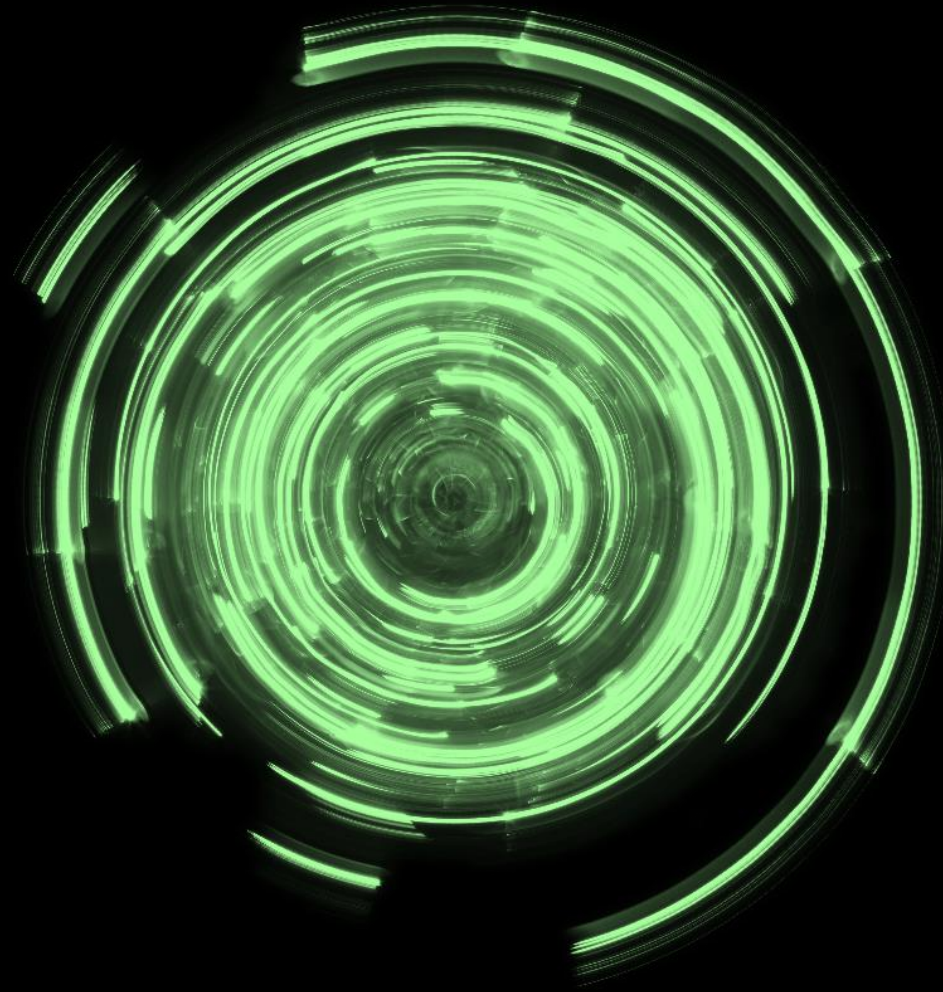


Deloitte.



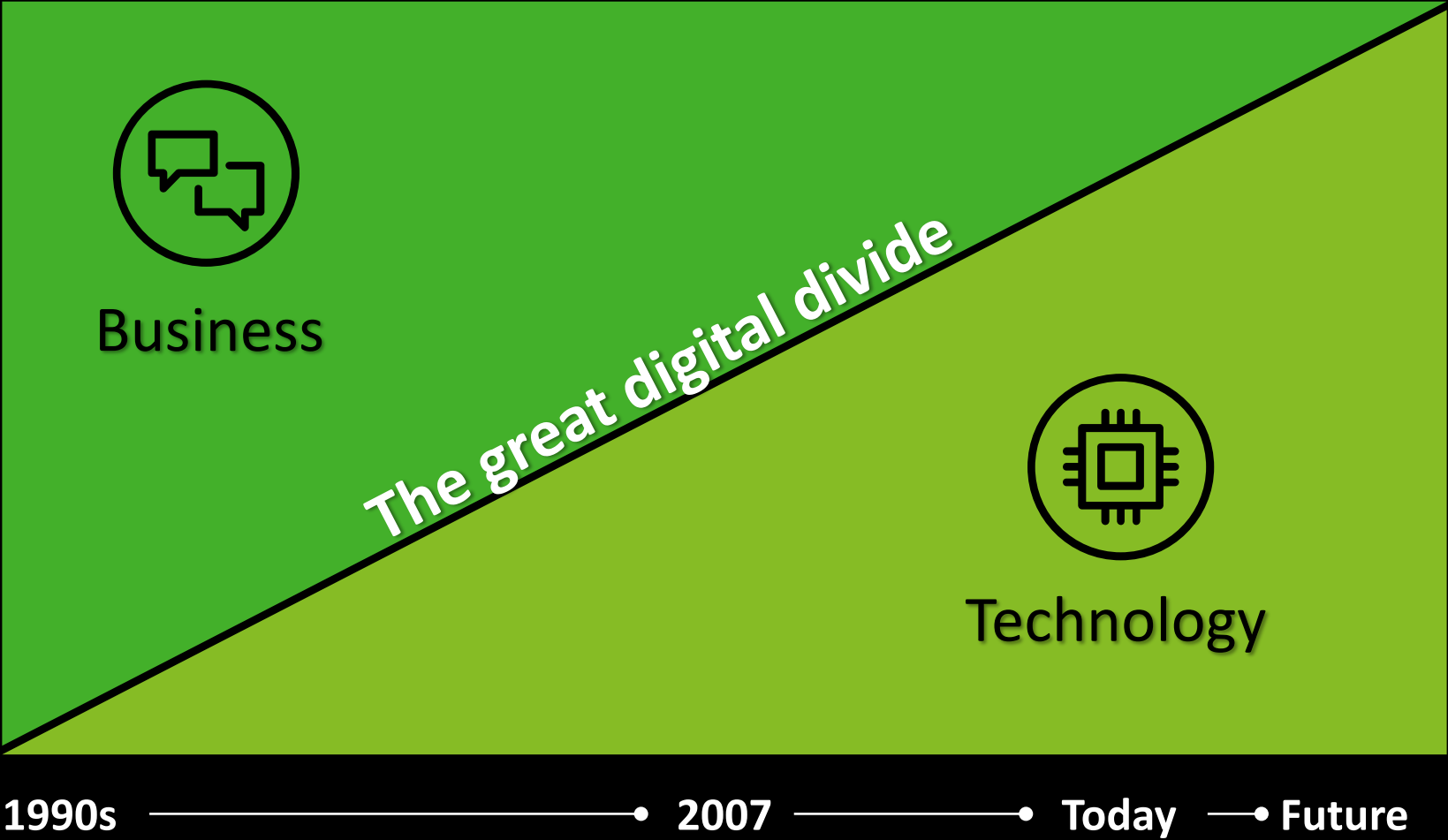
Cyber 2023 and Beyond

Rob Goldberg, Principal, Deloitte & Touche LLP
March 24, 2023

Where are we today and how did we get here?



We have crossed the great digital divide...



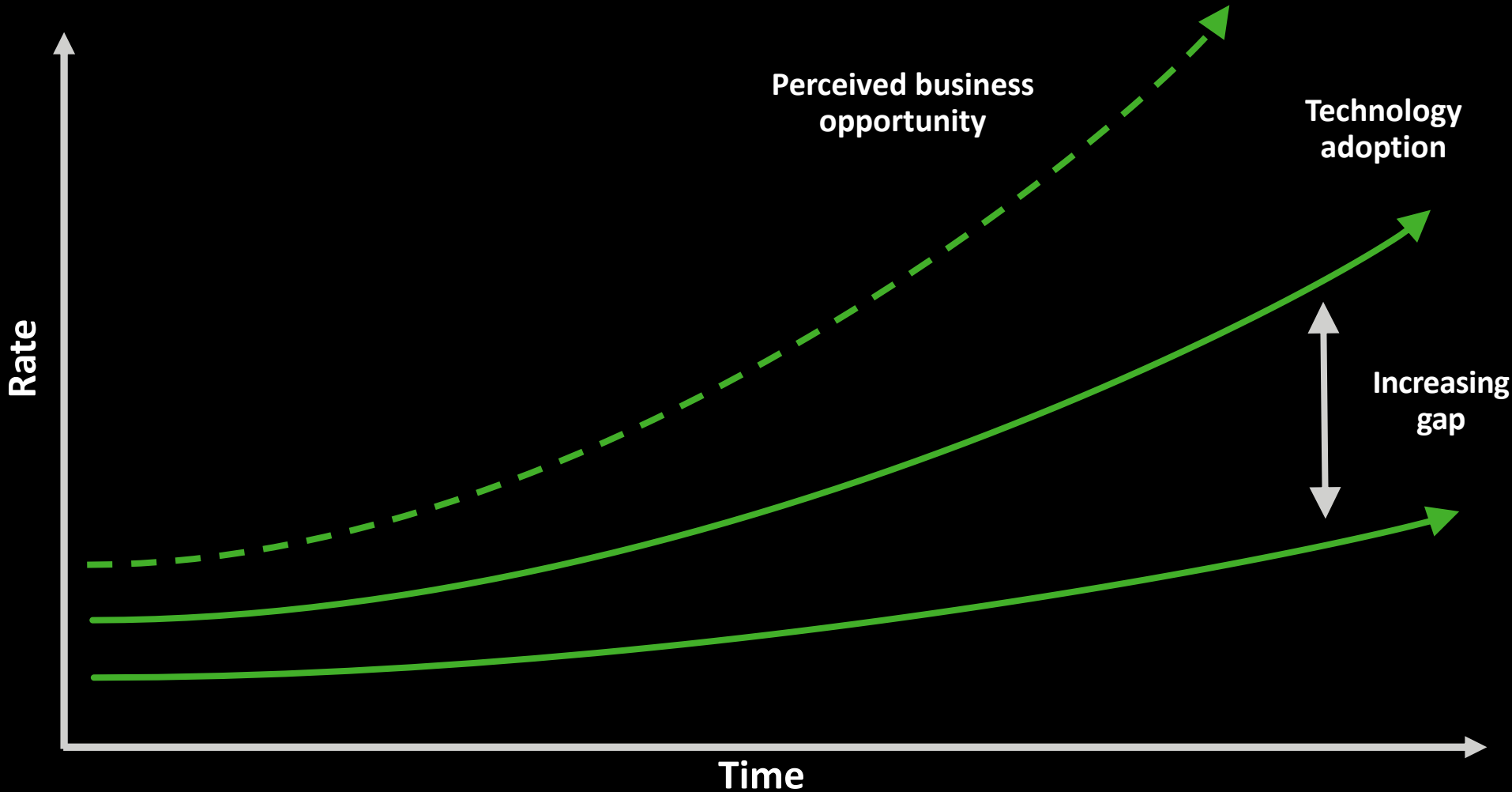
Polling question #1

What shift occurred in 2007 that fundamentally changed the business environment?

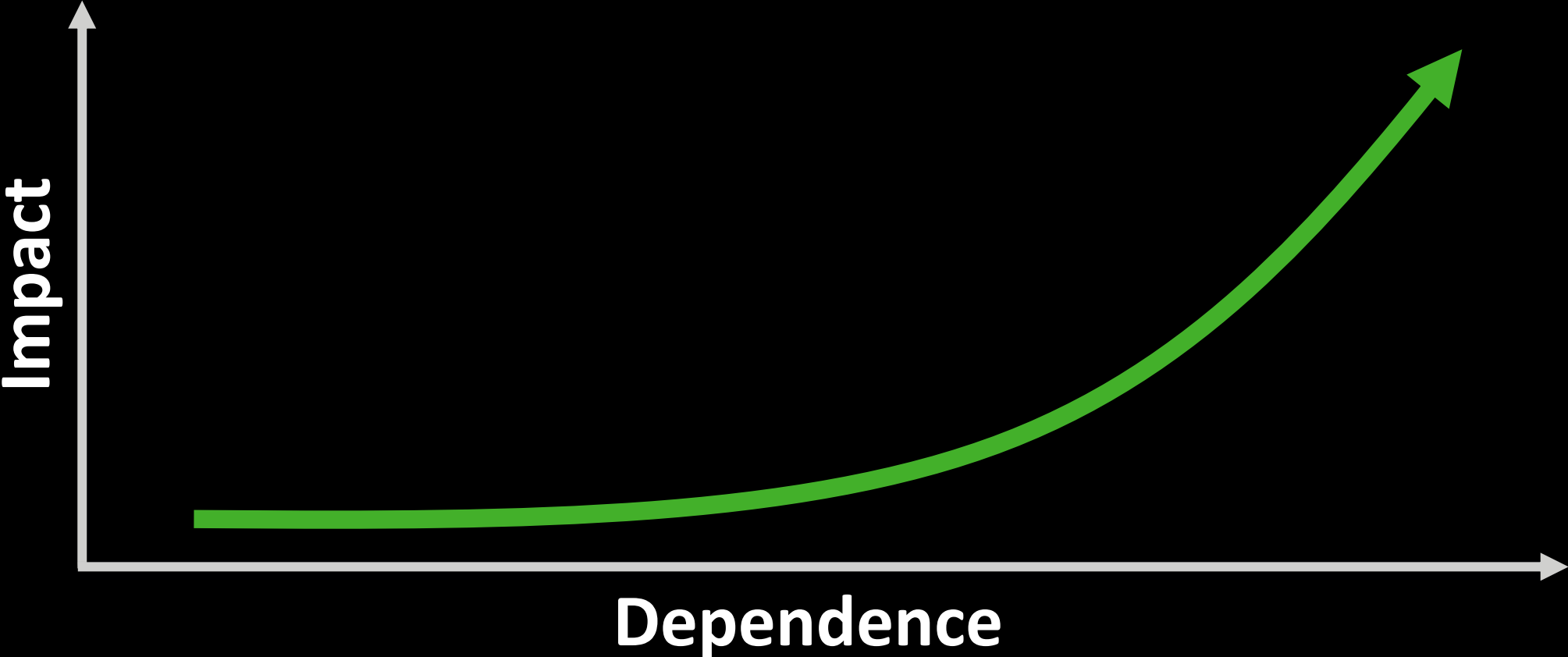
- a. Steve Jobs introduced us to a smartphone
- b. Technology *became* the business rather than just a tool
- c. Elon Musk had his first child
- d. The Bachelor first aired



...which has increased implications for cyber security...



...and implications on impact.



Polling question #2

Have you or your company been impacted by a ransomware attack?

- a. Yes
- b. No
- c. Don't know



Where are we going and what should we do?



The pandemic, changing expectations, and forward economic uncertainty...

...require us to think differently about cyber going forward...



An increasingly complex threat environment with expanding coverage needs

As threats mature, operations change, new technology is introduced, protection of assets and data demands near-constant refinement.



Greater disruption posed by a dynamic risk landscape

Multifaceted risks propagate and change rapidly in an increasingly interconnected global ecosystem.



Growing customer expectations for trust, privacy, and transparency

Consumers and third parties demand evolving standards for privacy, visibility, and control over the data they share.



Business transformation initiatives requiring agile development and operations to compete

Innovation is happening faster than ever before—promoting agility, productivity, and operational integrity is imperative.



Developing programs that foster exceptional performance today and into the future

Leaders face mounting pressure to meet short-term performance goals, while preparing for future opportunities and disruptors.

...and involve an increasingly diverse set of organizational stakeholders.



Security

*CISOs, CROs, CSOs, COOs,
CTOs, CPOs, CIOs, CDOs*



Risk

*CROs, CISOs, CCOs, CIOs, CTOs,
COOs, CMOs, CEOs*



Privacy

*CIOs, CISOs, CPOs, CDOs, CTOs,
CMOs*



Technology, Information, Data

*CISOs, CTOs, CDOs, CIOs,
COOs, CLOs*



Broader C-Suite & Board

*CEOs, COOs, CMOs, CISOs, CFOs,
CROs, Boards of Directors*

Meanwhile, the SEC is pushing for more transparency

The Securities and Exchange Commission (SEC) has proposed enhancements to disclosures regarding cybersecurity risk management, strategy, and incident response in their ruling Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure issued on March 9, 2022.

Proposed rule at a high-level

- 1** **Intends** to boost investor confidence toward organizations cybersecurity governance and incident disclosures, reduce mispricing of securities, and facilitate decision making by driving reporting consistency
- 2** **Includes** enhancements in current reporting about material cybersecurity incidents and periodic disclosures about cybersecurity policies and procedures, management's role, and the board's expertise in implementing a cybersecurity risk program
- 3** **Impacts** all public companies that are subject to the reporting requirements of the Securities Exchange Act of 1934, as well as foreign private issuers (FPIs) who are required to update Form 20-F. The scope includes all companies with relevant disclosure obligations on Forms 10-K, 10-Q, 20-F, 8-K, or 6-K, and proxy statements

Details of the proposed SEC rule

-  **Accelerated reporting:** Disclose information about a cybersecurity incident within four business days after it is determined as material
-  **Determination on materiality:** Determine incident materiality diligently and quickly. Material incidents change current information available or will be important to shareholders
-  **Consistent in specificity:** Incident reports to include discovery time, nature and scope, data and operational impact, and remediation efforts
-  **Material aggregation:** Disclose singular immaterial incidents having material aggregate impact
-  **Risk management:** Periodically disclose policies and procedures for identifying and managing cybersecurity risks and threats
-  **Governance:** Periodically disclose governance structure, including the board of directors and management's oversight role regarding cybersecurity risks
-  **Cybersecurity expertise:** Disclose if registrant's board of directors has cybersecurity expertise through work experience or certification in security
-  **Third-party oversight:** Disclose the selection process and cybersecurity risks associated with its use of any third-party service provider







How should organizations be responding, and what actions can they take?

Companies must continue to shift from a protection mindset to a risk management and enablement mindset. This can be done by organizing cybersecurity efforts according to value-based outcomes that align with organizational objectives and goals.

Value Themes	Protect the Enterprise	Manage Multifaceted Risk	Build and Restore Trust	Spearhead Business Enablement	Provide Vision and Drive Growth
Focus areas	<ul style="list-style-type: none"> Secure, connected devices Secure, intelligent operations Secure, efficient workforce experience 	<ul style="list-style-type: none"> Dynamic risk programs Resilient digital operations Enhanced response and recovery 	<ul style="list-style-type: none"> Trusted customer experiences Trusted data use 	<ul style="list-style-type: none"> Agile, secure modernization Supply chain security and risk transformation 	<ul style="list-style-type: none"> Future forward readiness Governance and optimization

What can organizations do?

Organizations should prepare for a future of greater transparency about their cybersecurity governance program and a streamlined incident reporting approach that continues to drive trust in investors.

- 
Investing in cyber means investing in your governance: While senior/board level engagement is now a leading practice, it might become a requirement for public companies
- 
Adopt a continuous evaluation mindset: Integrate technical and business capabilities to drive post incident management, including analysis of incidents in aggregation
- 
Enhance your cybersecurity framework: Ensure your policies and procedures reflect not only your expertise but also experiential and situation learning and awareness
- 
Understand your state of readiness for reporting: Explore monitoring and response program best suited to meet your incident reporting compliance requirements
- 
Evolve from response to resilience in your extended enterprise: Develop and invest in risk intelligence tools that consolidate internal and external information on third parties
- 
Transcend from digital risk to digital advantage: Drive a focused effort on analytics and automation to manage and mitigate cybersecurity risks



This presentation contains general information only and Deloitte is not, by means of this presentation, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This presentation is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte shall not be responsible for any loss sustained by any person who relies on this presentation.

As used in this document, "Deloitte" means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.