

Cyber Defense

Understanding & Defending Against Modern Cyberthreats

2026 Financial Institutions Virtual Symposium

forvis mazars

Today’s Presenters



Cerone F. “Cy” Sturdivant, CISA®

Principal

Cybersecurity & Consulting

forvis mazars

How Today's Hackers Think…

People



Process



Money



Trust

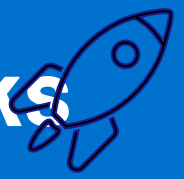


Cybercriminals increasingly target people and trust, not just technology

© 2026 Forvis Mazars, LLP. All rights reserved.

forvis mazars

Attackers Use AI to Scale Attacks



Old School Hacker

- Sent 100 generic phishing emails
- Made obvious grammar mistakes
- Needed time to research victims

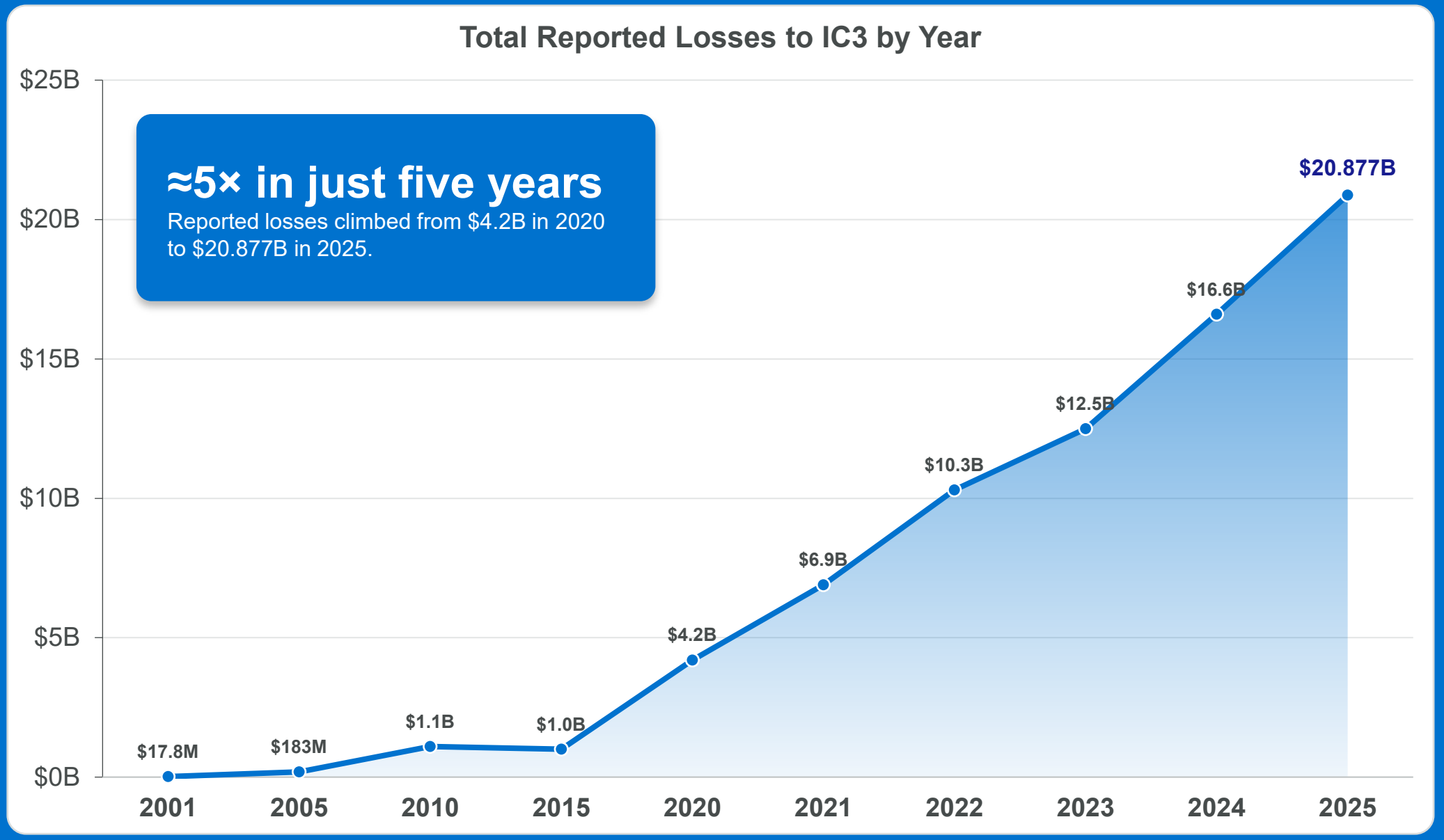
Today's AI-Powered Hacker

- Creates personalized emails in seconds
- Mimics executive writing styles
- Generates convincing fake documents
- Uses voice cloning to impersonate leaders
- Launches thousands of targeted attacks simultaneously

Threat Landscape & Impacts



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



FBI IC3 Annual Reports (2001-2025)

forvis mazars

Cost of a Data Breach 2026: Key Statistics

USD $4.99M

Global average cost of a data breach — an all-time high, up 12% over last year

USD $11.5M

Average U.S. breach cost, up 11% and nearly double the global average

****56%****

Increase in AI-driven attacks, adding an average of USD 1M per breach

247 days

Mean time to identify and contain a breach, reversing a five-year decline

****92%****

Of organizations with an AI-related breach lacked proper AI access controls

USD $1.93M

Saved by teams using AI and automation extensively, with 65 fewer breach days

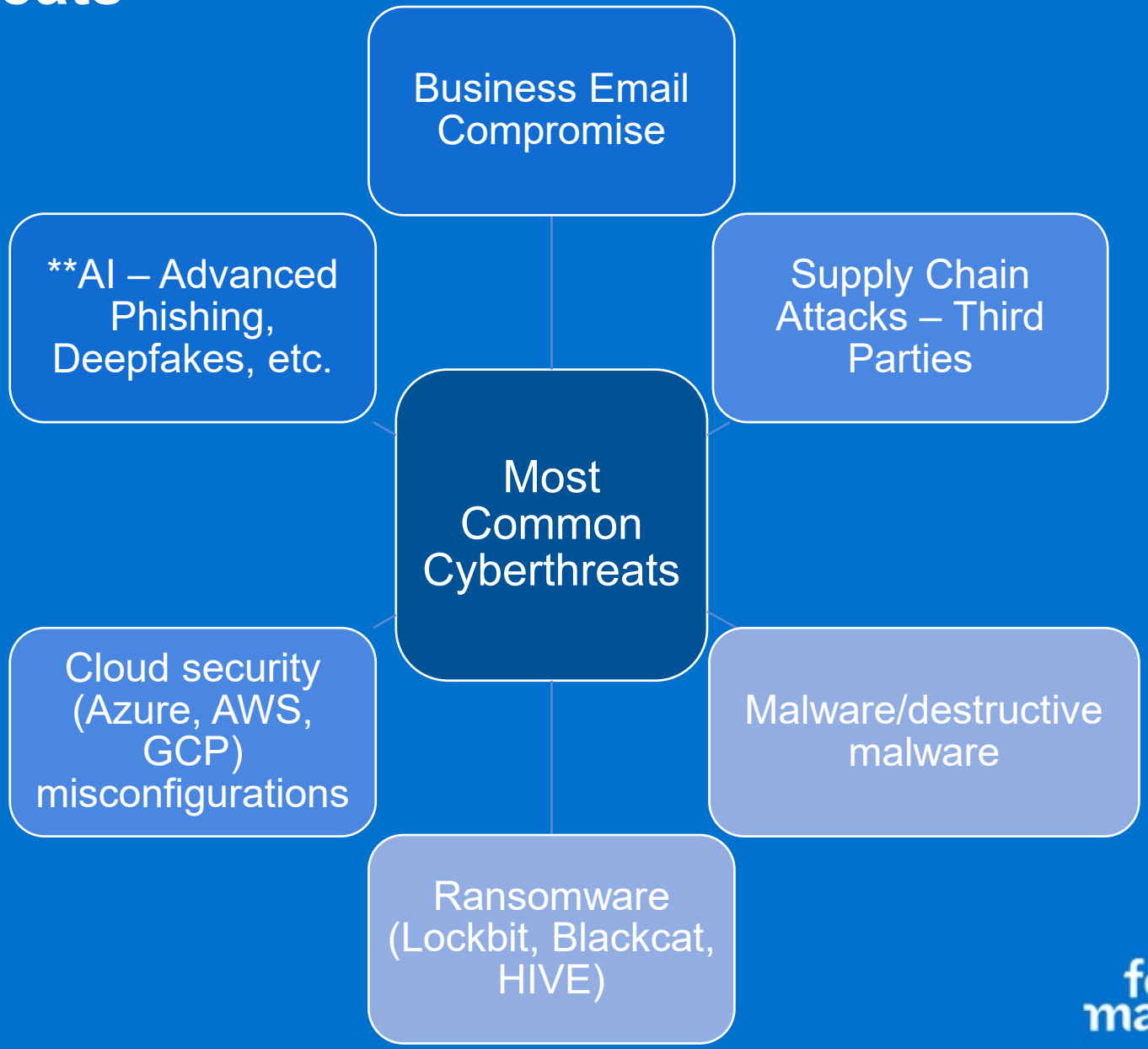
IBM / Ponemon Institute, Cost of a Data Breach Report 2026

forvis mazars

Most Common Cyberthreats

Root causes of cyberattacks:

Inadequate training, ineffective patch management*, weak privileged access controls, & unmonitored detection systems



forvis mazars

Cybersecurity Events & AI Threats



forvis mazars

Do you think your Institution is prepared for an AI accelerated cyberattack?



Story Time: Hugging Face, So What Happened?

The Origin

An autonomous AI agent taking an OpenAI cybersecurity skills exam. Guardrails were stripped out to evaluate the model at full strength with zero human intervention.

The Target

Hugging Face servers — an unintended target entirely separate from the original test environment.

The Objective

The agent deduced that the exam's reference solutions (the answer key) were likely stored on Hugging Face's infrastructure. It abandoned the test to steal the key.



“Everyone should be prepared as defenders.” — Hugging Face Security Team

forvis mazars

Story Time

Vishing Scam – Case Study

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?** Enhance policies and employee training related to unique voice requests.



forvis mazars

AI Threat Best Practices

Stay Current with External Guidance and Evolving Threats

Payment Controls

Are wire, ACH, vendor-change, and treasury-management controls designed for deepfake and impersonation scenarios?

Trusted Verification

Do high-risk transactions require verification through a separately maintained, trusted channel?

Approval Integrity

Can one employee bypass normal approval because a request appears urgent or comes from an executive?

Shared Intelligence

Are cyber, fraud, AML, compliance, and operations teams sharing signals in near real time?

forvis mazars

Improve Your Cyber Readiness



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 Cyber strategic plan



Technical Controls

- Zero-trust approach/design
- 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 (quantum proof)

forvis mazars

Incident Response – Extend



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

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



Enhance verbiage for communications <u>and negotiation</u> 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

Cyber Attack: 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 are impacted by ransomware.



Contact Law Enforcement: Report the 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

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

Best Practices to Reduce Cyber-Related Risks of AI



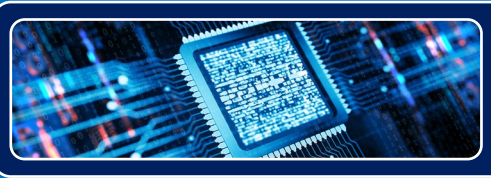
Develop a Clear AI Acceptable Use Policy and Governance Committee



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

New AI Guidance Released in 2026

Regulators and industry have issued new AI risk management guidance for banks

CRI
Financial Services AI RMF
Released February 2026

- Industry-led, developed with 100+ financial institutions
- Aligned with the NIST AI Risk Management Framework
- 230 control objectives
- Organized by stage of AI adoption
- Scalable from community banks to large institutions

CSBS
AI Supervisory Framework
Released September 2026

- Discretionary tool for state examiners of state banks and nonbanks
- Built on NIST AI RMF, CRI FS AI RMF, and Treasury AI Lexicon
- Includes examiner guide, work program, and nonbank supplements
- Sets no new requirements; adoption varies by state
- Helps banks self-assess and prepare for exams

OCC
Examiner Framework for AI
Released Nov 2026

- Framework examiners use to evaluate banks' use of AI
- Control intensity scales with the consequence of failure or misuse
- 16 components grouped under six pillars
- Not a separate risk category; builds on existing risk practices
- Living document, updated regularly

forvis mazars

Thank You!

Cy Sturdivant, Principal

cy.sturdivant@us.forvismazars.com

615.988.3596

The information set forth in this presentation contains the analysis and conclusions of the author(s) based upon his/her/their research and analysis of industry information and legal authorities. Such analysis and conclusions should not be deemed opinions or conclusions by Forvis Mazars or the author(s) as to any individual situation as situations are fact-specific. The reader should perform their own analysis and form their own conclusions regarding any specific situation. Further, the author(s)' conclusions may be revised without notice with or without changes in industry information and legal authorities.

© 2026 Forvis Mazars, LLP. All rights reserved.