KPMG

Unlocking Opportunities

Global Financial Reporting and Valuation Conference

December 2025

Cybersecurity: A Business Imperative

Global Financial Reporting and Valuation Conference

December 2025

Introduction

Matthew Posid

Chief Security Officer

KPMG LLP

01 Leads all security functions for KPMG LLP, including cyber and information security, insider risk, physical security, safety, enterprise resilience, crisis management, and third-party risk management.

02 Prior experience as Chief Information Security Officer at KPMG LLP and at the Central Intelligence Agency.

03 In addition to operational role, supports client engagements across numerous industry sectors.

04 Chair of Advisory Board for George Mason's "Center of Excellence in Government Cybersecurity Risk Management and Resilience".

Agenda

1. Finance-related cyber trivia
2. Threat and regulatory developments
3. Emerging trends in cybersecurity
4. Governance and leadership

Cybersecurity is Everyone's Concern

Work

Individual companies worry about risk to themselves and to their consumers, as well as complying with applicable regulations.

Investors	Consumer	3rd Parties
Supply Chain	Vendors	Partners

Home

Every one of us is dependent on security to manage finances, communicate with others, seek out healthcare, consume media, and shop.

Media	Smart Homes
Supply Chain	Healthcare

Government

Cybersecurity is of particular concern to the government, because it is a major target for threat actors and because it has an obligation to create regulations and policies.

Loss of Sensitive Data	War Crimes
Breaches of Govt. System	Geopolitical Implications of Attacks

Industry

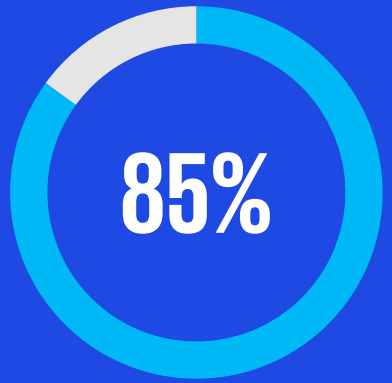
Industry sectors all care about cybersecurity, but each may have a different primary focus area based on their unique objectives.

Telecom	Healthcare	Insurance
Financial Services	Energy	Retail

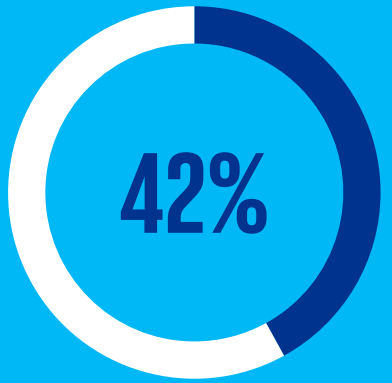
Cyber Trivia #1

What percentage of CEOs believe cybersecurity is critical to revenue growth?

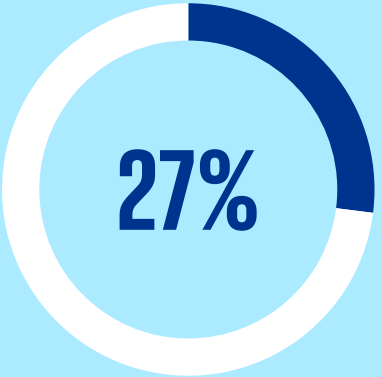
A



B



C

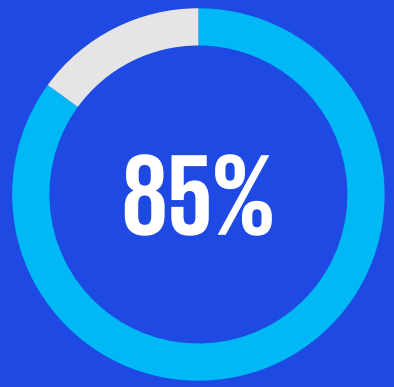


Cyber Trivia #1 (Cont.)

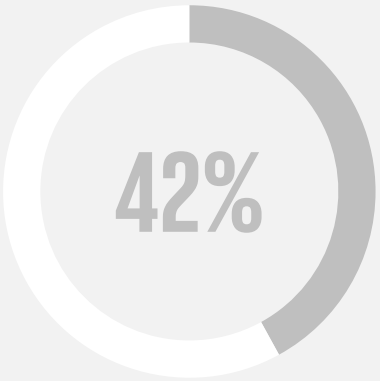
"Cybersecurity is no longer just about protection; it's a critical driver for business growth. With 85% of CEOs recognizing its importance, security leaders have a unique opportunity to demonstrate the value of cybersecurity investments not only in safeguarding assets but also in enabling strategic business objectives."

What percentage of CEOs believe cybersecurity is critical to revenue growth?

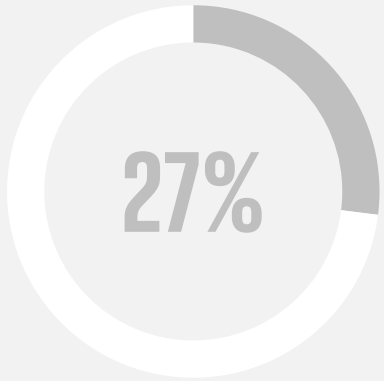
A



B



C



Source: Gartner 2025 CEO survey

Cyber Trivia #2

What is the average cost of a data breach in the United States in 2025?

A	B	C
$4.44M	$7.35M	$10.22M

Source: Gartner 2025 CEO survey

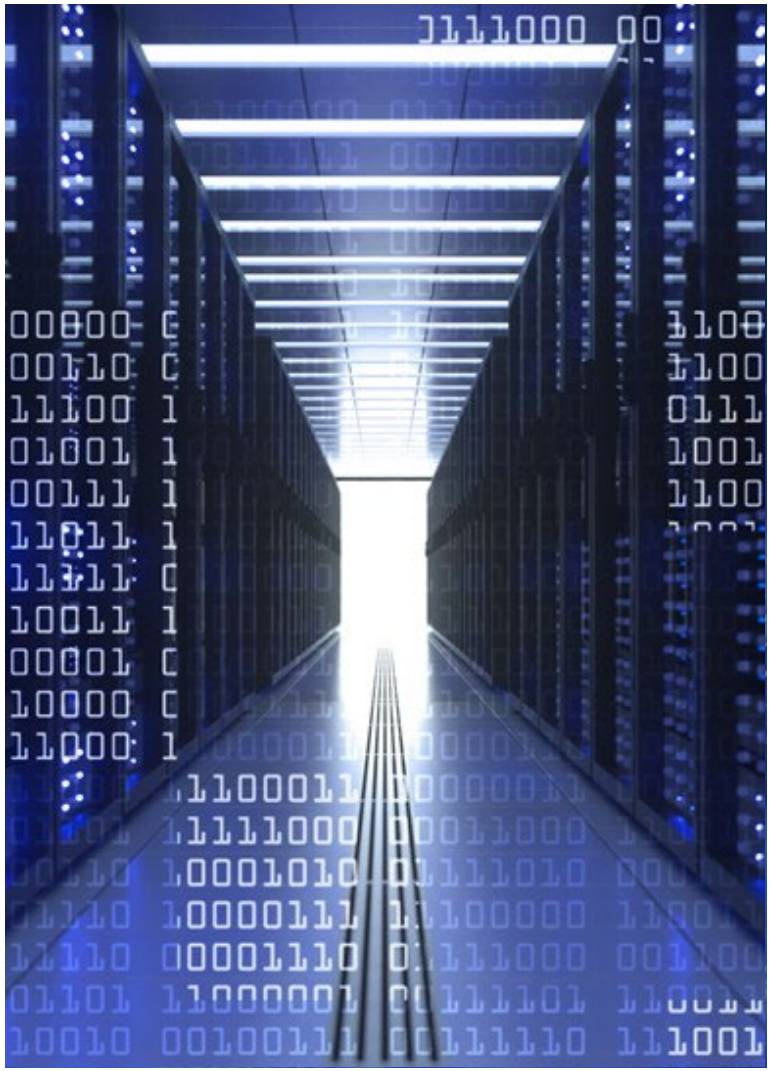
Cyber Trivia #2 (Continued)

What is the average cost of a data breach in the United States in 2025?

A	B	C
$4.44M	$7.35M	$10.22M
2025 **global** average cost		2025 US average cost

Source: IBM – Cost of a Data Breach Report 2025

Cyber Trivia #3



On average, how much more expensive is a breach that takes more than 200 days to identify?

A	B	C
$0.0M	$0.62M	$1.14M

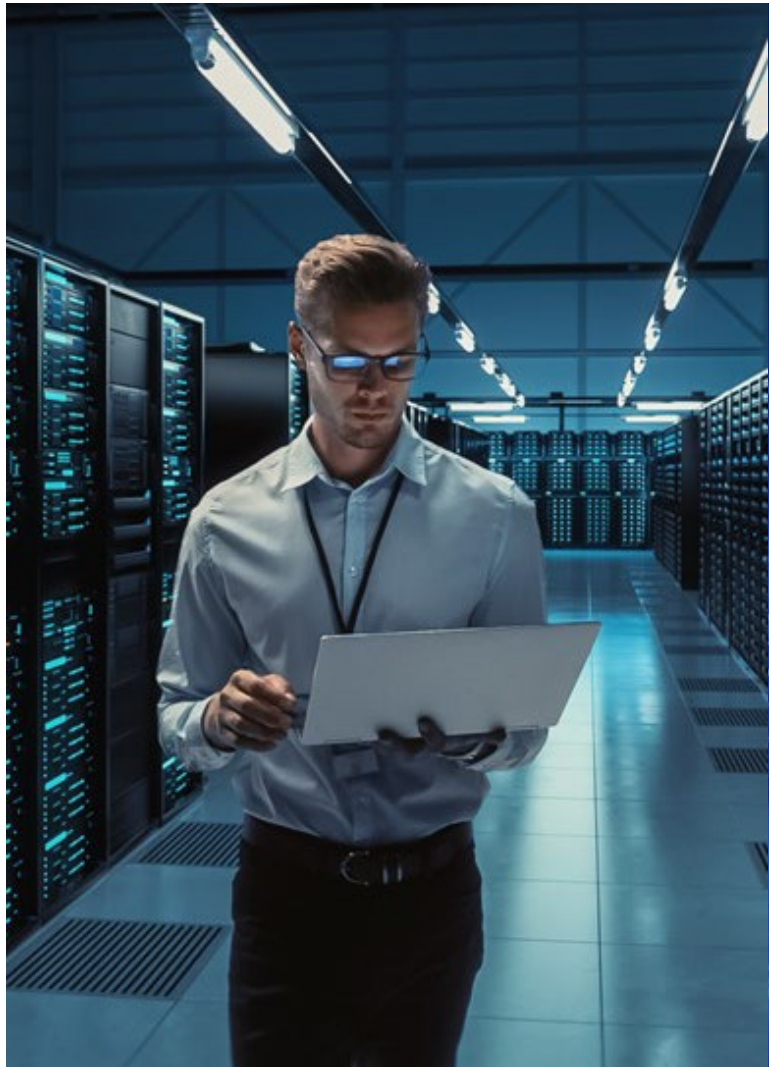
Cyber Trivia #3 (Continued)

On average, how much more expensive is a breach that takes more than 200 days to identify?

A	B	C
$0.0M	$0.62M	$1.14M

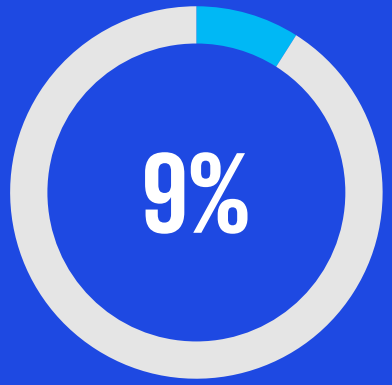
Source: IBM – Cost of a Data Breach Report 2025

Cyber Trivia #4

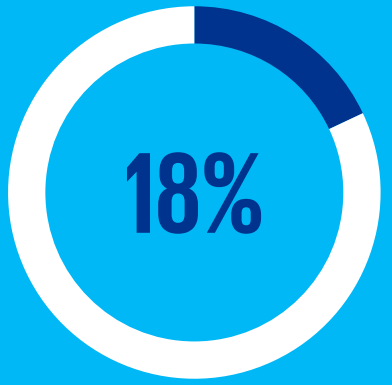


What percentage of breaches are caused by insiders?

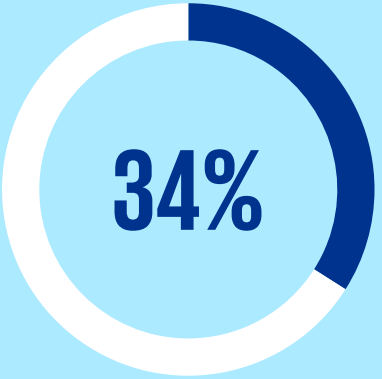
A



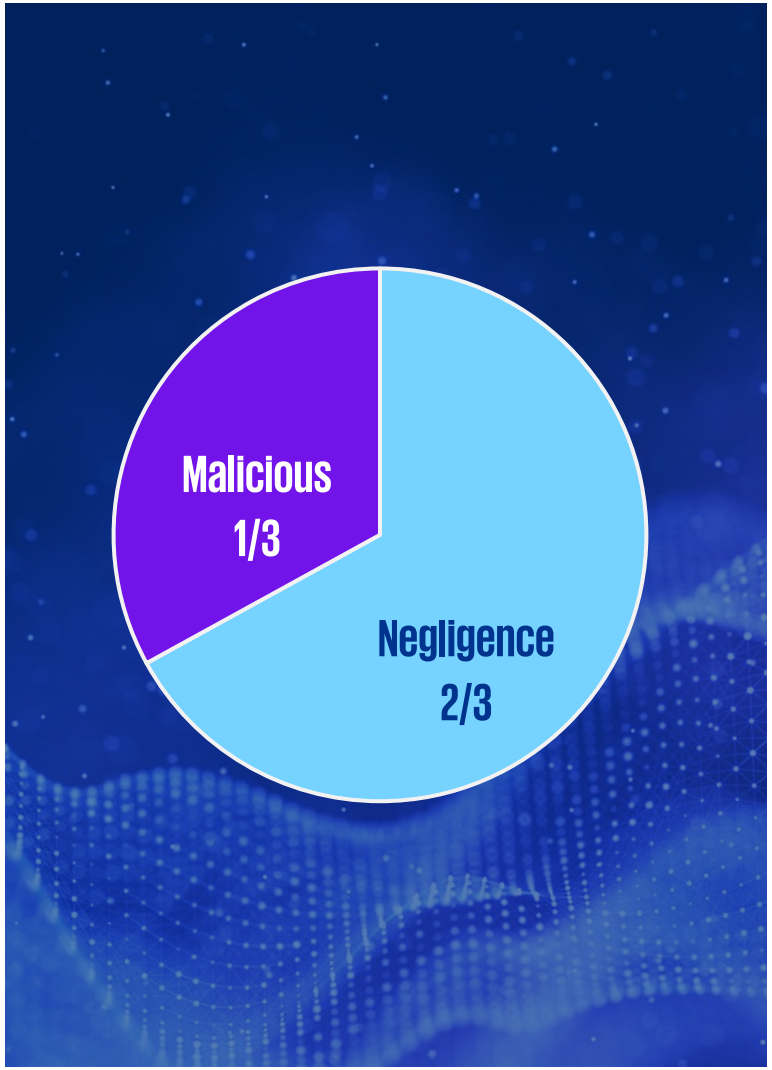
B



C



Cyber Trivia #4



What percentage of breaches are caused by insiders?

A

9%

B

18%

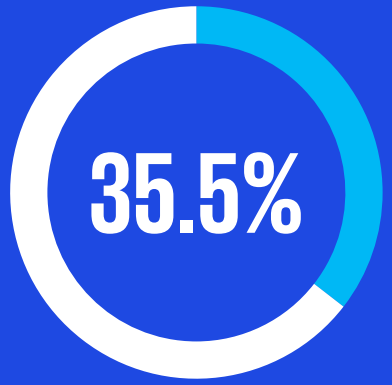
C

34%

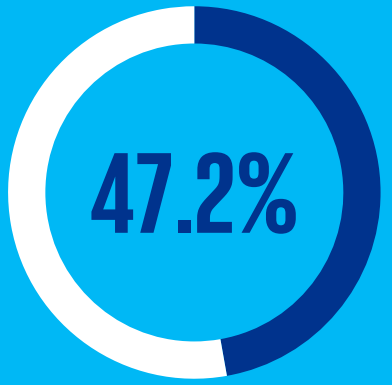
Cyber Trivia #5

What percentage of breaches were linked to a third party?

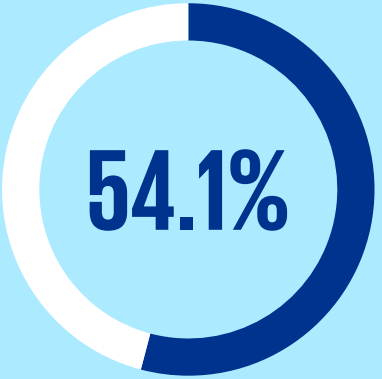
A



B



C

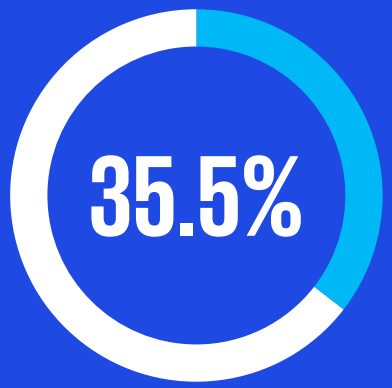


Cyber Trivia #5 (Continued)

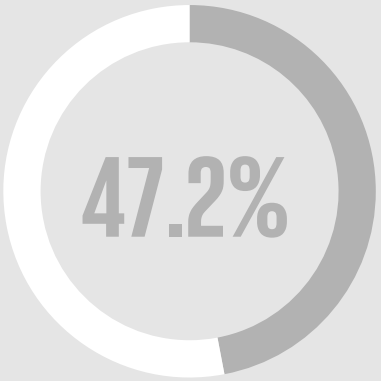
"**Surging Risk**: 35.5% of all breaches in 2024 were third-party related. This figure is likely conservative due to underreporting and misclassification."

What percentage of breaches were linked to a third party?

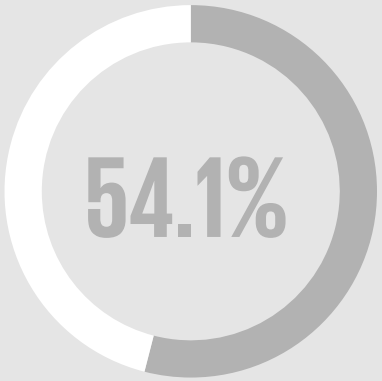
A



B



C



Source: SecurityScorecard 2025

Cybersecurity Strategy – Key Influencers

A modern cybersecurity strategy is not static; it is a dynamic response to a set of driving forces to manage risk, protect reputation, and sustain growth.

Threat Landscape

Assessing the threat landscape shapes an effective cybersecurity strategy by focusing investments on critical risks.

Regulations and Standards

Assessing the compliance landscape enables KPMG to align its information and data environment in accordance with privacy, contractual, and global security standards.

Business Drivers

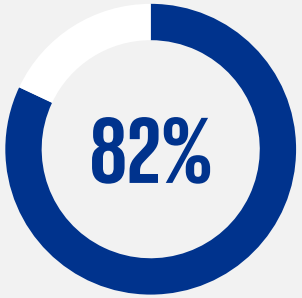
Aligning cybersecurity strategy with business priorities requires understanding key drivers, competition, and investments.

Technology Change

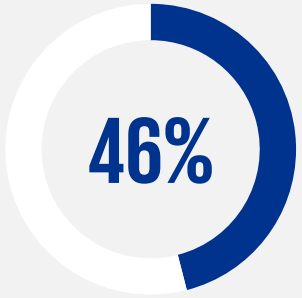
Engaging with CTOs, Legal, Risk, Infrastructure, and AI Governance teams helps formulate a business-aligned cybersecurity strategy that reduces friction.

Key perspectives from U.S. CEOs

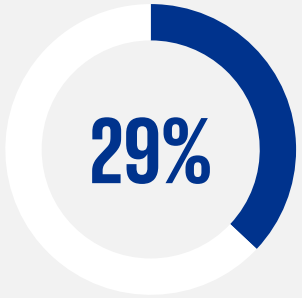
When asked to identify the top trends that could negatively impact their organization's prosperity over the next three years, U.S. CEOs most highly ranked **cybercrime and cyber insecurity**.



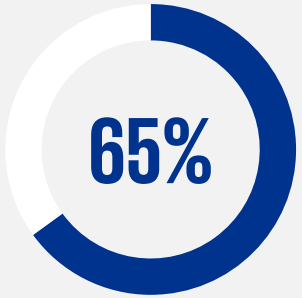
of CEOs say cybercrime is high on their near- and long-term risk radar



have increased investment in cybersecurity and digital risk resilience to mitigate pressing business risk over the next three years



of CEOs report cybersecurity risk is a top pressure driving short-term decisions only behind supply chain resilience



of CEOs are extremely concerned about cyber risks specifically related to fraud detection, identity theft, and data privacy

U.S. CEOs cite these top pressures driving short-term decisions

- Supply chain resilience
- Cybersecurity risk
- Global economic uncertainty
- AI integration into business processes
- Regulatory pressures

Source: The 2025 KPMG U.S. CEO Outlook Survey

Zero Trust

Technology is fundamental to its success...

But it is not a technology

It will cost you money to deliver...

But it cannot be bought

It's a journey...

But there is no destination

Key Principles

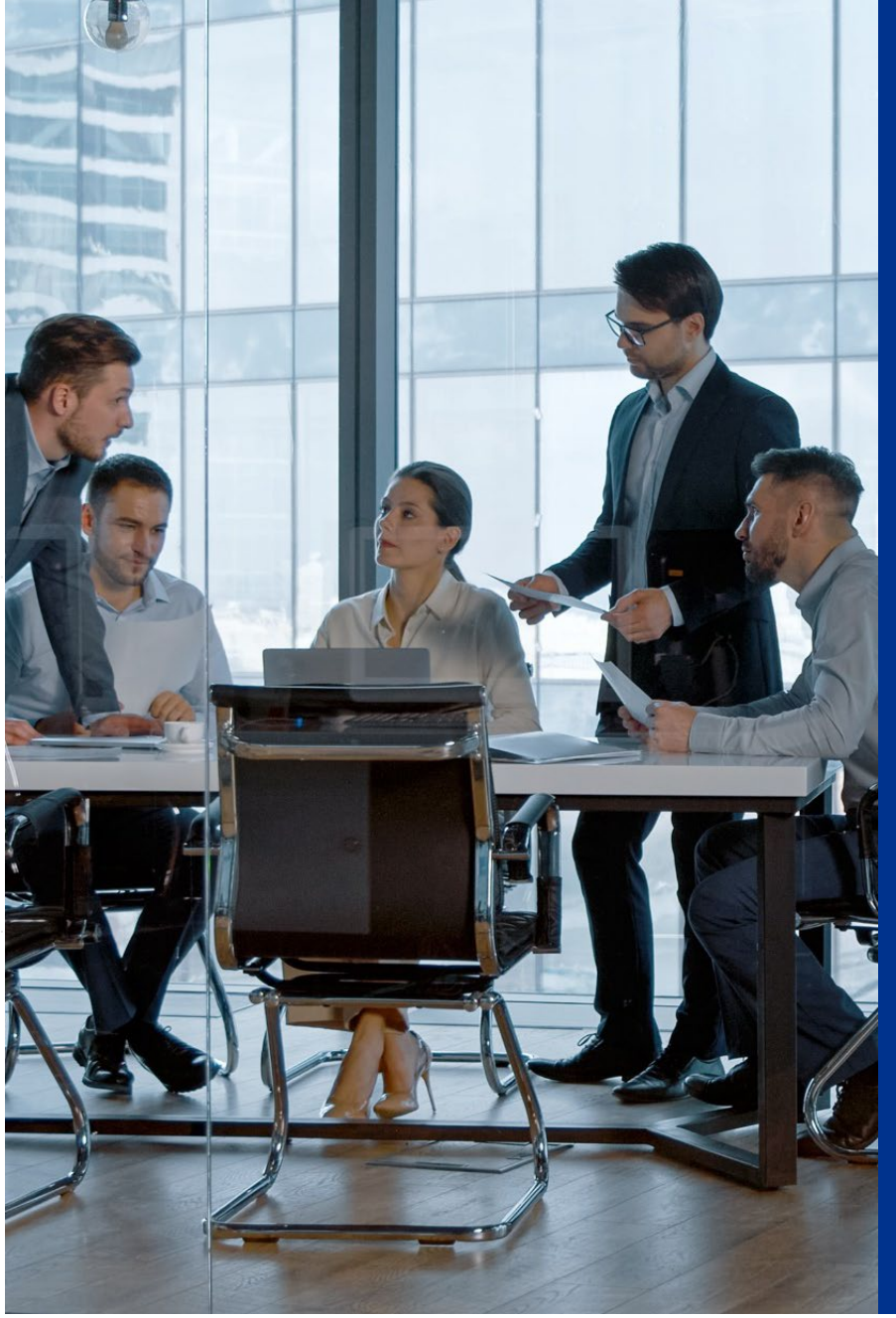
- Enforce standards
- Never trust
- Minimize privilege
- Assume breach
- Monitor everything

Key things to consider while evaluating solutions

- Identity
- Devices
- Networks
- Applications
- Workloads
- Data

Typical impediments to success

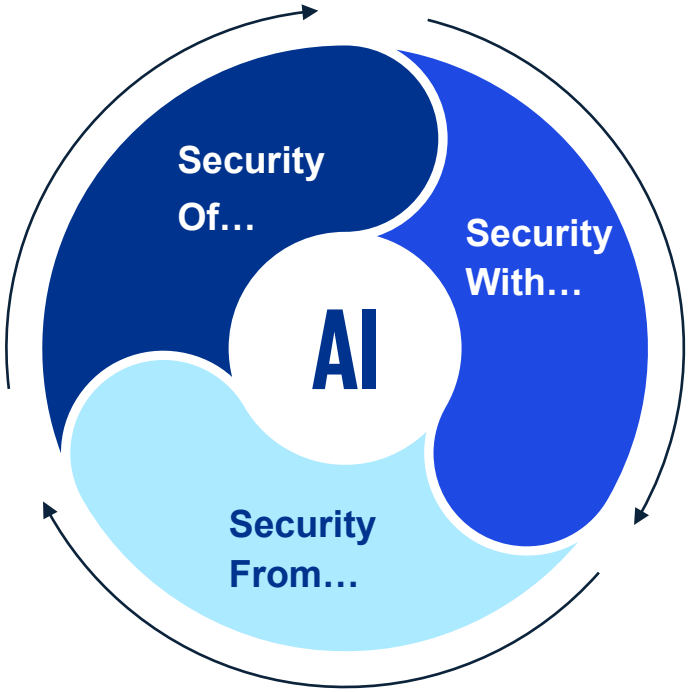
- Legacy IT/architecture dependencies that rely on implicit trust
- Poor lifecycle management habits
- True leadership commitment
- Attempt to do too much all at once



AI Security

Are my AI tools secure?

- Business vs. security responsibilities
- Unapproved technologies
- Citizen developers and vibe coding
- Model development/ supply chain security



Can AI improve our security posture?

- Improved threat monitoring and detection
- Advanced analytics and prioritization
- Faster and higher quality security risk assessments

How to we protect from adversaries using AI?

- Targeted social engineering
- Deepfake attacks
- Speed of exploitation
- Democratization of hacking

Third-party risks

Increasing source of risk for most organizations

- Increasing rate of incidents with third-parties
- Increasing use of third-parties, including dynamic “as a service” providers
- Growing complexity of regulatory environment
- Relationship complexities – fourth parties and 360° relationships

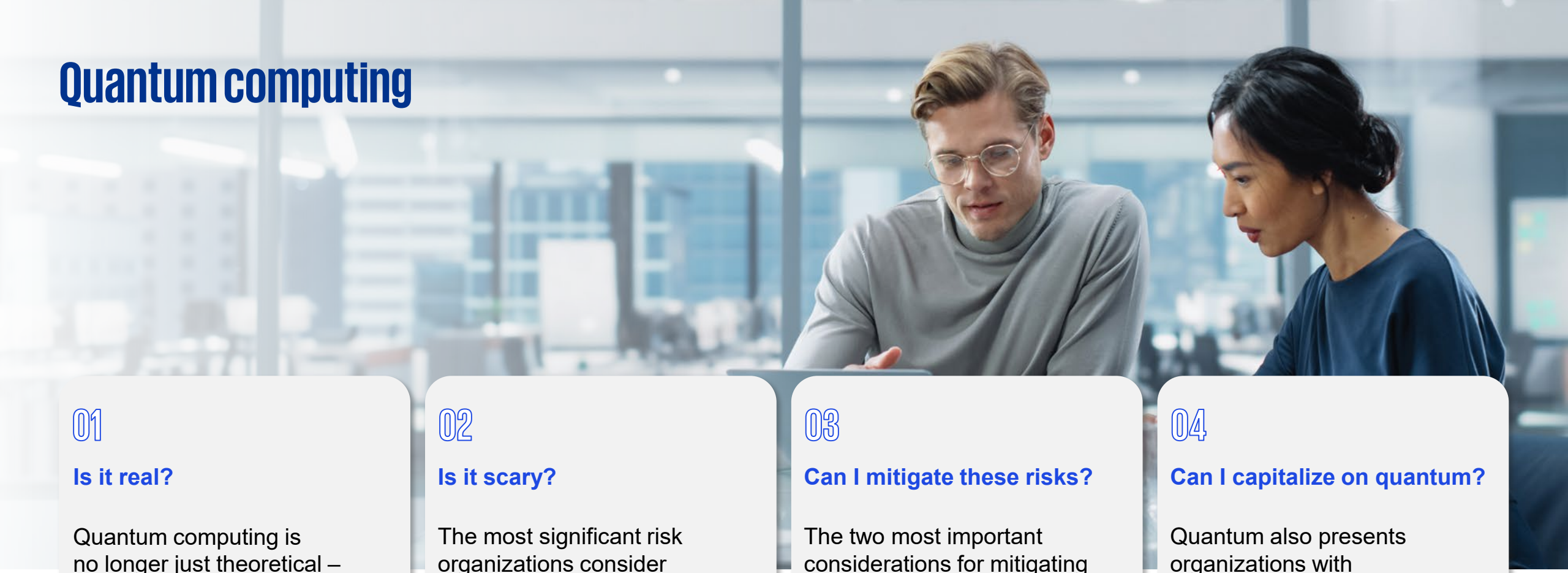
Third-party risk assessment processes are time consuming and expensive

- Numerous dimensions of third-party risk assessments
- Continuous monitoring is often limited

Third-party risk programs don’t eliminate third-party risks

- Good third parties have bad days
- Organizational resilience is key to holistic third-party risk reduction

Quantum computing



01

Is it real?

Quantum computing is no longer just theoretical – real quantum computers exist and are becoming more powerful.

02

Is it scary?

The most significant risk organizations consider related to quantum is “cracking encryption” and exposing sensitive information.

03

Can I mitigate these risks?

The two most important considerations for mitigating quantum-related risk:

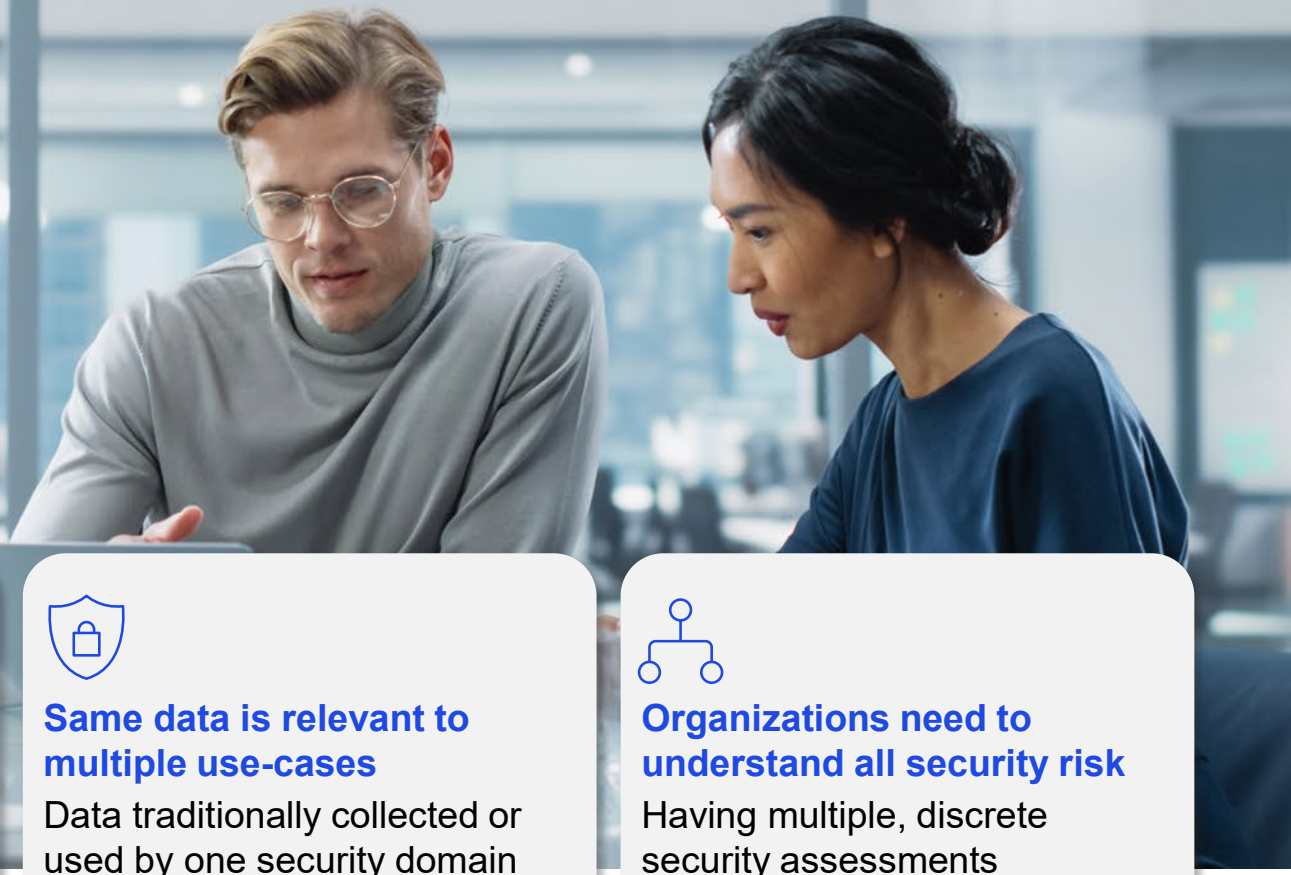
- Understanding your data and retention/protection requirements
- Adopting post-quantum cryptography solutions

04

Can I capitalize on quantum?

Quantum also presents organizations with opportunities, including increased analytic capability and increased security.

Multi-domain security challenges



Properly protecting organizations in today's threat environment requires a complete integration of security strategies, capabilities, and processes

Threats are multi-domain

The threats we face don't care about traditional security domains or organizational models

Gaps are exploitable

Inconsistences between security domains create risk for organizations

Same data is relevant to multiple use-cases

Data traditionally collected or used by one security domain is increasingly relevant to other areas

Organizations need to understand all security risk

Having multiple, discrete security assessments requires business leadership to try to piece together total exposure

Governance & Leadership

Leadership Empowerment

Ensure leadership buy-in on the importance of security, providing the Chief Information Security Officer (CISO) with clear authority and a defined mandate

Continuous Governance

Routine engagement with Management and Board leadership about changes in the operating environment, how those changes impact risk posture, and what is being done

Centralized Oversight

Implement a centralized cyber monitoring and response program capable of comprehensive end-to-end oversight across the firm to minimize blind spots and eliminate shadow IT

Shared Accountability

Establish clear and consistent shared risk decisions where accountability for outcomes rests with the business sponsors of IT systems, rather than solely with the security team

Rapid Adaptability

Maintain flexibility to quickly deploy resources for rapid threat response, recognizing that threats are unpredictable and administrative processes must be adaptable

Any questions?

Thank you!

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

kpmg.com

DAS-2025-19303