Navigate the Digital Battleground

With Insights from BDO's State of Cyber Report

NOVEMBER 7, 2024

With You Today

WAYNE ANDERSON
Director, Cybersecurity

wanderson@bdo.com

JYOTI DALAL
Assurance Principal, Third Party Attestation

jdalal@bdo.com

Learning Objectives

1

Review how AI is being leveraged to both defend against and perpetrate cyber threats

2

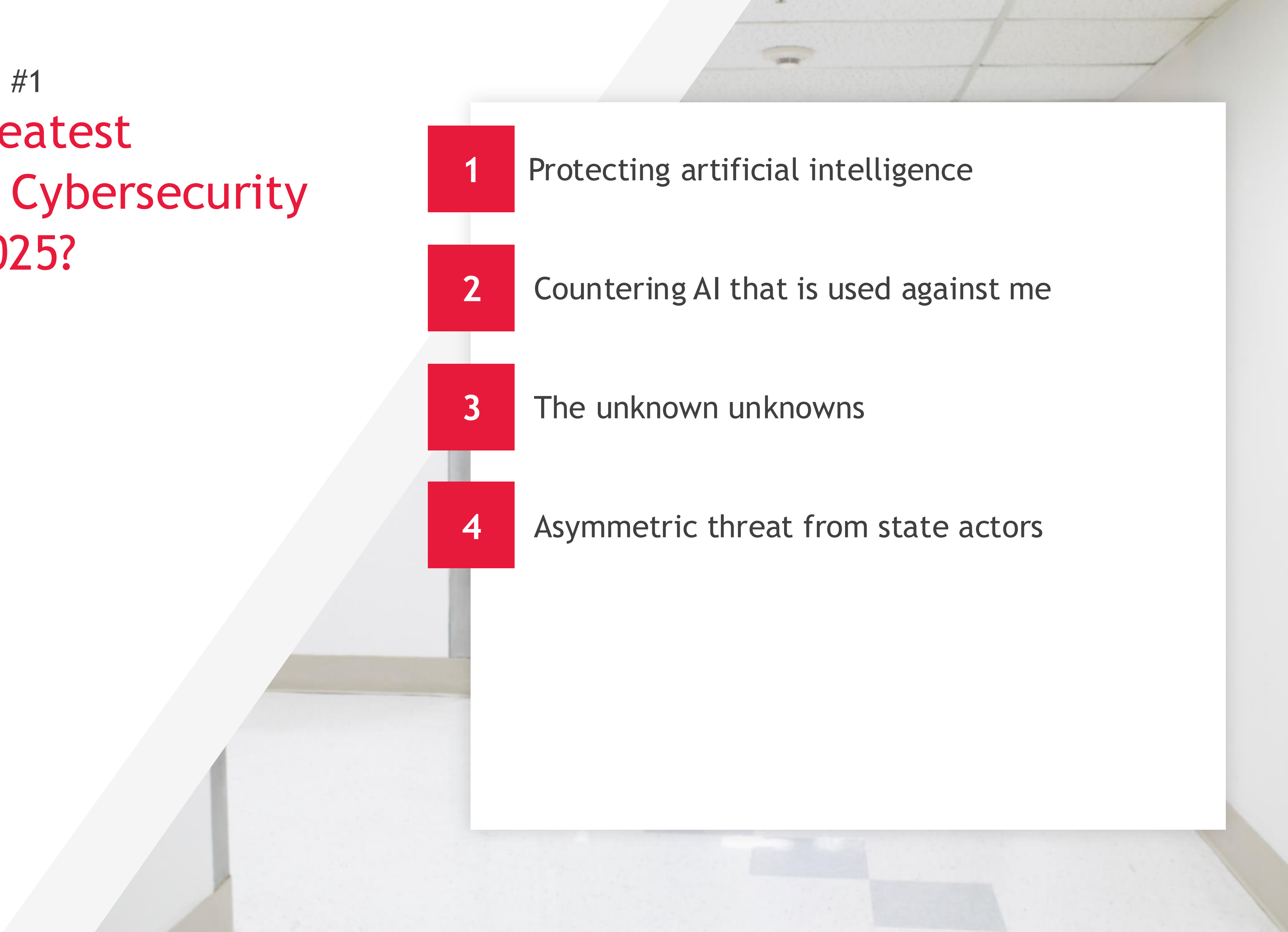
Discuss the evolving regulatory requirements and how to ensure your company remains compliant

3

Identify the potential vulnerabilities and best practices for securing your cloud infrastructure

DISCUSSION QUESTION #1

What is the greatest uncertainty in Cybersecurity thinking for 2025?



1 Protecting artificial intelligence

2 Countering AI that is used against me

3 The unknown unknowns

4 Asymmetric threat from state actors

CHALLENGE 1

Generative AI is Enhancing Cyberattacks

Dual Nature of Generative AI:

- Generative AI introduces new challenges
- Support Role: Also aids in enhancing cybersecurity defenses

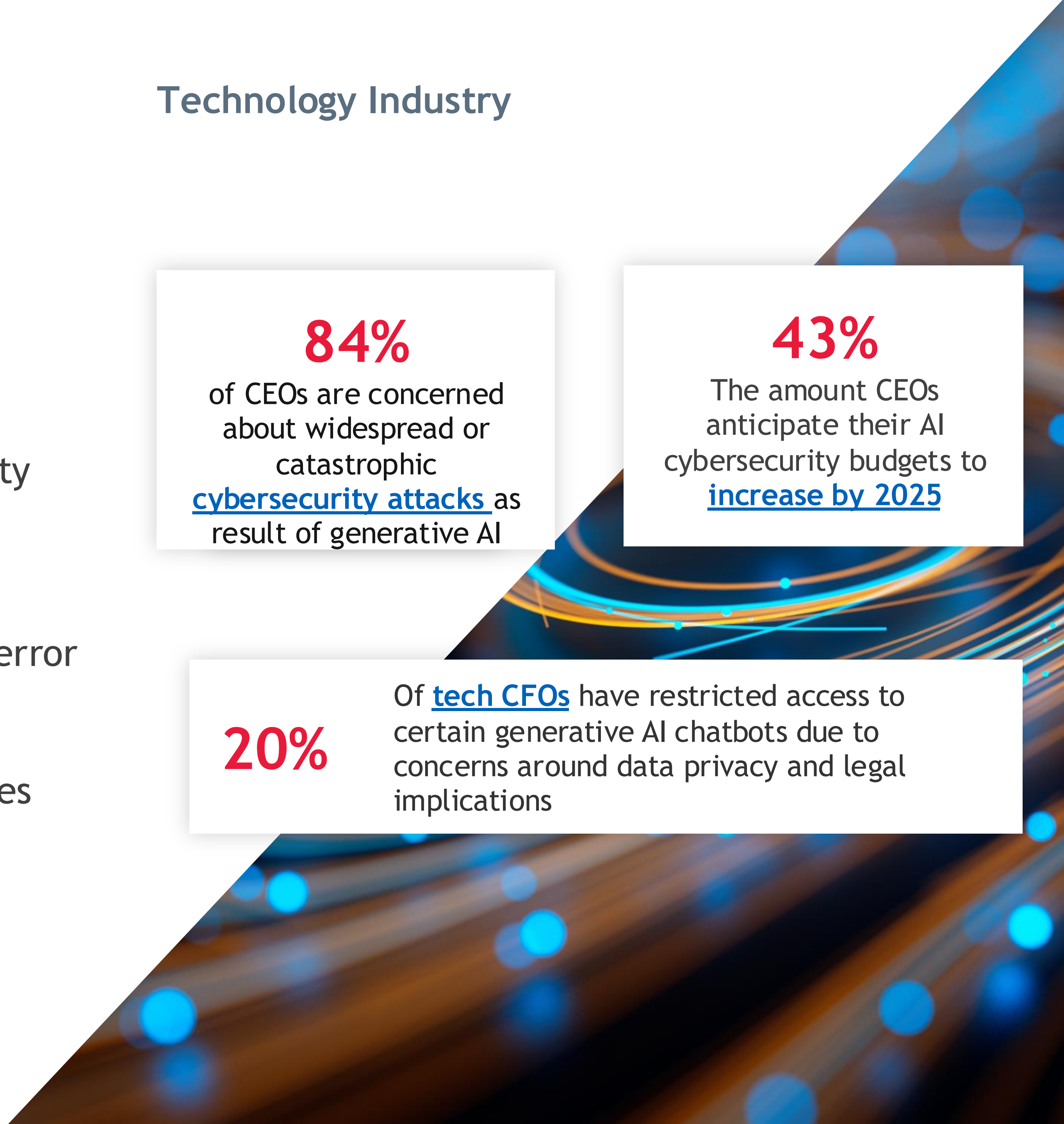
Impact of Human Error:

- Over 80% of cyber incidents are due to human error

AI's Contributions to Cybersecurity:

- Helps cyber leaders address critical vulnerabilities
- Automates routine cybersecurity tasks
- Detects patterns that are invisible to humans

Technology Industry



84%
of CEOs are concerned about widespread or catastrophic cybersecurity attacks as result of generative AI

43%
The amount CEOs anticipate their AI cybersecurity budgets to increase by 2025

20%
Of tech CFOs have restricted access to certain generative AI chatbots due to concerns around data privacy and legal implications

CHALLENGE 1 Generative AI

Recommendations

1

INCREASING RESPONSE SPEED

Automating early threat detection shortens the time between attack and discovery through early warnings, speeding up responses.

2

IDENTIFYING TRENDS IN DATA

Generative AI can effectively leverage historical data sets, like ticketing logs, data from previous attacks, industry insights, and more, to predict potential attack vectors.

3

UNDERSTAND THREAT LANDSCAPE

Having the right tools in place to help improve risk detection is crucial. These tools analyze network changes and large data sets, using behavioral analytics and anomaly detection to identify unusual activities.

CHALLENGE 2

Ransomware Threat is Growing

New Methods of Growing Concern

- Double Extortion and triple extortion
- Affects both companies and individuals.
- Threatens reputational damage and loss of sensitive data.

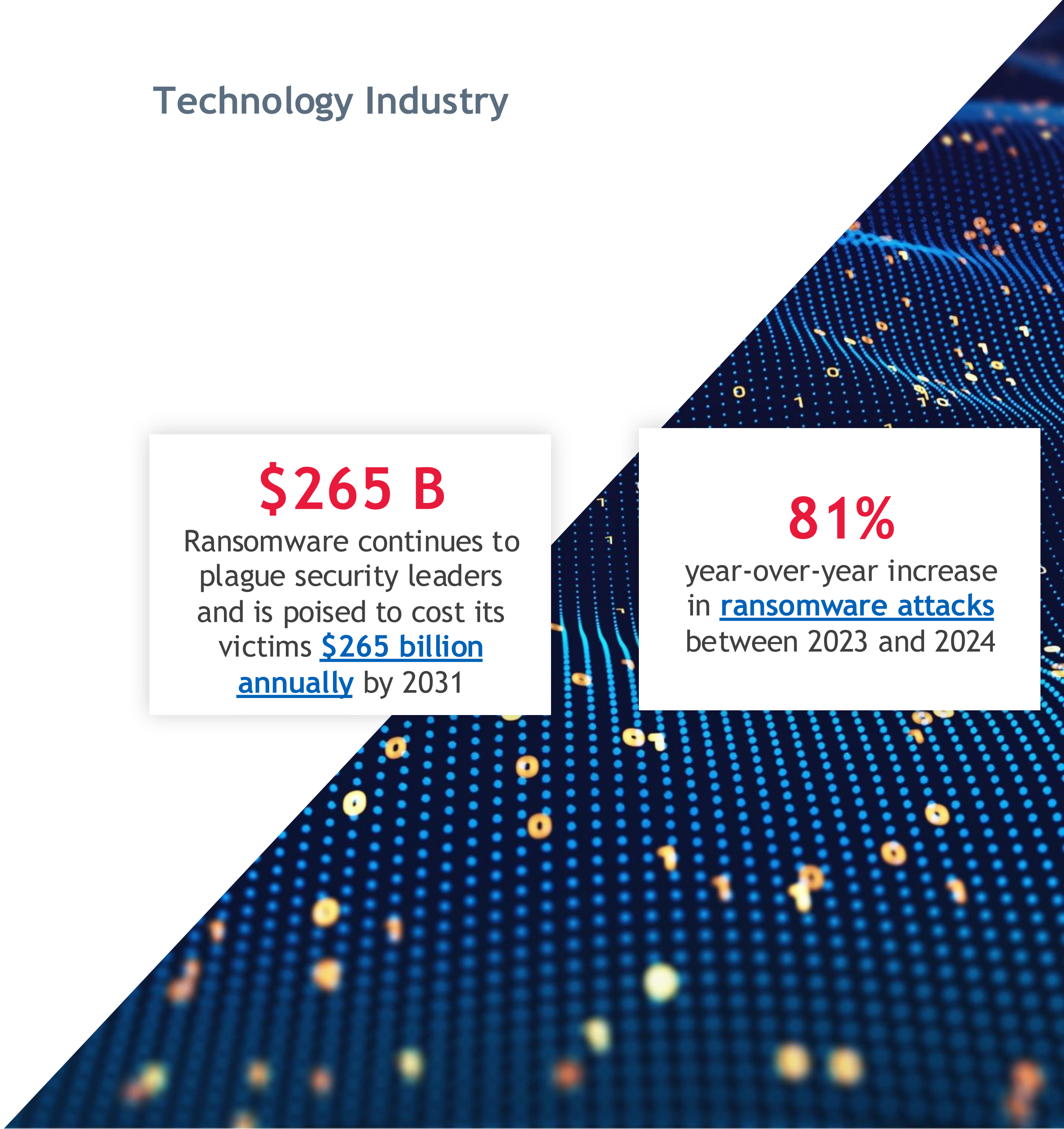
Historical Context:

- Traditionally time-consuming and manual

Types of Data at Risk

- Trade secrets
- Personally identifiable information (PII)
- Other sensitive data

Technology Industry



$265 B

Ransomware continues to plague security leaders and is poised to cost its victims [$265 billion annually] by 2031

81%

year-over-year increase in [ransomware attacks] between 2023 and 2024

CHALLENGE 2 Ransomware

Recommendations

1

CREATE A CULTURE OF VIGILANCE

Research from Gartner indicates that organizations with a strong security culture experience **30%** fewer security incidents than those without one.

Source: HoxHunt

2

PLAN FOR THE WORST

Organizations with an IR team and tested IR plan in place saw an average cost of a data breach of **$3.25 million**, compared to **$5.71 million** for those without these measures. This represents a cost savings of nearly **50%**.

Source: IBM

3

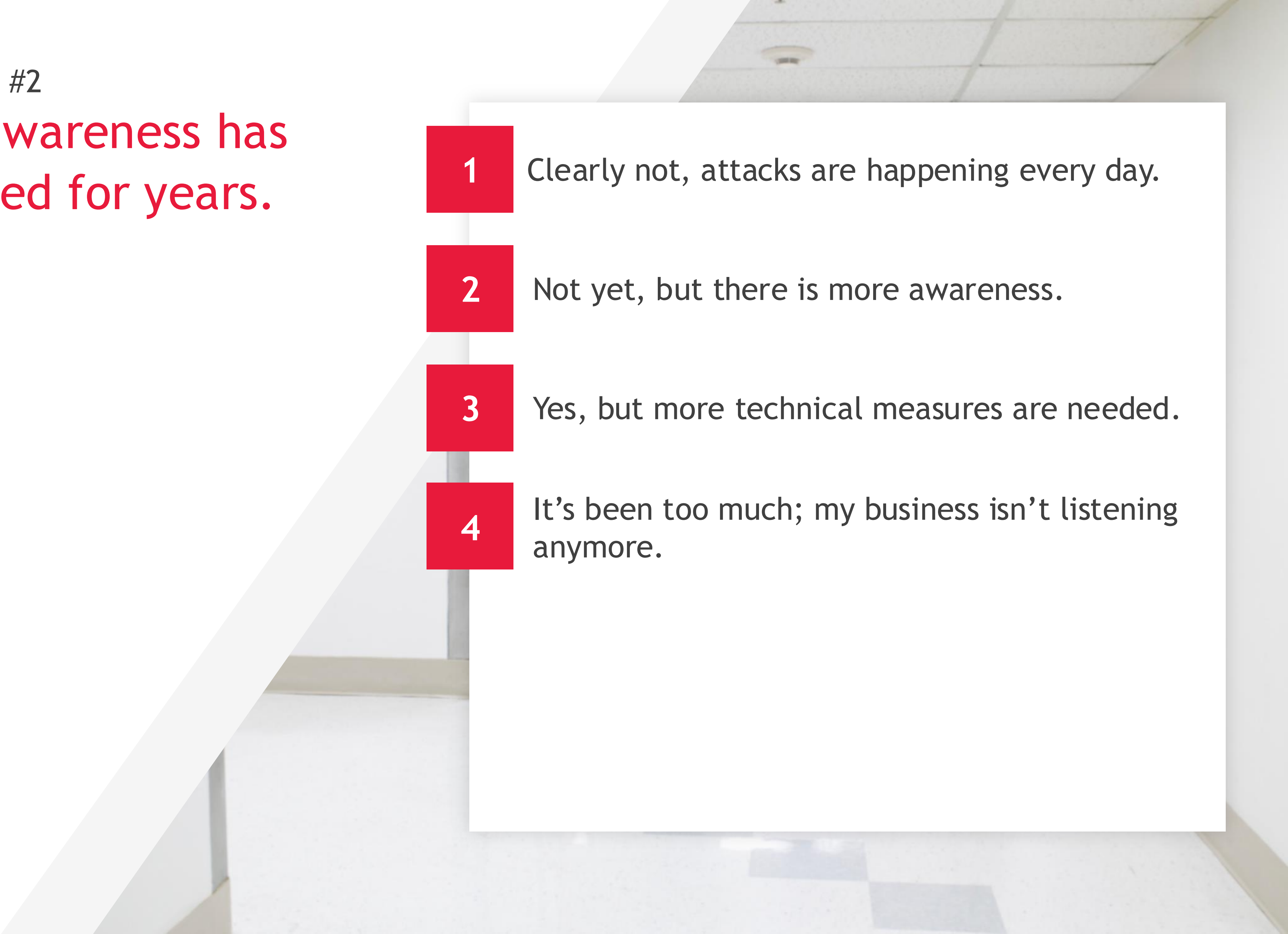
PRACTICE, PRACTICE, PRACTICE

Organizations that engage in regular cyber resilience exercises, including tabletop scenarios, see a **60%** increase in employee awareness and preparedness for cyber incidents.

Source: SANS Institute

DISCUSSION QUESTION #2

Ransomware awareness has been highlighted for years. Is it enough?



1 Clearly not, attacks are happening every day.

2 Not yet, but there is more awareness.

3 Yes, but more technical measures are needed.

4 It’s been too much; my business isn’t listening anymore.

CHALLENGE 3

Maintaining Compliance in Evolving Landscape

GDPR Influence

- The GDPR sets data protection standards, influencing many U.S. organizations to adopt similar practices.

Quick Incident Disclosure

- Increasing regulatory pressure requires quicker disclosure of material incidents, as outlined by the SEC and FTC.

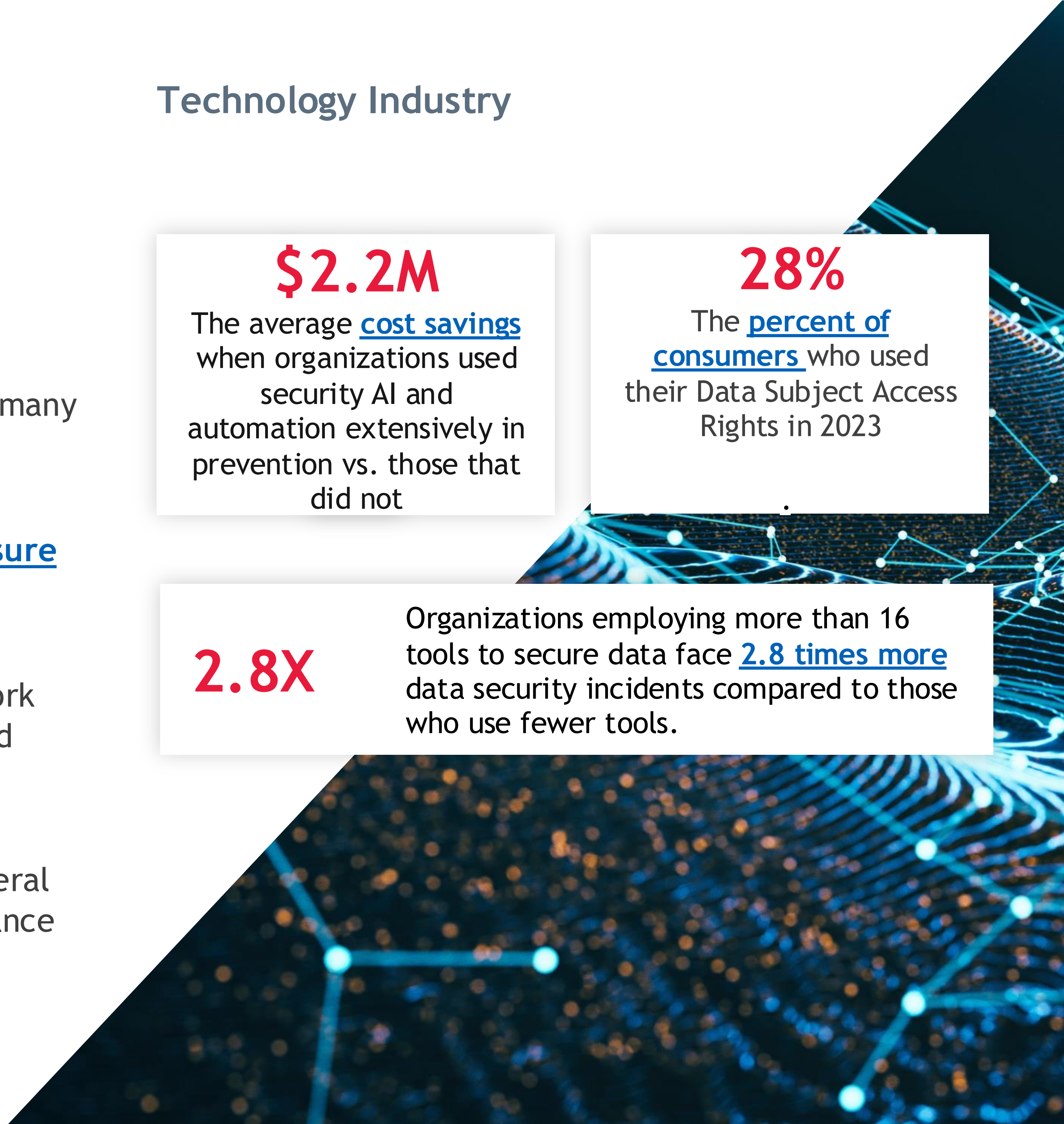
Broader Impact

- Regulations affect public companies and those who work with them, necessitating broader risk management and governance.

Zero-Trust Strategy

- The White House's zero-trust strategy mandates federal agencies to complete tasks by fiscal year 2024 to enhance cybersecurity.

Technology Industry



$2.2M

The average cost savings when organizations used security AI and automation extensively in prevention vs. those that did not

28%

The percent of consumers who used their Data Subject Access Rights in 2023

2.8X

Organizations employing more than 16 tools to secure data face 2.8 times more data security incidents compared to those who use fewer tools.

CHALLENGE 3 Maintaining Compliance

Recommendations

1

INVEST IN EDUCATION

Organizations that implement regular cybersecurity training programs are **58%** more likely to achieve and maintain compliance with regulations such as GDPR, HIPAA, and PCI-DSS.

These organizations experience **50%** reduction in fines/ penalties related to non-compliance.

Source: Ponemon Institute

2

REGULAR RISK ASSESSMENTS

Organizations that conduct regular risk assessments are **2.6X** more likely to identify and mitigate threats effectively compared to those that do not, according to Gartner's research on security and risk management.

These organizations are **2.5X** more likely to have higher levels of trust from their customers and partners.

Source: Gartner

3

CONDUCT COMPLIANCE AUDITS

The cost of non-compliance is **2.71X** higher than the cost of maintaining compliance, emphasizing the financial benefits of regular audits.

These companies also have response times that are **30%** faster in mitigating threats and breaches

Source: Forrester

CHALLENGE 4

Risks of Poor Cloud Migration and Management

Increased Data Breach Costs

Organizations that do not effectively manage their cloud security face breach costs that are **2.5 times** higher than those with robust cloud security practices.

Source: Forrester

Higher Likelihood of Data Breaches

93% of organizations have experienced a data security incident in the cloud in the past **18 months**.

Source: IDC

Compliance Failures

49% of companies that fail to comply with cloud security regulations will face fines and penalties, with an average cost of **$1.2 million** per incident.

Source: Forrester

Operational Disruptions

Gartner predicts that through 2024, **60%** of organizations that implement appropriate cloud visibility and controls tools will experience **one-third** fewer security failures.

Source: Gartner

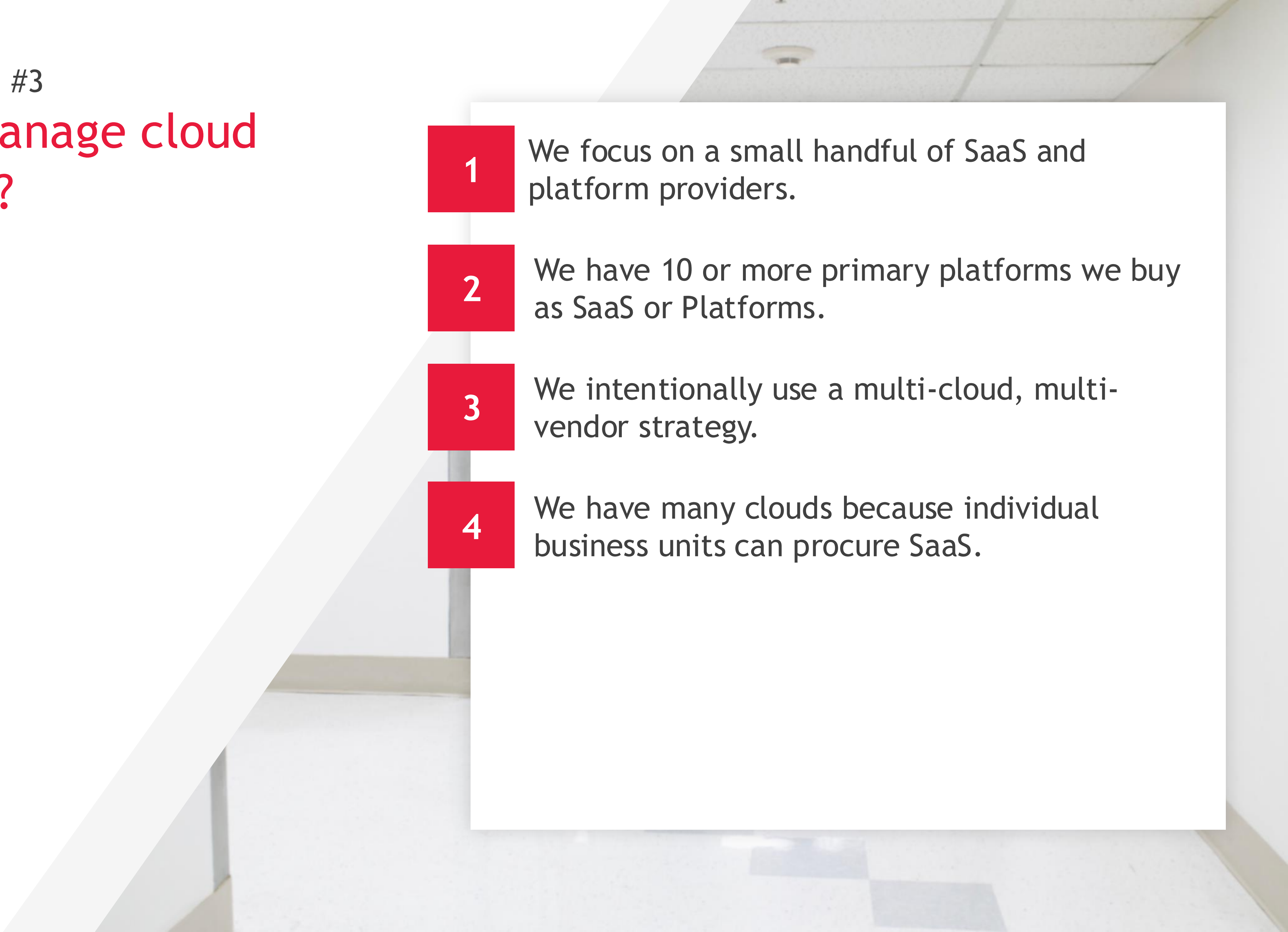
Increased Vulnerability

Poor identity verification and clod management practices contribute to **70%** of unauthorized access incidents in cloud environments.

Source: Microsoft

DISCUSSION QUESTION #3

How do you manage cloud vendor sprawl?



1 We focus on a small handful of SaaS and platform providers.

2 We have 10 or more primary platforms we buy as SaaS or Platforms.

3 We intentionally use a multi-cloud, multi-vendor strategy.

4 We have many clouds because individual business units can procure SaaS.

CHALLENGE 4 Cloud Inconsistencies

Recommendations

1

IMPLEMENT A ZERO TRUST POLICY

In addition to reducing data breach costs, faster detection, enhanced compliance, etc., organizations with a Zero Trust framework experience a **70%** reduction in insider threats, as the model enforces strict access controls and continuous monitoring.

Source: Cybersecurity Insiders

2

LEVERAGE A COMPREHENSIVE MONITORING SOLUTION

Companies without comprehensive threat detection tools take **60%** longer to detect security incidents, increasing the potential for damage.

These companies also experience an average dwell time of an attacker that is **2.5 times** longer, allowing attackers more time to cause harm.

Source: Ponemon

3

CREATE A CLOUD INCIDENT PLAN

By 2025, **99%** of cloud security failures will be the customer's fault.

This highlights the importance of having a robust cloud incident response plan to mitigate risks associated with cloud environments

Source: Gartner

Artificial Intelligence

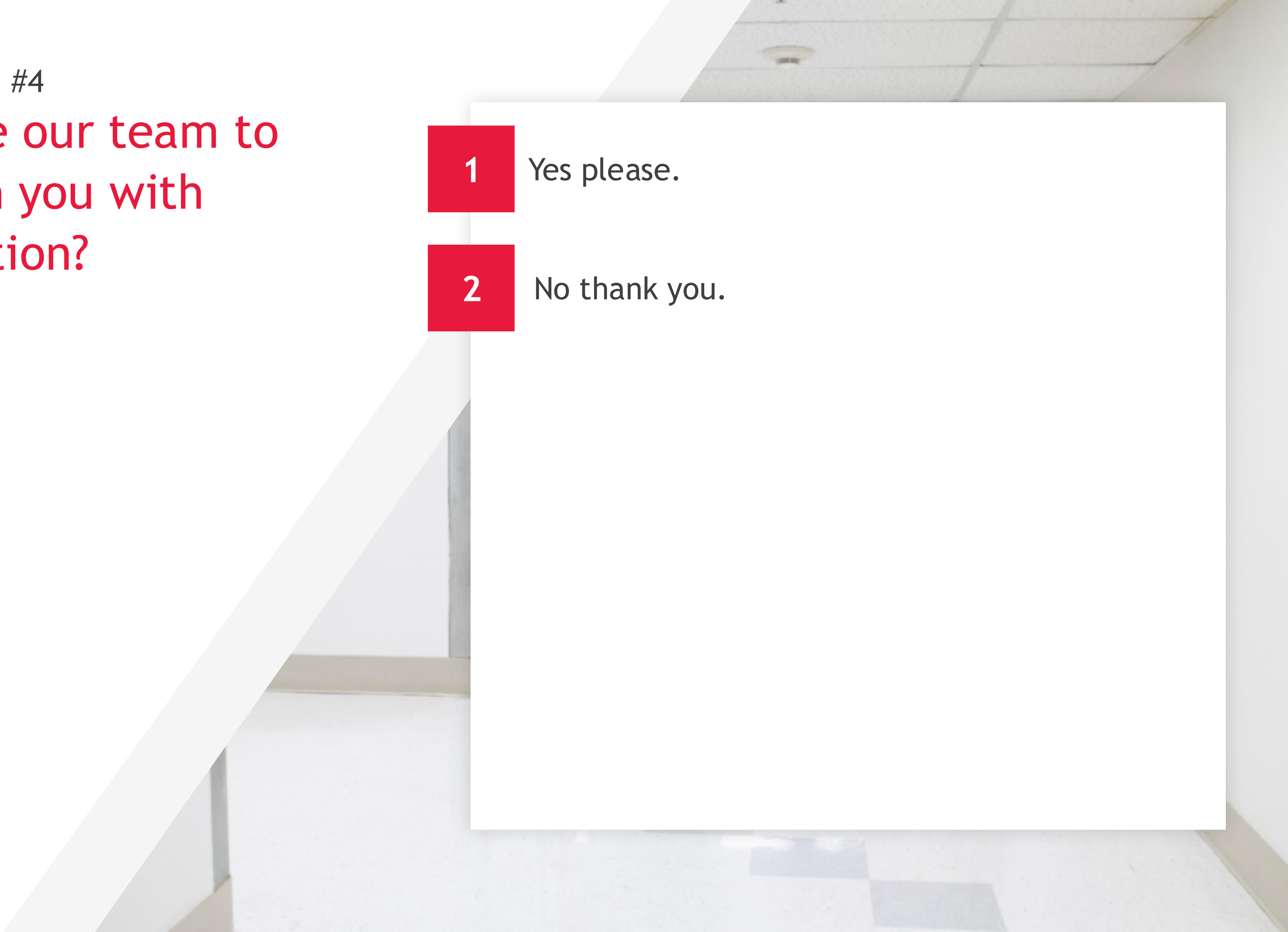
Technology Clients are Investigating. Build New Outcomes. Manage Risks.

BDO helps you empower your everyday with AI.

- We help you navigate AI – its risks and applications, embedding it into your day-to-day operations, empowering your team to work smarter, faster, and more strategically.
- We'll give you a step-by-step roadmap that aligns AI to your business goals and company values, prioritizing initiatives that delivers high ROI and sustainable impact.
- We're here every step of the way, from initial education and planning through to implementation, adoption, and beyond.
- We evaluate risk holistically, weighing potential benefits against harm.

DISCUSSION QUESTION #4

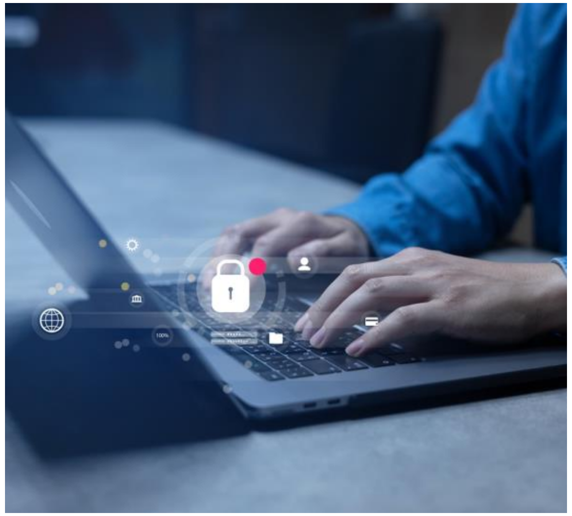
Would you like our team to follow up with you with more information?



1 Yes please.

2 No thank you.

How to Get Started

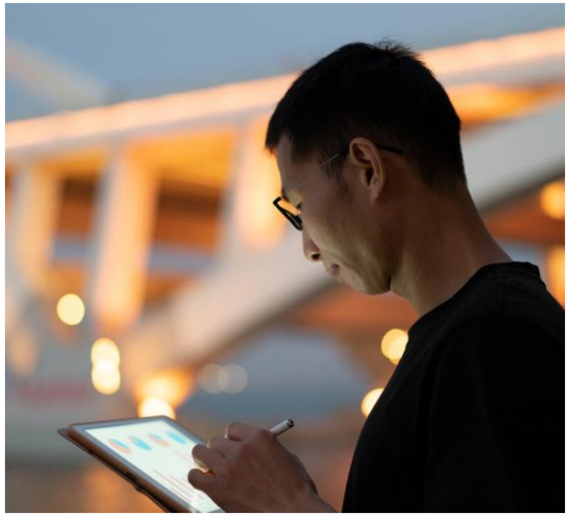


Cyber Insights

A short, free discovery workshop to interview the team, assess Microsoft 365 and Azure cloud assets and prepare a cyber enhancement plan.

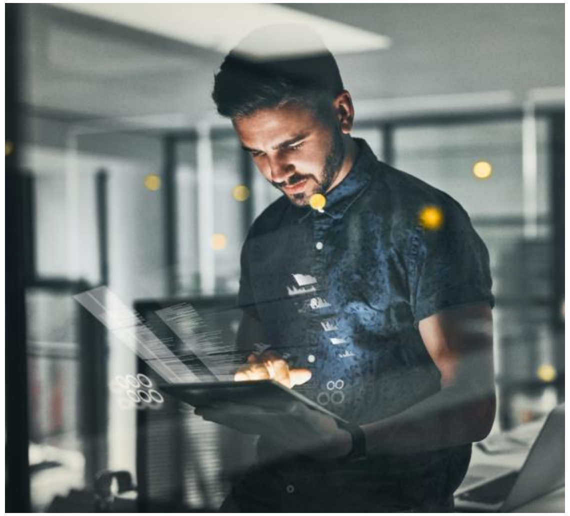
Data Security

Get a baseline discovery and prioritized steps to reduce risk to your sensitive data. Know what you hold and protect it.



AI Workshop

In our AI workshop, we'll do a short AI briefing, company strategic overview, talk through AI readiness, and focus on brainstorming scenarios.



Active Assure

Cyber-attack simulation and purple teaming services deliver continuous simulation of known cyberattack methods.

Thank You!

Questions?

About BDO USA

At BDO, our purpose is helping people thrive, every day. Together, we are focused on delivering exceptional and sustainable outcomes — for our people, our clients and our communities. Across the U.S., and in over 160 countries through our global organization, BDO professionals provide assurance, tax and advisory services for a diverse range of clients.

BDO is the brand name for the BDO network and for each of the BDO Member Firms. BDO USA, P.C, a Virginia professional corporation, is the U.S. member of BDO International Limited, a UK company limited by guarantee, and forms part of the international BDO network of independent member firms.

www.bdo.com

Material discussed is meant to provide general information and should not be acted on without professional advice tailored to your needs.