KPMG

Building cyber resilience: Prepare, protect, and prevail

Identify and prioritize cyber vulnerabilities to keep minor issues from becoming major problems

kpmg.com

Don't get caught off guard—Develop a proactive cyber risk and resiliency approach

The urgency is clear: Today's organizations must elevate their cybersecurity programs to unprecedented levels. Rapid technological advancements, sophisticated new threats, and an ever-expanding attack surface have escalated the challenge of developing and maintaining robust defenses. The risks are manifold, and chief information security officers (CISOs) are at the forefront of mitigating them and ensuring organizational resilience.

The heightened complexities of cybersecurity

The expanded digital footprint and its inherent complexities necessitate a new era of vigilance and proactive defense. Consider these ongoing challenges:

Cloud computing: The shift to cloud computing introduces significant security concerns, such as increased data exposure and the complexities of managing a shared responsibility model. Ensuring data protection and maintaining stringent access controls in this distributed environment is paramount.

System fragmentation: Fragmented data systems can create critical blind spots and inefficiencies, impeding the organization's ability to maintain a coherent security posture.

Budget constraints: Tight budgets and an increased reliance on third-party services elevate the need for strategic investments in adaptable cyber defenses. Financial constraints should not compromise the efficacy of cybersecurity.

Disruptive technologies: Artificial intelligence (AI) and other emerging technologies open new vectors for sophisticated cyber threats, including identity-based attacks, social engineering, and advanced ransomware. These technologies enhance business operations but simultaneously present new security challenges.

Infrastructure misalignment: Misaligned security infrastructure can derail the support of critical business objectives, leading to vulnerabilities that can be exploited by sophisticated threat actors.

> **Asset identification is key to proper asset management. You can't protect what you haven't identified.**

Jason Haward-Grau
Principal, Global Cyber Recovery Services Leader
KPMG LLP

Why proactive cyber defense is imperative

In this evolving threat landscape, a reactive approach to cybersecurity is no longer sufficient. CISOs must adopt a proactive and holistic strategy to safeguard their organizations. This approach involves anticipating potential threats, implementing robust preventive measures, and ensuring swift recovery from any cyber incidents.

Tackle threats with the right strategies

CISOs must act now to strategically manage challenges to ensure the ongoing resilience of their organizations. Similarly, they must determine in advance which business processes are truly mission-critical and should be prioritized for quick recovery in the event of a disruption. Understanding these processes in relation to the technology stack, vendors, and desired business outcomes enables the development of appropriate controls based on several strategic imperatives:

1. Proactive investment: Strategically invest in the right cyber controls and defenses to ensure business protection and resilience. This requires an in-depth understanding of the threat landscape and the specific risks faced by the organization.

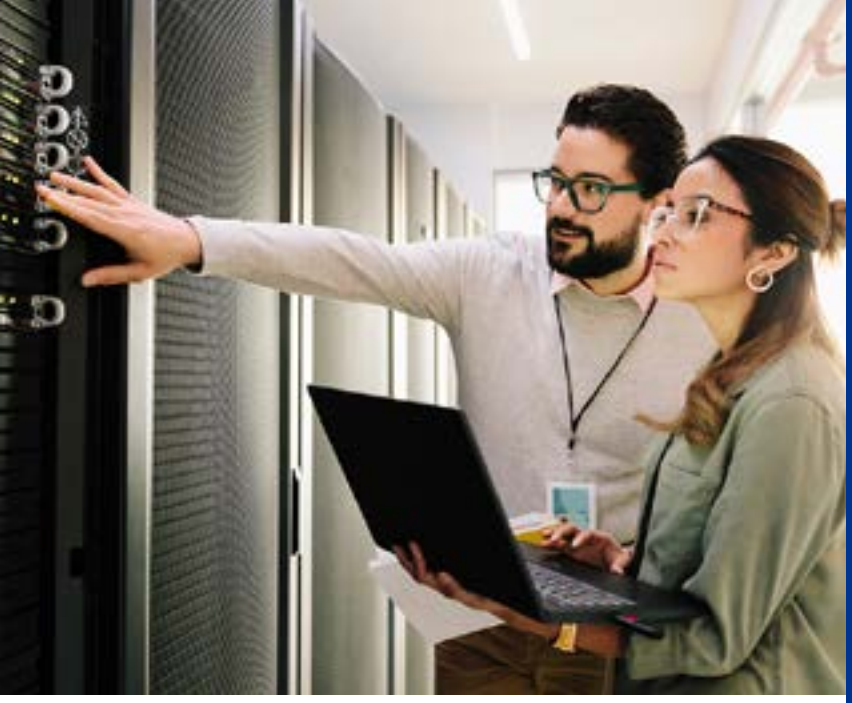
2. Vulnerability prioritization: Identify and prioritize the most significant cyber vulnerabilities, ensuring that critical assets are protected and business continuity is maintained. A risk-based vulnerability management approach helps in efficiently allocating resources to the most impactful areas.

3. Threat management: Stay ahead of emerging threats like deepfakes and advanced social engineering. Enhanced monitoring, automated incident response tools, and holistic management of AI-related risk, particularly those in connection with generative AI (GenAI), are crucial.

4. Third-party security: Adopt comprehensive strategies for third-party risk management to safeguard your ecosystem. This involves stringent vetting processes, continuous monitoring, and ensuring vendor and supplier compliance with security protocols.

5. Zero trust implementation: Enforce strict identity authentication and authorization through a zero trust posture. This includes continuous verification of user identities and limiting access based on the principle of least privilege.

6. Cloud and data security: Maintain stringent access controls and data security in distributed environments. This entails encrypting data both in transit and at rest, implementing robust access controls, and continuously monitoring cloud environments for security breaches.



Key security goals

An effective cybersecurity strategy must be rooted in clearly defined goals that guide the organization's efforts:

- **Protecting the business:** Establish robust defenses against cyber threats to safeguard valuable assets, including intellectual property, customer data, and operational systems.
- **Staying prepared:** Develop and maintain a proactive security posture that anticipates potential threats and prepares the organization for swift, effective responses.
- **Mitigating escalation:** Identify and address vulnerabilities before they escalate into significant issues. Early detection and prompt remediation of security weaknesses are vital.
- **Ensuring continuity and recovery:** Create detailed plans to recover quickly from cyber incidents, minimizing downtime and operational disruption.
- **Achieving desired outcomes:** Align cyber policies with business objectives through a proactive risk and resilience approach that includes a corporate playbook for rebuilding trust after a cyber incident.

Assess your cybersecurity posture

CISOs must realistically assess the current state of their defenses, identifying both strengths and areas for improvement. Key questions to guide this assessment include:

- **Current threats:** What are the most significant cyber threats we face today?
- **Proactive approach:** Do we have an integrated, proactive approach for managing cyber risk and maintaining resilience?
- **Continuous controls monitoring (CCM):** Have we adequately implemented CCM?
- **Asset priority:** Have we prioritized our most important assets and identified our vulnerabilities?
- **AI and GenAI risks:** Are we able to manage AI and GenAI risks holistically?
- **Data access:** Is data access properly managed for all users?
- **Third-party security:** Are our third-party vendors securely managed?
- **Emerging threats:** Are we fully up to date on new cyber threats like deepfakes and social engineering?
- **Business alignment:** Do we work closely with partners across the business to ensure cyber policy aligns with business objectives?

The CISO roadmap for enhanced security

1 The path to cyber resilience and continuous controls monitoring

Building a robust incident response and business continuity plan begins with prioritizing security vulnerabilities, needs, and solutions. The plan should include detailed, coordinated responses based on a clear understanding of critical controls and proactive strategies such as CCM, a technology-driven approach designed to manage and monitor information technology (IT) risks and compliance issues in near-real time.

CCM can help optimize governance, risk management, and compliance by streamlining audits and outcomes, and providing real-time assessment, analysis, and reporting about the status of the organization's security controls.[1]

2 Structured scenario-based exercises

CISOs and other security leaders should conduct structured, scenario-based tabletop exercises in advance of a cyber incident. These exercises expose strategic choices and prepare organizations for major disruptive events, such as ransomware attacks or software malfunctions. They build confidence that leadership is ready to coordinate response efforts, lessening the impact on customers, clients, employees, and vendors.

3 Privileged access management

In addition, CISOs can maintain a robust privileged access management program for internal and third-party users, identify key assets, and support the security management of these assets. Privileged access management ensures that sensitive data and critical systems are accessible only to authorized personnel.

4 Collaborative security culture

Security is everyone's job, and organizations should work to maintain a collaborative security culture across business functions. CISOs can raise awareness of cyber risks and facilitate ongoing training of team members on policies and roles before, during, and after a breach or IT outage.

Encouraging a "speak-up" culture where staff members are rewarded for identifying gaps in security and resiliency is also crucial. Resilience tasks can be embedded within the business with the help of internal security specialists and/or third-party providers.

[1] "What is Continuous Controls Monitoring & Its Impact on Cybersecurity?," Cloud Security Alliance, 2024

5 Prioritize swift recovery

CISOs can empower business information security officers (BISOs) to identify critical business processes to quickly restore key, prioritized processes after an incident. This involves reviewing revenue, profit, and impact assessments for prioritization, assessing which processes provide the most revenue and profit, determining which systems have the most reach and impact in supporting business-critical operations, and considering where the most valuable organizational data resides and how this information should be shared with and used by third parties.

Failover and switchover processes can help minimize damage and support swift recovery in the event of an attack. Failover allows for automatic transition to a redundant component or a standby operational mode, while switchover requires human intervention to initiate the transition. These processes can ensure continuous system availability during hardware or software failures, preventing potential disruptions to critical security functions.

6 Focus on trust and credibility after a cyber incident

In the event of a data breach or other cyberattack, organizations must quickly acknowledge the incident and its ramifications, communicate with affected parties, outline plans to improve security, and maintain ongoing transparency to rebuild confidence. A prepared playbook can guide organizations through the recovery process, including critical first steps such as alerting the press and contacting key customers, vendors, and business partners.

Ongoing efforts to build trust and credibility include enhancing security across the enterprise, improving cybersecurity awareness for employees, and evaluating the security posture of third-party vendors with access to sensitive data.

7 Stay vigilant amid changing threats

Security is never a “one and done” exercise. CISOs must keep pace with new and evolving threats by following a dynamic approach to security and resilience. Regularly test recovery processes to ensure the quick restart of value chains after disruptions, stay updated on new threats and issues, and proactively plan for future threats.

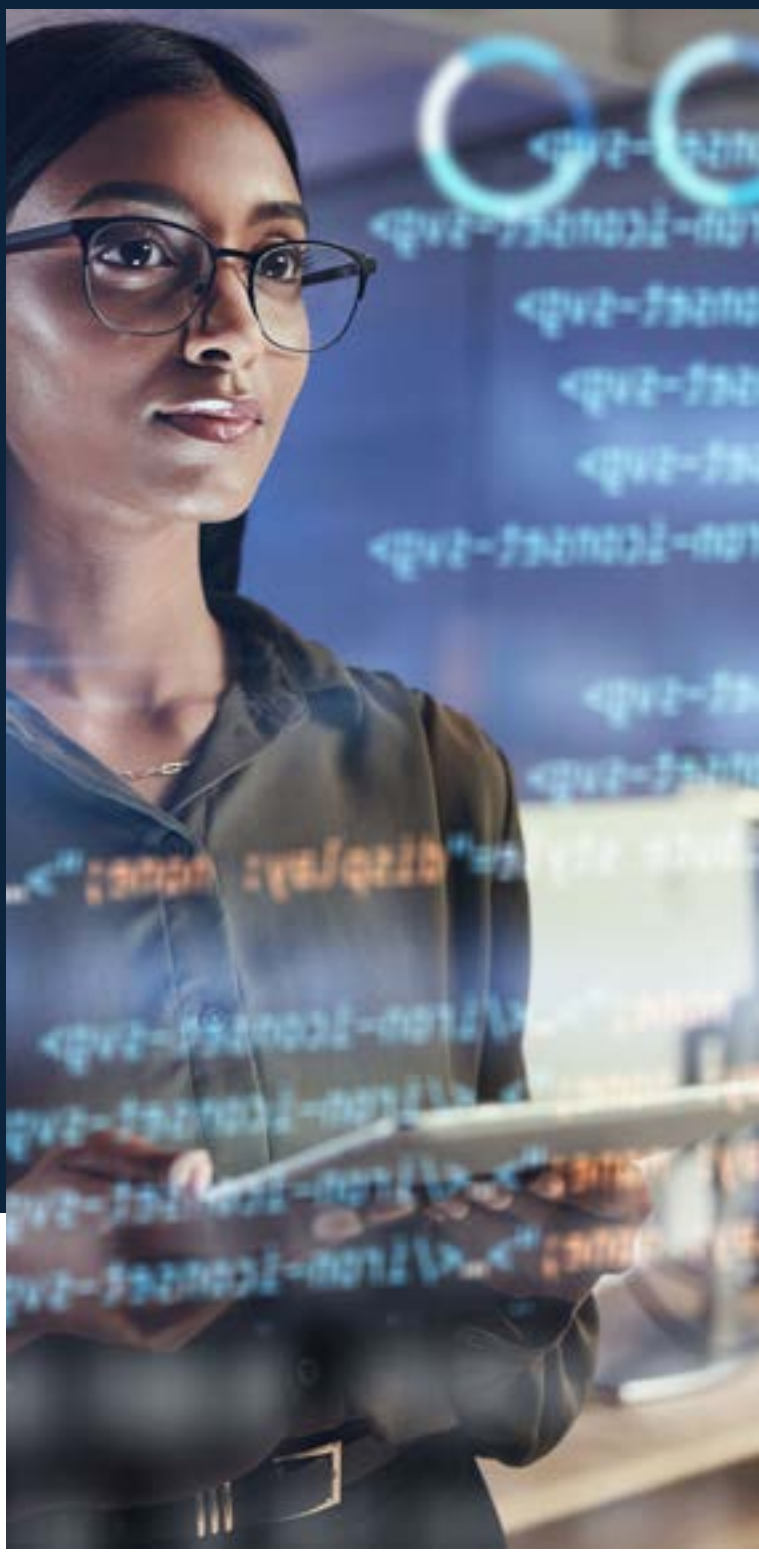
Real-world cyber risk and resiliency stories

The experiences of organizations across different industries highlight the importance of robust cybersecurity measures.

Financial services: Breaches on secure file transfers create financial losses

In a recent cyber event, attackers exploited vulnerabilities in a key financial network to create fraudulent money transfer requests, resulting in significant financial losses. These breaches had a serious impact on several financial services firms that rely heavily on secure file transfers to protect sensitive data. The potential exposure of confidential financial information, along with service outages and delays in critical processes, posed a serious threat to the affected organizations, compromising client privacy and security and exposing them to legal and regulatory consequences.

Affected companies had to allocate significant resources to investigate the extent of the breaches, identify compromised data, assess operational impacts, and implement additional security measures to prevent future breaches and regain client trust. This episode was a wake-up call for the financial services industry, highlighting the need for robust cybersecurity measures and proactive risk management strategies, including regular software updates, thorough security assessments, and comprehensive ongoing employee training.



The response team collaborated with an external cybersecurity firm focused on threat hunting and digital forensics. Using advanced AI-powered tools, the team was able to identify the threat origin, its mechanism, and potentially targeted data. They were also able to deconstruct the malware code to predict its behaviors and isolate vulnerable servers.

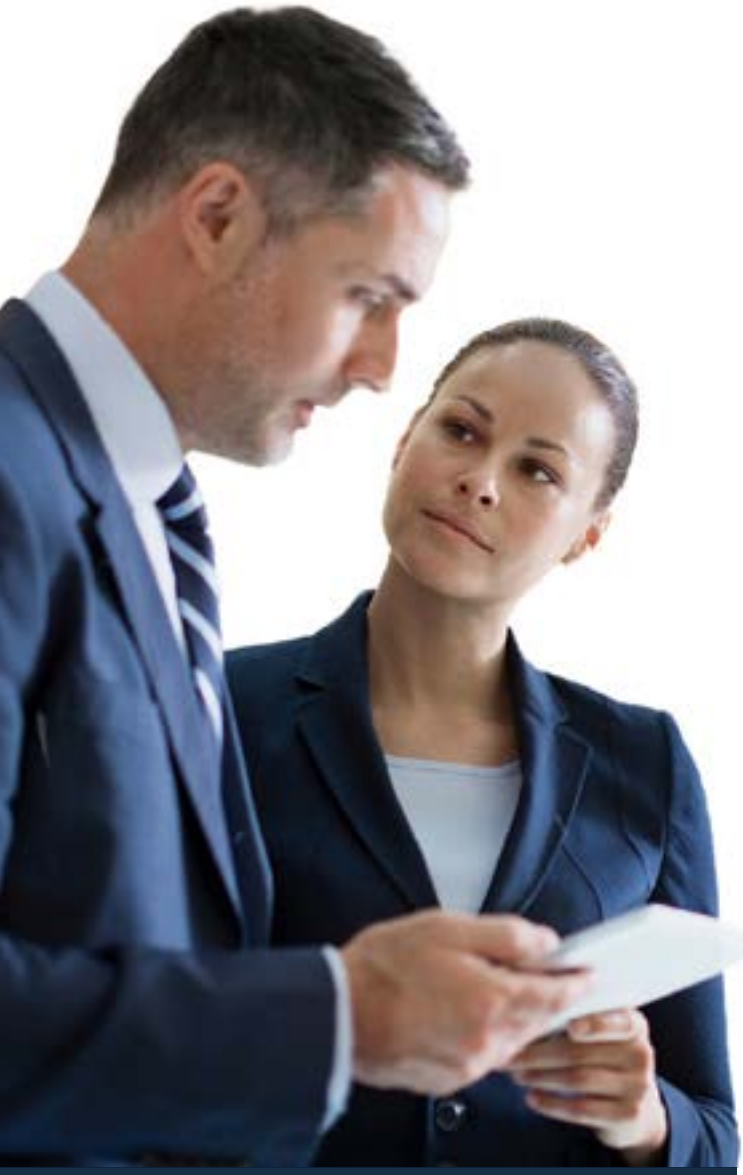
Meanwhile, the PR team communicated with stakeholders, including affected patients, about the breach and mitigation steps taken. The incident was reported to legal bodies and regulators to comply with data-breach notification regulations.

Following the incident, the company conducted a thorough review to extract relevant lessons, addressing identified gaps, installing necessary patches, and updating firewalls and intrusion detection systems. Committing to regular monitoring and auditing of their overall cybersecurity policies was pivotal in enhancing their security posture.

Life sciences: Sophisticated cyberattacks compromise intellectual property and patient data

A leading biomedical research company experienced a sophisticated cyberattack. The attackers used a malware-infected email to infiltrate the company's network, aiming to compromise intellectual property and sensitive patient data. Upon discovering the incident, the company activated its response team, which immediately assessed the breach's severity, isolated affected systems, and gathered critical information.

The cybersecurity team conducted a malware analysis and developed countermeasures to neutralize its impact. The response team collaborated with an external cybersecurity firm specializing in threat hunting and digital forensics. Using advanced AI-powered tools, they identified the threat's origin, its mechanism, and potentially targeted data. This involved scanning all systems for signs of similar malware and removing them before they could cause significant damage.



How KPMG can help

Protect, invest, and innovate

Business leaders rightly concern themselves with today's evolving cyber threat landscape. However, there's a light at the end of the tunnel, and KPMG LLP (KPMG) can help you reach it. Our professionals assist organizations across multiple industries in building resilience for critical processes, developing advanced digital solutions, advising on the implementation and monitoring of ongoing risks, and effectively responding to incidents.

KPMG has a detailed approach that includes applying leading cyber recovery practices and developing new ones. Our client-centric perspective helps ensure we deliver relevant tools through a transparent plan, supported by specialists who deeply understand your business and technology.

Whether entering a new market, launching new products, or engaging with customers in innovative ways, KPMG professionals help you anticipate issues and operate more efficiently and confidently. Our team's technological experience, business perspective, and creativity combine to help protect your network and build stakeholder trust.

In short, KPMG can help you safeguard your business, make strategic investments in cyber defenses, support proactive cybersecurity measures, and maintain robust continuity and disaster recovery plans across the enterprise.

Closing thoughts

The evolving cyber threat landscape demands that CISOs remain vigilant and proactive. By prioritizing the right investments, managing emerging threats, ensuring third-party security, implementing zero trust principles, and maintaining robust cloud and data security, organizations can protect their business, stay prepared, and prevent small problems from becoming significant issues. KPMG can help you navigate these challenges, enhance your cybersecurity and strengthen your resilience.

Contact

Jason Haward-Grau
Principal
Cybersecurity & Technology Risk
KPMG LLP

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

Learn about us: **kpmg.com**