KPMG

Balancing speed and safety: The CISO's evolving role

2026 Cyber and Technology Risk Survey

kpmg.com

Contents

Foreword

The chief information security officer (CISO) role is being redefined in real time. As digital platforms, artificial intelligence (AI), and third-party ecosystems accelerate the pace of change, security leaders are increasingly expected to enable response speed while assuming accountability for enterprise-level risk. The mandate has expanded beyond protection to disciplined judgment—setting guardrails, defining risk tolerance, and guiding the organization on where velocity creates value and where restraint is required.

Our CISO survey results reveal persistent barriers to effective cyber defense. Leaders are grappling with everything from a lack of qualified professionals and AI-powered social engineering to fragmented security systems and the ever-growing complexity of information technology (IT) infrastructure.

Generative AI (GenAI) crystallizes this tension for today's CISOs. It is both a powerful source of business opportunity and a significant new risk vector. GenAI expands the threat landscape—enabling more sophisticated attacks, faster misuse, and broader exposure—while also strengthening defensive capabilities through improved detection, response, and automation. This duality places cybersecurity leaders in a high-stakes, albeit tenuous, position: governing adoption tightly enough to maintain trust, without constraining the speed and scale the business expects.

Our research points to another critical reality. Advanced technologies cannot compensate for weak fundamentals. Many organizations continue to struggle with core cybersecurity execution, from data protection and process discipline to consistent policy enforcement. These basics are the foundation of resilience. Without them, emerging technologies only amplify existing risk.

This report delves into these complex themes, drawing on data from our survey of more than 300 security leaders and the pragmatic insights of experienced experts. Our goal is to move beyond the buzzwords and provide a clear, actionable perspective on the way forward—a direction defined by a holistic strategy that empowers businesses to move at speed, safely, rather than a single tool or platform.

Michael Isensee
Partner, US Leader,
Cybersecurity & Technology Risk
KPMG LLP

Key findings

83%

of organizations saw increased cyberattacks over the past 12 months, with phishing, denial-of-service, and ransomware being the most common

Only 24%

have fully integrated AI into their cyber function

45%

select managed services providers (MSPs) based on their scalability, flexibility, and integration with existing infrastructure

70%

dedicate more than 11% of their cyber budget to AI-related initiatives

74%

anticipate an increase of more than 11% in their cyber team headcount

Only 27%

are actively implementing post-quantum cryptography (PQC) solutions

Source: KPMG cyber and technology risk survey, 2026

Introduction: A new mandate for the CISO

In an environment where 74 percent of security leaders have experienced a slight increase in cyberattacks and another 9 percent have seen a significant increase, the key question clearly is not if a breach will occur, but how prepared the organization will be when it does.

The modern CISO operates at a crossroads of immense technological opportunity and unprecedented risk. This requires a fundamental evolution of the CISO role itself, from that of a pure technologist to one of a business leader and, critically, a storyteller who can translate complex threats into a business context.

CISOs are under intense pressure to not only defend the enterprise but also to reframe their own strategic value. This requires articulating their purpose in a new, more dynamic way. The CISO's role is now that of a strategic facilitator of secure innovation, whose mission is to help the business move at speed in a trusted, safe manner.

To navigate this landscape, CISOs must embrace pragmatic automation, cultivate a deeply embedded security-aware culture, and master the foundational elements of a modern security architecture.

"Framing cybersecurity as generic 'business enablement' is outdated. The real mandate is speed with safety—helping the business move fast, pursue growth, and scale confidently without compromising trust or resilience."

Charles Jacco
Principal, Cybersecurity & Technology Risk
KPMG LLP

1 Confronting the paradox of AI technologies

Our survey results reveal a fascinating dichotomy in how security leaders view AI. On the one hand, AI-powered attacks are the most anticipated cyber threat over the next two to three years. On the other, leaders see AI as the most effective technology for future defense, with 57 percent pointing to its power in fraud prevention and 56 percent in predictive threat analytics.

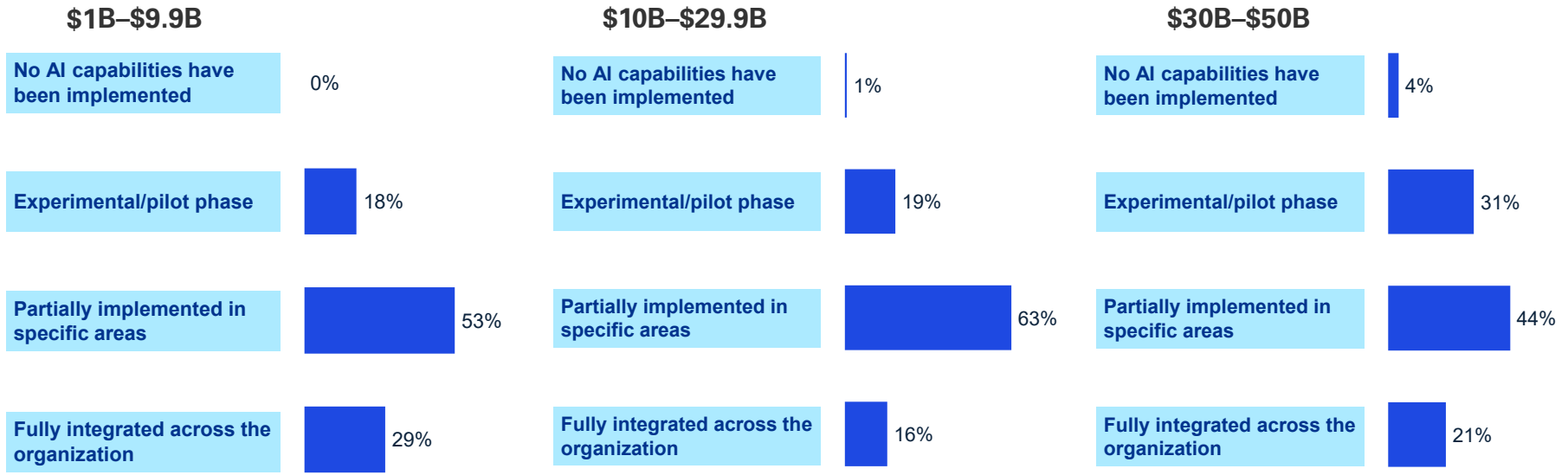
This is the frontline of the new cybersecurity arms race. The core challenge for CISOs is navigating the tension between the business's need to innovate with AI at speed and the security team's mandate to protect the organization and build trust in AI technologies. CISOs can't afford to be seen as an impediment to innovation, but the risks of ungoverned AI adoption are significant.

The integration of AI is an important indicator of security maturity, yet adoption levels differ. Among our survey respondents, just 24 percent (33 percent in the consumer and retail (C&R) sector) have "fully integrated" AI in cybersecurity; 53 percent have "partially implemented" it in specific areas. Also, 29 percent of organizations with $1 billion-$9.9 billion in revenue have fully integrated AI, more than other revenue categories. Larger organizations are more likely to be in the evaluation phase.

The top challenge to AI adoption remains trusting that AI applications are accurate, reliable, and explainable. Building trust requires identifying specific, high-value use cases where AI can solve a concrete problem, such as reducing complexity in the IT environment. It's about applying AI pragmatically, not just theoretically.

Maturity level of AI integration

AI integration and deployment across cybersecurity function by revenue



Nearly 30 percent of smaller organizations have fully integrated AI, while more midsize companies have only partially done so, indicating momentum but room for full-scale implementation.

N = 119 | N = 98 | N = 84

Source: KPMG cyber and technology risk survey, 2026 | Percentages may not add up to 100 due to rounding.

Ranked challenges of using AI in cybersecurity

1. Trusting that AI recommendations are accurate, reliable and explainable
2. Lack internal knowledge and difficulty in demonstrating ROI
3. Massive effort required to set up and train AI solutions

> *"Managing AI-related cyber risk requires a proactive, strategic approach to governance and compliance. When done well, it enables CISOs to protect the business, anticipate emerging threats, and prevent small issues from becoming material problems."*

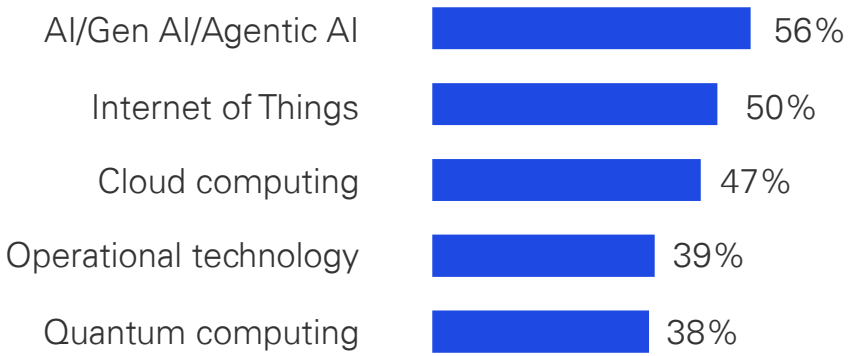
Michael Gomez
Principal, Cybersecurity & Technology Risk, KPMG LLP

Our respondents' anxiety over sophisticated threats is clearly not abstract. It is directly tied to the specific assets and operations that define an organization's business model. When asked about the consequences of a breach, leaders cited reduced productivity, erosion of customer trust, theft of intellectual property, and supply chain disruptions as the most significant negative impacts.

It is worth noting that different industries have varying priorities. For C&R leaders, the top concerns are reduced productivity (53 percent) and loss of revenue (45 percent). In contrast, financial services (FS) firms, which operate as critical nodes in a vast economic network, cite supply chain and communications disruption (50 percent) and loss of customer trust and a decrease in brand value (47 percent). This indicates that while the threat vectors may be similar, business context dictates which risks are deemed most critical to overall safety.

Source: KPMG cyber and technology risk survey, 2026. Weighted average of the ranks has been calculated by assigning 50% weight to Rank 1, 30% to Rank 2, and 20% to Rank 3. Top ranks are based on figures rounded to two decimal points, with data having higher decimal precision within the same percentage considered higher. N = 310

Top high-impact emerging-technology threats



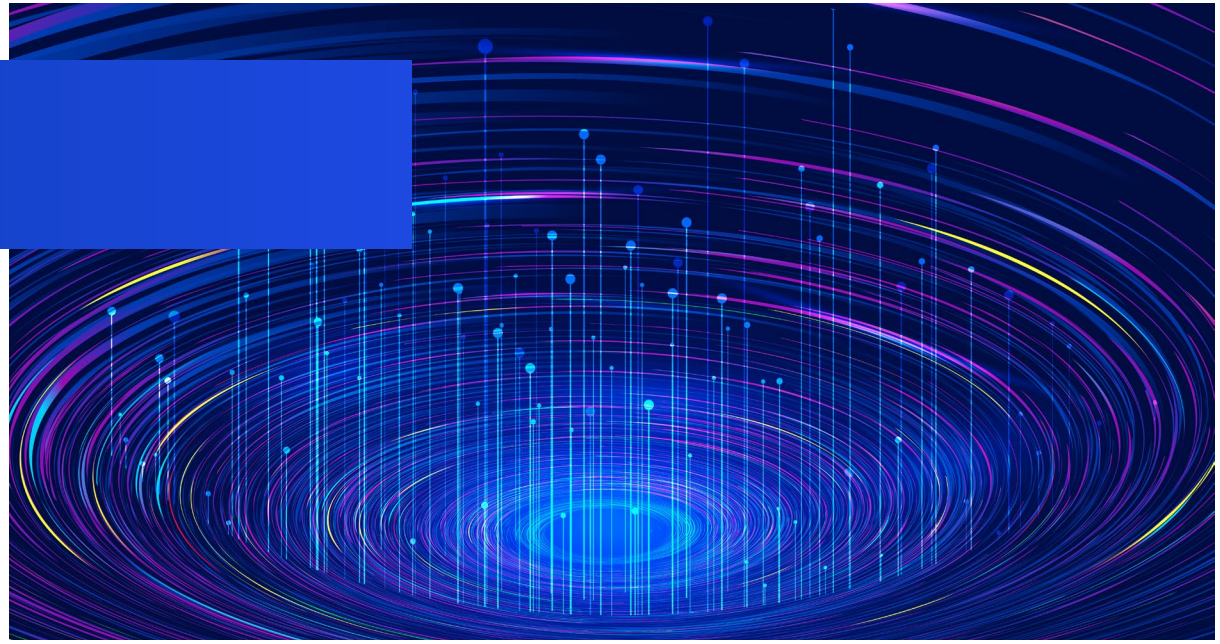
Source: KPMG cyber and technology risk survey, 2026

Multiple responses allowed.

"A key practical application for AI in security is not just threat detection but identifying and reducing complexity within the IT environment itself—because complexity is the enemy of security."

Matthew P. Miller
Principal,
Cybersecurity & Technology Risk,
KPMG LLP

2 Predict, don't react: Unifying security architecture



Despite rising investment in cybersecurity, most organizations largely remain in a reactive security posture. Making the pivot to a proactive, predictive, and risk-driven approach is no longer an aspiration—it is a critical strategic imperative.

The push to adopt AI, despite its inherent risks, is fueled by a clear vision of its transformative potential. However, becoming consistently proactive is not a function of simply buying more tools. It requires a fundamental shift in security architecture. Our survey reveals that only 14 percent of organizations claim to have achieved an advanced, predictive state of vulnerability management. The primary barriers are the complexity of IT infrastructure (47 percent) and fragmented security systems (45 percent).

This fragmentation is the core of the problem. The path forward requires a convergence of security operations center (SOC) actions and continuous threat exposure management to yield more proactive and targeted cyber defense capabilities. Centralizing disparate data sources and creating an inventory of cybersecurity assets can reduce silos and provide a clear view of the enterprise environment.

For organizations that lack the resources to undertake such a massive architectural lift, utilizing a MSP can be a powerful accelerator, offering access to a preintegrated security platform and the expertise to manage it effectively.

> *"Effective cyber operations require enterprise-wide visibility, extensive and continuous situational awareness of exposures, and monitoring and responding to suspicious activity targeted at exploiting defense gaps. The desired state of cyber operations is to anticipate, discover, validate, and defend by means of advisor-led, AI-powered cyber initiatives."*

Chris Crevits
Principal,
Cyber Managed Services,
KPMG LLP

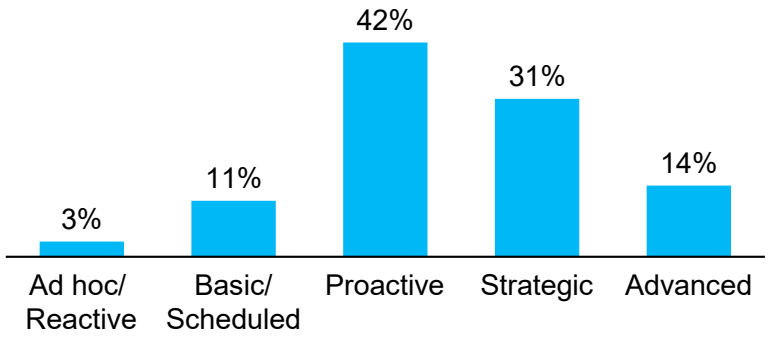
Most anticipated AI-driven improvements in cybersecurity

57%
Fraud prevention

56%
Predictive analytics to identify potential threats

53%
Better threat detection and response, and identifying anomalies

Threat vulnerability management approach



Only a small fraction of organizations, 14 percent, are capable of anticipating rather than just reacting to threats.

Source: KPMG cyber and technology risk survey, 2026 | Percentages may not add up to 100 due to rounding.

"The architectural aspect of cyber planning and ongoing management is critical. Organizations can't do advanced detection or effectively utilize AI without ensuring their data is clean, organized, and accessible. It's the foundational move."

Matthew P. Miller
Principal,
Cybersecurity & Technology Risk,
KPMG LLP

Investing in the fundamentals: A data-centric approach

Mastering the fundamentals of architecture and data is a prerequisite for achieving the operational speed needed to outpace adversaries and ensure the safety of critical assets. Our survey data highlights a direct correlation between the two objectives—organizations with high cybersecurity maturity are nearly twice as likely to experience zero breaches (22 percent) compared to those with moderate maturity (12 percent).

CISOs are directing their growing budgets toward the foundational pillars of a more mature security program, with data security and privacy leading the way. This aligns with a critical security principle: The last line of defense is effective data privacy and protection. Before an organization can grant an AI model access to its information, it must first know where that sensitive data is located and how it is controlled.

But even as they shore up the fundamentals, CISOs and other cyber leaders must look to the horizon. The survey finds that leaders see emerging technologies such as quantum computing as a significant future threat. While it may seem like a distant consideration, the challenge of post-quantum cryptography (PQC)—existing cryptography that can protect current systems and data from future quantum computing risks[1]—is that adversaries can "harvest now, decrypt later," meaning encrypted data stolen today could be read by a quantum computer in the future.

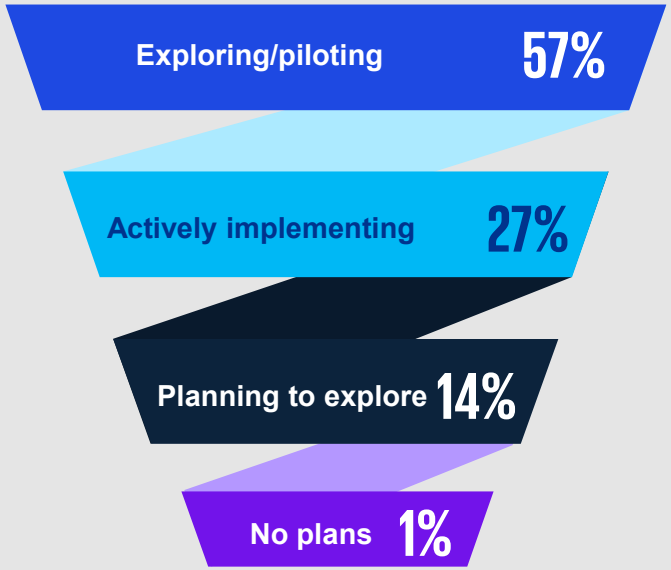
This creates a difficult justification for CISOs to make to senior management and boards: committing significant resources now to prevent a problem that may be years away.

> *"Securing investment for risks that may be years away requires sustained board education—particularly around long-term exposure and the cost of acting too late. Upcoming regulatory requirements for post quantum cryptography and other emerging technologies are likely to be the forcing mechanism that moves organizations from awareness to action."*

Mick McGarry
Cybersecurity & Technology Risk, KPMG LLP

[1] KPMG, 2025 Futures Report.

Post-quantum cryptography adoption status



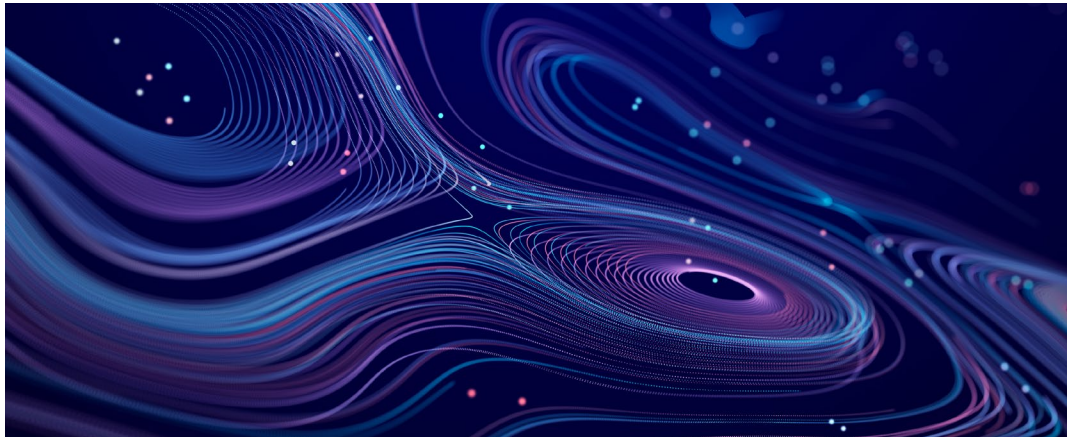
42 percent of C&R organizations are "actively implementing" post-quantum cryptography, the highest among all categories

Source: KPMG cyber and technology risk survey, 2026 | Percentages may not add up to 100 due to rounding.

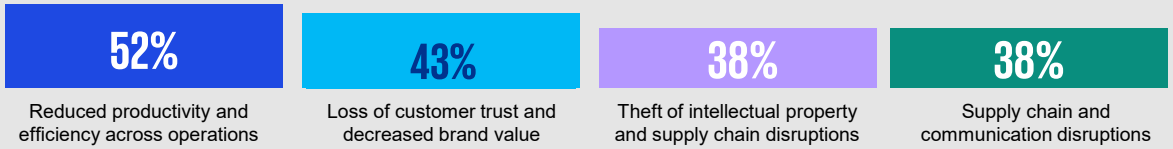
3 Translating security into strategy: The board conversation

A recurring theme from the survey is the recognition that CISOs can no longer rely on technical acumen alone. The modern CISO also must be a masterful communicator who can bridge the gap between the security operations center (SOC) and the boardroom. This means translating complex technical details into the language of business implications and risk.

Forty-two percent of our respondents say they have difficulty demonstrating the ROI of cybersecurity investments. To secure investment and strategic alignment, the conversation with the board cannot be about patching vulnerabilities. It must be about protecting the business from the impacts that survey respondents cite as most damaging: reduced productivity, erosion of customer trust, theft of intellectual property, and supply chain disruption.



Damaging impacts of cyberattacks on organizations



The impact of reduced productivity is particularly pronounced among TMT (57 percent) and C&R (53 percent) organizations, while more FS firms (50 percent) report supply chain and communication disruption as the top impact area.

The key is determining, in collaboration with the business, which risks matter most and illustrating how they relate to financial and operational objectives. This is how CISOs can effectively pursue resilience: establish disciplined, repeatable operational cyber processes despite inevitable disruptions. Creating a common language for risk and resilience enables consistent discussion at the executive and board levels, sets a measurable basis for risk appetite across the enterprise, and directs investment where it can have the greatest effect.[2] Ultimately, a successful board conversation results in strategic investment.

[2] KPMG, Cyber Risk Insights, CRQ Accelerator, From guess work to governance, 2026.

Source: KPMG cyber and technology risk survey, 2026

Focus areas for cybersecurity budget increases

Current priorities for cybersecurity investments

1. Data security and privacy
2. Threat intelligence and detection
3. Cloud security

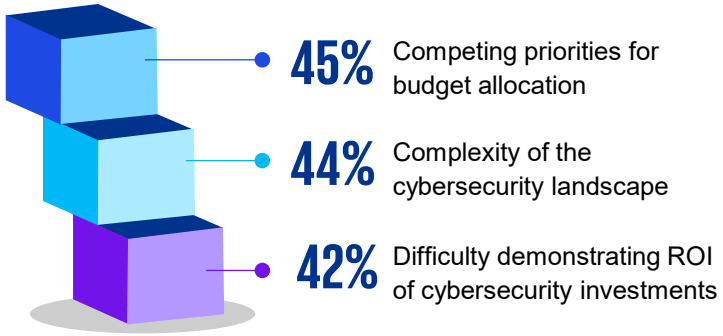
Based on weighted average score[b]

Priorities for cybersecurity investments in next 2-3 years

1. Data security and privacy
2. Cloud security
3. Threat intelligence and detection

Based on weighted average score[b]

Top three challenges to obtaining funds for cybersecurity



45% Competing priorities for budget allocation

44% Complexity of the cybersecurity landscape

42% Difficulty demonstrating ROI of cybersecurity investments

Source: KPMG cyber and technology risk survey, 2026. Data represents weighted average of the ranks that has been calculated by assigning 50% weight to Rank 1, 30% to Rank 2, and 20% to Rank 3. Top ranks are based on figures rounded to two decimal points, with data having higher decimal precision within the same percentage considered higher.

The power of focused metrics

An essential part of creating a clear narrative is moving away from overwhelming dashboards. While operational metrics, such as the number of security incidents (employed by 53 percent of respondents), vulnerability remediation rate (52 percent), and mean time to detect (51 percent), are vital for the security team, they often fail to resonate with nontechnical boards. Rather, we believe CISOs should focus on a few key performance indicators that clearly articulate the health of the security program's impact on the business, such as dwell time, patching cadence, and phishing success rates.

For at least 20 years, CISOs and their teams have been reporting on metrics that have a certain validity but are very point-in-time related. The conversation needs to change to how an organization's cyber investments are reducing risk over time.

> *"Effective threat response is measured by outcomes, not activity. Dwell time—how long an attacker remains in the environment—has emerged as a critical metric for demonstrating cyber ROI and the SOC's ability to detect and remove threats while protecting critical assets."*
>
> **Charles Jacco**
> Principal,
> Cybersecurity & Technology Risk,
> KPMG LLP

The good news is that this shift is already happening. More than half of organizations (53 percent) are now using threat intelligence platforms and nearly as many (49 percent) are using formal risk quantification methodologies such as FAIR (Factor Analysis of Information Risk) to translate technical findings into financial and operational risk terms that a board can understand and act upon.

Metrics to measure effectiveness of cybersecurity programs

Source: KPMG cyber and technology risk survey, 2026

> *"Compliance does not equal security. Organizations that treat a single regulation or metric as a proxy for cyber readiness create blind spots. Strong security comes from operating the business efficiently and effectively day to day, with compliance following as a result."*

Michael Gomez
Principal, Cybersecurity & Technology Risk, KPMG LLP

4 The human element: Bridging the talent and identity divide

The effectiveness of any cybersecurity program is fundamentally limited by the professionals who manage it and the employees who must adhere to its principles. Our survey respondents cite a lack of qualified professionals (53 percent) and insider threats/employee awareness gaps (51 percent) as their top two high-impact cybersecurity challenges, highlighting that the human factor remains a central variable in the security equation.

The persistent talent shortage

The difficulty of attracting and retaining skilled cybersecurity professionals remains a primary obstacle to achieving operational speed and scale. As a direct response, organizations are increasingly turning to AI and automation to augment their teams. The goal is not necessarily to replace people but to empower them by automating laborious tasks and freeing human analysts for more strategic work.

Despite the march toward AI adoption, the demand for human proficiency is expanding, with many organizations expecting to grow their security teams. Indeed, 74 percent of organizations anticipate an increase of more than 11 percent in their cybersecurity team's headcount over the next two to three years.

Notably, a hybrid approach seems to be taking hold. Considering respondents' acknowledgment of a lack of qualified cyber professionals and the specter of insider threats—most of which are not intentional or malicious—and employee awareness gaps, it's not surprising that many organizations are turning to MSPs. A substantial 41 percent of survey respondents say they are engaging with partners specifically to enhance their cyber expertise and capabilities.

> *"With cyber talent being scarce and expensive, modern managed services provide advanced capabilities, continuous innovation, and on-demand expertise that reinforce internal teams and may improve security outcomes."*
>
> **Chris Crevits**
> Principal,
> Cyber Managed Services,
> KPMG LLP

Top three high-impact cybersecurity challenges

Financial services

53%
Lack of qualified professionals

51%
Insider threats and employee awareness gaps

49%
Technological integration issues and geopolitical risks

Consumer and retail

58%
Lack of qualified professionals

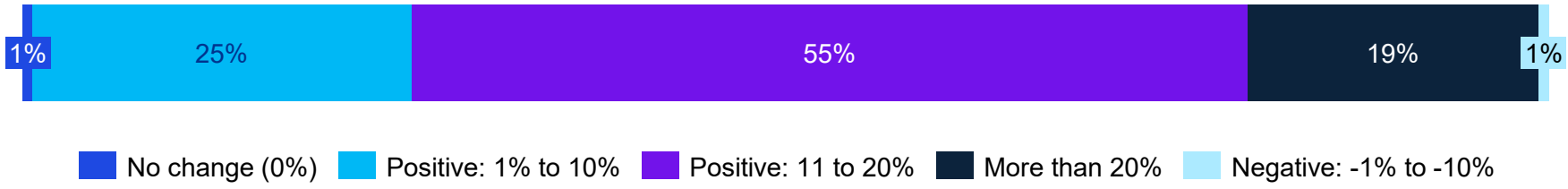
56%
Evolving regulatory/ compliance landscape

55%
Insider threats and employee awareness gaps

Organizations reporting a lack of qualified professionals cite "difficulty attracting qualified candidates due to competitive market" as a key factor limiting their ability to maintain optimal cybersecurity staffing levels.

Source: KPMG cyber and technology risk survey, 2026

Anticipated percentage change in cybersecurity teams' headcount over the next 2–3 years



The rise of nonhuman identities

While human talent is one side of the coin, the definition of "identity" itself is the other. A critical and often overlooked aspect of this dynamic landscape is the rise of nonhuman identities (NHIs), which now outnumber human users 82 to 1.[3] NHIs are digital credentials such as service accounts, API keys, open authorization tokens, machine credentials, and autonomous AI agents, often created by business users outside of traditional IT processes and establishing a massive, often poorly governed attack surface.[4] NHIs operate continuously across SaaS, cloud, on-premises, and third-party integrations, often with privileged access and minimal oversight.

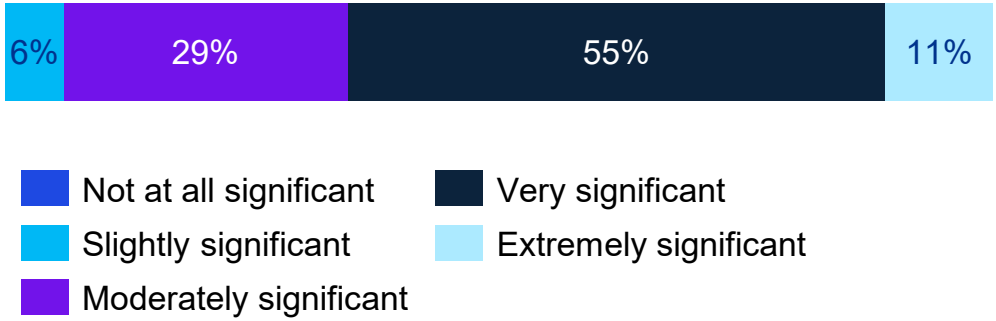
Our survey respondents have taken notice of the increasing security risks NHIs represent, with 60 percent characterizing it as either very or extremely significant. Smaller firms with revenue of $1 billion to $9.9 billion and larger firms with revenue of $30 billion to $50 billion are most concerned, with two-thirds citing the risk as very or extremely significant. For their part, half of midsize companies attribute this level of concern to NHIs.

[3] CyberArk, "Machine Identities Outnumber Humans by More Than 80 to 1: New Report Exposes the Exponential Threats of Fragmented Identity Security," April 23, 2025.

[4] KPMG, "Invisible access, visible risk: making non human identities a cybersecurity priority," 2026.

Source: KPMG cyber and technology risk survey, 2026 | Percentages may not add up to 100 due to rounding.

Significance of NHI proliferation



"We've got an entire universe of machine-based identities that doesn't follow controlled provisioning processes as humans do. And it's growing exponentially with the adoption of generative AI, making it harder to track, manage, and trust."

Mick McGarry
Cybersecurity & Technology Risk, KPMG LLP

Source: KPMG cyber and technology risk survey, 2026 | Percentages may not add up to 100 due to rounding.

What's next for the CISO?

The findings in this report make one thing clear: The old paradigms of cybersecurity are no longer sufficient. The modern CISO is tasked with defending an expanding and evolving digital frontier. The journey from a reactive to a predictive security posture is challenging but essential. Simply bolting on another tool only adds to the cacophony of siloed systems and fails to address the challenges of architectural complexity, the explosion of NHIs, and the dual-use nature of AI. These are not individual problems to be solved. Rather, they are interconnected forces that are fundamentally reshaping the risk landscape.

Why does this matter? Because in an era where cybersecurity is a top concern for chief executives, the CISO is at a critical fork in the road. The choice is between two distinct paths: one that leads back to a reactive posture, buried in the fog of endless security alerts, and another that leads forward in a direction defined by a unified data architecture, a strategy for building trust in AI, and the ability to translate the language of vulnerabilities into the language of business value.

This is the difference between being a cost center and being a strategic partner. The ultimate takeaway is that the CISO must evolve from being a defender of technology into a protector of business value.

The following action steps are not just a security checklist; they are also a guide to embedding this mission into the heart of your organization.

- **Establish a formal AI security and governance program.** Champion AI as a force multiplier for your team, not as a silver bullet. Build trust and ensure operational safety by implementing a robust framework for testing models and ensuring a "human in the loop" for all critical decisions.
- **Focus on foundational "blocking and tackling."** While emerging threats are important, mastering the fundamentals of data protection and identity governance provides the strongest defense against most cyberattacks.
- **Build a unified security data architecture.** Break down the silos among your security tools. A unified data lake is the foundation for achieving the analytical speed and clarity needed to stay ahead of adversaries in the AI offense/defense arms race.
- **Govern all identities, human and nonhuman.** The exponential growth of machine identities requires a new governance model. CISOs are encouraged to work with the business to establish controlled processes for provisioning and monitoring these identities to close a rapidly expanding security gap.
- **Start planning for a post-quantum world.** Begin the journey of quantum readiness by creating an inventory of your cryptographic systems and developing a multi-year roadmap for migration. Educate your board on the "harvest now, decrypt later" threat to secure the necessary long-term investment.
- **Vet your partners for deep technical expertise.** As you increasingly rely on MSPs and consulting firms, prioritize partners based on their expertise and their AI/automation capabilities. Ask the hard questions to determine if a partner can truly help you achieve your goals for speed and safety.

> *"Many companies still perceive the CISO as a business blocker. When CISOs aren't seen as collaborative partners who enable innovation safely, they risk losing their seat at the table, literally and figuratively. Projects move forward without them—in the shadows, and the organization becomes less secure, the exact opposite of the CISO's mission."*

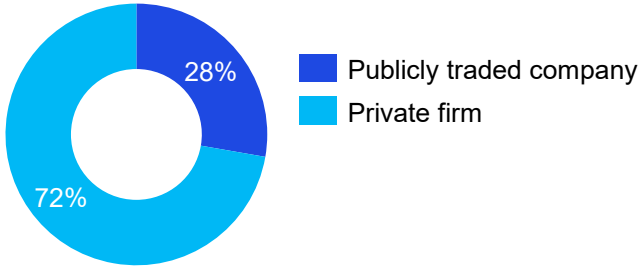
Michael Isensee
Partner, US Leader,
Cybersecurity & Technology Risk,
KPMG LLP

About the research

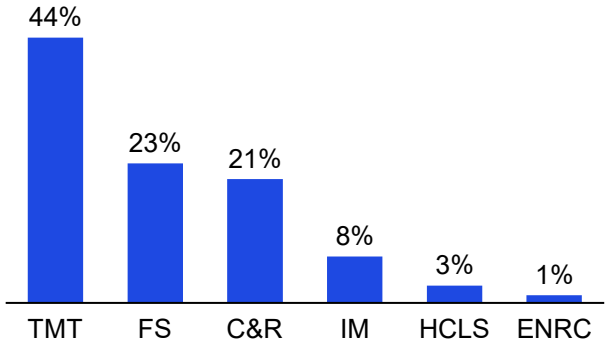
N=310

Respondent headquarters

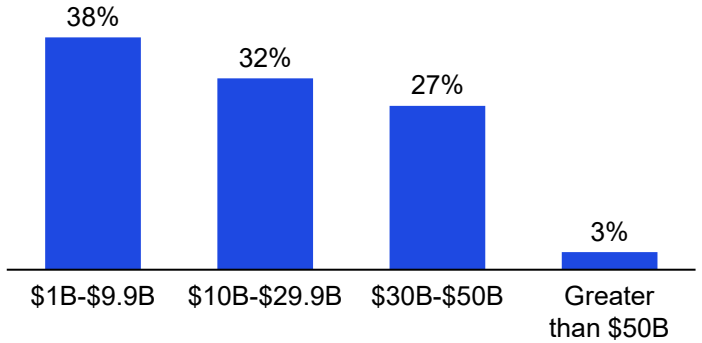
Respondent organization type.[a]



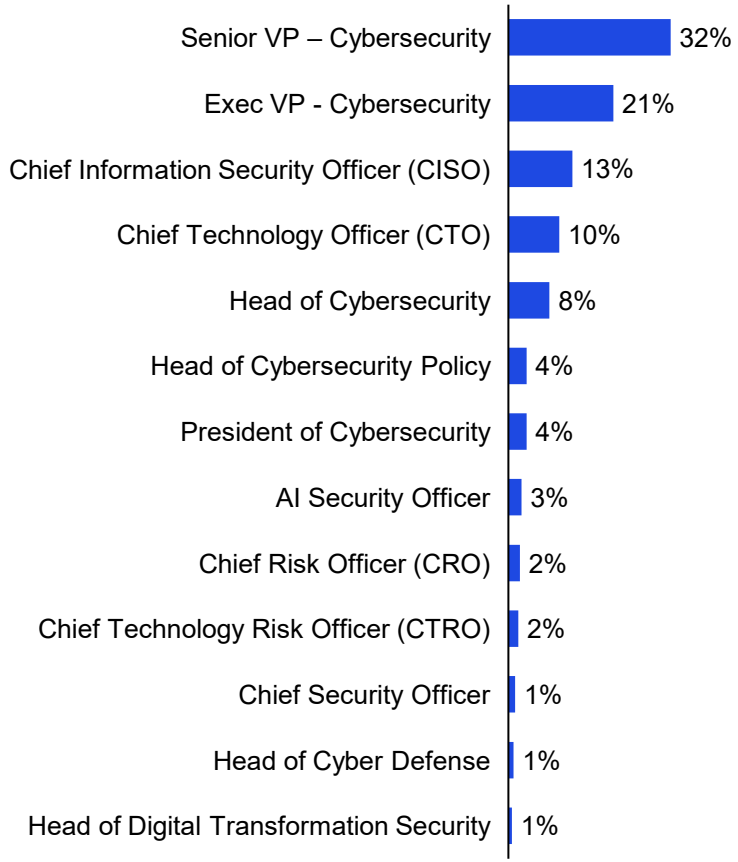
Industries[a]



Annual revenue[a]



Respondent roles[a][b]

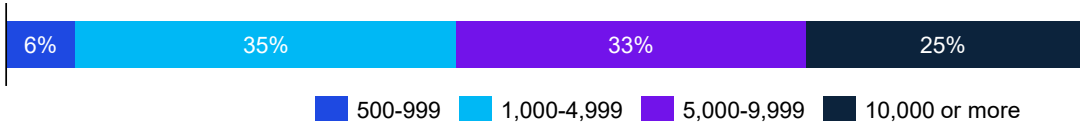


Note(s): (a) Sum of percentages may not add up to 100 due to rounding. (b) Some of the options are not included in the graphical representation, due to zero respondents

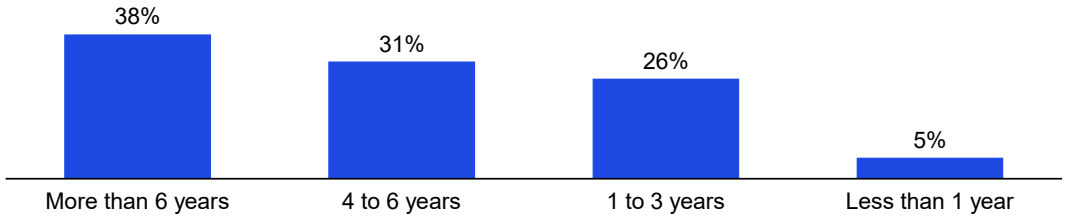
Source: KPMG cyber and technology risk survey, 2026

N=310

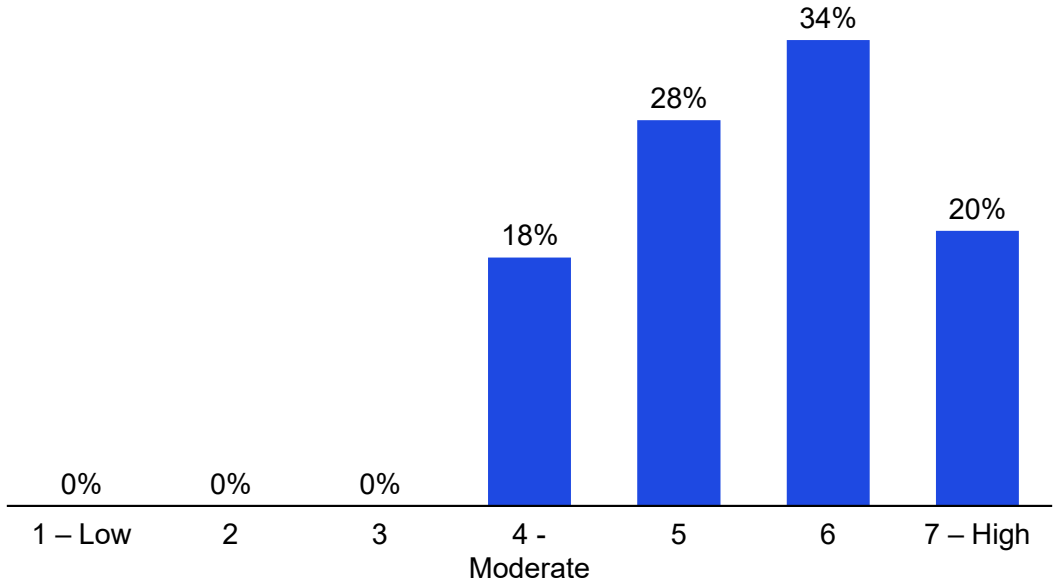
Respondent organization employee size[a]



Respondent length of service with organization



Current cybersecurity maturity level



Methodology

The KPMG Cyber and Technology Risk Survey was conducted online in the US in October 2025. Respondents included 310 security leaders from public and private organizations with revenue of $1 billion or more. The sample included chief information security officers (CISOs), heads of cybersecurity, and chief technology officers (CTOs). A mix of industries was represented in the survey. The research objective was to understand cybersecurity leaders' priorities and perspectives on the evolving threat landscape, the impact of emerging technologies such as generative AI/agentic AI, cyber risk preparedness, cybersecurity challenges and mitigation strategies, budget priorities, and outlook for the future.

Note(s): (a) Sum of percentages may not add up to 100 due to rounding.

Source(s): Cyber and Technology Risk Survey, Oct'25

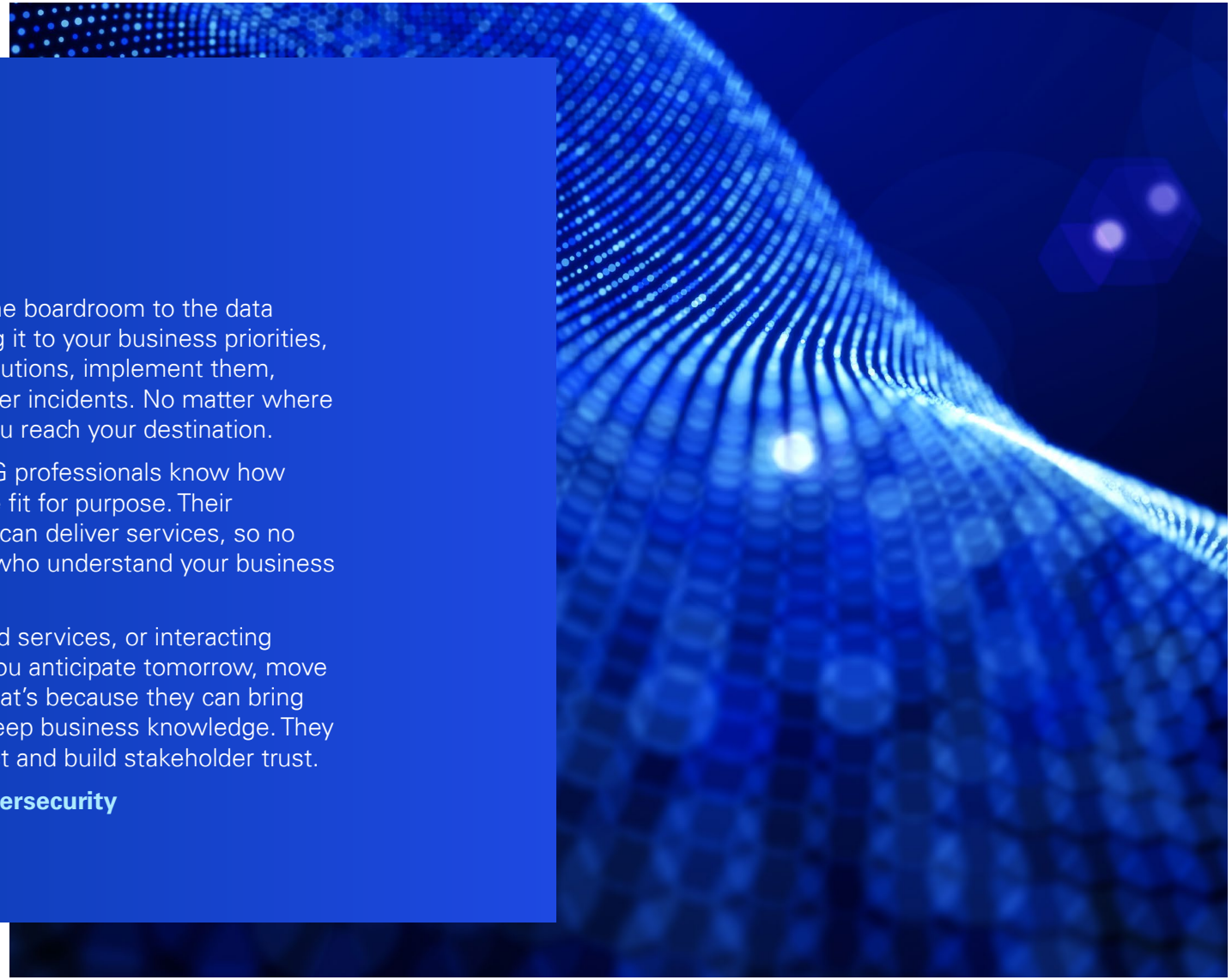
How KPMG can help

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 and deep business knowledge. They are creative professionals passionate about helping you protect and build stakeholder trust.

KPMG. Make the Difference. Learn more at kpmg.com/cybersecurity



Meet the authors

For more information, contact us:

Michael Isensee

Partner, US Leader, Cybersecurity & Technology Risk, KPMG LLP
misensee@kpmg.com

Michael leads the KPMG US Cyber and Technology Risk practices. With 30 years of experience and an international background in IT risk management, he specializes in driving the modernization of technology programs, including automation and AI.

Chris Crevits

Principal, Cyber Managed Services, KPMG LLP
ccrevits@kpmg.com

Chris Crevits is the KPMG US principal advisor for solutions and technology. He supports organizations in designing resilient, agile, and cost-effective cybersecurity programs that align with their business objectives and risk appetite.

Michael Gomez

Principal, Cybersecurity & Technology Risk, KPMG LLP
michaelgomez@kpmg.com

Michael is the KPMG cybersecurity lead partner for Strategy, Governance, Risk & Compliance. His expertise includes advising organizations on enterprise cybersecurity governance, regulatory compliance, risk management, and control transformation.

Charles Jacco

Principal, Cybersecurity & Technology Risk, KPMG LLP
cjacco@kpmg.Com

Charlie is the KPMG US cyber threat management leader and global cyber managed services leader. He focuses on helping clients drive toward automation across complex cyber defense, cyber response, and device security transformational programs.

Mick McGarry

Principal, Cybersecurity & Technology Risk, KPMG LLP
hmcgarry@kpmg.com

Mick is the KPMG US leader for cybersecurity protection services. His focus areas include identity and access management, ERP security and controls, data privacy and protection, platform security, securing AI, and quantum security.

Matthew P. Miller

Principal, Cybersecurity & Technology Risk, KPMG LLP
matthewpmiller@kpmg.com

Matthew is the KPMG global cybersecurity industry leader for financial services. His focus areas include insider threat and internal fraud, third-party risk, quantitative and qualitative risk assessment, and incident management.

We would like to thank our contributors: Kathleen Nichols, Rama Ramaswami, Constance Thaete, Michael Thayer, and Christopher Thomas.

Related insights

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

Please visit us: | **kpmg.com** | **Subscribe**