Cybersecurity considerations 2025

In an AI-dominated business environment, the foundational principles of cybersecurity are even more critical

KPMG International

kpmg.com/cyberconsiderations

Contents

© 2025 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Foreword

As 2025 takes form, the digital landscape continues to evolve at an unprecedented rate, bringing forth new challenges and amplifying the urgency for robust cybersecurity measures. Against this backdrop, the sixth global installment of the annual *Cybersecurity considerations* report aims to shed light on the current and upcoming obstacles facing organizations across various industries and highlight several strategic actions they might undertake, all of which are aligned with eight key cyber considerations that are thoroughly explored in this report.

At a time when technology is intertwined with every facet of our professional and personal lives, cybersecurity emerges not just as a business concern but as a broad issue that impacts all aspects of society. According to KPMG research, CEOs view cybersecurity as the top threat over the last decade.[1]

The incorporation of AI across virtually every industrial sector brings to light the critical issue of embedding trust within AI models and processes by establishing a thorough and robust governance program through which CISOs can understand the various business cases, determine where and how AI is already being used in the organization, and identify the related vulnerabilities.

The proliferation of smart products, from automobiles and medical instrumentation to home appliances and other Internet of Things-related devices, continues to expand the attack surface, aligning physical and digital threats in unprecedented ways. The advent of deepfakes and the resurgence of digital assets such as cryptocurrency — which remains largely unregulated and volatile — augment the complexity of these threats, necessitating vigilance and innovative countermeasures.

In this environment, CISOs are urged to focus on educating themselves and their teams about AI technologies, not only to assemble the best teams but to understand the unique risks each use case presents. As for talent acquisition and development, CISOs face the daunting task of assembling teams capable of comprehending AI's complexities and often subtle risks — a task complicated by the rapid innovation occurring in this space, as well as the difficult-to-govern pockets of "shadow AI" that are cropping up across the business.

While all this occurs, a rationalization or consolidation of cyber capabilities appears to be at hand with security teams moving from perhaps dozens of solutions in their security operations centers (SOC) to a leaner suite of best-of-breed tools to integrate solutions more effectively and economically and to better leverage new AI capabilities offered by the providers of these tools.

Today's cybersecurity hurdles transcend the realm of traditional technical skills, necessitating a multidisciplinary approach that also encompasses a deep understanding of risk management, as well as an array of soft skills, such as problem-solving, critical thinking and communication. Cybersecurity professionals can come from unconventional backgrounds and must be able to adapt quickly and acquire tangible knowledge beyond what is typically taught in the training for traditional degrees in computer science, software engineering or information technology.[2] It's imperative for cybersecurity professionals to prioritize situational risk assessment without losing sight of the need for explicit, yet flexible controls.

[1] KPMG 2024 Global CEO Outlook, August 2024.

[2] World Economic Forum, *Strategic Cybersecurity Talent Framework*, April 2024.

© 2025 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Cybersecurity is not a static function, but rather a dynamic and ever-evolving challenge. For example, the rise of quantum computing, through which attackers can circumvent encryption tools at an alarming speed, potentially compromising everything from banking and retail transactions to business data, documents, email and more; the potential for "superintelligent" AI systems, which perpetually improve and expand their knowledge while protecting themselves when sensing danger; and the velocity at which misinformation is spreading, especially through deepfake audio and video content, are just several of the emerging issues over which CISOs are losing sleep. These and other threats highlight the urgent need for innovation and strategic foresight.

Legislative landscapes are shifting toward more localized regulations, presenting a multifaceted challenge for global security operations. This, coupled with the economic imperative to justify security budgets not solely based on return on investment alone but also on the mitigation of risk, places CISOs in the precarious position of advocating for resources without the traditional financial assurances.

CISOs are similarly challenged by ascending geopolitical complexities. With rising state-sponsored attacks, the fluid regulatory environment and cross-border data flows, CISOs must navigate a vast array of intricacies to effectively safeguard their networks. Clearly, the pressure to stay ahead of emerging threats and ensure compliance is more daunting than ever.

The broad experience among today's CISOs — both those who have weathered significant incidents and those who may have only faced minor skirmishes — underscores the need for a nuanced appreciation of the ever-fluid threat landscape.

In this report, a wide cross-section of KPMG specialists delves deeper into these issues, providing comprehensive analysis of the current state of cybersecurity and offering actionable strategies for CISOs aligned to eight cybersecurity considerations. Our enduring goal is to equip leaders with the knowledge and tools necessary to navigate the complexities of the digital age, ensuring the security and resilience of their organizations in the face of a fascinating and exciting, yet often uncertain future.

Akhilesh Tuteja
Global Cybersecurity Leader
KPMG International

> "The technology landscape is evolving rapidly, with new threats emerging daily. To stay ahead, businesses must be proactive — not reactive — to safeguard their digital assets, ensure compliance, and foster an environment where innovation can thrive securely."

Bobby Soni
Global Technology Consulting Leader
KPMG International

© 2025 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Reflections on a five-year journey 2020–2025

Over the past five years of producing this report, an ever-evolving cybersecurity landscape has emerged as a tangible focal point for organizational leaders. Many key themes continue to resonate — resilience, identity access management (IAM), cloud security, talent and skills gap, to name a few.

However, the fundamental underpinning of this fascinating and pivotal subject has shifted from traditional security measures to the priorities and challenges of a global and multifaceted digital landscape, to which CISOs and their teams must respond in near real time. Above all, it's crucial to emphasize how pervasive cybersecurity has become, expanding beyond technology risks to encompasses broader business threats, affecting industries and society alike.

Digging a bit deeper:

- With the COVID-19 pandemic and the normalization of remote working arrangements, a focus on cloud and AI security have become key CISO objectives.
- Talent, and the always-looming skills gap, has long been critical given emerging technologies and the new and varied skills required.
- Identity has moved from traditional IAM, an important albeit separate function, to the heart of Zero Trust strategies and a means for identifying digital identities and deepfakes.
- Resilience has become an essential objective throughout and will remain so going forward.
- CISOs continuously strive to reinforce, particularly as cyber threats have transformed into far-reaching business threats, which hold the potential to disrupt industries and cause harm to society.

Looking at the trend analysis 2020-2025 exhibit on the next page, much of the basic security foundation examined remains central to the research conducted. But between new technologies, expanding regulations, more sophisticated tooling, and a mounting threat landscape, the role of the CISO is growing in scope and accountability.

© 2025 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Trend analysis 2020 – 2025

Key themes

	2020		2025
Strategy and leadership	• The CISO has become a trusted internal advisor and operational leader.	• Moving the conversation from cost and speed to strategic and effective security. • CISOs budgets increasingly tied to risk reduction for the business.	• As cyber becomes more pervasive across the organization, the pressure on the CISO to deliver increases. • The CISO role disperses but accountability increases partially due to regulatory developments.
People and talent	• Security teams are transforming into a key resource with a relevant voice at the strategy table.	• Cyber exists to support not hinder — from organizational enforcers to influencers. • Weaving cyber into the organizational fabric.	• The cyber skills gap persists — AI might offer some viable solutions, but the workforce needs new skills to adapt and adopt.
Technology and data	• New virtual infrastructure models and collaboration tooling. • Accelerated cloud transformation (due to COVID-19) but security was an afterthought. • Traditional identity authentication and management (IAM).	• Enhanced security through automation. • Rapid advancements in Gen AI create excitement around use cases in cyber. • Securing a perimeter-less and data-centric world. • Placing identity at the heart of zero trust.	• Investment in AI for cyber becomes more strategic and forward-looking. • Enterprise-wide cost-saving, efficiency, security and innovation (especially AI implementation) drive platform consolidation. • The rise of digital identities and deepfakes.
Digital trust	• Cyber and privacy regulations focus on business priorities and responsibilities — the importance of trust.	• Digital trust is a shared responsibility that starts with the business and involves multiple stakeholders, e.g. CISO, DPO, CDO, CIO, etc.	• Embedding trust as AI pierces all fabrics of business and society — focus on security, privacy, safety, ethics, etc.
Resilience	• From scenario-to impact-based — focus on critically and regulation.	• No longer just about prevention — focus on response and recovery.	• CISOs continue to build on resilience as cyber threats have evolved from tech risks to business and industry threats, with potential harm to society.

© 2025 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Eight key cybersecurity considerations for 2025

Click on each consideration to learn more.

01

The ever-evolving role of the CISO

What CISOs and their teams focus on, and how they interact with the rest of the organization is fluid, as the cybersecurity function becomes more broadly embedded within and better understood across the organization.

02

The power of the people

As organizations continue to transform their business models in the face of new digital disruptions, many are experiencing real challenges around workload, which is exacerbating the long-discussed cyber skills gap. AI and automation can help, but there is an underlying risk of talent attrition as many teams struggle to cope.

03

Embed trust as AI proliferates

AI is here to stay and has a place in virtually every organizational function, but there are a number of key cyber and privacy challenges that have the potential to affect the adoption and deployment of AI.

04

Harness AI for cyber: Racing ahead vs. racing safely

Many factors appear to be contributing to the buzz around AI adoption, from a lack of training to the fear of missing out and possibly falling behind. A key challenge is weighing the potential benefits of integrating AI into cyber and privacy functions against the potential risks.

05

Platform consolidation: Embrace the potential but recognize the risks

Increasingly, many global organizations are looking to reduce the complexity and cost of their technology. Organizations that choose to do so by consolidating tools and services onto a single or a limited number of platforms must identify and navigate the inherent risks.

06

The digital identity imperative

Although there are several initiatives around digital identity sprouting up worldwide, interoperability between systems and enhanced authentication due to the emergence of deepfakes remain a challenge, whether due to regulations, risk appetite and/or public opinion regarding the processing of personal and biometric data.

07

Smart security for smart ecosystems

The rise of smart devices and products worldwide is challenging and changing traditional views and approaches toward security, prompting many regulators to introduce new regimes to ensure these products meet basic security requirements.

08

Resilience by design: Cybersecurity for businesses and society

Resilience is becoming central to the CISO agenda as the prospect of attackers using ransomware or other malicious means to cause large-scale industrial disruption, risking both data and human lives, remains alarming.

© 2025 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Consideration 1

The ever-evolving role of the CISO

A combination of factors is reshaping cybersecurity and significantly transforming the role of the Chief Information Security Officer (CISO). Heightened regulatory scrutiny, the pressure to deliver virtually without failure, and increasing accountability and personal risks are all contributing to this momentum shift. At the same time, traditional CISO functions are gradually being dispersed across organizations, raising important questions about the future of the role and the evolution of the cybersecurity function. The success of CISOs will likely depend on their ability to effectively establish decision-making authority, manage the impact of emerging technologies, particularly AI, and adapt to new threats.

Rising expectations as operating models evolve

The role of the CISO is becoming increasingly complex. Regulatory scrutiny and the need to ensure strong cybersecurity outcomes across the entire organization are largely driving this. This complexity is further compounded by changes in the operating model and a growing reliance on external vendors. However, these controls may not always align with the unique needs of the organization, particularly in the case of global operations spanning multiple countries.

CISOs now face the challenge of managing and configuring vendor-provided controls to ensure they are fit for purpose and comply with local laws and regulations. This shift in the operating model means that CISOs have less direct control over the implementation of security measures. While the embedded cybersecurity and privacy controls offered by these vendors can be beneficial, they often lack the flexibility and granularity required by CISOs to effectively manage risk across diverse environments. CISOs must navigate this growing complexity while still enabling people to work efficiently and maintain visibility into the operation of controls across the organization.

> “When it comes to cloud-based software vendors, there is added complexity because typically they’re binary — they’re either on or off. Ideally, CISOs would like to see specific controls positioned as on or off based on circumstance or location — on for the US, but off for Germany, on for Singapore but off for Switzerland.”
>
> **Paul Spacey**
> Global Chief Information Security Officer
> KPMG International

© 2025 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Designing a blueprint for cybersecurity's organizational role and scope

The organizational structure surrounding the CISO role is evolving, with a growing trend toward splitting responsibilities with the Technology Information Security Officer (TISO) if there is one on staff. This division of roles enables the CISO to focus on risk management and broader cybersecurity strategies. The TISO typically is embedded in the organization's technology functions, overseeing the implementation of relevant controls and managing day-to-day operations.

Additionally, larger organizations may have multiple CISOs, each responsible for different lines of business, such as the supply chain network or commercial online presence. This segmentation of responsibilities recognizes that a single individual may struggle to maintain detailed knowledge across all areas while effectively managing the overall cybersecurity landscape.

As the cybersecurity domain continues to expand, CISOs are finding themselves with a broader scope of responsibility. They must serve as the source of truth for a wide range of aspects, including controls, performance, risks, intelligence, identity management and overall cyber hygiene. CISOs are tasked with presenting this information in a manner that is relevant and consumable for the business, enabling informed decision-making.

While CISOs may delegate many security priorities to other teams, such as reporting on key risk indicators, running risk assessments and performing penetration testing, they must still maintain oversight and awareness of these activities. The challenge for CISOs is to effectively manage this expanded scope while ensuring agility, efficiency, and situational awareness across the organization.

Walking the tightrope: Balancing accountability and authority in the face of growing risks

The increasing regulatory scrutiny and potential for personal liability have highlighted the need for clearly defined accountability and decision-making authority for CISOs. In the event of a cybersecurity incident, CISOs may find themselves exposed to legal and professional consequences, particularly in heavily regulated industries.

To mitigate this risk, organizations must establish formal governance processes that empower CISOs to take necessary actions during an incident without fear of repercussions. This includes providing CISOs with a clear understanding of their authority and the limits within which they can operate. With this, they can make critical decisions quickly and confidently.

The reporting line of the CISO also determines the ability to effectively manage cybersecurity risks. While having a direct line of communication with the C-suite, general counsel and the board is important, CISOs must also have the autonomy to make decisions based on their technical expertise.

In emergency situations, such as a supply chain breach, CISOs need the authority to take immediate action without waiting for approval from superiors who may not have the necessary technical understanding. However, this autonomy must be balanced with a clear set of accountability controls and guardrails, developed in collaboration with senior management. CISOs should be encouraged to pause at critical moments, consider the potential consequences, and assess the most effective course of action.

> "CISOs used to start off by trying to identify, protect and secure the organization's 'crown jewels' — key data, intellectual property, trade secrets, etc. But today, CISOs really need to focus on the security and resilience of the business."
>
> **Wendy Lim**
> Partner, Cyber, Advisory
> KPMG Singapore

© 2025 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Rewriting the CISO playbook for the future

As organizations increasingly adopt automation and AI technologies, the role of the CISO is set to undergo significant changes. The growing automation of security operations centers (SOCs) is expected to result in smaller teams and reduced focus on day-to-day operations. The cybersecurity remit is so vast that organizations have to split responsibilities. CISOs will struggle to effectively oversee a tech delivery team, manage capabilities, interpret signals from controls and handle all aspects of reporting, data engineering, personnel management, outreach and training. This overwhelming workload will likely lead to them becoming bogged down and ultimately paralyzed in their roles.

Thus, CISOs are expected to expand their attention to other critical and strategic areas. With the rapid adoption of generative AI across industries, CISOs can play a crucial role in ensuring that organizations understand and mitigate the associated risks. They will need to become more strategic and proactive, engaging with the business at the early stages of AI projects to explain potential risks and outline necessary steps for mitigation.

Bottom line, CISOs need to determine how AI can help better protect the company, its people and customers while investing in and embedding the necessary AI-specific safeguards within the models. To that end, KPMG research has found that 64 percent of global CEOs acknowledge they will invest in AI regardless of economic conditions.[3]

In the future, CISOs will likely need to continuously broker tradeoffs with other areas of the organization, balancing the demands of the board, the business, technology managers and their own need to manage inherent risks. This will require CISOs to be skilled stakeholder managers, able to navigate complex relationships and effectively communicate the importance of cybersecurity priorities.

To facilitate this, CISOs may consider embedding security personnel within key business functions, allowing for better alignment of security culture and priorities across the organization. By cultivating a holistic perspective, CISOs can provide valuable insights to the board and ensure that cybersecurity is integrated into the fabric of the organization.

And then there's the resilience objective on which many regulators are focused. Resilience entails mapping critical business processes and the systems organizations need to recover after an incident. CISOs can't just flick a switch and engage business and technical teams to address these issues.

That's why organizations are splitting responsibilities. Companies are realizing that for all these things to proceed efficiently, they can't fall to one individual. The broad security team has to protect the entire enterprise at all times, but attackers only need one unprotected vector to access the network.

Clearly, it's an asymmetric battle and to do it all well, multiple parts of the company must work together. The CISO may be best positioned to oversee it all, but they can't do it all alone.

> "Cybersecurity has become much more of a delegated and shared function. But while the CISO today works very closely with many counterparts across the business, they must speak in one unified voice to manage risks while supporting the organization's commercial interests."
>
> **Oscar Caballero**
> Partner, Head of Cybersecurity
> KPMG Mexico

[3] KPMG 2024 Global CEO Outlook, August 2024.

© 2025 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Suggested actions

Stay informed about regulatory changes, communicate with the board, and clarify limits of authority to mitigate personal liability risks.

Prepare for the CISO role's evolution due to AI automation and the shift to cloud-based services.

Take the lead in discussing the adoption of disruptive technologies like AI, explaining risks and mitigation steps.

Continue to build security in by design across DevSecOps processes, in addition to embedding cyber-focused team members into business functions.

As the boundary between personal and enterprise data within cloud-based and AI services blurs, conduct thorough due diligence on third-party vendors to ensure their contractual obligations are clear and consistent with the organization's overarching data governance framework.

> "Fundamentally, reducing the probability of an attack starts with an understanding of the environment. You can't secure what you don't know. CISOs must know the entire cybersecurity estate: their organization's critical business applications and services, what's public-facing, what controls are in place, how they can be more proactive, their security posture and the vectors bad actors tend to use, to name just a few pieces. All that is fundamental. Only then can they determine how to reduce the chances of something bad happening."

Lou Fiorello
Vice President — Security Products
ServiceNow

Learn more

© 2025 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Consideration 2

The power of the people

Among the range of challenges for cybersecurity leaders, the workforce skills gap is prominent. The human element continues to be the most critical factor in the fight against cyber threats. New sophisticated technologies and rapidly evolving threats are only exacerbating an already-widening skills gap. To address these challenges and secure their digital assets, organizations must adopt a holistic approach that recognizes the power of people in building a resilient cybersecurity ecosystem. Empowering talent with the necessary tools, cultivating a robust security culture, optimizing the use of AI, and strengthening the talent pipeline are some viable solutions.

Addressing the cybersecurity skills gap and talent retention

According to the World Economic Forum, more than half (52 percent) of public organizations cite a lack of resources and skills as the greatest challenge to creating effective cyber resilience programs.[4] Much has been reported around the dearth of experienced cyber talent and the skills gap, which have created an attrition rate nearly eight percentage points higher than other roles, making team consistency difficult to maintain.[5] At this point in time, the rapid growth of cybersecurity as a profession, and the ongoing need for specialized knowledge, have conspired to outpace the ability of our educational institutions to produce enough qualified candidates.[6]

The growing disconnect between technical and non-technical skill sets is particularly striking. While strong technical abilities remain essential, non-technical skills such as effective communication, problem-solving, adaptability and collaboration are increasingly important for privacy, risk and compliance professionals. To address this disconnect, industry leaders are encouraged to prioritize comprehensive training programs.

Talent retention is another important part of the story, with nearly half (47 percent) of security leaders in a recent KPMG security operations center (SOC) survey telling us they have "major issues" retaining good workers.[7]

As the demand for experienced cybersecurity professionals continues to outpace the available talent, CISOs must develop strategies to attract and retain a diverse workforce. This needs to include partnering with human resources (HR) to understand and address the unique needs of a multi-generational workforce.

For example, Gen Z and Millennials, the youngest and fastest-growing generations in the workforce, place particular value on work-life balance, recognition, and career mobility.[8] By offering flexible work arrangements, clear career paths and opportunities for professional development, organizations can create an attractive environment for cybersecurity talent.

Inclusion, diversity and equity (IDE) initiatives will also be important in addressing the cybersecurity skills gap. By actively encouraging and supporting the participation of women and diverse groups in cybersecurity, organizations can tap into a wider pool of talent and benefit from unique perspectives and creative skills. However, promoting diversity is not enough; employers must also create supportive and inclusive environments that enable diverse staff members to thrive, especially those who fall on the neurodiversity spectrum.

[4] World Economic Forum, *Strategic Cybersecurity Talent Framework white paper,* April 2024.
[5] STI Group, *The State of US Cybersecurity Employment: Analyzing Growth, Demand, and Retention Challenges,* April 5, 2024.
[6] KPMG, Matthew Miller, *Addressing the Cybersecurity Talent Gap in the SOC,* LinkedIn, August 1, 2024.
[7] KPMG Cybersecurity Survey, *Security Operations Center Leaders Perspective,* April 2024.
[8] Paychex, *Navigating the New Workforce: Engaging Millennials and Gen Z in the Workplace,* April 23, 2024.

© 2025 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

AI is integral to cybersecurity, not reductive

While many organizations are still in the early stages of AI adoption, as cybercriminals increasingly turn toward AI to enhance their attack strategies, CISOs should explore how this technology can be securely and responsibly integrated into their cybersecurity strategies. To stay ahead of the curve, AI-enabled areas such as real-time threat detection, faster incident response and predictive modeling should be a primary focus.

This can also help reduce the burden on understaffed teams. AI is going to be a true enabler for security teams in addressing the skills gap — not, in most cases, a replacement for human workers. In fact, according to the KPMG SOC survey, at least six out of ten security leaders consider AI to be a "game changer" for all security functions, including identity and access management, threat detection and response, and perimeter monitoring.[9] By automating routine tasks with AI, organizations can significantly increase efficiency, freeing cyber teams to focus on the more complex and strategic tasks that are essential to safeguarding the network.

The human element will have a key role in adoption. CISOs should ensure that their teams are properly trained to work alongside AI systems, understanding their capabilities, limitations and potential biases. AI is also a source of anxiety in the workplace. In that context, consensus and trust will be the keys to progress. According to KPMG research, more than three-quarters of organizations (78 percent) are concerned that many users continue to view AI as an arcane "black box." Almost as many (77 percent) expect AI to pose operational challenges that will lead to job reduction and create ethical concerns.[10]

Ultimately, however, we believe the union of human intuition, creativity and contextual understanding with the speed, scalability and data analysis capabilities of AI should contribute to a more resilient cybersecurity ecosystem.

To better understand this relationship, KPMG has collaborated with Massachusetts Institute of Technology (MIT) to study cybersecurity culture, its challenges and how AI can make an impact.[11] Although many organizations are early in their cybersecurity culture journey — and more so when it comes to using AI to support it — 74 percent of respondents in a KPMG-MIT quantitative survey agreed that building a cybersecurity-focused culture is central to successful integration of AI across the enterprise.[12]

From awareness to action: Cultivating a proactive cybersecurity culture

A strong cybersecurity culture is established when every individual within the organization actively participates in effectively managing cyber risks. CISOs must recognize that people are not the weakest link, but rather the strongest cyber defense capability when properly engaged. If a culture of risk avoidance is not prioritized and embedded across the organization, the burden of defending against threats and proactively identifying risks falls solely on the shoulders of the cybersecurity team. This is not only unsustainable but also leaves the organization vulnerable to potential breaches.

To create a truly resilient cybersecurity ecosystem, CISOs must focus on bridging the gap between the security team and the broader workforce.

This involves actively engaging with both team members and senior leadership, educating them about the importance of cybersecurity and empowering them to take ownership in protecting the organization's digital assets.

Moving hearts and minds and creating a shared understanding of cyber risks can transform the way the entire organization approaches cybersecurity. Thus, cybersecurity is seen not just as another siloed function but a collective responsibility. This requires CISOs to become influential leaders who can connect technical and non-technical stakeholders.

> "The perception should be that cyber exists not to interrupt business operations and act as a speed bump but to solve problems quickly, safely and build trust with internal and external stakeholders."
>
> **Breah Sandoval**
> Director, Cybersecurity and Technology Risk
> KPMG US

[9] KPMG Cybersecurity Survey, *Security Operations Center Leaders Perspective,* April 2024.
[10] KPMG 2024 Global CEO Outlook, August 2024.
[11] Joint research between KPMG and Cybersecurity at Massachusetts Institute of Technology/Sloan School of Management, September 2024.
[12] KPMG, A new age of cybersecurity culture: How to harness AI to promote secure workplace behaviors, December 2024.

© 2025 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

To create a more user-friendly and efficient cybersecurity environment, CISOs should adopt a human-centric design approach when evaluating and refining security processes. This means identifying and targeting specific processes that cause frustration or friction for employees. Many of these pain points lead to decreased productivity and increased risk of non-compliance. By carefully analyzing these processes, CISOs can determine which controls are essential for protecting critical assets and which ones can be streamlined, rationalized or even eliminated.

With this approach, CISOs can create a more intuitive and less disruptive security experience for employees, adding to a culture of compliance and shared responsibility. This can promote a positive view of cybersecurity and encourage employees to become active participants. From a broader cyber-HR management perspective, CISOs can play a vital cross-functional role in measuring security knowledge, attitudes and behaviors among the workforce to reveal potential drivers of human-centric risks and shift the perception of cybersecurity from a restrictive function to a key capability and business enabler.

A public-private partnership can support cyber as a function and promote it as a career

In addition to addressing the current skills gap, governments, academic institutions and organizations should collaborate to promote cybersecurity as an appealing career choice.[13]

This effort should start early, engaging younger, pre-high school students — girls, in particular — but also include men and women who are embarking on a second career or perhaps are re-entering the workforce post-family leave, to showcase the diverse range of opportunities available.

Governments can support this initiative by investing in robust cybersecurity education programs, offering scholarships and internships, and partnering with industries to provide hands-on learning experiences. With exposure from a young age, an active ecosystem can spark interest and encourage more individuals to pursue careers in this critical field.

In addition to early education and awareness, governments and industry leaders must work together to develop alternative pathways for individuals to enter the cybersecurity workforce.

While traditional university degrees in computer science and related fields remain valuable, they often fail to keep pace with the rapidly evolving threat landscape and the specific skills needed by employers.

In response, investments in shorter-term certification programs and specialized training courses can help quickly upskill and re-skill professionals from diverse backgrounds. With a more flexible and inclusive talent pipeline, building a stronger, more resilient cybersecurity workforce capable of tackling the challenges of the future can be possible.

> Our greatest cyber challenge and vulnerability lay not so much in the codes or the systems, or necessarily the digital pathways anymore. It's in the very people who manage and navigate these networks every day. They require support, training and nurturing to equip them with the skills and defenses they need to protect our data and systems every day.

Dominika Zerbe-Anders
Cyber Human Risk Partner & Solution Owner
KPMG Australia

[13] World Economic Forum, *Why closing the cyber skills gap requires a collaborative approach,* July 23, 2024.

© 2025 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Suggested actions

Recognize the expanding role of the CISO from solely a network defender to risk manager, lobbyist and influencer. Develop and refine influencing skills to effectively communicate the importance of cybersecurity and drive change across all levels and departments.

Develop and deploy continuous training programs that go beyond traditional methods, utilizing innovative and immersive techniques to drive sustainable behavior change among employees.

Implement human-centric risk-reduction strategies that focus on addressing the human element of cybersecurity, as it accounts for three-quarters of cyber breaches.[14]

Empower employees by engaging them in cybersecurity initiatives, providing proper education and creating a culture that recognizes their role as the organization's strongest cyber defense capability.

Invest in AI technologies to measure, quantify and track human-centric risk, enabling more effective risk management and alignment with the evolving threat landscape.

Establish an annual cyber influencer program that ensures regular engagement with staff and senior management to raise cybersecurity awareness and collaborate.[15]

[14] Verizon, *Data Breach Investigation Report,* 2023.
[15] World Economic Forum, *Bridging the Cyber Skills Gap,* 2024.

Learn more

© 2025 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Consideration 3

Embed trust as AI proliferates

Organizations continue to explore how AI can add value to their business operations. However, leaders remain skeptical about AI adoption, especially when it comes to security and privacy. The risk of data breaches, unauthorized access and misuse remains high. Moreover, there is a lack of clarity regarding how some AI algorithms can lead to bias, discrimination and other unintended consequences. In this environment, greater transparency, accountability and governance around the development and deployment of AI is likely to remain a top CISO priority.

Managing AI data is key

Clearly, data is a critical organizational asset, fueling the development and deployment of AI systems. Many businesses continue to struggle to establish clear guidelines and processes for managing the vast amounts of data at their disposal. This has also brought into focus challenges related to data access, use, classification and quality. All of these factors directly impact how AI systems generate reliable insights and make sound decisions. When data quality is poor, AI models are more likely to produce unreliable results, leading to suboptimal performance and potentially harmful outcomes.

Indeed, although many organizations are investing in data accessibility, KPMG research indicates that only 24 percent are focusing on establishing a data-centric culture and ensuring data interoperability. This is shortsighted and undermines the ability to effectively use and understand data across all levels of the organization.[16]

Moreover, the speed at which organizations are embracing AI has put tremendous pressure on data management practices. On the positive side, it makes clear the importance of competent data management in connection with reliable AI practices. Traditional approaches to data governance often involve manual processes and siloed systems. These are insufficient in the face of the volume, velocity and variety of data generated by AI applications. Businesses now need to adopt more agile and automated data management strategies to keep pace.

> “Whether companies rely on their own or third-party data to generate and train their AI models, it’s become clear that poor data quality produces poorly performing AI models.”
>
> **Samantha Gloede**
> Managing Director, US & Global Trusted Leader
> KPMG US

[16] KPMG Global Tech Report 2024, September 2024.

© 2025 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

This requires a fundamental shift in the way organizations think about data, from a static asset to a dynamic resource. To mitigate the risks associated with inferior data quality, organizations must prioritize strong information governance practices. This involves establishing clear policies and procedures for data collection, storage and management, as well as implementing robust data validation and cleansing processes. Doing so can enable businesses not only to improve the performance of their AI models but also build trust with stakeholders by demonstrating a commitment to responsible and transparent data practices.

Confronting the minefield of AI adoption risks

AI adoption comes with a wide range of risks that organizations must carefully navigate; operational, technical, legal, compliance and human safety are just a few. AI systems can introduce new vulnerabilities and points of failure that can disrupt business processes and lead to financial losses. Technical risks, such as algorithmic bias and data drift, can undermine the accuracy and reliability of AI models. This is why 70 percent of CEOs say their organization is increasing its investment in cybersecurity specifically as a means of protecting operations and intellectual property from AI-related threats.[17]

AI systems that do not comply with privacy regulations, discriminate against protected groups, or infringe on intellectual property rights can lead to legal and compliance risks. The most concerning risks are the ones to human safety, particularly in healthcare and transportation, where AI failures can have life-threatening consequences.

There is another significant risk associated with AI: the erosion of the ability to be forgotten, which means removing personal data from the model. Doing so requires the model to be completely retrained with a new dataset, which is expensive and complex.

But even if personal data is removed and the model is retrained, it can still make fairly accurate inferences about an individual based on patterns and correlations learned from other data points. Unfortunately, the ability to truly be forgotten in the digital realm is becoming more elusive.

As AI becomes more accessible and embedded in many different "smart" products, many organizations, even smaller businesses with limited budgets, are turning to third-party providers to access AI capabilities. While this can offer cost savings and rapid deployment, it also introduces new risks. Organizations may have limited visibility into the inner workings of the AI system, such as the data the model was trained on, the algorithms it uses and the potential biases it may have.

"Shadow" AI — the use of AI systems within an organization without the knowledge or oversight of leadership and security teams — is another emerging risk. Shadow AI can arise when individual departments or employees deploy AI solutions on their own, often without proper checks. The heightened risk is not just about the vulnerabilities of ungoverned AI, but also the possibility that the undesired, potentially biased output may be integrated into business decision-making without understanding the implications. As a result, unmanaged AI systems can introduce security exposures and compromise data privacy.

To mitigate these risks, organizations should proactively establish clear policies and procedures around the procurement, deployment and monitoring of internal and third-party AI systems. In addition, CISOs are encouraged to explore the universe of new security tools and capabilities that enable organizations to identify and analyze AI usage patterns to reduce the risk of shadow AI. Close collaboration between business leaders, IT teams, and security experts is key here.

> "Relying solely on the CISO or the CPO to address AI risks may mean overlooking critical issues such as transparency, reliability, and potentially even safety."
>
> **Katie Boswell**
> Managing Director, Cybersecurity and Technology Risk
> KPMG US

[17] KPMG 2024 Global CEO Outlook, August 2024.

© 2025 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Take a bottom-up approach to AI-related risks

Even as adoption accelerates, many leaders lack a complete understanding of AI governance and the complex technical, ethical and legal implications. As a result, many take a reactive approach. Organizations that align their AI risk management strategies with their overall business objectives and values are much more likely to achieve success.

Indeed, to establish and maintain trust in AI systems, organizations must prioritize the interests of stakeholders, including customers, employees and society at large in AI decision-making. Organizational leaders, including CISOs, data protection officers and privacy officers, have a crucial role to play in embedding security and privacy into the AI development lifecycle.

Further, leaders must maintain visibility into the various business cases for AI and clearly identify where and how AI is being used across the organization. This can guide the development of secure and ethical data management practices and the appropriate controls within the broader AI security framework.

Solidifying trust and monitoring external risks

When it comes to AI-related risks, organizations need a forward-looking approach that goes beyond simply reacting to issues and addresses potential risks early. Establishing an AI security framework is not a project with a distinct end point; it must be ongoing and supported by existing security domains through identity and access management, multifactor authentication, and crisis response and recovery plans, among other factors.

In short, ongoing monitoring and evaluation of AI systems should be baked into the organization's business-as-usual processes. By mapping out the data flow across the AI landscape, organizations can better assess potential risks and vulnerabilities and develop targeted strategies.

One of the key external considerations is the potential impact of AI-related regulations, such as the EU AI Act (the Act), which took effect in August 2024. The Act has wide-ranging impacts on any business that operates in the EU and offers AI products, services or systems that can be used within the EU.

Although it is perhaps the most well-known and far-reaching rule, the Act is part of a wider trend of rising regulatory guidelines for AI globally. Many policymakers around the world are looking to the Act as an example and seeking some level of alignment with its perspective on topics such as safety, security, privacy, governance and compliance, as well as fairness, transparency and trustworthiness. CISOs of companies that provide services of any kind to the EU need to evaluate how the Act applies and take steps to comply.

Organizations must stay closely attuned to all regulatory developments and proactively align their AI governance practices to build trust with stakeholders and realize the full potential of AI while mitigating its risks and challenges.

> "Many companies have put off data projects for a long time because they don't necessarily see the value. But they're going to have to realize they need to clean up their data and train their large language models (LLMs) with relevant and accurate information. Unfortunately, in a lot of cases, CISOs are not necessarily the data owner. To build those bridges and strengthen the relationships between the data and security teams, there needs to be shared data classification definitions and common rules of engagement, especially as it relates to AI. Bottom line, bad data yields bad decisions."
>
> **Erin Hughes**
> Head of Cybersecurity Advisory — North America
> SAP

© 2025 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Suggested actions

Bring together cross-functional stakeholders, including CISOs, data protection officers and privacy officers, to update policies and align on the organizational approach to addressing the potential impact and risks associated with AI implementation.

Understand regulatory obligations and assess existing compliance requirements related to AI implementation. Develop and communicate clear AI usage policies, standards and procedures. Collaborate and maintain an open dialogue with other industry leaders and federal and global policy makers.

Uplift existing governance processes and communicate clear AI usage policies, standards and procedures. This should include an AI intake process that takes a consistent approach to identifying AI risk, determining the appropriate controls and establishing the corresponding incident management plans to address potential AI-related issues.

Determine and establish ownership of the necessary controls to mitigate AI-related risks and clearly define who owns and is accountable for those controls is clear and consistent with organization's overarching data governance framework.

Establish a red teaming structure to perform testing of AI models, ensuring their robustness and reliability to avoid generating inaccurate or undesirable information. Define roles and responsibilities to support AI capabilities between the first and second lines of defense.

Learn more

© 2025 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Consideration 4

Harness AI for cyber: Racing ahead vs. racing safely

The potential benefits of AI continue to captivate business leaders across industries. For CISOs, AI is viewed as a means to increase efficiency, cut operational costs, improve risk management and possibly tackle escalating workloads, particularly in security operations centers (SOCs). Still, questions remain: Does my organization fully understand the range of AI risks? Do we have a robust AI-specific security foundation in place? What if I don't know where to start or how to identify areas where AI will be most useful? Against this backdrop, CISOs must strike a delicate balance between the desire to implement AI across the enterprise and the need to prioritize good security practices.

Building a strong security foundation for AI

In an ever-fluid cybersecurity ecosystem, staying ahead of would-be attackers requires not just vigilance but innovation. AI has emerged as a powerful tool for security operations centers (SOCs), transforming the way security professionals perceive and respond to threats. While 2024 was the year for Gen AI, 2025 is the year of agentic AI. Agentic AI has the potential to transform security operations, whereby 'bots' could proactively analyze, detect and respond to cyber threats in a way we have not seen before.

Indeed, nearly three-quarters of organizations are realizing business value from their AI investments, but only one in three has been able to achieve these gains at scale.[18]

But before diving headfirst into AI adoption, organizations must ensure they have a solid foundation of basic cybersecurity practices. This includes everything from effective patch management and device encryption to secure identity and access management. Simply rushing to deploy AI tools can expose an organization to greater risks.

CISOs have a critical role to play here. They must assess their organization's current cybersecurity posture and identify any gaps or weaknesses for AI to be introduced gradually and strategically. In short, the investment should be measured and strategic to avoid disjointed implementations.[19]

> "To be blunt, it doesn't make sense to employ AI tools when your patch management and authorizations are not under control. The basics always need to be right."

Koos Wolters
Head of Cybersecurity
KPMG Netherlands

[18, 19] KPMG Global Tech Report 2024, September 2024.

© 2025 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

The talent equation: Bridging the AI skills gap

The conversation around AI in cybersecurity inevitably turns to talent. There's a significant skills gap, not just in understanding AI but in leveraging it effectively within the cybersecurity domain. The development of AI technologies, particularly generative AI (Gen AI), has outpaced the skills available in the market.

Strengthening workforce AI skills is one of the top CISO challenges in this environment. Teams are learning that the quality of the prompts used to interact with and query AI models can significantly impact the accuracy and relevance of the output. Without a strong understanding of best practices, security teams may struggle to obtain the desired insights and actionable intelligence from AI implementation.

To address this skills gap and ensure that security teams can keep pace with the rapid advancements in AI technology, CISOs must prioritize upskilling and training initiatives — for their teams and themselves, so they are able to identify the right talent needs and the best people to hire. This involves investing in educational programs focused on AI concepts such as prompt engineering, data analysis and model evaluation.

CISOs should foster a culture of continuous learning, encouraging other security professionals to explore new AI capabilities, share their findings with colleagues, and ensure they and their teams have the intellectual curiosity and knowledge to harness the power of AI, protect the organization's digital assets and increase cyber resilience.

Navigating the hype vs. the reality of AI

KPMG research has found that the hype surrounding AI in cybersecurity has led to a growing sense of fear of missing out (FOMO) among organizations, particularly at the senior management and board levels. In fact, 82 percent admitted they are choosing to invest in tech investments such as virtual and augmented reality, which are enabled by AI, in order to keep pace with their competitors.[20] However, leaders need to make decisions based on the current realities of AI's capabilities and limitations. While AI has the potential to revolutionize cybersecurity, its current use in the SOC is still relatively immature and limited in scope.

CISOs need to set realistic expectations and communicate the true potential of AI to senior management and the Board. This involves highlighting the current limitations and having a strategic approach to adoption. By encouraging a culture of experimentation, CISOs can help with the discovery of appropriate use cases that align with the organization's unique needs and priorities. As AI continues to mature and evolve, CISOs must remain vigilant in assessing its capabilities and limitations.

> "In cyber, we have more tolerance for false positives than false negatives. I would rather AI think something bad is happening and prompt me to investigate through manual processes to see whether the network is compromised versus actually having a cybersecurity issue, not knowing about it, and not mobilizing to address it."

Matt Miller
Principal, Cybersecurity Services
KPMG US

[20] KPMG Global Tech Report 2024, September 2024.

© 2025 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Identifying and deploying use cases with the most impact

CISOs must carefully assess and prioritize potential AI use cases that offer the greatest impact and align with their organization's specific needs. A promising area is the analysis of large volumes of data to identify potential threats or anomalies, as AI excels at processing vast amounts of information to extract insights. Additionally, AI can be used to automate repetitive, manual tasks, freeing up human analysts to focus on more complex and strategic initiatives. AI-driven analysis can enable developers to patch small vulnerabilities before they become big problems.

By empowering team members to explore AI's capabilities and propose ideas for implementation, CISOs can uncover areas where AI can be most effectively deployed. Carefully assessing and selecting use cases that address real-world problems positions CISOs to ensure that their AI investments are targeted, effective and aligned with the organization's overall cybersecurity and business goals.

Preparing for AI-powered cybersecurity threats

While adopting AI technologies to enhance their cybersecurity efforts, CISOs must also be prepared to face the emerging threats posed by AI-powered attacks.

One particularly concerning example is the rise of deepfakes and the reality that AI algorithms can now quickly, easily and inexpensively create highly realistic and convincing manipulated audio and video content. In fact, deepfake technology has become democratized to the point that essentially any threat actor can obtain and operationalize it with minimal effort.

This purposely deceptive material is increasingly being used in social engineering attacks or to spread disinformation, making it more challenging for cybersecurity teams to distinguish between genuine and fraudulent content.

Also, the growing use of AI in voice detection and biometric authentication in call centers can inadvertently make it more difficult to detect and defend against deepfakes. Attackers may exploit these same technologies to bypass security measures and manipulate systems.

To combat these evolving risks, CISOs must stay informed about the latest developments in AI-powered threats and adapt their defense strategies accordingly. This may involve investing in advanced AI-driven security tools, such as those designed to detect and flag potentially manipulated content, as well as educating employees. They need to ensure that any AI deployment is supported by clear roles, responsibilities and context to maximize its impact on cybersecurity efficiency and effectiveness.

> "Unfortunately, in regard to AI, security holds a lot of the liability. CISOs were already in difficult waters, but the rapid pace at which it is now being rolled out is exponentially increasing stress levels around what good security looks like when you start introducing these LLMs at scale. However, there are effective strategies and tools available to manage the evolving environment."

Terence Jackson
CISM, CDPSE, GRCP
Customer Security Officer
Microsoft Security Solutions

© 2025 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Suggested actions

Address the basics of good security — patch management, safeguarding data, IAM, etc. — before turning to more sophisticated activities like implementing and scaling AI across the enterprise.

Work to enhance awareness among employees and customers of the risks associated with enterprise and adversarial use of AI.

Continue to assess use cases for AI for SOC Level 1 and Level 2 tasks.

Provide a clear vision of the roles and responsibilities of people utilizing AI and be transparent about the context and initiatives in which AI is being used.

Prioritize upskilling the security workforce with the necessary technical skills and ensure they stay up-to-date with the latest AI developments.

Encourage teams to be intellectually curious about AI and to propose ideas for experimentation and potential use cases.

Learn more

© 2025 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Consideration 5

Platform consolidation: Embrace the potential but recognize the risks

To tackle increasingly complex cybersecurity risks, organizations continue to add to their arsenal of tools and solutions designed to protect their digital assets. From endpoint security and security information and event management (SIEM) to vulnerability management, Internet of things (IoT) security, extended detection and response (XDR) and managed detection and response (MDR), the sheer number of options available can be overwhelming. CISOs struggle to manage, maintain and integrate this complex patchwork of disparate tools. Worse yet, more time is spent on integration than harnessing the value of the data for usable security insights. In response, many organizations are exploring the adoption of security platforms, giving them greater efficiency, improved visibility and enhanced control over the security environment. This broader shift to platform consolidation offers both promises and pitfalls.

Recognizing the value of platform consolidation

Large organizations are particularly keen on the shift toward platform consolidation. One reason is that disparate tools produce a huge volume of data and signals, and they enforce different aspects of the overall security policy. This complexity makes integration and enforcing a consistent security policy a challenge. Streamlining the cybersecurity toolset by consolidating disparate solutions gives leaders a clearer, more comprehensive view of their organization's security landscape. This, in turn, facilitates the enforcement of consistent security policies across the board, closing potential gaps and vulnerabilities.

Consolidation also matters in the context of a zero-trust framework. At its core, zero trust requires the evaluation of every interaction within an organization's network, including the device used to access the network, the authentication methods employed, and the specific data being requested. However, implementing a zero-trust model can be incredibly challenging when organizations rely on a fragmented array of security tools. Platform consolidation can help enforce granular access controls and provide the required visibility.

> "There are economies of scale that come with consolidating with a particular platform or discipline, such as identity. Giving the security team improved, but perhaps less technologies to work with can help create a more well-rounded security workforce that is more effective across capability domains."
>
> **Jim Wilhelm**
> Principal, Global Microsoft Security Leader
> KPMG US

© 2025 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Moreover, organizations can benefit from economies of scale when it comes to managing identity, data security, threat management, endpoint protection and network control. Consolidation yields significant cost savings, as fewer tools require less maintenance, training and support. With consolidated data sources, the security team can also better harness the power of AI.

Understanding your security data (logging and monitoring, signals, threat intelligence, authentication policies, entitlement assignments, user account data, etc.) is critical to empowering security personnel with the capabilities of Gen AI to improve productivity in the security operations center (SOC) and beyond. The byproduct of this work is data consolidation and beginning the first steps of the journey toward an AI-enabled cyber program.

Working through possible pitfalls

While platform consolidation offers numerous benefits, it is crucial for CISOs to be aware of the potential risks and challenges. One significant, although not new, concern is concentration risk — wherein an organization may become overly reliant on a single vendor or platform. Putting too many eggs in one basket — a risk that has been on CISOs' radar since the early days of cloud adoption — companies expose themselves to heightened risk if there is a compromise or vulnerability in a particular product or platform. Recent high-profile IT-related disruptions have put this risk in the spotlight. So, CISOs must strike a delicate balance between reaping the benefits of a streamlined security stack and mitigating the potential impact of a single point of failure.

Another challenge from a commercial perspective that may emerge over time is vendor lock-in. As organizations become increasingly dependent on a specific set of products or services, they may find that the chosen platform no longer meets their needs. In such cases, switching to a different vendor can be a costly and complex undertaking. This can involve significant compatibility issues and additional training requirements. To mitigate these risks, CISOs should consider adopting a hybrid approach to platform consolidation.

By relying on platform providers for foundational security capabilities and augmenting gaps with purpose-built solutions, organizations can ensure they have the necessary resiliency and flexibility to adapt to changing circumstances. Thus, CISOs can minimize the potential downsides of overreliance on a single vendor or platform while still taking advantage of the core benefits of a platform-based approach.

The consolidation decision is rarely made in isolation. Rather, it is a collaborative effort involving key stakeholders such as the CISO, CIO, CFO, COO and CDO. Perspectives from all leaders play a role in ensuring the chosen platform aligns with the organization's overarching security strategy and business objectives.

Talent and upskilling need to keep pace

In the move toward platform consolidation, talent development and upskilling initiatives also need to evolve. Cybersecurity professionals need to be prepared to adapt and thrive in a new and very different environment. CISOs must prioritize continuous learning and talent development across all domains of security, from the SOC to monitoring personnel and beyond.

> "CISOs and their organizations are concerned about the shortage of talent. To enhance cybersecurity under these conditions, it is necessary to simplify and consolidate the number of tools and solutions used to protect digital assets."
>
> **Motoki Sawada**
> Partner, Technology Risk Services
> KPMG Japan

© 2025 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

With the right investments in skills and knowledge, security teams can establish the necessary agility and expertise to make the most of platform consolidation. By working with a more focused set of tools, security professionals will be able to devote their time and energy to high-impact initiatives and respond to threats with greater efficacy.

Platform consolidation also gives CISOs a unique opportunity to optimize their talent-development strategies. Working with fewer vendors enables CISOs to streamline their training efforts, making it easier and more cost-effective to upskill their teams. As SOC engineers and analysts receive training on a consolidated set of tools, they, too, will become more efficient and effective in their roles. This can contribute to a stronger overall organizational security posture. By aligning talent development with the goals of platform consolidation, CISOs can create a virtuous cycle of continuous improvement and risk reduction.

Keeping pace and operating at the speed of business

As organizations grow and expand into new markets and regions, the demands on cybersecurity teams are multiplying. CISOs must contend with an increasing number of users, devices, and data points, all of which require robust protection and monitoring.

At the same time, we've heard, anecdotally, from several clients, that budgets remain constrained with only modest year-over-year increases. In this context, the pressure to justify cybersecurity spending and demonstrate clear value to leadership has never been higher, requiring CISOs to continually look to extract more value from existing investments. The focus must be on making smart, strategic investments that deliver tangible value and return on investment.

Moreover, security needs to operate at the speed of business. However, as the business grows and new technology-enabled capabilities are rolled out, integration with security tooling cannot be exponentially expensive. It must be flexible and adaptable — and a platform approach helps make this process more repeatable and agile in the long run. Whether it's applying advanced authentication methods to a new application or technology asset or signals-based access control, common patterns and a platform approach to integration help to improve the resiliency and speed of adoption.

CISOs must be able to articulate how their investments in platform consolidation are helping to close critical capability gaps, reduce vulnerabilities and risk, and support the overall goals of the business. By striking the right balance between fiscal responsibility and strategic investment, CISOs can position their organizations for success.

> **Traditionally:** Most cybersecurity ISV's say they can communicate with disparate platforms, but the market has realized varying degrees of success of interoperability and effectiveness — often at high labor and maintenance cost.
>
> **New generation:** Some new cyber ISV's are consolidating traditionally disparate products into a new single, seamless tool with broader functionality and better data accessibility. This is a more effective approach, enabling companies to customize and contextualize those environments for individual clients and leading to improvements around data, speed, scale, efficiency, cost and functionality.
>
> **Philip Bice**
> Global Lead — Service Provider Partnerships
> Google

© 2025 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Suggested actions

Evaluate current vendors, assess platform compatibility with your technology landscape, and establish clear criteria for vendor selection and performance monitoring to ensure a strong foundation for consolidation.

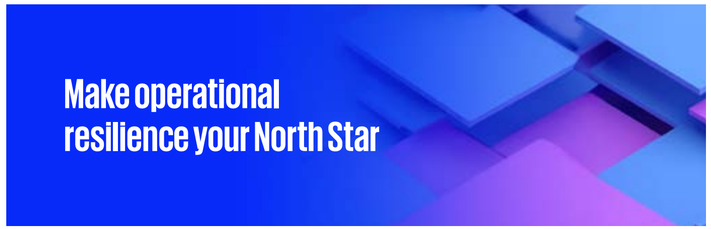
Identify areas where a hybrid approach can provide benefits; determine the right balance between consolidated platforms and specialized tools. Establish backup and recovery procedures to ensure resilience.

Recognize that complete consolidation may not be feasible; identify areas where specialized tools or providers may be necessary. Develop a phased approach to consolidation, prioritizing high-impact areas first.

Invest in training and upskilling your security team to work efficiently with a consolidated set of tools.

Implement continuous monitoring and auditing processes to ensure platform performance.

Learn more



© 2025 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Consideration 6

The digital identity imperative

Digital identities are paving the way to a more agile and efficient digital world. However, securing digital identities is becoming increasingly challenging for several reasons, from inadequate systems and controls to the rise of deepfakes. Consequently, there is an urgent need to incorporate new and more advanced security mechanisms into verification regimes. More importantly, CISOs and decision-makers need to develop a fuller understanding of the landscape, rethink entrenched processes and invest in innovative systems rooted in sound principles.

The increasing complexity of digital identity management

Ultimately, each individual possesses a unique identity that is distinct to them. However, across different contexts — government, finance or life sciences, for example — identity is applied in various ways to serve specific functions or satisfy different needs. It is essential to understand that while an individual's core identity remains singular, its interpretation and validation can differ across organizational environments.

As organizations strive to maintain the integrity of individual identities, they are increasingly turning to advanced authentication technologies — including biometrics, such as fingerprint, facial, voice and retinal scans — to enhance security and streamline processes. However, these modalities give rise to risks and the impact can go well beyond the scope of a typical data breach. If these unique identifiers are compromised, for example, individuals face the ongoing possibility of identity theft and misuse that is not easily rectified since biometric traits are inherently permanent and irreplaceable. The collection and processing of biometric data also raise concerns about potential data discrimination and bias in biometric systems, making diversity and accuracy in data coding practices to ensure fair and reliable recognition more important than ever.

Deepfakes present another daunting challenge as they increasingly blur the line between reality and manipulation. With current AI technology, more powerful, broadly accessible and inexpensive, personal information, voices and faces in particular, is increasingly susceptible to compromise and exploitation. While deepfakes pose a significant threat in terms of impersonation and the spread of misinformation, they also present an opportunity for both content creators and content consumers.

Improved authentication methods will help advance accountability, ethical standards and transparency among content creators. The resulting heightened awareness can lead to a more discerning consumer audience. Investing in better authentication will help safeguard the integrity of digital information and restore trust in the content we consume.

Another area of growing concern for organizations is the proliferation of machine identities, specifically in connection with privileged non-human service accounts, which have access to sensitive data to run specific applications. With the Internet of Things growing more prominent, machine identity is becoming a significant challenge for organizations to manage. Not surprisingly, CISOs direct most of their team's attention to human access, but they've got to keep a record of the non-human network users as well, to monitor if and when they are being attacked and potentially compromised.

© 2025 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Why businesses need a future-proof digital identity strategy

From a commercial perspective, whether in a B2B or B2C context, digital identity management revolves around establishing trust between organizations and the individuals accessing their networks. By empowering users with control over their personal information and providing transparency about its usage, businesses can cultivate trust and loyalty among their customer bases. This trust is built on the assurance that individuals can access the resources they require, the confidence that access will be promptly revoked when no longer necessary, and the certainty that all actions taken within the system will be logged and fully traceable.

Maintaining this trust requires a proactive approach to the entire identity and access management lifecycle, from provisioning and ongoing administration to deprovisioning of access. This is particularly important because long-tenured employees could amass access to numerous systems, granting them significant power. To mitigate these risks associated with the accumulation of privileges, CISOs and their teams must adhere to two key principles of cybersecurity: least privilege and need to know.

By ensuring that individuals only have access to systems essential to their specific roles, organizations can significantly reduce the potential for bad actors to compromise powerful administrator accounts and gain access to sensitive data.

As the lines between workforce and consumer identities continue to blur, organizations must adopt a holistic approach. For employees, a robust digital identity framework ensures that access to sensitive information is granted based on well-defined roles and responsibilities. This involves implementing secure onboarding and offboarding processes and conducting regular access control reviews and updates.

An effective digital identity strategy can also significantly enhance efficiency and user experience. A streamlined process can minimize the need for repetitive form-filling for tasks such as filing taxes, making insurance claims and going for medical visits. This can reduce friction and waiting times for both employees and customers. As organizations increasingly rely on digital technologies to drive growth and innovation, a strong digital identity framework becomes a cornerstone of their overall business strategy. By investing in secure, transparent and user-centric digital identity solutions, businesses can position themselves for success.

> “Organizations tend to focus on the human aspect of security because it’s more tangible. It’s much more difficult to verify a machine’s identity and usage and when it was created in the system.”

Anubha Sinha
Partner, Digital Trust & Identity
KPMG Australia

© 2025 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

How governments can enable trusted digital identity ecosystems

Digital identity remains a crucial touchpoint for secure and efficient verification processes across various government services and transactions. Governments and global corporations worldwide are actively pursuing improved solutions for personal and business-related digital identities. For instance, Australia recently introduced a comprehensive digital identity program, known as the "Trust Exchange," which is highlighted by a digital wallet that integrates different areas where identity authentication is needed, such as government, social, financial and workforce identities.[21]

By facilitating digital identity verification across multiple services, the Trust Exchange seeks to increase trust among organizations while granting citizens control over the personal information they share. Estonia is another example, issuing every citizen a digital identity at birth that remains valid throughout their life. Citizens have full transparency regarding when and where their identity is authenticated, which helps to combat privacy concerns.[22]

Despite these encouraging developments, interoperability between global systems remains a challenge. This is due to differing regulations, risk appetites and public opinion regarding the handling of personal and biometric data. When it comes to a global consensus on trusted identity exchange, a coalition of willing countries may emerge, such as the EU's interoperable framework to develop a shared trusted identity framework. However, not all countries prioritize the same values, especially concerning privacy, which may limit the extent of interoperability in the short term.

How CISOs can lead the charge in implementing digital identity strategies

In shaping digital identity strategies, CISOs can serve as the connective tissue between government, regulators and the enterprise. In an increasingly complex environment where much of the identity management process lies outside of their direct control, CISOs must adopt a proactive and collaborative mindset, engaging stakeholders from the top down to ensure awareness and drive the necessary changes.

Security leaders need to keep up with user needs and expectations, ensure adherence to core security principles and stay informed about the implications of emerging technologies like AI and deepfakes. Additionally, CISOs must elevate the discussion of digital identity at the board level, ensuring that senior leaders understand its importance and provide the necessary support.

By prioritizing identity as the new perimeter in cybersecurity and promoting a culture of security throughout the organization, CISOs can lay the foundation for successful digital identity management.

> "Transparency is the cornerstone of trust in the world of digital identity. I believe, by openly sharing how personal information is collected and used, we can alleviate concerns about privacy and empower individuals to make informed choices regarding their online presence. The more transparent the process, the more trust people will have in the system."

Imraan Bashir
Partner and National Public Sector Cyber Leader
KPMG Canada

[21] Australia Department of Social Services, *Trust exchange drives secure digital services,* August 13, 2024.
[22] e-Estonia, *Solutions and services: e-Identity,* 2024.

© 2025 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Suggested actions

Ensure adherence to core security principles, such as data minimization and timely deletion of unnecessary data, to maintain the highest standards of data protection.

Engage all stakeholders, from the top down, to ensure awareness and drive the needs around sustainable digital identity and access management.

Build strong relationships and trust with other business units to ensure efficient collaboration and coordination in identity management processes.

Prioritize identity as the new perimeter in cybersecurity, recognizing its role in securing the organization's assets and stakeholders.

Stay informed about the implications of AI and deepfakes on digital identities to proactively address emerging threats and vulnerabilities.

Streamline identity while maintaining security. Focus on user experience by simplifying the issuance and usage of credentials, reducing passwords, etc.

> "As deepfake technology advances, the risk of identity manipulation and fraud intensifies, making robust digital identity protections crucial to safeguarding both consumers and organizations from emerging threats."

Nancy Chase
Global and Canadian National Leader, Risk Services
KPMG International

Learn more

© 2025 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Consideration 7

Smart security for smart ecosystems

With improving technology, there has been an explosion of smart devices and IoT products, transforming the way we interact with the world around us. From home appliances and wearables to industrial equipment and vehicles, the proliferation of connected devices introduces new vulnerabilities for cybersecurity professionals to protect against, impacting both companies and consumers. Many of the risks are still unfolding. Protecting organizational data accessed by networked devices will be crucial for preserving the integrity, safety and security of entire sectors and infrastructures. The traditional methods used just a decade ago are no longer sufficient. There is an urgent need to develop effective strategies for securing connected assets throughout their entire lifecycle and across the organizational ecosystem.

The role of CISOs in securing smart products

As organizations across myriad sectors — industrial manufacturing, energy and defense, to name several — are looking to increase efficiency and gain competitive advantage, consumers are demanding convenience, accessibility and personalized experiences. Against that backdrop, we expect to see a surge in interconnected smart devices that will transform virtually every sector of the global economy, particularly healthcare, transportation, manufacturing and retail.

As these products — powered by what we call "Smart-X" technologies — become increasingly connected to companies' back-end systems and databases, CISOs will have to take a more product-centric approach to security. They need to become deeply involved in organizational and product-specific processes, ensuring that security is embedded throughout the entire lifecycle of smart devices, from secure design until the device is decommissioned.[23] According to KPMG research, 72 percent of organizations are embracing secure-by-design principles by ensuring cyber teams are involved in technology-related projects from the beginning.[24]

From the initial design and development stages to ongoing maintenance and updates, CISOs must collaborate closely with various teams. This includes engineering, development and product support to address the unique security challenges posed by these connected devices.

The expansion of these technologies introduces new risks and vulnerabilities. Further, this new reality brings cybersecurity much closer to broader society — if something goes wrong, it isn't just a business issue. Breaches can range from minor inconveniences to major threats to public safety, security and privacy. Therefore, securing Smart-X technologies is not just crucial for protecting individual entities, but also for preserving the integrity, safety and security of entire sectors and infrastructures.

> "CISOs must recognize that the supply chain around smart products is exceedingly complex. In relation to security, these external vendors and processes must be closely managed end-to-end because all aspects are interconnected."
>
> **Marko Vogel**
> Partner, Cybersecurity
> KPMG Germany

[23] KPMG, Smart-X: A holistic approach to cybersecurity for smart devices, January 2024.
[24] KPMG Global Tech Report 2024, September 2024.

© 2025 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

When tires meet technology

An example of a device that's changed significantly and now falls under the smart device ambit is an automobile. In recent years, vehicles have evolved from simple mechanical machines to complex, connected devices. Modern automobiles are now equipped with an array of sensors, processors and software systems that enable autonomous driving, real-time navigation and over-the-air updates. Moreover, OEMs (original equipment manufacturers) are increasingly offering additional features 'as a service', highlighting a shift toward service-based models for accessing advanced vehicle functionalities.

Clearly, connected vehicles have fundamentally changed the way we interact with our cars. However, the increasing sophistication has also introduced new challenges for cybersecurity professionals. As vehicles become more reliant on software and connectivity, they become vulnerable to the same types of cyber threats that plague other connected devices, such as hacking, data breaches and malware infections. Smart vehicles serve as an extension of the company, with direct access to back-end systems and databases. This can create a new risk of exposing sensitive organizational data to potential hackers.

From a consumer perspective, as electric, autonomous and connected vehicles become more prevalent, the threat of cyberattacks has risen considerably. Today's vehicles utilize millions of lines of code to power their many advanced functions, leaving them vulnerable to unauthorized access and hacking. CISOs in this sector must research and adopt tools and strategies to operationalize relevant cybersecurity protocols and procedures.[25]

Taking a healthy look at smart medical devices

Similarly, the frequency and severity of cyber attacks on medical equipment is escalating as these devices proliferate and cyberattackers recognize their vulnerabilities. Medical devices represent a ready target for threat actors. Despite rapid innovation, there is a significant number of older medical devices in use, many of which are not secure or inadequately managed.

Compromised medical devices can reveal sensitive patient information to unauthorized persons, disrupt connected technologies, harm patients and potentially shut down hospital operations. It requires all stakeholders — from manufacturers and healthcare providers to security teams — to communicate and work in collaboration to actively identify cyber risks and related threats, plan for mitigation and remediation, and ensure the ongoing safety and security of patients.

With the continuous evolution of cybersecurity standards and practices, manufacturers — and, by extension, CISOs — face the daunting task of ensuring these devices meet and are compliant with the latest recommendations and requirements.

The shifting landscape of IoT and Industrial IoT (IIoT) security regulations

The regulatory landscape surrounding IoT and IIoT security is also evolving. There are new regulations to address the growing concerns around the privacy and security of connected devices.

The EU Cyber Resilience Act (CRA), a groundbreaking EU regulation that came into force in 2024, governs connected hardware and software product manufacturers. The CRA "tackles the challenges consumers and businesses currently face when trying to determine which products are cybersecure and in setting them up securely." All manufacturers and suppliers, both inside and outside the EU, are required to comply with the CRA, for products that are sold and used in the EU. This is important, considering many global organizations have facilities and supply chain relationships in the region.

In the UK, the Product Security and Telecommunication Infrastructure Act (PSTI) has set standards for the protection of consumers using connectable technology products. It requires manufacturers to focus on security by design principles, such as banning simple preloaded passwords, providing transparency on the minimum duration of security updates, and offering a statement of compliance.[26]

The PSTI sets a precedent for other regions when it comes to security regulations for smart products. With the growing proliferation of IoT and IIoT devices, organizations must navigate an increasingly complex web of security regulations and directives, particularly in Europe. To effectively navigate this environment, companies must develop a harmonized approach to security that considers the full spectrum of regulations across jurisdictions. This requires CISOs to closely work with various stakeholders, including legal and compliance teams.

Similar legislation was enacted in Australia in 2024 to ensure manufacturers and suppliers of smart devices comply with the relevant security standards.[27]

[25] KPMG International, *Cybersecure Vehicles: Growing number of connected vehicles warrants better cybersecurity measures,* 2024.
[26] Center for Cybersecurity Policy and Law, The UK PSTI Act Comes into Effect, April 29, 2024.
[27] Australian Government, Department of Home Affairs, *Cyber Security Act,* November 29, 2024.

© 2025 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Managing the prolonged lifecycle of smart products

The extended lifecycle of smart products presents unique security challenges for CISOs and their teams. Unlike traditional devices, which may have a relatively short lifespan, smart products such as automobiles can remain in use for decades. The underlying architecture of these devices must be designed to accommodate periodic updates and upgrades to adapt with new technologies, regulatory requirements and evolving security threats.

In this fluid environment, CISOs must work closely with product development teams to embed security considerations into the long-term roadmap of smart products. Right now, this means exploring potential advancements like quantum computing that could impact the security landscape in the coming decades.

Unlike traditional IT systems, where patches and updates can be easily deployed, smart devices often have embedded software that is more difficult to update due to factors such as connectivity limitations and the inability to patch in real time. Therefore, CISOs need robust strategies to manage software updates throughout the product lifecycle. Additionally, CISOs must work to educate end users about the importance of regular software updates and provide clear guidance.

The supply chain surrounding all smart products — not just automobiles and medical devices — adds another layer of complexity. With numerous components sourced from various suppliers, it is crucial to understand the software modules that comprise each smart product. CISOs need to ensure the integrity and security of the supply chain by accounting for potential vulnerabilities. This includes maintaining a detailed software bill of materials, which enables manufacturers to quickly detect and address critical vulnerabilities, even after devices have been deployed to end users.

Taking a holistic approach to smart device security and incorporating it into every aspect of the Smart-X lifecycle is critical not only for protecting sensitive information and assets but also for maintaining the trust of customers and stakeholders.

Assessing the impact of emerging technologies on Smart-X security

AI and other emerging technologies, such as automation, robotics, 5G and edge computing, present both opportunities and challenges for CISOs in ensuring the security of smart products. By leveraging DevSecOps principles and building AI capabilities into smart products from the earliest stages of development, organizations can create a more robust and adaptable security framework that works throughout the product lifecycle.

However, there are also new complexities and risks. As these technologies become more sophisticated and deeply embedded into the functionality of smart products, the potential impact of security breaches or malfunctions becomes more significant. CISOs should work to develop a deeper understanding of how AI and other emerging technologies interact with smart devices, identifying patterns and potential vulnerabilities that could be exploited by malicious actors. This requires close collaboration with product development teams and a commitment to ongoing testing and evaluation to ensure that security measures remain effective as the technology evolves.

AI has the potential to revolutionize the way security threats are detected and mitigated, enabling security teams to proactively predict and plan for potential vulnerabilities. Ultimately, CISOs must strike a balance between embracing the benefits of emerging technologies in smart devices and maintaining a robust and adaptable security framework.

> “A harmonized view of security is the first priority. Without it, organizations can’t conduct business efficiently or effectively because there are now so many security requirements built into contracts — and rightly so.”
>
> **Jayne Goble**
> Partner, Cybersecurity
> KPMG UK

© 2025 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Suggested actions

Implement a security framework that covers the entire lifecycle of Smart-X devices, from secure design to decommissioning, that includes specific strategies for IoT and IIoT devices.

Encourage investment in a variety of networking protocols and standards (such as Bluetooth, Ethernet, 5G/6G) to optimize connectivity and security.

Establish early assurance mechanisms and maintain a detailed software bill of materials to enable swift detection and recall of devices to manage critical vulnerabilities.

Address potential physical safety issues and build customer trust through transparent security practices, third-party audits, and compliance with regulatory requirements.

Develop and implement security plans that are tailored to the specific usage environments of smart devices and recognize the importance of security and trust in enhancing overall device reliability and customer confidence.

Learn more

© 2025 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Consideration 8

Resilience by design: Cybersecurity for businesses and society

Resilience is a focal point for organizations and societies, especially in critical infrastructure and the relationship between information technology (IT) and operational technology (OT). It involves reducing the probability of an attack by managing the attack surface, quickly identifying and responding to incidents while minimizing their impact and recovering quickly. The theme is becoming central to the CISO agenda as the prospect of attackers using ransomware or other malicious means to cause large-scale industrial disruption, risking both data and human lives, remains alarming. To effectively embed resilience, CISOs need to factor in several elements — the threat landscape, the evolving form of organizational assets, the role of governments, and regulations.

Strengthening cyber resilience through comprehensive asset management

Effective asset management continues to be the foundation of cyber resilience. CISOs must acknowledge that they cannot secure what needs to be secured unless they know what they have. This includes not only the assets within the organization's data center that maintain day-to-day processes, but also the mission critical systems and endpoints outside of enterprise IT that run factories, regulate mass transportation networks and keep energy grids online. Without this oversight, identifying systems like enterprise resource planning (ERP) systems and the threats that could compromise them becomes a guessing game, leaving organizations vulnerable.

The likelihood of continued and increasing cyberattacks on critical infrastructure is high, with motivations ranging from financial gain to geopolitical issues and terrorism. The impact of these attacks can be devastating, potentially leading to substantial societal harm. The financial toll of cybercrime is also skyrocketing, with the global average cost of a data breach reaching nearly US$5 million between Q1 2023 and Q1 2024, a 10 percent increase from the previous period.[28]

> "It's truly amazing that in 2025 we are still having conversations around how to properly discover, understand, categorize and, ultimately, protect an organization's critical assets."
>
> **Jason Haward-Grau**
> Global Cyber Recovery Services Leader
> KPMG US

[28] IBM, Cost of a Data Breach Report 2024, July 2024. Research conducted between March 2023 and February 2024.

© 2025 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

To address this challenge, organizations have increasingly turned to endpoint detection and response (EDR) and extended detection and response (XDR) solutions. EDR focuses on monitoring and securing endpoints, such as laptops, desktops and mobile devices, while XDR integrates data from multiple security tools and systems, providing a more comprehensive view of an organization's security posture. Although EDR and XDR have become more widely adopted, they are not yet ubiquitous. These solutions are not themselves silver bullets and should be viewed as important components of a broader security controls framework that organizations should have in place. Can effectively manage assets, gain visibility, detect anomalies and threats quickly, and respond to incidents effectively.

Navigating the risks of an expanding ecosystem and third-party relationships

As organizations increasingly rely on third-party providers for software and services, there is a heightened risk of weak links in the supply chain. An expanding ecosystem also increases the attack surface, as the potential entry points for attackers grow with each additional third-party relationship. Hackers often look for the path of least resistance to gain network access, which could be as simple as an unprotected printer.

A single vulnerability in an external provider's security can jeopardize the entire system, potentially leading to catastrophic events such as a "blue screen of death" scenario, where critical systems become unresponsive and inaccessible. This makes it crucial for CISOs to manage these risks effectively by assessing and addressing the security postures of their partners, vendors and suppliers.

To tackle these challenges and ensure compliance with emerging regulations like the EU's DORA (Digital Operational Resilience Act), Network and Information Security Directive 2 (NIS2) and Cyber Resilience Act (CRA), organizations are adopting a more proactive approach to third-party security. These initiatives seek to formalize operational resilience, with DORA focusing on resilience for financial institutions. DORA's objective is to provide a framework for resilience, including how to prepare for disruptions, what to do when they occur and how to report a disruption.[29]

Establishing clear expectations from the outset, and demanding transparency and accountability in both software and hardware supply chains, organizations can better protect themselves against a wide range of supply chain attacks. It is worth noting that the CRA requires vendors to provide a software bill of materials (SBOM) in addition to the more routine hardware bill of materials (HBOM) to ensure a comprehensive understanding of the libraries and components used in their products and services.[30]

Embracing a holistic approach to security in the face of merging physical and virtual threats

When it comes to cyberattacks, the physical and virtual worlds are no longer as distinct. It's impossible to separate one from the other. This means that organizations must consider the potential impact of cyber threats on their physical assets and operations, as well as the ways in which physical security breaches can lead to virtual vulnerabilities. CISOs need to shift the focus of their teams from constant monitoring to proactively identifying potential entry points for deepfakes.

A holistic approach to security that considers both the physical and virtual realms is essential for protecting against the full spectrum of threats. This includes securing VPN tunnels for remote workers and ensuring that all devices, whether company-owned or employee-owned, are adequately managed and protected.

Organizations must also be prepared for the fact that cyberattacks can have real-world consequences. In the case of critical infrastructure, a successful attack could lead to widespread disruption, economic damage, and even loss of life. By recognizing the interconnectedness of the physical and virtual worlds, organizations can better prepare for and respond to these types of incidents.

> "Every day you hear about cyberattacks on one country by another and vice versa. In the modern era of warfare, nearly every physical attack between sparring nations is mirrored by an equally devastating but unseen cyber assault, highlighting the critical need for robust cyber defenses."

Merril Cherian
Partner
KPMG India

[29] KPMG, Rise to the challenge of DORA compliance, 2024.
[30] Manifest Cyber, SBOMs Take Center Stage in the EU's Cyber Resilience Act, March 6, 2024.

© 2025 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

The evolving role of government in cybersecurity

As the impact of cyberattacks on critical infrastructure grows, the role of government in protecting businesses against attacks that result in substantial societal harm becomes increasingly important. While organizations cannot rely solely on the government for protection, there are measures that governments can take beyond regulatory solutions to support organizations in their cybersecurity efforts.

For instance, governments can play a crucial role in facilitating information sharing among organizations and drafting regulations aimed at protecting companies from large-scale cyberattacks and increasing their overall resilience posture. Groups like the Information Sharing and Analysis Centers (ISACs) in the US are working to democratize insights across various industries. By encouraging and supporting these types of initiatives, governments can help break down the barriers that have historically prevented organizations from openly discussing cyberattacks.

While proactive, targeted attacks on cybercriminal syndicates by governments are unlikely, there is potential for takedowns of specific groups by targeting their funding sources and hampering their ability to carry out attacks. However, many of these groups operate in countries where they are difficult to reach.

Suggested actions

- Remain aware of the evolving regulatory landscape and actively lobby for and push government into helping legislate controls that increase overall resilience.
- Implement proactive security measures, such as analyzing user behavior and identifying abnormalities, to strengthen real-time organizational resilience.
- Develop a resilience plan that identifies critical assets and strategies to maintain operations during a cyberattack.
- Regularly test and drill cybersecurity response plans to prepare leaders for significant attacks and improve organizational readiness.
- Assess third-party security gaps and view regulations as an opportunity to strengthen the organization's cybersecurity foundation.
- Prioritize continuous learning and evolution to stay informed about the latest threats, vulnerabilities and best practices in cybersecurity.
- Conduct thorough post-incident reviews to identify root causes, develop remediation plans and strengthen cybersecurity defenses.

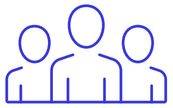
Learn more

© 2025 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Cyber strategies for 2025

What actions can CISOs, and the broader business lines, take in the year ahead to help ensure security acts as a true enabler of enterprise objectives, particularly as organizations strategically invest in AI capabilities and more in the year ahead? Following is a short list of recommendations CISOs should consider as they seek to protect – and enable – the business amidst growing global complexity.

People



- Prepare for the CISO role's evolution due to AI automation and the shift to cloud-based services.
- Recognize the expanding role of the CISO from solely a network defender to risk manager, lobbyist, and influencer. Develop and refine influencing skills to effectively communicate the importance of cybersecurity and drive change across all levels and departments.
- Develop and deploy continuous training programs that go beyond traditional methods, utilizing innovative and immersive techniques to drive sustainable behavior change among employees.
- Determine and establish ownership of the necessary controls to mitigate AI-related risks and clearly define who owns and is accountable for those controls are clear and consistent with organization's overarching data governance framework.
- Work to enhance awareness among employees and customers of the risks associated with enterprise and adversarial use of AI.
- Provide a clear vision of the roles and responsibilities of people utilizing AI and be transparent about the context and initiatives in which AI is being used.
- Prioritize upskilling the security workforce with the necessary technical skills and ensure they stay up to date with the latest AI developments.
- Invest in training and upskilling your security team to work efficiently with a consolidated set of tools.

Process

- Continue to build security in by design across DevSecOps processes, in addition to embedding cyber-focused team members into business functions.
- Implement human-centric risk-reduction strategies that focus on addressing the human element of cybersecurity, as it accounts for three-quarters of cyber breaches.
- Establish a red teaming structure to perform testing of AI models, ensuring their robustness and reliability to avoid generating inaccurate or undesirable information. Define roles and responsibilities to support AI capabilities between the first and second lines of defense.
- Streamline identity while maintaining security. Focus on user experience by simplifying the issuance and usage of credentials, reducing passwords, etc.
- Implement a security framework that covers the entire lifecycle of Smart-X devices, from secure design to decommissioning, that includes specific strategies for IoT and IIoT devices.
- Regularly test and drill cybersecurity response plans to prepare leaders for significant attacks and improve organizational readiness.
- Conduct thorough post-incident reviews to identify root causes, develop remediation plans, and strengthen cybersecurity defenses.

© 2025 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Cyber strategies for 2025

Data and technology

- Take the lead in discussing the adoption of disruptive technologies like AI, explaining risks and mitigation steps.
- As the boundary between personal and enterprise data within cloud-based and AI services blurs, conduct thorough due diligence on third-party vendors to ensure their contractual obligations are clear and consistent with organization's overarching data governance framework.
- Address the basics of good security — patch management, safeguarding data, IAM, etc. — before turning to more sophisticated activities like implementing and scaling AI across the enterprise.
- Continue to assess and invest in use cases for AI for SOC Level 1 and Level 2 tasks. Invest in AI technologies to measure, quantify, and track human-centric risk, enabling more effective risk management and alignment with the evolving threat landscape.
- Identify areas where a hybrid approach can provide benefits, determine the right balance between consolidated platforms and specialized tools. Establish backup and recovery procedures to ensure resilience.
- Ensure adherence to core security principles, such as data minimization and timely deletion of unnecessary data, to maintain the highest standards of data protection.
- Stay informed about the implications of AI and deepfakes on digital identities to proactively address emerging threats and vulnerabilities.

Regulatory

- Stay informed about regulatory changes, communicate with the board, and clarify limits of authority to mitigate personal liability risks for the CISO.
- Assess third-party security gaps and view regulations as an opportunity to strengthen the organization's cybersecurity foundation.
- Remain aware of the evolving regulatory landscape and actively lobby for and push government into helping legislate controls that increase overall business and societal resilience.
- Understand regulatory obligations and assess existing compliance requirements related to AI implementation. Develop and communicate clear AI usage policies, standards and procedures. Collaborate and maintain an open dialogue with other industry leaders and federal and global policy makers.
- Address potential physical safety issues and build customer trust through transparent security practices, third-party audits, and compliance with regulatory requirements.
- Establish early assurance mechanisms for smart devices in line with regulatory requirements, and maintain a detailed software bill of materials to enable swift detection and recall of devices to manage critical vulnerabilities.

© 2025 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

How KPMG professionals can help

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

As a leading provider and implementer of cybersecurity, KPMG professionals 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.

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

KPMG. Make the Difference.

Learn more at kpmg.com/cybersecurity

© 2025 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

Meet the authors

Akhilesh Tuteja
Global Cybersecurity Leader
KPMG International
Partner, KPMG India
atuteja@kpmg.com

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

Kyle Kappel
Cybersecurity Services Network Leader
Principal, KPMG US
kylekappel@kpmg.com

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

Dani Michaux
EMA Cybersecurity Leader
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 Cyber Security and Emerging Technology Risk practices for KPMG Malaysia and the ASPAC region and also led KPMG's global IoT working group.

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

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

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

Prasanna is a principal in KPMG's Cyber Security Services based in the US. He's 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.

© 2025 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

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
Samar Iqbal
Billy Lawrence
Leonidas Lykos
Michael Thayer

Our global collaborators:

Imraan Bashir
KPMG Canada
ibashir@kpmg.ca

Katie Boswell
KPMG US
katieboswell@kpmg.com

Oscar Caballero
KPMG Mexico
ocaballerochavanel@kpmg.com.mx

Nancy Chase
KPMG International
nchase@kpmg.ca

Merril Cherian
KPMG India
mcherian@kpmg.com

Samantha Gloede
KPMG International
sgloede@kpmg.com

Jayne Goble
KPMG UK
jayne.goble@kpmg.co.uk

Jason Haward-Grau
KPMG US
jhawardgrau@kpmg.com

Matthew Miller
KPMG US
matthewpmiller@kpmg.com

Wendy Lim
KPMG Singapore
wlim@kpmg.com.sg

Breah Sandoval
KPMG US
breahsandoval@kpmg.com

Motoki Sawada
KPMG Japan
motoki.sawada@jp.kpmg.com

Anubha Sinha
KPMG Australia
asinha12@kpmg.com.au

Bobby Soni
KPMG International
bobbysoni@kpmg.com

Paul Spacey
KPMG International
paul.spacey@kpmg.co.uk

Marko Vogel
KPMG Germany
mvogel@kpmg.com

Jim Wilhelm
KPMG US
jameswilhelm@kpmg.com

Koos Wolters
KPMG Netherlands
wolters.koos@kpmg.nl

Dominika Zerbe-Anders
KPMG Australia
dzerbe@kpmg.com.au

Our alliance collaborators:

Philip Bice
Global Lead — Service Provider Partnerships
Google

Lou Fiorello
Vice President — Security Products
ServiceNow

Erin Hughes
Head of Cybersecurity Advisory — North America
SAP

Terence Jackson
CISM, CDPSE, GRCP
Customer Security Officer
Microsoft Security Solutions

© 2025 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

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

kpmg.com

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

© 2025 Copyright owned by one or more of the KPMG International entities. KPMG International entities provide no services to clients. All rights reserved.

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

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization.

Throughout this document, "we", "KPMG", "us" and "our" refers to the KPMG global organization, to KPMG International Limited ("KPMG International"), and/or to one or more of the member firms of KPMG International, each of which is a separate legal entity.

The views and opinions expressed herein are those of the interviewees and do not necessarily represent the views and opinions of KPMG International.

Designed by Evalueserve.

Publication name: Cybersecurity considerations 2025 | Publication number: 139845-G | Publication date: March 2025