SBIA Lunch & Learn Series: Navigating Cybersecurity and Privacy Threats for SBICs

David Sun
Principal - Cyber
703-744-8508
David.sun@cohnreznick.com

Ali Khraibani
Senior Manager - Cyber
862-245-5166
Ali.Khraibani@cohnreznick.com

Joe Sjoholm
Partner - CPA, Assurance Private Equity Practice
203-399-1998
Joe.Sjoholm@cohnreznick.com

CohnReznick LLP

Landscape: Data Breaches by the numbers

55%
caused by malicious or cyber attacks vs. IT failure or human error

$9.36 (↓$0.12)
million average cost of a data breach in the US

$4.88 Million (↑$0.23M)
average cost of a data breach Globally

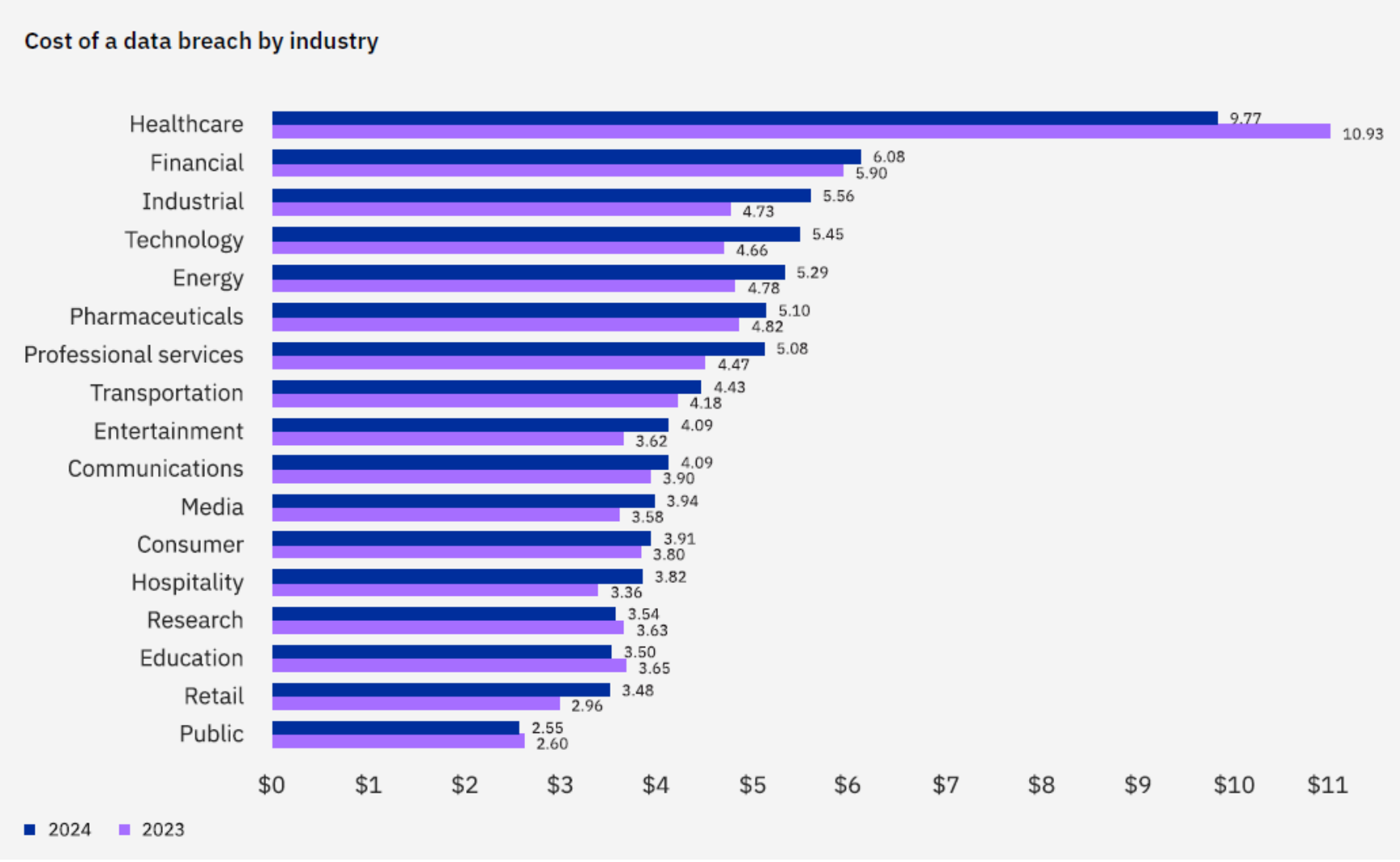
194+64
(258) days (↓19)
average time to detect and contain breach

$143/record of PII (↑$17)
average cost per lost or stolen data

$384,441 (↑$90k)
average pay for full time CISO

Source: IBM Security Cost of a Data Breach Report 2024, Glassdoor

Costs by Industry



Source: IBM Security Cost of a Data Breach Report 2024

Increasing Trends of Cyber Concerns

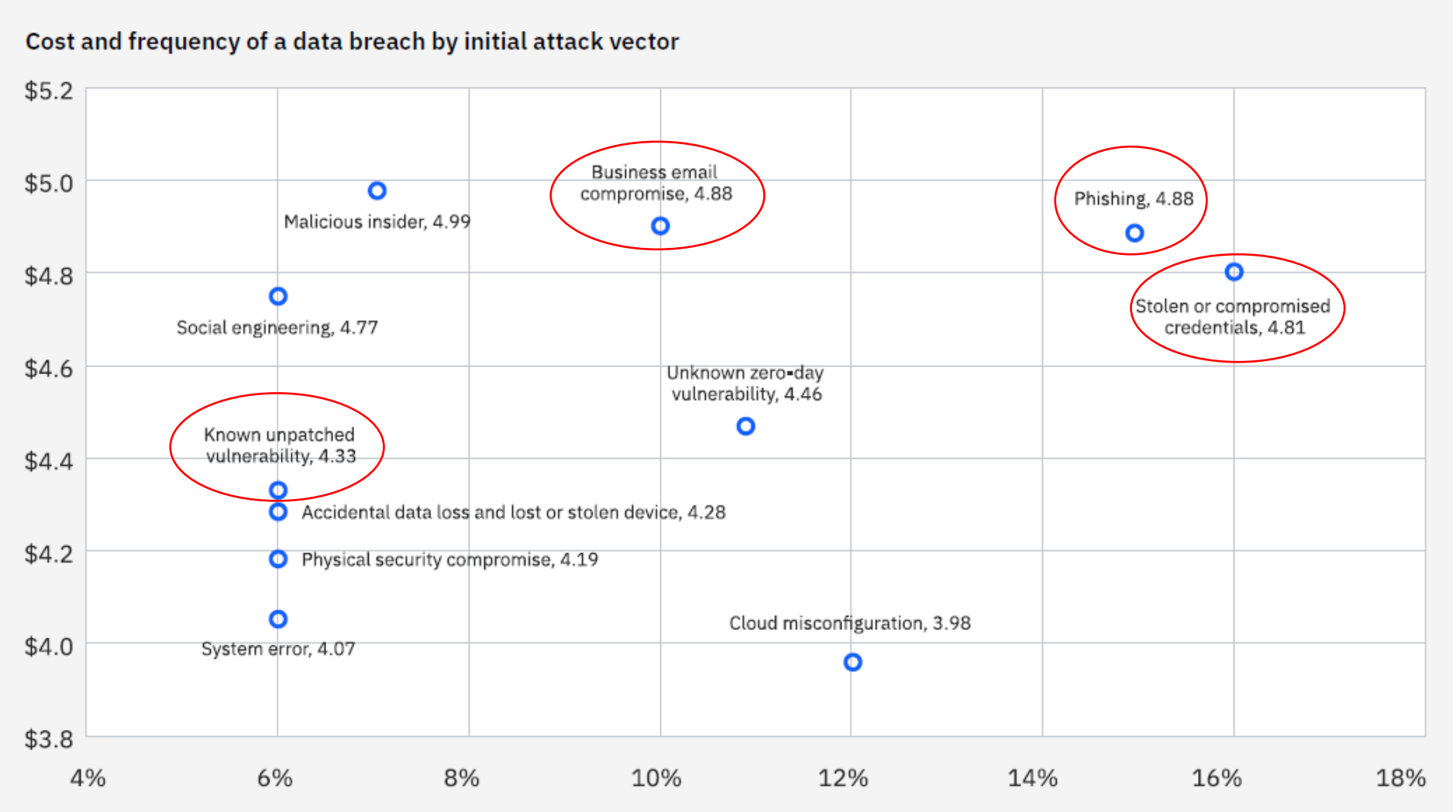
Financial/PE/Investment Services firms have growing concerns about their cybersecurity posture, on top of ensuring their portfolio companies are invested.

In the financial industry, cybersecurity attacks are evolving and not typically targeting one specific organization. Rather, there is a growing attack surface once organizations establish partnerships and outsource services. Hackers target third-party and fourth-party organizations (or portfolio companies) that financial organizations rely on and, therefore, become victims of such attacks due to inadequate preparedness.

Also, there's an increased rate of financial disruption for Private Equity Firms and Hedge Funds due to limited visibility of how well cybersecurity is embedded into business operations. Other trends include:

- Challenging Cybersecurity Insurance Renewals
- Decentralized balance of security focus across people, process and technology
- Limited enforcement of protecting organization resources
- Increased attacks at portfolio-level leading to high-risk investments and deal transactions
- Limited cyber investments that result in unexpected expenses of portfolio
- Delay in acquisitions due to increased cybersecurity risks and attacks

Types of Attacks



Source: IBM Security Cost of a Data Breach Report 2024

Double the Problem

	Fund-Level	Portfolio Company-Level
Poor Cybersecurity Management	Executives may lack technical knowledge to make informed cybersecurity decisions.	Inconsistent cybersecurity policies and practices across different Portfolio / Investment companies, lack of skilled labor
Costs	Difficult to correlate cybersecurity cost with benefits	IT spend only keeps the lights on, Cybersecurity costs are underinvested
Understanding IT and Cyber Expectation	Executives may lack technical knowledge to make informed cybersecurity decisions	Leadership may not fully grasp the importance of cybersecurity, leading to inadequate support
Lack of Accountability	Limited accountability to oversee cyber programs at portfolio / investment companies	Without strong governance, cybersecurity responsibilities may be unclear
Establishing Checks and Balances	Firms may provide shared IT/Security services to portfolio companies, without establishing independent functions for both IT and cybersecurity	Smaller companies may not have the capacity to separate these functions, leading to less effective security

Gramm-Leach-Bliley Act (GLBA)

The cybersecurity requirements under the Gramm-Leach-Bliley Act (GLBA) for the Small Business Investor Alliance (SBIA) and Small Business Investment Companies (SBICs) are designed to ensure the protection of customer information.

Key requirements outlines by GLBA

- **Comprehensive information security program** – Written program with administrative, technical, and physical safeguards
- **Designate a Qualified Individual** to oversee the information security program
- **Conduct Risk Assessments**: Regularly assess risks to customer information
- **Implement Controls:** Address identified risks with appropriate controls
- **Continuous Monitoring and Testing:** Ensure ongoing monitoring and testing of the security program
- **Access Controls**: Implement controls to limit access to customer information
- **Penetration Testing and Vulnerability Scanning:** Conduct regular testing and scanning to identify vulnerabilities
- **Incident Response Capabilities:** Develop and maintain capabilities to respond to security incidents
- **Reporting security events** to the FTC no later than 30 days after discovering a security breach involving at least 500 customers

SEC's final rule 33-11216

- Cybersecurity Risk Management:
  - The need to adopt and implement written policies and procedures to address cybersecurity risks.
  - Registrants must provide periodic disclosures about their processes to assess, identify, and manage material cybersecurity risks.
- Incident Reporting and Disclosures
  - Material cybersecurity incidents must be disclosed on Form 8-K within four business days of being deemed material.
    - This includes describing the nature, scope, timing, and impact of the incident on the company's financial condition and operations
- Periodic Disclosures:
  - Companies must provide periodic disclosures about their cybersecurity risk management, strategy, and governance in their annual reports. Registrants are required to disclose the board of directors' oversight of cybersecurity risk.
    - This includes describing processes for assessing, identifying, and managing material risks from cybersecurity threats, as well as the board of directors' oversight and management's role in these processes
- Delayed Disclosures:
  - Disclosure may be delayed if the U.S. Attorney General determines that immediate disclosure would pose a substantial risk to national security.

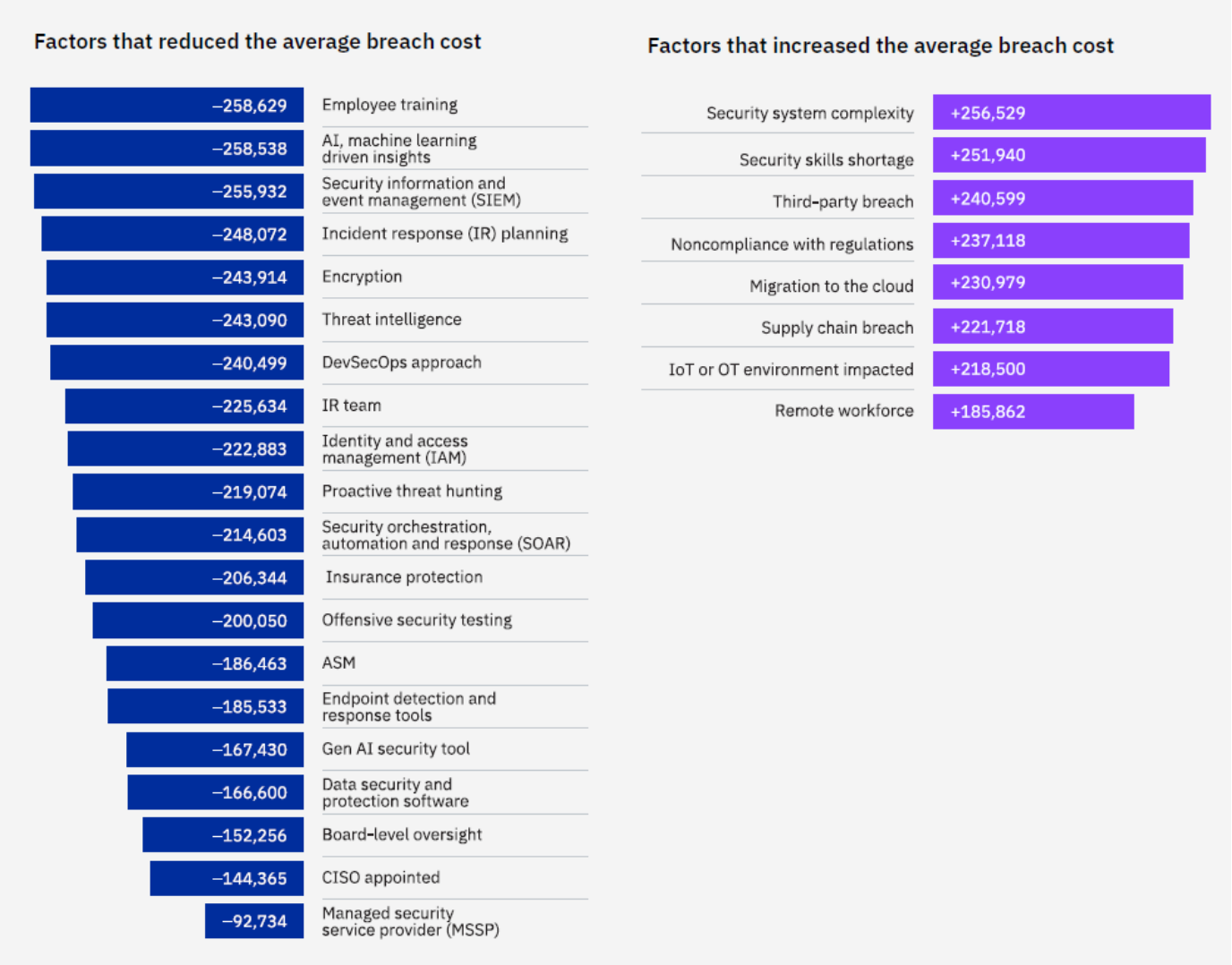
https://www.sec.gov/files/rules/final/2023/33-11216.pdf

Potential expansion of rulings

While direct impact of SEC rulings may be limited, SEC's actions may influence private companies in several ways:

- **Best Practices:** Adopt regulatory standards as guideline of best practices for improving the cybersecurity posture.
- **Third-Party Relationships:** When working with a public company or providing services, private companies may be required to align its cyber practices with standards expected by the SEC.
- **Preparation for IPO:** If there is a plan to consider going public, companies must implement SEC's cybersecurity rules.
- **Investor Confidence:** Aligning with SEC standards may be a factor to attract investors to show commitment to protecting stakeholders' interests.

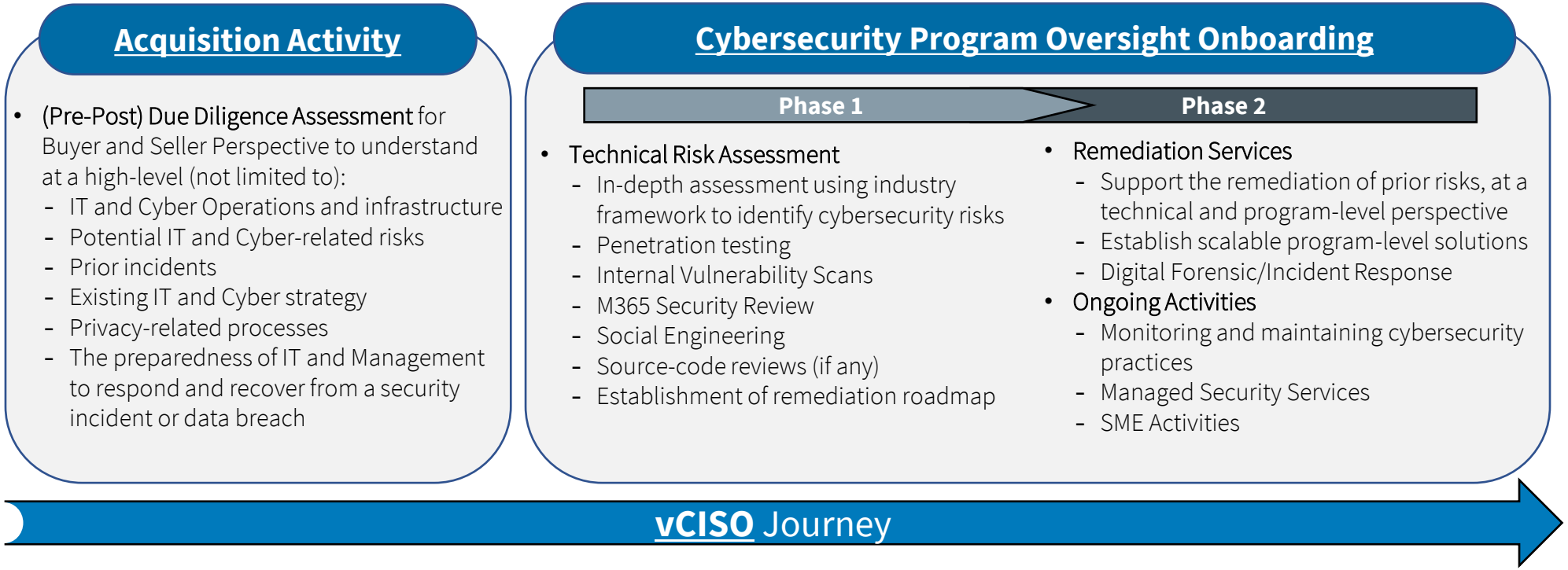
Managing Cyber Risks makes a Difference



Source: IBM Security Cost of a Data Breach Report 2024

Considerations Solution for PE/Capital/Investment Firms

Financial Sponsors, PE/Capital/Investment Firms need to establish cybersecurity program offices for pre- and post-acquisitions using a *consistent* approach.



Assessment Services for Organization Maturity Level

Lower IT and cyber maturity organizations should focus on foundational cybersecurity services to build their programs, while more mature organizations should invest in advanced services to enhance compliance and security insights

Initial Baseline

- Organizations that have not conducted prior cyber reviews
- Smaller Organizations
- Limited IT staff or capabilities

Recommended Activities:

1. M365 Security Review
2. High-level Cyber Risk Assessment
3. Social Engineering (standard phishing)

Somewhat Mature

- Organizations with an existing cyber program established
- Has some awareness of cybersecurity needs
- Dedicated IT staff and capabilities
- Some security services (internal/external)

Recommended Activities :

1. M365 Security Review
2. Cyber Risk Assessment (high-level or industry standard)
3. Penetration Testing (scrape the surface approach)
4. Vulnerability Scan
5. Social Engineering (standard phishing)

Mature Organizations

- Organizations with well-established cyber programs and capabilities
- Dedicated investments and teams for IT and cyber
- Programs to monitor existing compliance commitments

Recommended Activities :

1. M365 Security Review
2. Compliance-based cyber risk assessment
3. Privacy risk assessment
4. Penetration Testing (intrusive approach)
5. Incident Response Tabletop
6. Vulnerability Scans
7. Social Engineering Testing (comprehensive)

CohnReznick Case Study

Problem

Typically, audit clients have several concerns:

- **Experienced a security incident** that warranted additional visibility and awareness of technical risks
- **Reaffirm commitments** made to executive leadership through cybersecurity and technical assessments of being proactive
- **Cybersecurity insurance premiums increased**
- **Needed additional assurance for understanding** risks and alignment with best practices
- **Limited objective testing processes** to evaluate the cybersecurity posture to ensure unbiased insights

Solution

CohnReznick proposed a **high-level cybersecurity risk assessment** coupled with **some technical testing** to provide the stakeholder with a high-level awareness of cybersecurity risks and maturity of the client.

During scoping, we defined a list of **controls from industry standards** commonly adopted across the industry and **selected business critical systems** to include in a **penetration testing exercise** to identify vulnerabilities that can lead to a cybersecurity incident.

Results

Our independent assessment informed leadership of critical risks that may adversely impact the organization's role in protecting its resources and its overall maturity against industry leading standards.

- **Increased visibility** and awareness to executives of remediation needs to address cyber risks, improve maturity, and a deeper understanding of industry expectations.
- **Increase stakeholder confidence** by demonstrating commitment through independent assessments.
- **Cost savings** to proactively protect organization resources and prevent security incidents or breaches

Thank You!

JOIN US FOR OUR **UPCOMING EVENTS**

WEST COAST CAPITAL SUMMIT
THE SMALL BUSINESS INVESTOR ALLIANCE PRESENTS THE 2025

West Coast Capital Summit
March 25-27, 2025
Fairmont Century Plaza
Los Angeles, CA

2025 DEAL SUMMIT & DEALINX
THE SMALL BUSINESS INVESTOR ALLIANCE PRESENTS THE SBIA MIDWEST

Midwest Deal Summit
May 28-29, 2025
The Four Seasons Hotel Chicago
Chicago, IL

Invest with experienced independent sponsors engaged in the lower middle market.

This first-of-its-kind dealmaking series puts you in the room with the independent sponsors you want to meet.

Learn More

The invitation-only **Independent Sponsor Forum (ISF) Deal Series** connects capital providers with vetted independent sponsors in a format designed to maximize your return on investment and time.

- Highly actionable **one-to-one meetings**
- Valuable background information **on every attendee**

Independent ISF SPONSOR FORUM
POWERED BY THE Small Business Investor Alliance

2025 Independent Sponsor Forum Deal Series Events

1. **March 12, 2025**
   ISF Deal Series Nashville
2. **June 25, 2025**
   ISF Deal Series Los Angeles
3. **May 6, 2025**
   ISF Deal Series Philadelphia
4. **September 10, 2025**
   ISF Deal Series Chicago