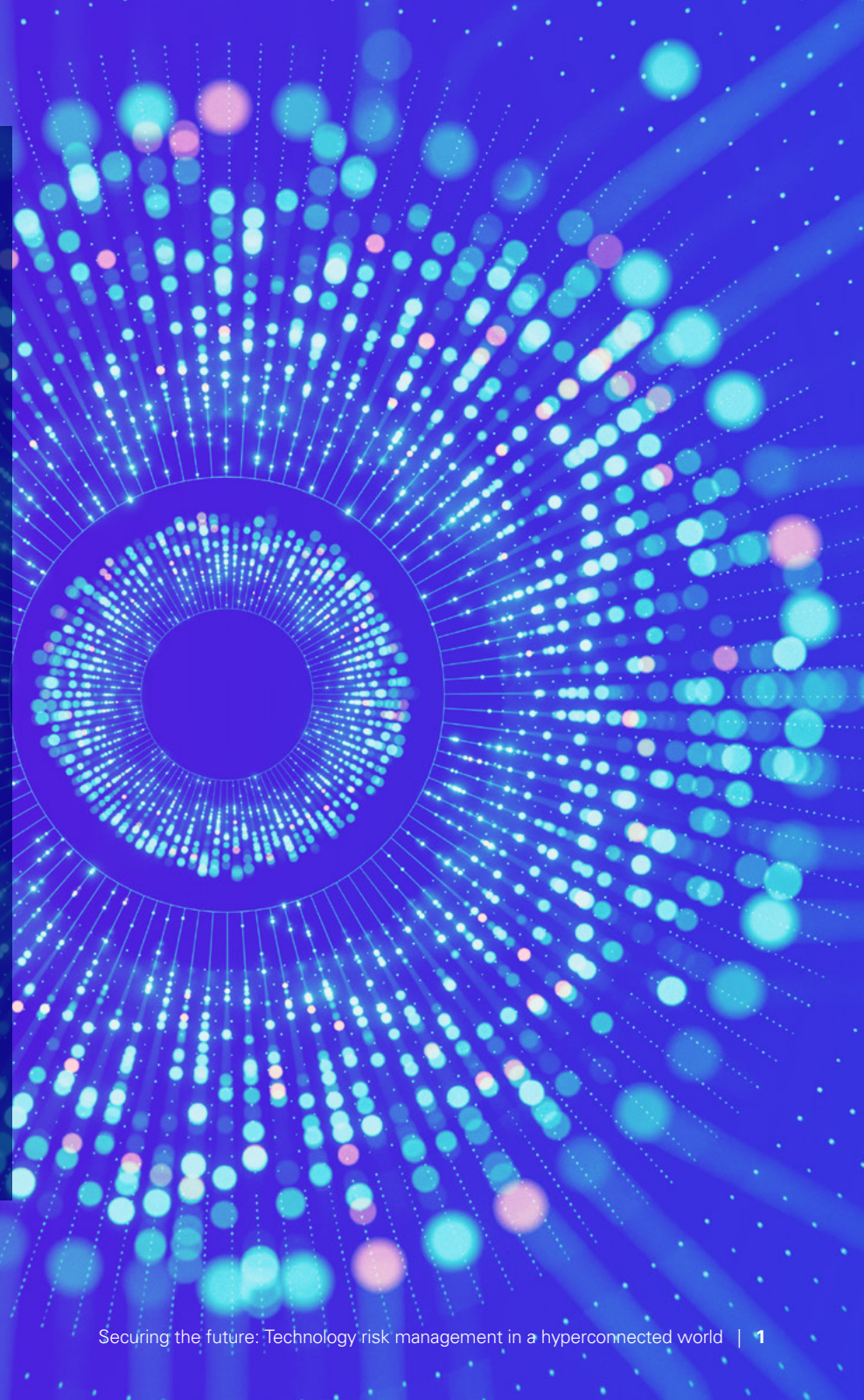

KPMG
Securing the future
Technology risk management and cybersecurity transformation in a hyperconnected world

Effective technology governance is needed to manage cyber risks, enhance operations, and gain competitive advantage.

In a world where even refrigerators and coffee makers are internet enabled, it's hardly shocking that in today's enterprise, both the number and variety of networked devices have exploded. Information technology (IT), operational technology (OT), and internet of things (IoT) assets are everywhere. They're scattered across different business units and geographies. They're distributed throughout supply chains. They're on the manufacturing floor, in warehouses, in retail locations, and in vehicles. The once-reliable model of perimeter-based cybersecurity protecting a relatively small number of servers in a handful of datacenters has become a relic of the past.



Many organizations are not prepared for the expanding scope of cybersecurity threats that accompany this new reality, and traditional technology risk management approaches are falling short. As businesses transform and modernize the technology stack, their technology risk management infrastructure and controls must evolve and keep pace. And the very concept of technology risk management must shift away from a strictly "defensive orientation" to one where businesses leverage risk to enable enterprise-wide growth and optimization.

This demands a refocus beyond IT proper to business operations and the translation of technology risk into clearly understood business risk. It entails proactive monitoring and automated controls to address risk events while at the same time improving the odds of successful execution of business strategy. Today, ensuring cybersecurity, sound risk management, protection of business operations, and expansion of competitive business offerings is a high-stakes team effort.

A critical component in this effort is technology governance—deploying a governance infrastructure designed to meet regulatory requirements and mitigate legal risks, configure security tools to detect threats proactively, optimize IT asset spend, understand points of failure to plan effectively for disaster, and more. To be effective, such an infrastructure relies on a clear view—from macro to micro level—of all technology assets across the enterprise. This can be a tall order, spanning every business sector, but especially for organizations that span across different business units, subsidiaries, and geographies.

KPMG LLP believes that an articulated approach to identifying all technology assets across an enterprise, assessing security and governance vulnerabilities, and devising and adopting an appropriate governance infrastructure are essential to help minimize disruption to business operations, manage compliance risk, and safeguard customer trust and competitive standing. Forward-thinking business leaders are addressing technology risk and cybersecurity transformation today.

Leaving the door open to cyberattacks

In 2017, the WannaCry ransomware attack became a global epidemic, infecting 230,000 computers in 150 countries, impacting schools, hospitals, and mission-critical operations across a variety of sectors. Spread through computers operating Microsoft Windows, WannaCry held users' files hostage, threatening deletion if a ransom payment was not received within three days. Overall, it is estimated that WannaCry caused $4 billion in losses around the world. Sadly, much of its reach and damage could have been prevented; the weakness it exploited had already been addressed by Microsoft with the release of a security patch that could have provided protection to thwart the breach. Many organizations who failed to regularly update their operating systems were left exposed to the attack.[1] The continued use of outdated computer systems, the lack of visibility into assets requiring attention, and the absence of a governance structure around updating software combined to create a fertile field for the attackers.

Understanding your technology risk profile

Every enterprise has a unique technology risk profile. In general, the proliferation of IT, OT, and IoT assets, right down to the individual desktop, mobile device, and connected product levels, makes complete visibility and oversight extremely difficult within any enterprise. Decentralized procurement or business unit-specific processes and protocols often exacerbate the problem.

For certain types of large, distributed organizations, the risk profile becomes exponentially higher. Perhaps an organization does business in multiple states or countries, each with their own regulatory environment. Perhaps those regulatory requirements are changing constantly or are even contradictory. An enterprise might operate joint ventures or do business through multiple subsidiaries, each with varying levels of integration with the parent company. Lack of broad visibility, complex operational legal structures, and ambiguity over oversight responsibility across such distributed operational entities all leave critical gaps in security. These can lead to serious risks to the enterprise.

To define their technology risk profile, enterprises must take a fresh look at their current IT operating model in the context of the overarching business operating model and business goals. The goal is to determine where there are weaknesses in risk management processes as well as opportunities for value creation. There are several key questions to ask in this assessment, among them:

- **Do you have broad visibility** into where your technology assets are located, cataloged, and monitored—and who is responsible for them?
- **Do you understand** which assets support the mission-critical operations necessary for your business to run smoothly?
- **Do you have a firm grasp** of where your most vulnerable assets are hosted?
- **Is there a standardized taxonomy and language** in place to classify **assets and build foundational data?**
- **Are risk management processes** standardized, well understood, uniformly adopted, measured, and rewarded?
- **Do you understand** how your technology risk management policies and governance infrastructure compare to leading practices and those of competitors?
- **Is there a cross-functional committee** in place to monitor and assess your risk management strategy, tactics, and success metrics?
- **How is technology risk management** embedded into your organization's culture?

Effective risk management transformation starts with a solid understanding of the current situation. Many organizations choose to utilize their internal audit function or to outsource assessment of technology risk management to a neutral third party. In whatever way the appraisal is accomplished, objectivity is key. With foundational assessment in hand, the organization is better equipped to develop a migration program tailored to its unique roadmap, challenges, priorities, and resources.

The costly impact of cybersecurity failures

The inability to identify and track technology assets—including software, hardware, and third-party applications and services—and the failure to appreciate their critical interdependencies—increases the risk of organizations going under-protected.

Regulatory compliance is critical

Insufficient asset visibility, coupled with policy and governance deficiencies, has played a significant role in several high-profile, high-impact security breaches. Enterprise cybersecurity risks go far beyond the financial realm and impact a broad base of stakeholders. Regulatory filings are difficult to keep accurate without proper oversight and organizations may face repercussions—such as legal action—when there are inaccuracies in legal filings or breaches of privacy. Organizations may suffer reputational damage and loss of customer trust and confidence.

Digital trust is at the heart of stakeholder confidence

Digital trust is the expectation by individuals that digital technologies and services, and the organizations who provide them, will protect all stakeholders' interests and uphold social expectations and values. A breach of this trust can undermine brand reputation, customer loyalty, business relationships, and profitability. Organizations that demonstrate high levels of digital trust have become the preferred choice for customers. Those that ignore the digital trust imperative are most likely to see a lack of support over time if transparency is not provided or there are cybersecurity incidents that break the trusted relationship.

Digital trust is essential for businesses to thrive in a fast-paced market, with a focus on addressing cybersecurity, data privacy, responsible AI, and information risk management. Technology risk can be mitigated—and digital trust enhanced—through an integrated and deliberate risk management transformation effort.[3, 4]

Asset visibility enables long-term planning

A lack of visibility around assets can impede the ability to identify and prioritize remediations as well as create weaknesses in long-term planning. This limits the capacity to respond not just to cyber threats, but also to market opportunities, blunting competitive advantage. Downstream impacts of poor asset tracking can include loss of investment value, suboptimal performance, and missed optimization opportunities using new technologies such GenAI and machine learning.

A catastrophic, cascading impact

In the summer of 2024, a software update from a software firm caused more than 8.5 million systems to crash, disrupting operations for days across thousands of organizations worldwide, including hundreds of Fortune 1000 companies in a diverse array of sectors—transportation, shipping, hospitals and healthcare, banks and financial institutions, and restaurants and retail among them. This event resulted in losses estimated to be more than $5 billion, including costs to insurers of around $1.5 billion in payouts, under business interruption, cyber, and system failure coverages.[2]

This failure, while not a cyberattack or breach per se, is representative of the huge cyber risk and potentially negative cascading business impacts of the interconnected technologies and operations in today's enterprise. It underscores the need for broad visibility into assets, deep understanding of critical interdependencies across an entire organization and its business operations, and a governance infrastructure that defines who responds to failures, and when and how they do so. With such information at hand, a business is far better equipped to respond swiftly and effectively to any adverse cyber events that may arise, whatever their source.

Here to stay

Unfortunately, cyber incidents are only increasing, as sophisticated hacking operations exploit new technologies (including AI), find weaknesses in operational practices, and keep pace with prevention measures. What enables these attacks?

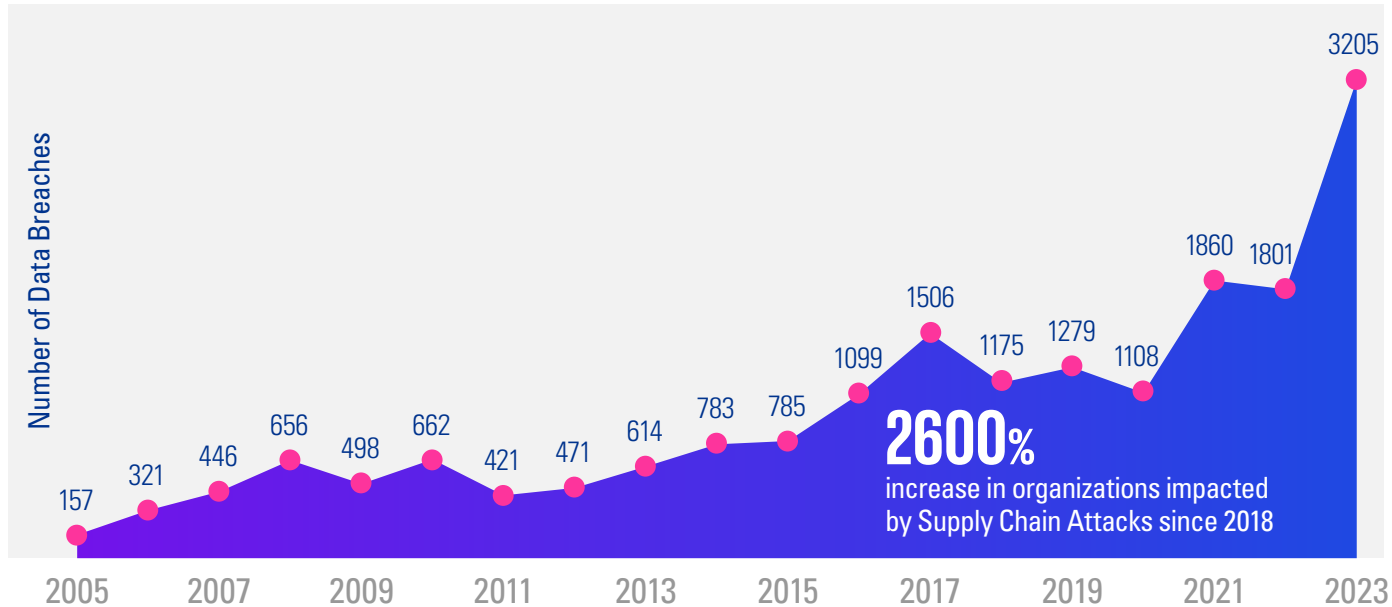
There are several contributing factors: Incomplete attack surface visualization, out-of-date support hardware and software, high variability in architecture, expensive internal and external support costs, distributed and difficult to manage infrastructures, and limited support resources, to name only a few. Sound prevention and mitigation strategies begin with a solid understanding of your organization's current risk profile, including analysis of supply chain, OT, and IoT processes and technologies.

Cyberattacks in supply chain management

As organizations increasingly standardize on common products, and optimizing supply chain operations, vulnerabilities can be created become difficult to contain. In the case of third-party products, clear procedures and policies must be established on how to conform with the organization's security standards and protocols. Without sound third-party risk assessment frameworks, shared tools can introduce susceptibilities at multiple points of entry. If exploited, any one point of vulnerability can threaten multiple entities simultaneously and bypass large organizations' cyber security and data protections.[5] Cyberattacks in supply chain management often target companies in IT and technology, manufacturing, finance, and healthcare sectors.

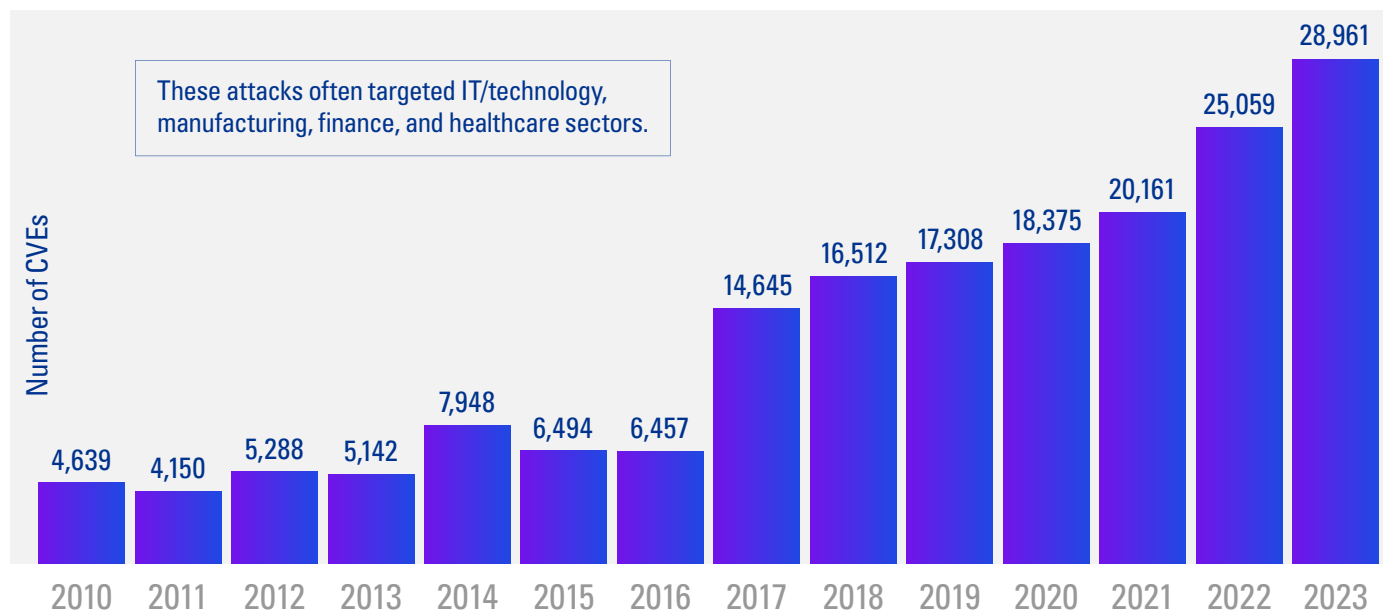
Here to stay *continued*

Data breaches and Compromises 2005-2023



Source: OT Cybersecurity The Year in review, Dragos, February 2024

Common vulnerabilities and exposures (CVEs) 2009-2023



Source: OT Cybersecurity The Year in review, Dragos, February 2024

Here to stay *continued*

Cyberattacks in OT
Historically, cyberattacks have been considered a problem specifically affecting the IT side of the house. However, there has been an uptick in attacks targeting the manufacturing floor, posing an increasingly significant threat to critical infrastructure systems.[6]

70% of all ransomware attacks targeted
638 manufacturing entities in
33 unique manufacturing subsectors

50 active threat actor groups (APTs) impacting industrial organizations

80% of vulnerabilities reside deep within the ICS network

+50% Cyber attacks against industrial organizations **increased 50 percent over the last years**

905 reported ransomware incidents impacting industrial organizations in 2023, a **49.5 percent increase** from 2022

From business interruption to national security

In 2021, a major refined petroleum pipeline in the United States, was hacked by a group known as DarkSide. Their cyberattack infiltrated the company's computer systems and encrypted billing files, interrupting access to its servers. Once discovered, the company shut down its OT systems to halt further infection and eventually paid the hackers millions of dollars to restore its operating systems. After recovering the decryption key, it still took days to restart the pipeline, with the organization incurring incremental costs associated with business interruption and downtime.[7] Meanwhile, gas shortages caused widespread panic at the pump and an uptick in price to consumers. In this instance, a failure of cybersecurity in one organization escalated to an issue of national security.

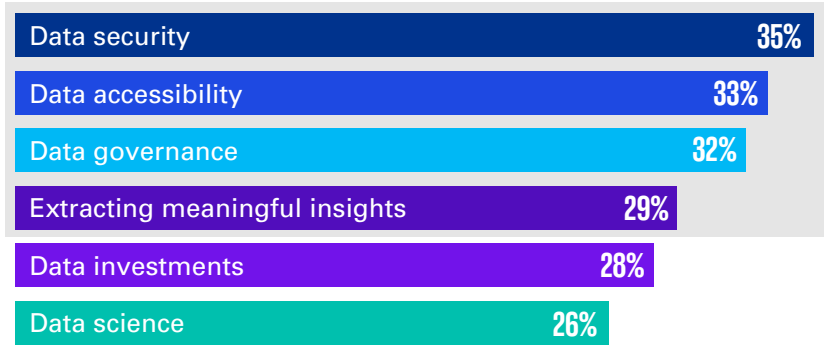
Recognizing the ongoing and evolving threat posed by cyberattacks, many organizations have already started to consider their preparedness and take action. Perhaps somewhat ironically, companies operating in highly regulated industries, such as financial services and power utilities, tend to be more advanced in their technology risk management initiatives than companies operating in the technology sector.

Here to stay *continued*

A universal concern for the world's largest organizations
Securing the most value from identified opportunities relies on robust data-driven processes, security, and governance. As they troubleshoot the risk factors that threaten their enterprise resilience and competitive standing, organizations are placing cybersecurity and data proficiency at the top of their priority lists. The **2024 KPMG Global Insights Survey** identified six areas of focus for technology leaders in eight industries across 26 countries[8]:

What are your organization's areas of focus for technology risk management and cybersecurity?

Key focus areas for the next 12 months for top technology executives



IoT and managing distributed threat vectors

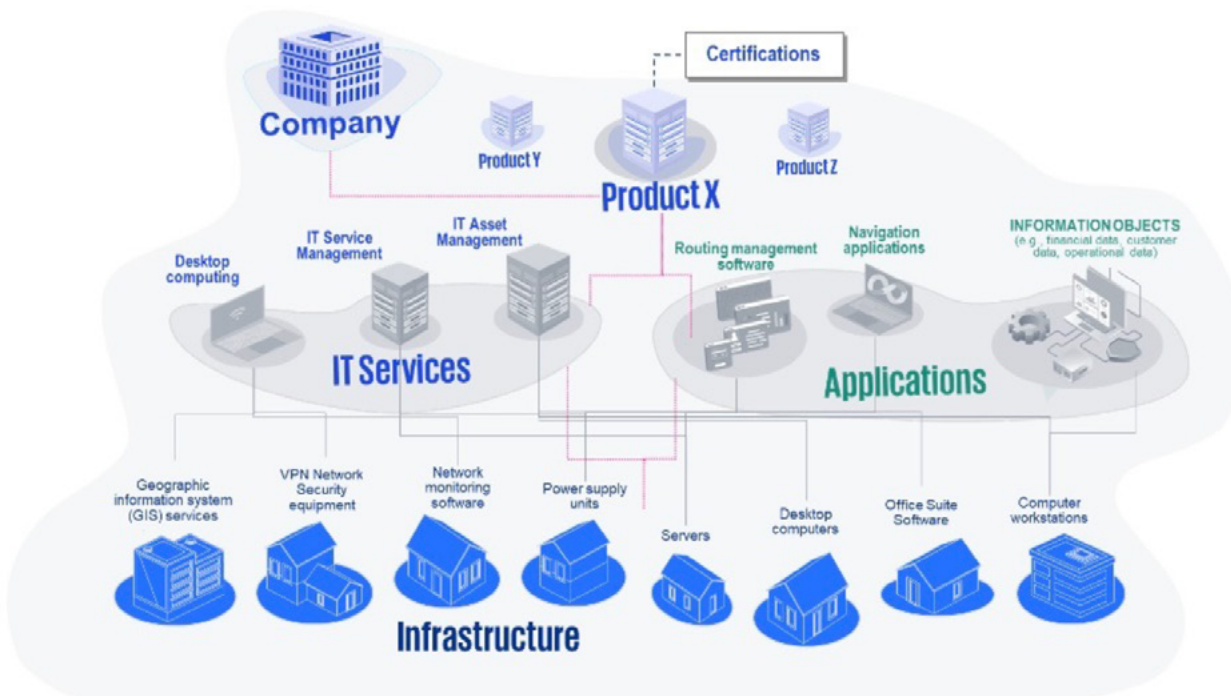
IoT is enabling new products and services and complicating risk management. Product diversification and the technology that supports those products create a new technology landscape and a totally different attack surface that must be monitored and controlled. A major automotive manufacturing company, for example, parlayed its in-vehicle telemetry technology into a fleet management offering, extending its technology risk beyond the confines of its own operations and primary product to those of other third-party entities. In turn, those entities must manage their own threat vectors and accordingly demand assurances about the automaker's data and technology management processes. Where not strictly governed by regulatory mandates, many companies are responding by voluntarily adding market certifications, such as International Organization for Standardization (ISO) compliance.

The critical importance of technology governance

Technology governance is a function that oversees how an organization inventories, deploys, maintains, upgrades, and decommissions its IT, OT, and IoT assets. It should go beyond simply assigning roles, responsibilities, and authorities. The strongest technology risk frameworks include a core governance structure that cuts across various functions within the organization, with a central team or committee to review and approve technologies, whether built or bought. A dedicated and robust technology governance program enables organizations to improve their ability to manage their data, drive insights, and create value by creating a data-centric culture from the top down, with:

- **Clear visibility** into assets and their configuration, improving inventorying, accounting, and reporting abilities
- **Enhanced central oversight capability**, bolstering compliance with external regulations and improving the ability to reduce the risk and impact of a breach
- **An open business and technical architecture** accommodating flexibility and rapid adaptation to emerging opportunities
- **Strong data foundations**, yielding trustworthy data underpinning analytics, and allowing leadership to make ongoing, informed technology investments to reach IT and broader business goals
- **Improved data management**, reducing technical debt by streamlining system efficiency, limiting redundancies, reducing overhead costs, and ensuring data integrity
- **Expanded transformational opportunities**, such as accelerating AI-enablement by ensuring high-quality and well-structured data to train models.

Technology governance: enterprise-wide visibility



The critical importance of technology governance *continued*

A holiday saved

When a financial services company was tackling a very significant software deployment, risking hundreds of millions of dollars in potential fines if the newly acquired software was not deployed safely, it stood up a cross-functional team—incorporating software deployment, database analysts, business application owners, and infrastructure stakeholders—to evaluate the profile of assets and applications in place, contemplating hardware and software, both on premises and in the cloud. The team assessed what risks might be introduced along with the new software and strategized how these might be triaged and mitigated. When, during the Christmas holiday, a Log4J vulnerability arose, opening the company to malicious hacking events, they were prepared. Because they had a thorough view of what technology was deployed where, had a proactive process and workflows in place to address adverse events, and a clear vision of roles and responsibilities, they could respond rapidly and effectively, leaving plenty of time to enjoy their holiday.

All aboard!

Cybersecurity is not just an IT matter; it's a business concern—a shared problem with enterprise-wide reach and implication. It demands collective ownership of the problem and the solution. In the face of the evolving and increasingly dangerous cybersecurity landscape, it is critical that technology leaders, the C-suite, and boards prioritize an enhanced and proactive cyber posture.

The Cybersecurity and Infrastructure Security Agency (CISA) Cybersecurity Advisory Committee has stated that, "Cyberattacks and their impact could be better mitigated or even prevented if corporate boards of directors were more educated and engaged on matters related to cybersecurity, placed a higher priority on cyber resilience, and exercised stronger oversight over the development and execution of their companies' cybersecurity strategies." CISA has declared the "need to prioritize cybersecurity at the highest levels," noting that "the days of relegating cybersecurity to the CIO or the CISO must end. CEOs and Boards of Directors must embrace cyber risk as a matter of good governance and prioritize cybersecurity as a strategic imperative and business enabler."[9]

All aboard! *continued*

Funding risk management transformation initiatives

When a leading industrial manufacturing company wanted to fund its technology risk management transformation initiative, it recognized that making the business case and generating awareness at board and executive leadership levels were critical. It took a data-driven approach, cataloging breaches experienced over time, their extended business repercussions, and points of ongoing vulnerability. It ran "red team" technical tests, including executive management, to simulate its ability to respond effectively to a breach, surfacing unresolved problem areas and quantifying the potential costs of associated risks. It received its funding. Awareness, understanding, and education drive buy-in and help secure appropriate technology risk transformation budgets.

All stakeholders—going well beyond chief information officers (CIOs), chief security officers (CSOs), chief compliance officers, (CCOs), and chief risk officers (CROs)—must collaborate to enable high-functioning, low-risk operations in support of business goals. A top-down approach to cybersecurity, originating at the highest levels, must penetrate all layers of the organization, right down to the individual "boots on the ground." This will likely entail behavioral changes and cultural shifts, and there may be resistance from individuals who are comfortable with current processes or legacy systems, or who might feel "ownership" of a siloed application. Several change management strategies can help achieve buy-in that sticks:

- **Broad communication** of roadmap, rationale, and vision of what success looks like, with emphasis on the value proposition for specific functional roles.
- **Leadership buy-in and endorsement,** key components of success, can often be effectively secured by capturing value outcomes and showcasing them at the board level. Motivated leaders at the top of the organization, who clearly and consistently articulate a vision for technology risk management and put their weight behind transformation initiatives, can get and keep the ball rolling at all levels of the organization.
- **Aligned performance metrics** to measure and reward desired behavioral shifts are critical. For example, an internal audit professional who once spent days every quarter manually gathering asset compliance information but now can see it at the click of a button in an asset visibility tool, must have new performance goals, measurements, and rewards. As roles and responsibilities evolve in risk management transformation, so must performance metrics.
- **Engaging and accessible training** implementing fun, "bite-sized" training programs using videos, games, and hands-on user experiences.

Six steps to future-proofing cyber resiliency in your enterprise

KPMG has identified six key steps in building cyber resiliency and future-proofing your organization for safety and competitive advantage moving forward:

1 **Create your risk profile:** It is essential to take a hard look at the areas of asset vulnerability in your enterprise to assess and prioritize risks more effectively. This will consider the legal and operational structure of your operations across subsidiaries, joint ventures, and geographies. You will want to assess your level of visibility into IT, OT, and IoT assets and determine if you have a standardized classification taxonomy for them in place to identify areas for improvement and opportunities to inform the technology risk management transformation you undertake.

2 **Identify and categorize enterprise assets:** You cannot manage what you cannot see. Ensuring that you are in possession of foundational data elements, such as individual user and business unit information, is critical. It is important to tag assets to the enterprise products and services they support. You might also assign levels of risk to different assets or processes. This will help you monitor asset risk based on a defined risk framework which right-sizes oversight to the impact of potential failures.

3 **Define a technology governance infrastructure:** Successful risk management transformation initiatives establish and codify lifecycle management policies for inventorying, deploying, maintaining, upgrading, and decommissioning assets. They standardize a structure for storing, analyzing, and aggregating threat and vulnerability level data across IT assets and subsidiaries, enable swift response to adverse events, and provide the opportunity to continually optimize efforts.

4 **Explore possible tooling and automation solutions:** Tools and automation can help improve visibility, increase efficient management of IT assets, bolster cyber resilience, improve processes and compliance within an organization, and facilitate competitive advantage and value generation. Many organizations incorporate next-generation automation tools such as role-based user interfaces, real-time intelligence and alerts, action-driven workflow capabilities, and normalization engines, to aggregate, transform, and normalize data being provided by multiple sources and automated analytics and reporting.

5 **Establish program implementation roll out and governance:** It's wise to have a clear vision of the desired end state and a map to get you there as expeditiously as possible. To stay on track, you might want to create an execution timeline and identify and track milestones.

6 **Remember the human touch:** Any successful technology risk management transformation initiative must be designed with people in mind, addressing their needs and pain points. It must supply the answer to "What's in it for me?", while promoting the value proposition for the organization at large.

KPMG is here to help

Are you ready to begin future-proofing the safety, productivity, and competitive advantage of your organization with risk and cybersecurity transformation? We can help.

KPMG LLP understands the multi-dimensional security challenges faced by enterprises across their technology, people, processes, and partners. Our teams of technology professionals are skilled and experienced with a diverse array of leading technologies, platforms, and modern development practices, including next-generation technology enablement applications, data science, and cyber security. We are well versed in the organizational changes that are required to extract maximum advantage from transformation initiatives. We can help curate risk mitigation initiatives from preliminary audit and assessment to conceptual framework, implementation, and deployment roadmap, providing a bespoke cyber resiliency approach for the needs of your organization and particular risk profile.

Whether it's helping you lead a cyber security, business continuity, or digital transformation, KPMG creates tailored, data-driven solutions that can help you safeguard security, deliver value, drive innovation, and build stakeholder trust.

References

1 Kaspersky, "What is WannaCry ransomware", Kaspersky.com.

2 Yahalom, Raphael (January 10, 2025). "What the 2024 CrowdStrike Glitch Can Teach Us About Cyber Risk". Harvard Business Review.

3 "State of Digital Trust," ISACA, May 2023

4 "Earning Digital Trust: Decision-Making for Trustworthy Technologies, Insight Report," World Economic Forum, November 2022

5 Identity Theft Resource Center, cve.org

6 OT Cybersecurity The 2023 Year in Review, Dragos, February 2024

7 Wood, Kimberly (May 7, 2023). "Cybersecurity Policy Responses to the Colonial Pipeline Ransomware Attack". The Georgetown Environmental Law Review.

8 The 2024 KPMG Global Insights Survey

9 Easterly, Jen (May 7, 2023). "The Attack on Colonial Pipeline: What We Learned and What We've Done Over the Past Two Years.", CISA News.

Contacts

Jeoung Oh
Partner, Technology Strategy and Architecture Lead
KPMG in the U.S.

408-367-4717
jeoungoh@kpmg.com

Garima Chugh
Managing Director, Technology Line of Business, Products
KPMG in the U.S.

973-467-9650
gchugh@kpmg.com

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 in: | kpmg.com