Think Like a Hacker – Cybercrime Tactics

Cyber Symposium 2025

forvis mazars

Cerone F. “Cy” Sturdivant, CISA

Principal
IT Risk & Compliance

- Focus areas
  - IT Consulting
  - IT Compliance
  - Cybersecurity Consulting

forvis mazars

Zach Shelton, CISA, CDPSE

Principal
IT Risk & Compliance

- Focus areas
  - IT Consulting
  - IT Compliance
  - IT Audit / SOX
  - Cybersecurity Consulting

forvis mazars

01.i

Cybersecurity: Discussion

- Do you think your company has a firm handle on cyber-related risks?
- Do you think employees understand cyber-related risks when using apps on their phones, *i.e.*, TikTok, etc.?
- Do you feel your company's Board or Executive level team members support a cybersecurity culture?

Why Are We Here?

“This invention has sparked a heated debate among educators, economists and lawmakers”

The invention of the modern calculator |Mid-1970s

“We need to safeguard our education system, our economy and our society from the dangers of this technology”

“What surprised us all is how quickly it caught fire in the consumer market”

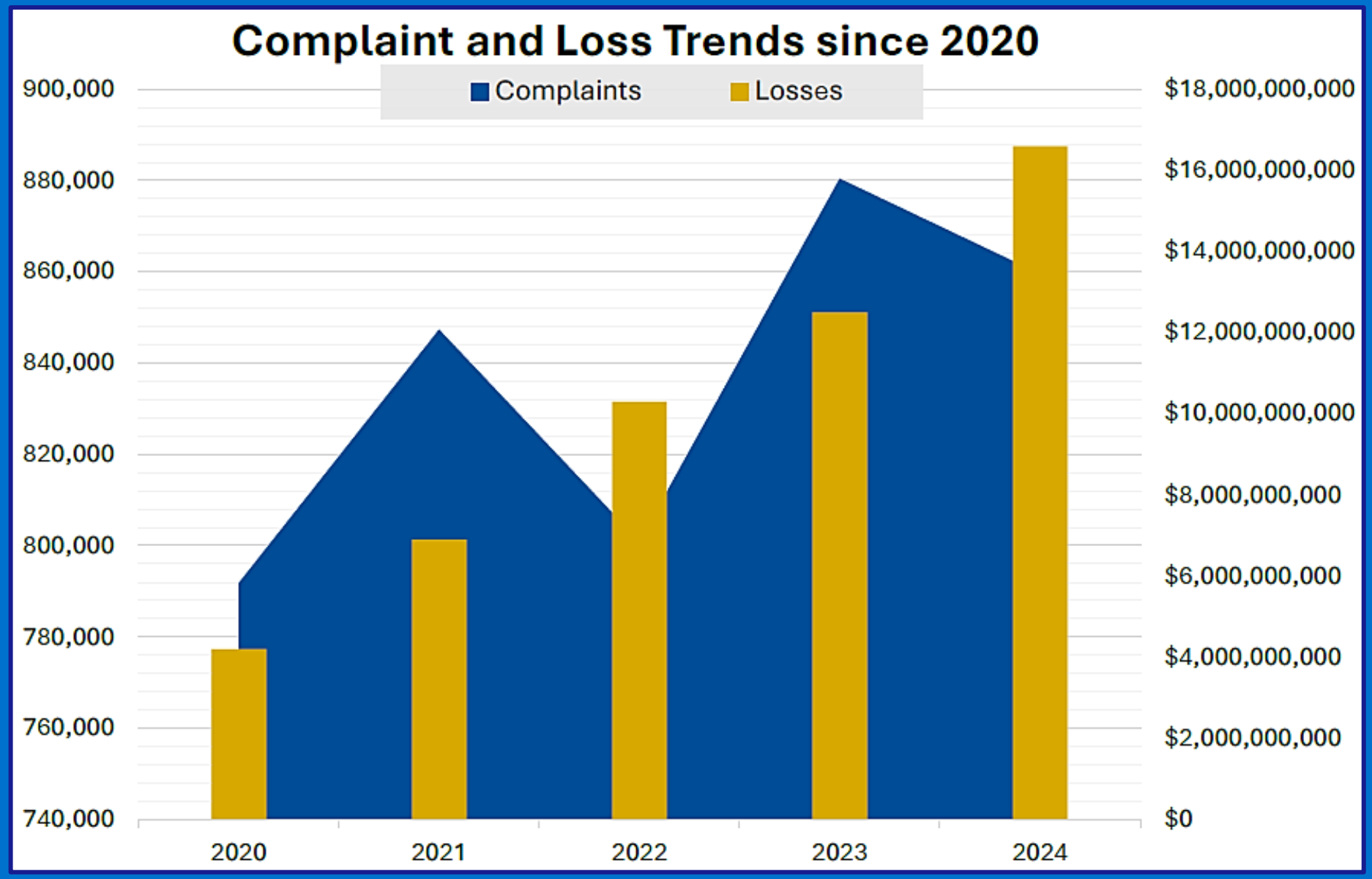
Source: Microsoft Corporation

forvis mazars

01.ii

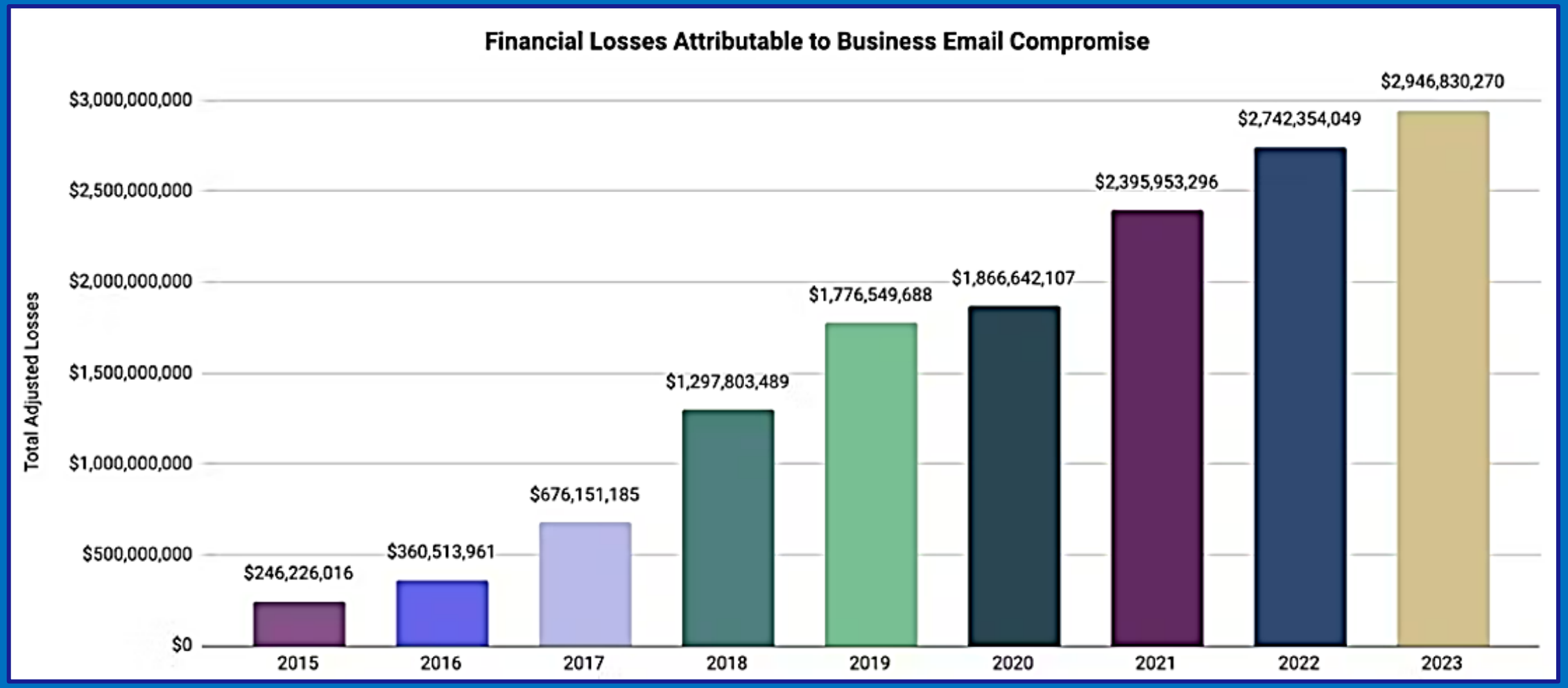
Threat Landscape & Impacts

FBI’s Internet Crime Complaint Center (IC3) Five-Year Statistics



forvis mazars

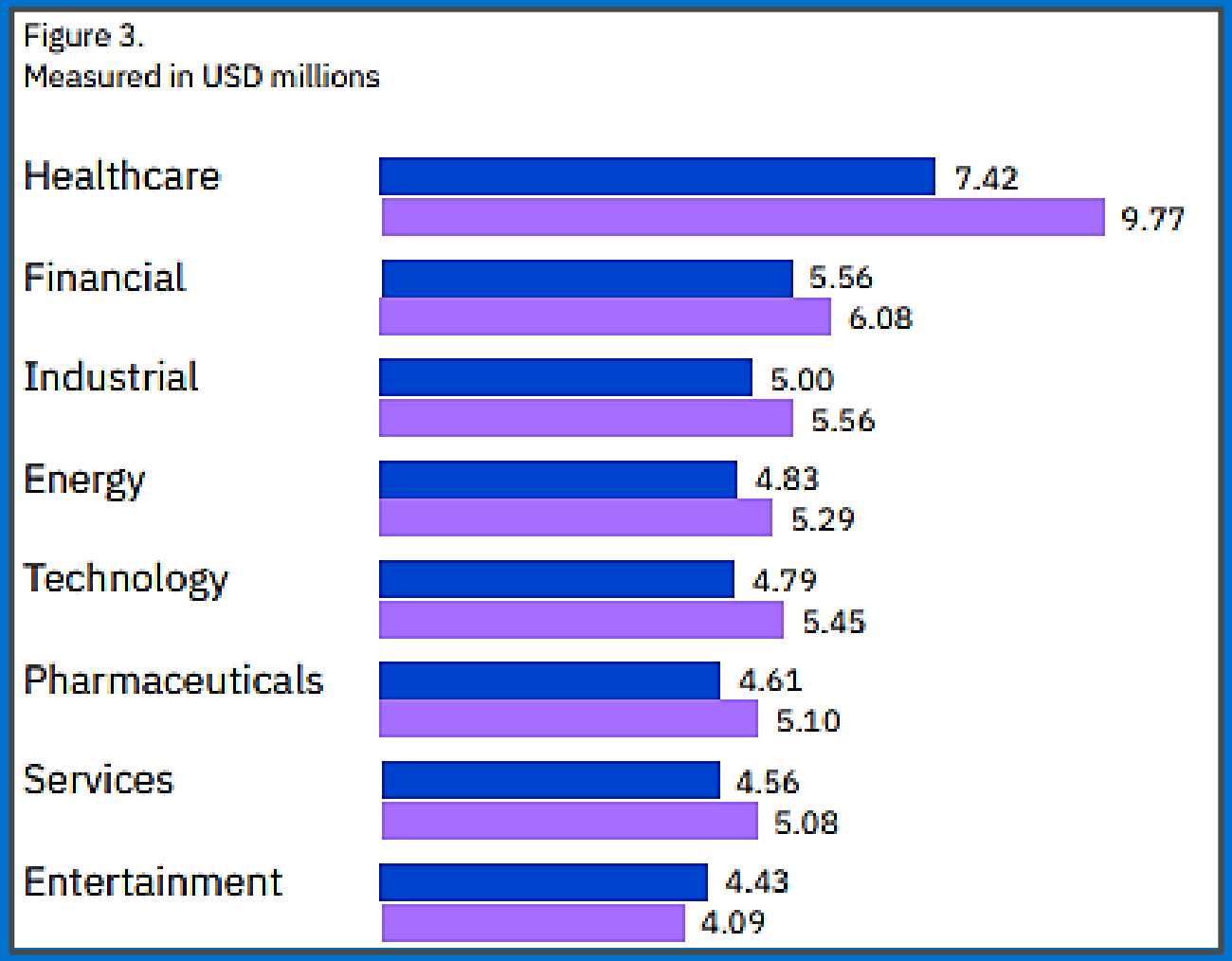
BEC Losses by Year (IC3)



2024 FBI IC3 Report

forvis mazars

Cost of a Data Breach Study – IBM

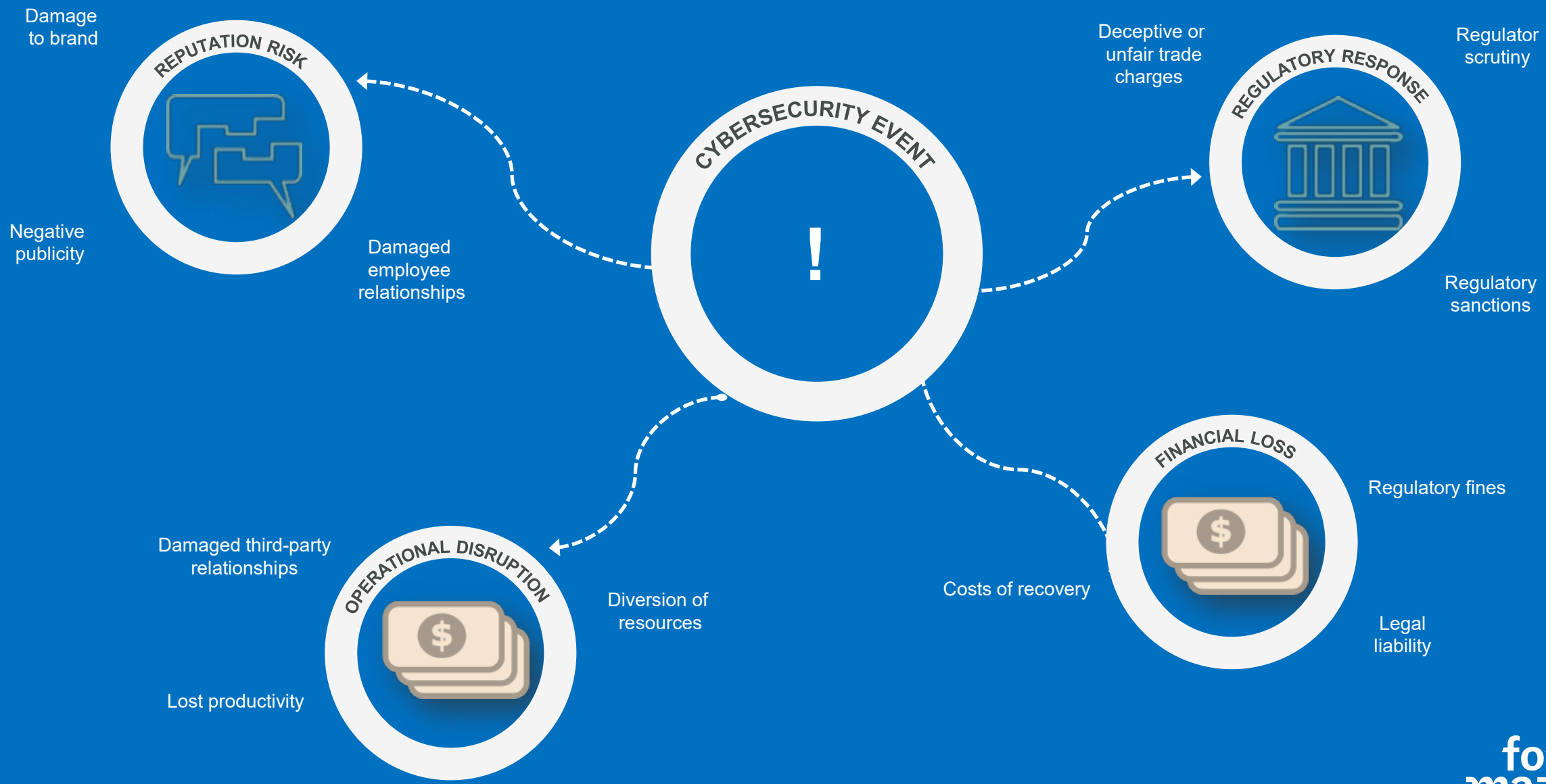


Average U.S. cost rose to a record $10.22 million.

This includes a 14% year-over-year jump in detection and escalation costs, driven by higher labor costs.

forvis mazars

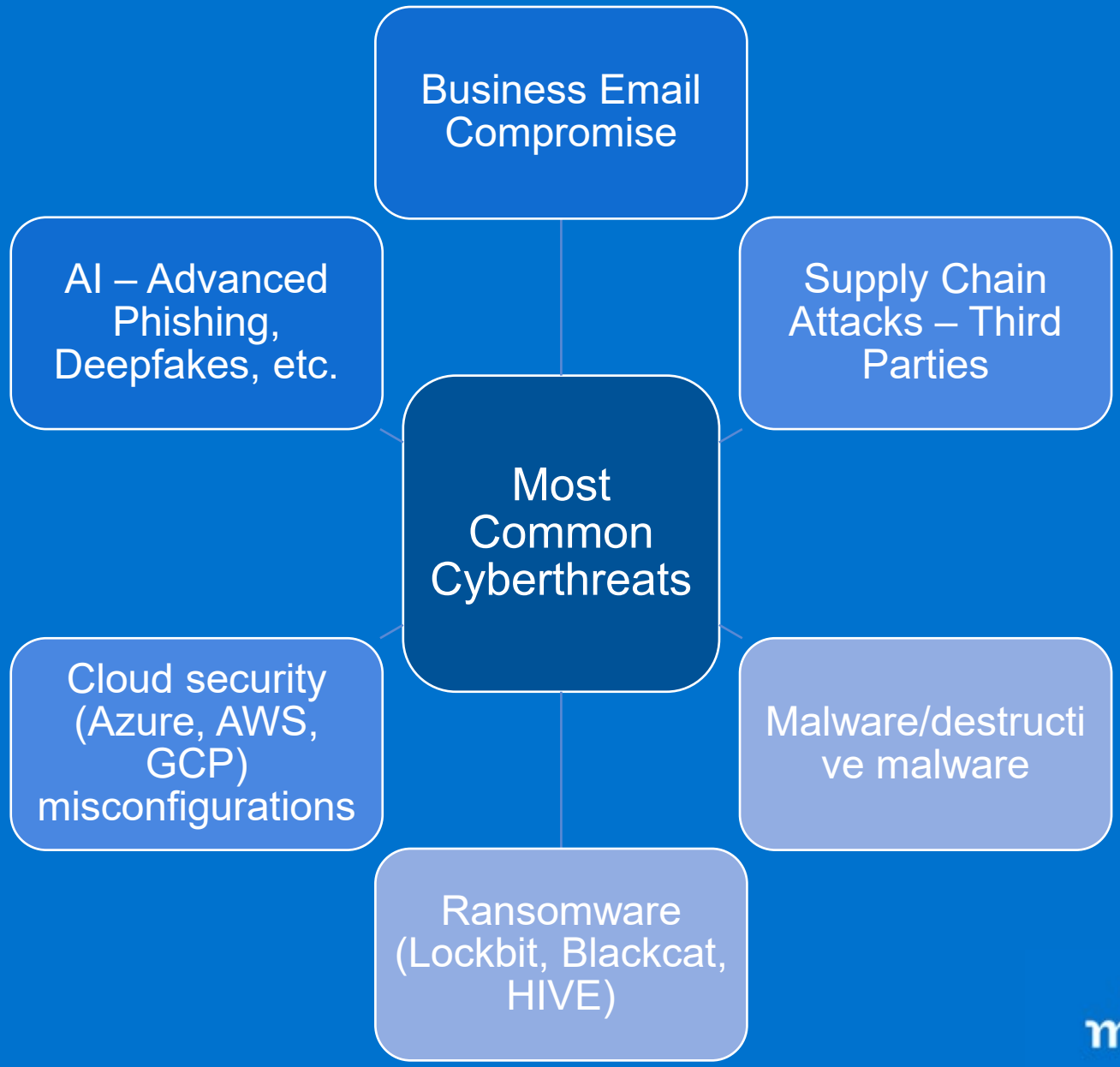
Cyber Breach Impacts



forvis mazars

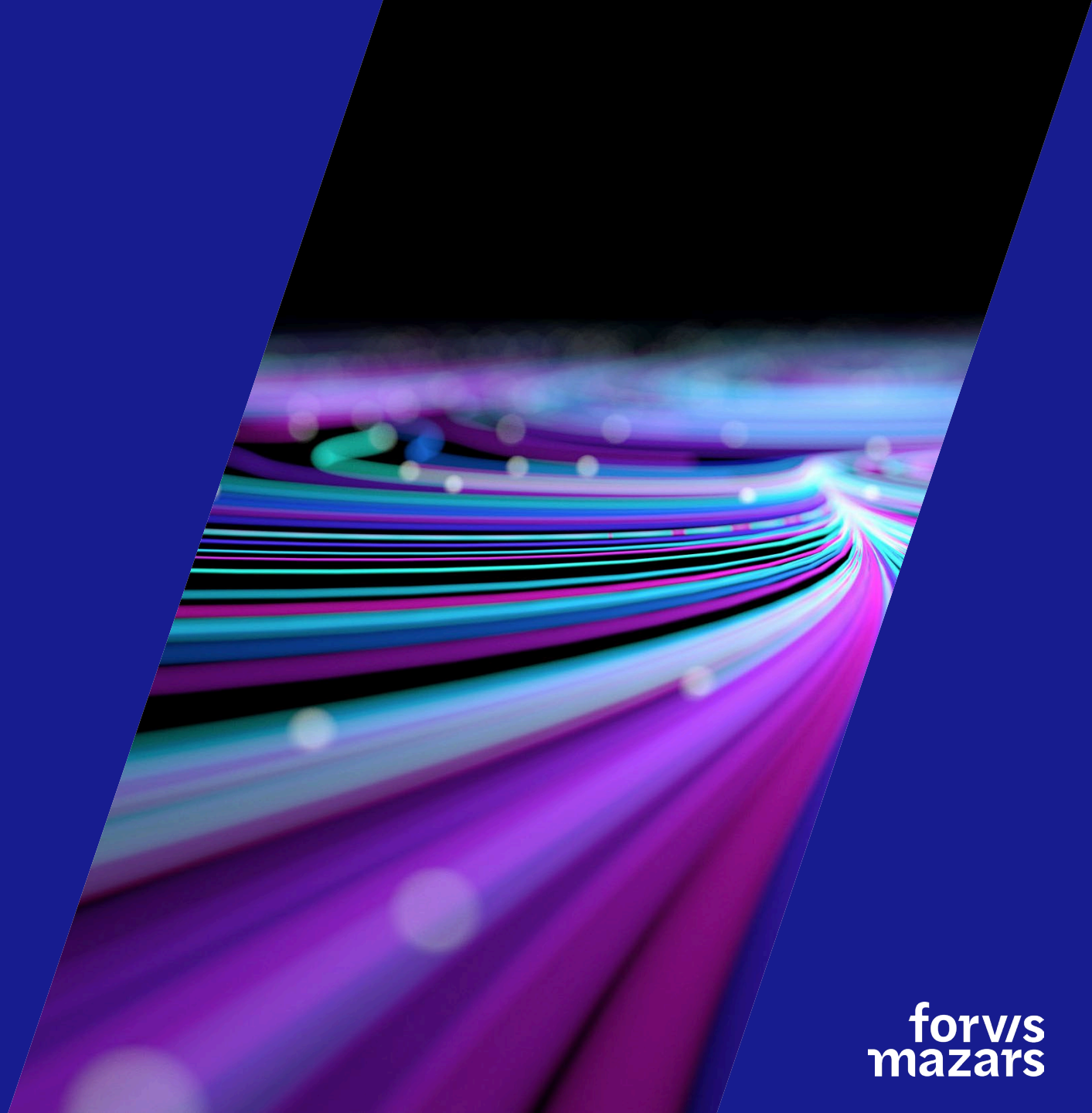
Most Common Cyberthreats

Root causes of cyberattacks: Inadequate training, ineffective patch management*, weak privileged access controls, & unmonitored detection systems



01.iii

Cybersecurity Events & AI Threats – Past 12 Months



forvis mazars

Attacks / Concerns – Past 12 months

- July 2025 – A SharePoint hacking campaign affected hundreds of systems globally
  - Allowed unauthenticated attackers to remotely execute code in a SharePoint server hosted on-prem – no user interaction required
  - Go back and make sure SharePoint (CVE-2025-53770) was patched quickly

Supply Chain /Cloud Attack

- **Arup** – Fell victim to a deepfake scam where cybercriminals used AI-generated videos to impersonate the CFO and other employees during a virtual meeting
  - Scam recreated Company's other employees in a video conference call and instructed an employee to transfer funds
  - Employee then completed 15 transfers to 5 different bank accounts, **resulting in a $25 million loss**

A.I. Deepfake Attack

forvis mazars

02

Real-Life Stories

02.i

Be Careful of New Friends

New Systems Engineer

- Charged with maintaining the company's legacy system
- Used online forums for research
- Targeted by a cybercriminal
- Shared company info, and other sensitive data through the social platform

Impact

- Cybercriminal crafted Deepfake Attack
- Impersonated the engineer
- Targeting key executives at the company
- Successfully influenced Executive to download malicious file

forvis mazars

02.ii

The Power of Approval

A Company was the victim of a **$2.7 million cyber scam**, with funds being sent to a ***fraudulent vendor*** who represented themself as a current vendor.

Claimed to be CEO of Construction Co.

- Contractor working a large project for customer.
- Three payments sent to fraudster.
- Feb: $128k
- March: $1.07m
- March: $1.5m

Incident Report

- Purchasing clerk received initial fraudster email, forwarded to payment admin, then controller.
- Requested change to Construction Co's invoice payment account.

forvis mazars

02.iii

Voice Phishing Scams – Now With AI!

AI voice cloning

- a trusted individual, such as an executive, family member, or colleague.
- All they need is 30 seconds of someone's voice to create an AI profile of that person's voice.

Phone call from your child

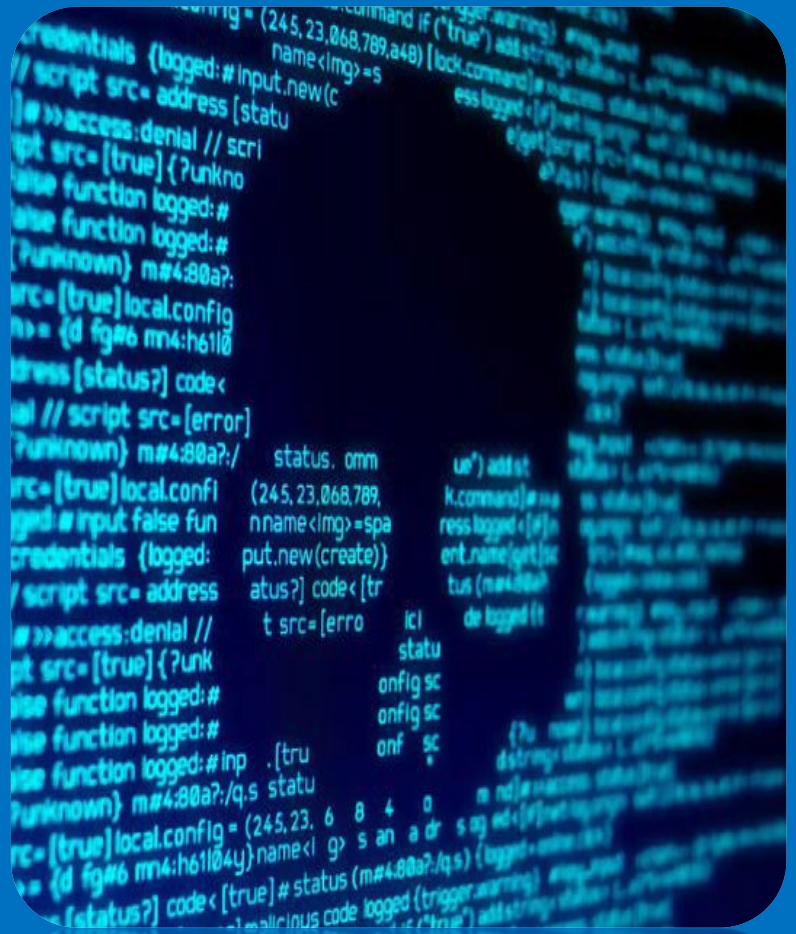
- "They got in a car accident, hit a pregnant woman, they arrested him,
- send money, they are out of time on the call."
- **How to Avoid?** Create a family password, if you can't get the caller to provide the family password, it's likely a scam.

CFO Wire Transfer urgent request:

- During a bank board meeting, a scammer using AI to clone CFO's voice, calls a branch to rush through a wire transfer.
- Bank loses $5M.
- **How to Avoid?** Develop policies and employee training related to unique voice requests.

forvis mazars

Best Practices for Verifying Email Requests



Confirm Sender's Identity

Before responding to any email request, especially those involving financial transactions or sensitive information, it's crucial to verify the sender's identity.

****Reach out to the sender through an alternate, verified channel to confirm the legitimacy of the request.****

Verify Request Details

Inspect the email request and ensure that all the details (requested action, dollar amount, or recipient information) align with your previous interactions and set procedures.

If anything seems unusual, do not hesitate to follow up with the sender directly (phone/person) to clarify and confirm the request before taking any action.

forvis mazars

03

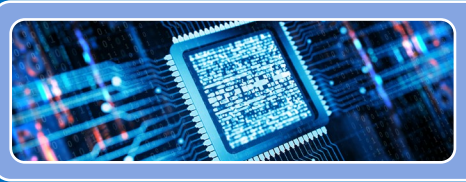
Quick Updates

Best Practices to Reduce Cyber-Related Risks of AI

Develop a Clear AI Acceptable Use Policy and Governance Committee

Leverage Technology – Both Existing Security Tools and New AI-Focused Ones

Educate and Involve Your Workforce



Adopt a Risk-Based, Incremental Approach

Stay Current With External Guidance and Evolving Threats

forvis mazars

Incident Response Plan Tips

Engage with **EXTERNAL** legal counsel first for privileged communications

- *Then other key parties,* i.e., *insurance, law enforcement, vendors, etc.*

Enhance verbiage for communications and negotiation to buy yourself time (if you don't, they could harass you and your customers)

Do not use the terms "breach," "personal information," or other legally defined terms until you are fully prepared to communicate to members

"The more you sweat in training, the less you bleed in battle."
– U.S. Navy Seals

forvis mazars

Ransomware: Essential Questions Executives Should Consider

Incident Response Plan: IT and Cybersecurity staff must develop, test, and execute a **company-centric IRP**.

Cybersecurity Experts: Engage with **professional incident response teams** to assess the situation and explore recovery options.

Verify Backups: Check the **integrity of your backups** and ensure they are not compromised. Use them to restore your data if possible.

Negotiate: Be prepared to **negotiate a lower amount** if you have no choice but to pay the ransomware.

Contact Law Enforcement: Report the ransomware attack to **authorities and cybersecurity agencies**.

Proof of Life: Ask the threat actors for copies of files that have been encrypted as **proof they can be decrypted**.

Cybersecurity Insurance Coverage: Consider acquiring cybersecurity insurance if you handle sensitive information or your business relies heavily on digital operations.

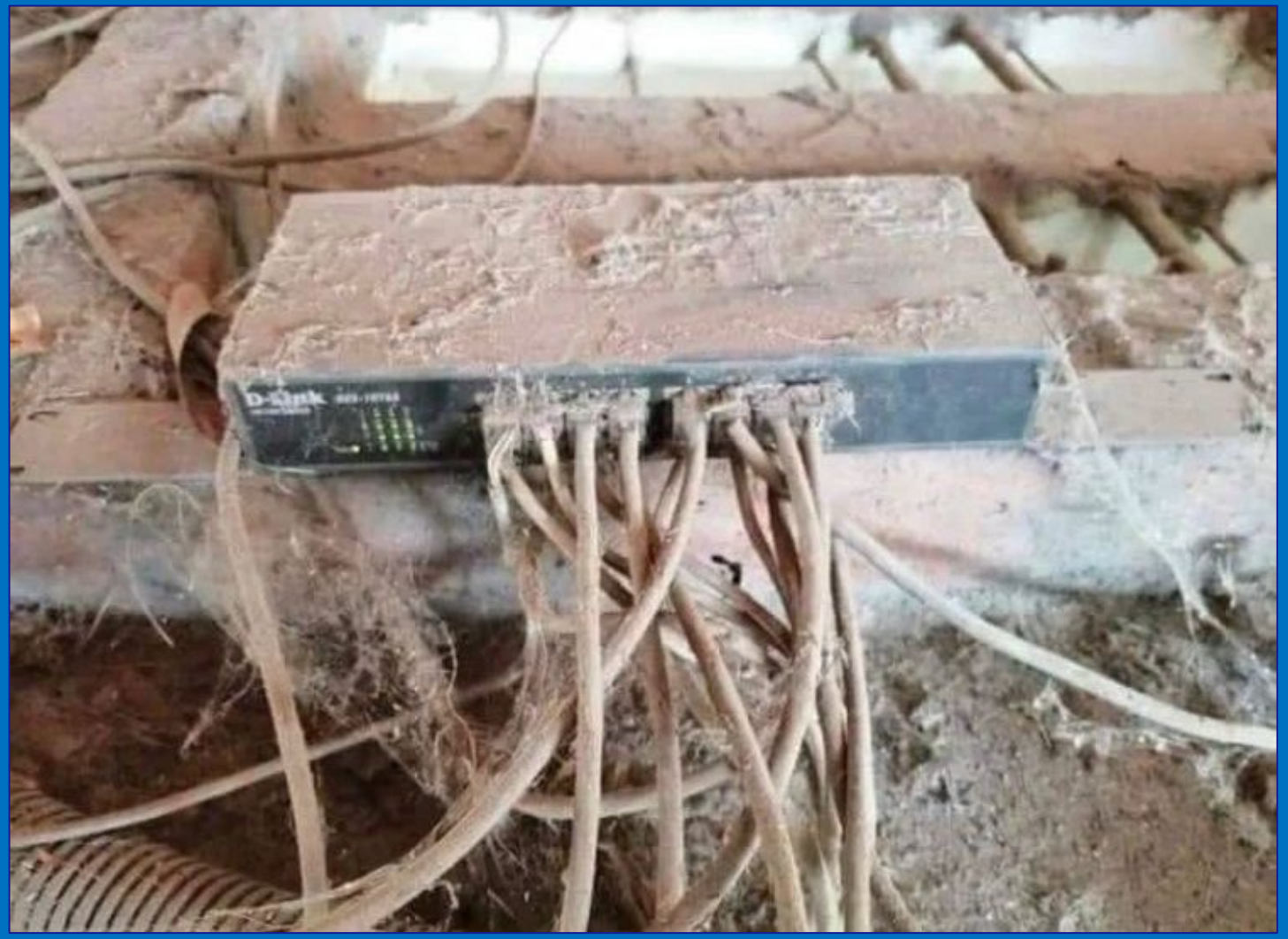
forvis mazars

End of Life Systems

One quick reminder …

Replace all Windows 10 devices NOW!

Deadline: October 14!



04

Final Thoughts

Work Smarter, Not Harder – Reminders

Complexity is the enemy, **simplify** as much as you can

The goal is to **mitigate risk**, not eliminate it

Focus on critical/sensitive **systems & data** more than any other

Focus on **key monetary processes** that could be compromised, *i.e., Wire, ACH, Accounts Payable, File Transfer, etc.*

Create synergies with **Security/Risk/Legal teams**, map industry best practices to risk assessments and controls

forvis mazars

Cybersecurity Key Focus Areas

Governance Controls

- Information security program
- Incident response program
- Business Continuity/DR Program
- Vendor Management Program
- Cybersecurity insurance
- Cybersecurity awareness training
- Cyber risk assessments, penetration tests, vulnerability assessments, & IT control audits
- Long-term IT/Cyber strategic plan

Technical Controls

- Multifactor authentication
- Strong patch management
- Network segmentation
- User access controls
- Application whitelisting
- Cloud-based security
- Data loss prevention
- Security monitoring tools
- Password controls
- Data encryption
- Zero-trust approach/design

forvis mazars

Cybersecurity Consulting

Services we provide to our Clients:

Cloud Penetration Testing

Web Application Security Assessments

Red Team Offensive Security Professionals

Mobile Application Testing

Compliance Assessments

Internal and External Network Security Assessments

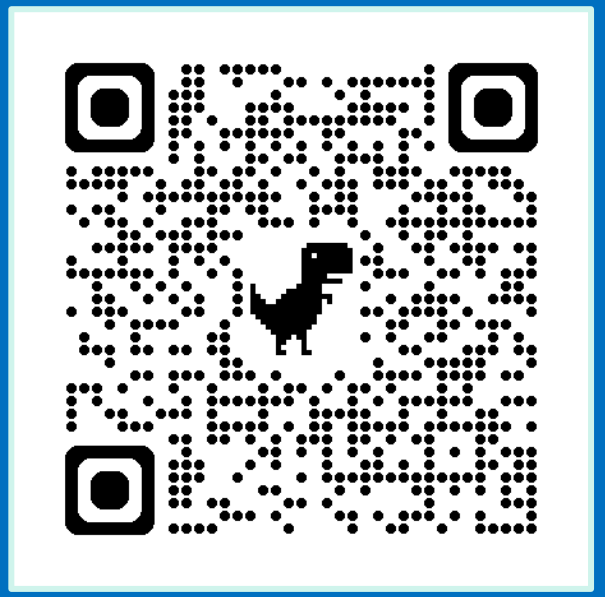
Social Engineering Assessments

Dark Web Research

Ransomware Simulation

forvis mazars

Thank You!



IT Risk & Compliance

Cy Sturdivant, Principal

cy.sturdivant@us.forvismazars.com

615.988.3596

Zach Shelton, Principal

zach.shelton@us.forvismazars.com

919.912.9224

forvis mazars