



Closing the cyber resilience gap

How CISOs can build a cybersecurity
operating model that converts investment
into measurable performance

Executive summary

Cybersecurity has reached a point where maturity can no longer be judged by how much coverage an organization has built. Many large enterprises have expanded telemetry, strengthened identity programs, formalized incident response plans, improved cloud controls, and elevated cyber risk to the board. Yet the operating environment continues to stretch the model those investments depend on. Threats are moving faster, digital ecosystems are more interdependent, and AI is changing both attack patterns and defensive expectations.

That is the cyber resilience gap: the distance between the capabilities organizations have accumulated and the consistency with which those capabilities perform when the business is under pressure. For CISOs, the issue is no longer whether the program has enough components. It's whether those components can work together when AI-driven threats, identity exposure, third-party dependencies, cloud complexity, and business disruption converge.

The pressure is visible. The KPMG 2026 Cybersecurity & Technology Risk (CTR) survey of 310 security leaders found that eight in ten organizations experienced an increase in cyberattacks over the past 12 months, with phishing, denial-of-service, and ransomware among the most common attack types. AI-powered attacks are expected to become the top cyber threat in the next two to three years, yet only 24 percent of organizations have fully integrated AI into cybersecurity functions. Only 25 percent are actively implementing post-quantum cryptography, and only 48 percent say they are well prepared for quantum threats.

The stronger response is not simply more tools or more activity. It's a cybersecurity operating model designed to reduce variability, accelerate decisions, strengthen identity and ecosystem visibility, operationalize incident response, and give leadership clearer evidence that resilience is improving.

Why cybersecurity performance matters more than coverage

Cybersecurity has reached a point where maturity can no longer be inferred from the size of the control estate, the sophistication of the tool stack, or the amount of activity flowing through the security organization. Many large enterprises have expanded telemetry, strengthened identity programs, formalized incident response plans, improved cloud controls, and elevated cyber risk to the board.

Yet the operating environment continues to stretch the model on which those investments depend. Threats are moving faster, digital ecosystems are more interdependent, and AI is changing both attack patterns and defensive expectations. Leadership

is asking for clearer proof that cybersecurity investments are improving resilience, not simply expanding coverage.

This is the cyber resilience gap: the widening distance between the capabilities organizations have accumulated and the consistency with which those capabilities perform when the business is under pressure. For CISOs, the issue is no longer whether the program has enough components. It is whether the system connecting those components can deliver repeatable outcomes when AI-driven threats, identity exposure, third-party dependencies, cloud complexity, and operational disruption converge.

Why cyber resilience is becoming the new test of security ROI

The cybersecurity ROI question has moved from spend justification to performance proof. Boards are not simply asking whether the organization has enough tools, controls, or coverage. They are asking whether those investments are reducing business disruption, improving response consistency, and giving leadership clearer evidence that resilience is improving.

The CTR survey makes that pressure clear. Eight in ten organizations report an increase in cyberattacks over the past 12 months, with phishing, denial-of-service, and ransomware among the most common attack types. Productivity is the most common business impact, with more than half of organizations reporting significant effects from cyberattacks.¹

Those numbers matter because they connect cyber risk directly to business performance. When attacks affect productivity, supply chain continuity, customer trust, or operational uptime, cybersecurity stops being measured only as a defensive function. It becomes part of how the business protects value.

The uncomfortable question is not whether organizations have invested. Many have. The question is whether those investments have reduced the variability that shows up when a serious incident cuts across identity, cloud, third parties, business operations, legal, communications, and executive decision-making. A more useful ROI conversation asks whether the organization can detect faster, respond more consistently, limit business impact, and prove that resilience is improving over time.

The path forward starts by naming the real issue: the cyber resilience gap. Many cybersecurity programs have expanded their capabilities faster than they have modernized the operating model that connects those capabilities into measurable resilience. The CISO's challenge is not only managing each domain, but ensuring the operating model can coordinate across them before a threat expands into a business impact

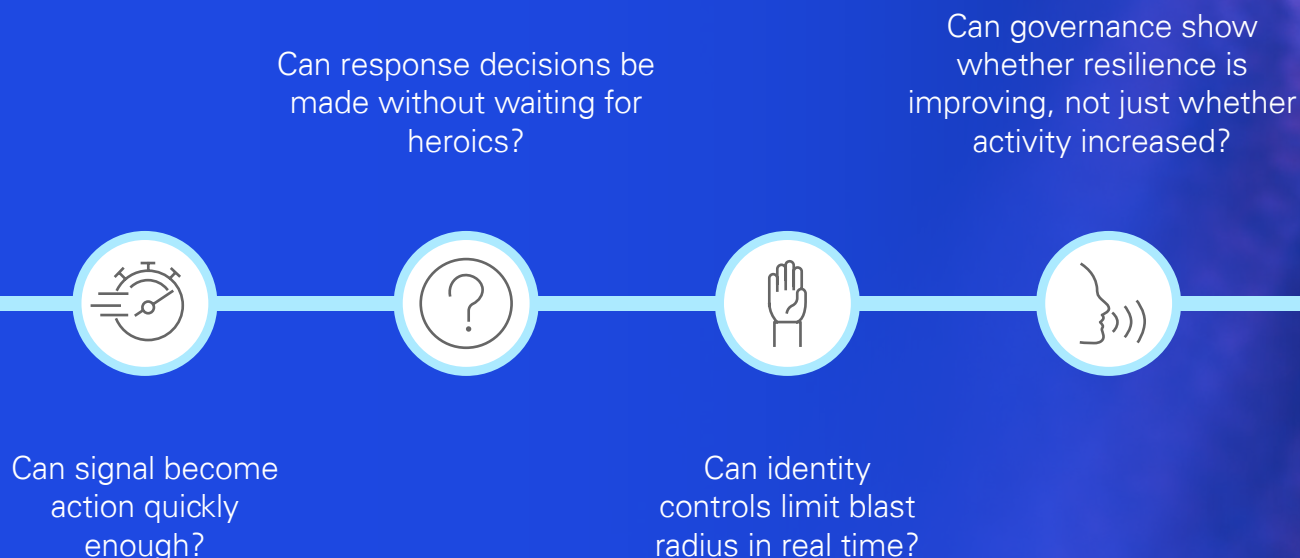
¹2026 KPMG Cybersecurity and Technology Risk Survey

When cyber posture looks strong but incident performance still breaks down

Many organizations have improved their cyber posture on paper: more tools, more coverage, more policies, more dashboards, more control evidence. But incidents do not test posture in isolation. They test whether identity, detection, response, governance, third-party coordination, communications, and recovery can work together under pressure.

That is where the cyber resilience gap often appears. A program can look mature in regard to control coverage and still struggle when an incident crosses cloud, identity, third parties, business operations, legal, communications, and executive decision-making at once. The question for CISOs is no longer only “Do we have the right controls?” It is “Can those controls produce consistent outcomes when the business is under stress?”

A stronger resilience lens asks:



Assess where cyber resilience breaks down across detection, response, identity, and governance

Achieving resilience means identifying where the security model depends on manual judgment, fragmented ownership, or retrospective reporting at the moments when consistency matters most. A cybersecurity program may appear mature on paper but still have resilience gaps if you cannot answer these questions with confidence:

Question

- Can detection reliably lead to prioritized action?
- Can response teams execute consistently across business units?
- Is privileged access continuously governed?
- Can leadership see whether resilience is improving?
- Are third-party dependencies part of response planning?
- Is quantum readiness being staged before urgency forces action?

Why it matters

- Visibility does not reduce risk unless signals become decisions.
- Resilience depends on repeatability, not individual heroics.
- Identity is often the path from initial compromise to business impact.
- Boards need evidence of performance, not just descriptions of activity.
- External exposure can initiate internal disruption.
- Cryptographic migration is too complex to defer until pressure peaks.

The value of this diagnostic is not in turning resilience into another checklist. It's in showing where the security model still depends on manual judgment, fragmented ownership, or retrospective reporting at the moments when consistency matters most.



Modernize cybersecurity operations for AI-driven threats and AI-enabled business

The most visible effect of AI is acceleration: more convincing social engineering, faster reconnaissance, greater attack variation, and the ability to scale targeting more efficiently. That matters, but the deeper issue is the way AI changes the conditions under which cybersecurity operates.

The paradigm shift is that AI destroys the defender's time advantage. Adversaries are using autonomous bots to map vulnerabilities and exploit supply-chain weaknesses faster than enterprise patch cycles can trigger. They are leveraging generative AI to craft hyper-personalized, multilingual campaigns that bypass traditional email gateways without human intervention.

This creates a dual challenge. Security teams must defend against adversaries using AI to compress the time between targeting and impact, while also helping the enterprise adopt AI without creating unmanaged exposure. The business is racing to deploy large language models (LLMs), autonomous agents, and AI copilots. This introduces novel risks—prompt injection, training data poisoning, and the inadvertent leakage of proprietary data through unsanctioned “Shadow AI”—that legacy security tools simply cannot monitor.

The 2026 CTR survey reflects this tension. Organizations expect AI-powered attacks to become the top cyber threat in the next two to three years, while nearly 70% already dedicate more than 11% of cybersecurity budgets to AI-related initiatives. Yet only 24% have fully integrated AI into cybersecurity, and 53% remain in partial integration.²

Taken together, these signals suggest that many organizations are moving toward AI-enabled cyber defense before they have fully modernized the operating model required to use it well. That creates a risk of misalignment: investment rises and capability

expands, but the underlying problems of inconsistent triage, fragmented ownership, manual handoffs, and uneven governance remain largely unresolved.

The workforce challenge reinforces the same point. Lack of qualified professionals, insider threats, and technology integration issues are among the top high-impact challenges reported by organizations, and 74% anticipate cybersecurity headcount growth of more than 11%.³ More headcount may increase capacity, but if the operating model remains highly manual and siloed, additional capacity does not automatically equate to resilience. The bigger question is around where the model still requires human effort because workflows, automation, governance, or operating discipline have not matured enough.

Bottom line, trying to hire your way out of an AI-driven threat landscape is a losing battle. Hiring remains important, but talent alone cannot solve a model problem. If skilled analysts are still expected to manually correlate alerts across disconnected tools, reconcile ownership across teams, and make high-consequence decisions without enough context, the organization has not solved the resilience gap; it has simply placed more pressure on its most valuable people.

A core issue for the modern Security Operations Center (SOC) is cognitive overload. Relying on overburdened analysts to manually correlate alerts across dozens of disconnected dashboards inevitably leads to alert fatigue, burnout, and critical threats slipping through the cracks. In an AI-driven threat environment, however, the real question is where human judgment adds the most value and where the operating model should be doing more of the work.

² 2026 KPMG Cybersecurity and Technology Risk Survey

³ 2026 KPMG Cybersecurity and Technology Risk Survey

Build a modern cybersecurity operating model for measurable resilience

To close the resilience gap, CISOs don't need to discard what they have built. Rather, they must find a different way to connect the capabilities they already have and a clearer view of where new capabilities must be added.

A modern cyber resilience operating model integrates domains that have often been managed separately: identity, threat detection, incident response, governance, security testing, third-party risk, platform security, data protection, and business continuity. The goal is to create a model that can continuously understand exposure, prioritize what matters, act consistently, and prove performance.

This shift from a capability-centric approach to a performance-centric model requires action across seven connected steps:

Step 1 Align cybersecurity to business operations and financial exposure

Resilience requires understanding how a cyber event disrupts specific business processes. The operating model must map critical business services to the technology, data, and third parties that support them, ensuring that detection, response, and recovery are prioritized by business impact, rather than technical severity alone.

Too often, security teams treat all critical vulnerabilities equally. A modern operating model demands a risk-based approach to resource allocation, conducting ongoing risk assessments to quantify exposures in financial terms. When a CISO can explicitly tie a cyber risk to potential revenue loss, regulatory fines, or a supply chain halt, the conversation with the board transitions from technical pleading to strategic business planning.

Step 2 Govern identity security continuously

Identity has become the control plane of modern cybersecurity. Privileged access, entitlements, non-human identities, and access pathways increasingly determine how quickly an attacker can move from foothold to business impact. Modern adversaries do not break through firewalls; they log in using compromised credentials.

In modern environments, reducing breach likelihood requires continuous oversight and automation across identity lifecycle and access governance—not periodic review alone. To harden this new control plane, organizations must implement advanced Privileged Access Management (PAM). By engineering an architecture built on Zero Trust principles—enforcing continuous authentication, context-aware access, and strict microsegmentation—you ensure that an initial compromise is boxed in, suffocating the attacker's ability to move laterally.

The machine identity blind spot

As enterprises adopt microservices and automated workflows, machine identities (API keys, certificates, service accounts) are proliferating at an uncontrollable rate. Unlike human users, machines don't use multi-factor authentication (MFA). If your IAM strategy isn't automatically discovering and rotating these non-human credentials, you are leaving your most critical pathways exposed.

Step 3 Secure the expanded attack surface: cloud, applications, and third parties

A modern operating model must account for an increasingly porous, borderless perimeter. System fragmentation and infrastructure misalignment often create critical blind spots.

Security engineering must shift left, implementing automated controls to maintain visibility and prevent misconfigurations across IaaS, PaaS, and SaaS environments. Simultaneously, safeguarding core enterprise applications (ERP, CRM) is paramount. However, resilience today is heavily dependent on the ecosystem. You can have a perfectly secured internal network, but if a key software vendor is compromised, your operations can be significantly impacted. CISOs must implement continuous third-party risk management strategies, moving beyond annual vendor questionnaires to dynamic, real-time ecosystem monitoring.

Third-party and supplier risk should be treated with the same continuity. A modern resilience model evaluates ecosystem risk through the lens of operational consequence: which providers are critical to continuity, which software dependencies could create cascading exposure, which third parties have access pathways that could become breach paths, and which vendors must participate in incident response.

Step 4 Modernize cyber detection, response, and incident readiness with AI

As the 2026 CTR survey confirms, fragmented security systems are a top hurdle to threat identification.⁴ In the age of AI-driven attacks, operational friction is a breach multiplier.

Organizations must transform their SOC from a reactive alert factory into a proactive, intelligence-driven nerve center. This is achieved through Managed Detection and Response (MDR) that leverages AI-assisted triage, playbook automation, and analytics-driven prioritization. AI must be deployed to fight AI, filtering out the noise of thousands of daily alerts so human analysts can focus on critical threat hunting and strategic containment.

Furthermore, as the enterprise deploys new digital agents, Managed Application Security Testing (MAST) provides continuous validation of applications and AI workflows. Integrating AI security testing allows organizations to validate tool boundaries and ensure vulnerabilities like prompt injection are caught before they reach production.

Step 5 Ensure business continuity through swift response and cyber recovery

Resilience is ultimately measured by how quickly organizations can take a punch and stand back up. When a major incident occurs, the primary impact is business disruption. The ability to minimize downtime, restore critical operations, and maintain customer trust is the true test of the operating model.

This requires mature cyber incident response and digital investigation capabilities to swiftly contain threats and conduct forensic analysis. But true resilience is built during peacetime. Organizations must conduct rigorous, cross-functional tabletop exercises and simulations.

These exercises build the necessary “muscle memory” across the executive suite, legal, PR, and technical teams, ensuring that when a crisis hits, everyone knows their precise role in facilitating a seamless restoration of operations.



⁴ 2026 KPMG Cybersecurity and Technology Risk Survey

Step 6 **Make cyber governance and IT risk measurable, continuous, and board-defensible**

You cannot manage what you do not govern. The rapid, often decentralized deployment of AI has created massive governance blind spots. Governance reporting is only valuable if it helps leadership understand whether risk is changing and whether resilience is improving.

Organizations must establish a converged risk operating model, adopting industry-accepted frameworks like the NIST AI Risk Management Framework (RMF) to define clear controls and escalation paths. Furthermore, the regulatory landscape is shifting dramatically, with new SEC disclosure rules and privacy mandates demanding unprecedented transparency.

To remain up to date, organizations must abandon the outdated practice of “check-the-box” annual audits. By implementing Governance, Risk, and Compliance (GRC) technology, organizations can automate Continuous Controls Monitoring (CCM). This transitions compliance from a point-in-time fire drill into a real-time, evidence-backed dashboard, proving defensibility to regulators and the board.

Step 7 **Start post-quantum cryptography readiness before urgency narrows options**

Quantum readiness is another signal that resilience is no longer only about current threats. According to the 2026 CTR survey, only 25% of organizations are actively implementing post-quantum cryptography, and only 48% say they are well prepared for quantum threats.⁵

Why act now if quantum computers capable of breaking modern encryption are still years away? Because adversaries are already executing “Harvest Now, Decrypt Later” campaigns. They are actively exfiltrating encrypted, highly sensitive data (intellectual property, state secrets, health records) with the intention of decrypting it once quantum technology matures.

Cryptographic migration requires discovery, ownership, prioritization, and phased execution across systems that may not be well inventoried today. Organizations that begin early gain optionality. Those that delay may discover that the hardest part of quantum readiness is not the cryptography itself, but the lack of visibility into where cryptography is embedded and who owns the path to change.

⁵ 2026 KPMG Cybersecurity and Technology Risk Survey



Use cyber managed services to create operating leverage

Cyber managed services should remain a major part of the solution narrative because the resilience gap is partly an execution and scale problem. Many internal teams are not short on commitment; they are constrained by tool sprawl, talent scarcity, manual workflows, and the constant pressure to prove value while keeping the business moving.

KPMG Cyber Managed Services can support human-led, AI-enabled operations across **detection, response, identity governance, threat intelligence, cyber risk management, and security testing**. Done well, managed services can provide operating leverage: greater consistency, broader expertise, better signal quality, and clearer evidence of performance.

Where managed services can strengthen the operating model:

- **Managed identity** helps strengthen privileged access and access governance.
- **Managed cyber risk** brings more continuity to third-party and supplier oversight.
- **Managed security testing** validates applications, APIs, cyber defenses, and AI systems before weaknesses become incidents.
- **Managed detection and response** combines monitoring, threat hunting, intelligence, and expert analysis to help teams move from alert volume to better-informed action.

For CISOs, the strongest outcome is a security operating rhythm that becomes more predictable over time: fewer ambiguous handoffs, faster movement from signal to action, stronger access discipline, and clearer evidence that the cyber program is improving.

From cyber resilience to business confidence

The CISO role is changing because the business has changed. Cybersecurity is no longer judged only by whether it prevents incidents. It is judged by whether the organization can keep operating, keep innovating, and keep earning trust when the environment becomes unstable.

That shift gives CISOs a more powerful story to tell. When the security operating model becomes more connected, the conversation moves beyond tool count and activity volume. It becomes possible to show where response variability is declining, where identity governance is becoming stronger, where third-party risk is being managed with more continuity, and where leadership has clearer evidence that resilience is improving.

This is what changes cybersecurity's role in the business. Security becomes less of a late-stage approval function and more of an operating discipline that enables responsible growth. AI adoption becomes easier to support because guardrails are clearer. Cloud and digital initiatives move with more confidence because exposure is better understood. Incident response becomes less improvised and more coordinated. Governance becomes less retrospective and more useful.

The modern CISO does not need another reminder that threats are increasing. The more useful question is whether the cybersecurity operating model is designed to perform under the conditions that now define the environment: AI speed, identity complexity, ecosystem dependence, regulatory scrutiny, and talent constraints.

The organizations that move ahead will not simply be the ones that spend more or deploy more. They will be the ones that connect their capabilities into a system that performs consistently, adapts continuously, and proves resilience in terms leadership can understand.

That is the shift from reactive defense to modern cyber resilience. It is not a theoretical future state. It is an operating model choice CISOs can begin making now.



How KPMG can help CISOs achieve cyber resilience at scale

Closing the cyber resilience gap requires more than a stronger strategy, a new platform, or another layer of controls. Most large organizations already have substantial cyber capabilities in place. The harder work is connecting those capabilities so the program performs with greater consistency when the business is under pressure.

KPMG connects cyber strategy, governance, implementation, managed services, protection, threat management, incident response, and continuous monitoring to help CISOs move from accumulated capability to coordinated performance. The goal is not to add complexity to an already crowded cyber environment. It's to help the security function operate with more clarity, stronger execution discipline, and better evidence of resilience.

To that end, our cyber and technology risk capabilities span cyber threat management, cyber protection, proactive threat intelligence, incident response planning, continuous monitoring, regulatory alignment, and implementation support.

The most useful starting point is not "what solution should we buy?" It's "where does the current model lose speed, control, or confidence?" In some organizations, the answer is identity and privileged access. In others, it's inconsistent incident response, fragmented compliance evidence, third-party exposure, AI security testing, or a SOC model that cannot scale with the pace of threat activity. The most effective path forward typically connects several of these areas because the resilience gap rarely sits in one domain. It sits in the handoffs between them.

Turn strategy and governance into a continuous operating capability

Cyber governance has become more demanding because the questions have changed. Boards and regulators do not only want to know whether controls exist. They want to know whether those controls are working, whether remediation is progressing, whether third-party risk is being managed, whether AI-related risks are governed, and whether resilience can be proven in terms the business can understand.

KPMG supports this shift through capabilities across **GRC technology, IT controls management, regulatory assessments, remediation planning, third-party risk management, digital safety, and strategy/risk/operating model execution**. The value is not simply better compliance documentation. It is a more connected view of controls, obligations, risk signals, and remediation activity so CISOs can move from explaining cyber activity to demonstrating cyber performance.

What our GRC and regulatory capabilities help address

- **Fragmented control evidence:** Connect risk signals, control status, and remediation progress so leadership can see whether resilience is improving.
- **Manual compliance burden:** Use GRC technology and automation to reduce retrospective evidence gathering.
- **AI governance uncertainty:** Establish clearer roles, controls, monitoring, and escalation paths for AI-enabled environments.
- **Board defensibility:** Translate cyber governance into a more coherent business-risk narrative.

Strengthen protection where compromise becomes business impact

A resilience strategy depends on understanding where a localized issue can become a business event. In modern environments, those pathways often run through identity, applications, platforms, data, cloud architecture, and third-party access. A compromised credential becomes a privilege issue and a privilege issue becomes a containment issue. Similarly, a vulnerable application becomes a customer trust issue and data exposure becomes a regulatory and reputational issue.

Our protection capabilities are designed to help reduce these pathways by strengthening **identity and access management, platform security, enterprise application security, data privacy and protection, and managed services** that help protect systems and data from unauthorized access and vulnerabilities.

What our protection capabilities help address

- **Identity-driven breach risk:** Strengthen IAM, privileged access oversight, and identity lifecycle governance.
- **Platform and application exposure:** Improve security across enterprise applications, cloud platforms, and critical systems.
- **Data privacy and protection pressure:** Protect sensitive data as it moves through AI, cloud, application, and partner environments.
- **Secure innovation:** Help the business adopt new digital capabilities without creating unmanaged exposure.

Identity deserves particular attention because it increasingly determines how quickly cyber risk moves. Access decisions affect containment and privilege affects blast radius. Non-human identities affect automation risk while third-party identities affect ecosystem exposure. With AI, cloud, and digital workflows expanding rapidly, identity is becoming less of an administrative function and more of a control plane for resilience.



Modernize threat management before incidents become business disruption

Prevention remains essential consideration, but sustainable resilience depends on how well the organization performs when incidents inevitably occur. A robust threat management model connects cyber defense, detection, response, recovery, device security, application testing, and managed detection into one operating rhythm.

Our firm's threat management capabilities help organizations **identify and mitigate vulnerabilities, monitor suspicious activity, protect endpoints and devices, continuously assess application resilience, respond quickly when incidents occur, and restore operations after disruption.**

What our threat management capabilities help address

- **Alert overload and slow triage:** Managed detection and response, threat hunting, and threat intelligence help teams focus on legitimate signals.
- **AI-speed threats:** AI-enabled analytics and playbook automation help accelerate prioritization while keeping human judgment in the loop.
- **Application and AI workflow risk:** Managed application security testing can help validate applications, APIs, and AI systems, including agent boundaries and vulnerabilities such as prompt injection.
- **Incident response uncertainty:** Response and recovery capabilities help teams contain, investigate, restore, and improve after incidents.

The practical value for CISOs is not just speed. It is control. A stronger response capability helps teams understand what is happening, who owns the next action, what evidence is available, what has been contained, and how recovery is progressing.



Turn cybersecurity into a performance engine

Working with KPMG means transitioning away from the daily friction of managing fragmented tools and fighting to retain scarce talent. Instead, you plug into a global delivery model infused with advanced AI automation, continuous controls monitoring, and deep environmental knowledge.

We operate the critical, high-complexity parts of your cybersecurity lifecycle at scale, delivering the consistency and continuous improvement that internal teams struggle to maintain.

By lifting the operational burden, we free your valuable internal resources to focus on what matters most: strategic business alignment and growth. We collaborate with you not just to expand your security coverage, but to accelerate and sustain transformational performance, helping you build a demonstrably secure, resilient, and trusted digital future.



Contact us

Matthew P. Miller

**Principal, Cybersecurity &
Technology Risk
KPMG LLP**

E: matthewpmiller@kpmg.com

Michael Gomez

**Principal, Cybersecurity &
Technology Risk
KPMG LLP**

E: michaelgomez@kpmg.com

Charles Jacco

**Principal, Cybersecurity &
Technology Risk
KPMG LLP**

E: cjacco@kpmg.com

Mick McGarry

**Principal, Cybersecurity &
Technology Risk
KPMG LLP**

E: hmcgarry@kpmg.com

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

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 upon such information without appropriate professional advice after a thorough examination of the particular situation.

© 2026 KPMG LLP, a Delaware limited liability partnership, and its subsidiaries are part of the KPMG global organization of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved. The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organization. USCS042197-3A

Learn about us:



[kpmg.com](https://www.kpmg.com)