and services, or interacting with customers in a new way, KPMG professionals can help you anticipate tomorrow and get an edge with secure and trusted technology.

Meet the authors

Laurent Gobbi
Global Cybersecurity and
Tech Risk Centre of Excellence Leader
KPMG International
lgobbi@kpmg.fr

Laurent is the Global Cybersecurity and Tech Risk Leader with over 30 years of experience in advisory services. He has been instrumental in shaping the technology practice in France, overseeing its growth from a team of 20 to over 600 professionals. Laurent has also held leadership roles in France's Risk Consulting and Management Consulting practices and was the EMEA Tech Risk Leader. He also launched the Global Trusted AI initiative in 2023. Laurent advises KPMG clients in various domains, such as Tech M&A, IT strategy, CIO Advisory Technology Risk (including Cyber and Privacy) and Internal Audit, Risk and Governance.

Jim Wilhelm
Global Cybersecurity
Investment Leader
KPMG International
jameswilhelm@kpmg.com

Jim is KPMG's Global Cyber Investment Leader and located in the Philadelphia office. He has more than 20 years of experience providing information security and identity and access management assistance to clients across a variety of industry verticals. During his time at KPMG, Jim has served as a member of the US Cyber and Tech Risk leadership team driving transformative cyber security solutions with clients in the financial services and healthcare sectors.

Dani Michaux
Cybersecurity Leader, EMA
Partner, KPMG Ireland
dani.michaux@kpmg.ie

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

Motoki Sawada
Cybersecurity Leader, ASPAC
Partner, KPMG Japan
motoki.sawada@jp.kpmg.com

Motoki is the ASPAC Cyber Leader with more than 25 years of experience in cybersecurity and IT. He has led the Cybersecurity Transformation practice in Japan, including Identity Management, Security Operation, Vulnerability Management, Microsoft security and OT security. With a strong background in both Cybersecurity and Risk Consulting, Motoki has extensive experience in assisting numerous clients across industries with developing their cybersecurity strategies and roadmaps, globally implementing cybersecurity solutions and recovering from cyber incidents.

Prasanna Govindankutty
Cybersecurity Leader, Americas
Partner, KPMG US
pkgovindankutty@kpmg.com

Prasanna is a principal in KPMG's Cybersecurity Services based in the US. He is the Americas Cyber leader with 20 years of specialized experience in cybersecurity and technology risk transformation. Previously, he led the Global and US Powered Cyber solution for KPMG. With a deep understanding of market leading technology solutions for cyber and governance, risk and compliance (GRC) functions, he helps clients with their integrated transformation. Prasanna leverages his extensive experience in technology-based transformation to help his clients in the energy, media and telecom sectors.

Acknowledgements

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

Our global cyber considerations team:
John Hodson
Billy Lawrence
Leonidas Lykos
Aman Manhas
Danielle Moriana
Peter Valentin

Our global contributors:

Raj Ahuja
KPMG US
rajeshahuja@kpmg.com

Hossain Alshedoki
KPMG Saudi Arabia
halshedoki@kpmg.com

Gary J Berletti
KPMG International
gberletti@kpmg.com

Chris Crevits
KPMG US
ccrevits@kpmg.com

Juan Manuel Zarzuelo Diaz
KPMG Spain
jzarzuelo@kpmg.es

Michael Egan
KPMG Australia
megan5@kpmg.com.au

Javier Aznar Garcia
KPMG Spain
jaznar@kpmg.es

Atul Gupta
KPMG India
atulgupta@kpmg.com

Ronald Heil
KPMG Netherlands
heil.ronald@kpmg.nl

Del Heppenstall
KPMG UK
del.heppenstall@kpmg.co.uk

Kristy Hornland
KPMG US
khornland@kpmg.com

John W Israel
KPMG International
johnisrael@kpmg.com

Charlie Jacco
KPMG International
cjacco@kpmg.com

Srijit Menon
KPMG India
srijitmenon@kpmg.com

Anna Poole
KPMG Australia
annapoole@kpmg.com.au

Alexander Rau
KPMG Canada
alexanderrau@kpmg.ca

Hemal P Shah
KPMG US
hpshah@kpmg.com

Marko Vogel
KPMG Germany
mvogel@kpmg.com

Our alliance collaborators:

Ben de Bont
CISO
ServiceNow

Chris Corde
Senior Director
Google Cloud Security Products
Google

Sitaram Iyer
Area VP
Emerging Technologies
Palo Alto Networks

Saira Mohammed
Chief Security Advisor
Microsoft

Learn about our services

Contact us

WALTER RISI
Consulting Lead Partner
KPMG Argentina
wrisi@kpmg.com.ar

NICOLÁS MANAVELLA
Cybersecurity Partner
KPMG Argentina
nmanavella@kpmg.com.ar

PABLO ALMADA
Cybersecurity Partner
KPMG Argentina
palmada@kpmg.com.ar