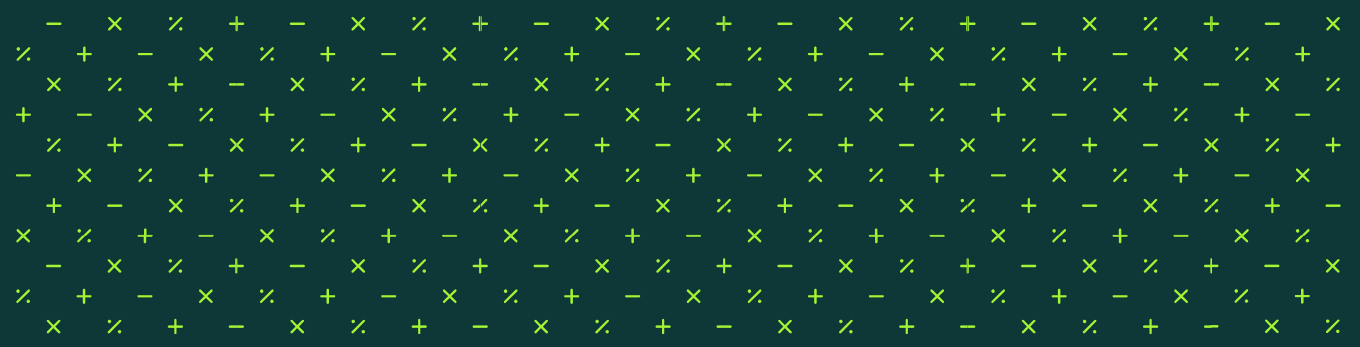


MOSSADAMS

Cybersecurity Trends and Hot Topics

Chris Wetzel, Director

Welcome

Chris Wetzel, CISA
Director, Financial Services Consulting

chris.wetzel@mossadams.com

(509) 777-0168

Agenda

01 REGULATORY FOCUS

02 CYBERSECURITY TRENDS

03 AI AND CYBERSECURITY

04 LOOKING AHEAD

Regulatory Focus

NCUA's 2024 Supervisory Priorities

- Interest Rate Risk
- Liquidity Risk
- Credit Risk
- Consumer Financial Protection
- ***Information Security (Cybersecurity)***
  - Establish a cybersecurity program that can adapt and evolve
  - Robust information security program
  - Cyber Incident Notification Reporting Rule, effective September 1, 2023

Regulatory Focus – Interagency

- Cybersecurity Assessment Tool (CAT) sunsetting in August 2025
- FFIEC Exam Manual Update (8/29/24) – Development and Acquisition booklet revised and renamed to *Development, Acquisition, and Maintenance (DA&M)* to incorporate updated information technology (IT) risk practices and frameworks
- OCC – 2024 Bank Supervision Operating Plan includes focus on "system and data backup techniques that enable recovery from disruptive and destructive attacks" and "validation of third-party controls and data protections"
- FINRA – Recent Disciplinary Actions/Fines: Inadequate Cybersecurity Practices; Social Engineering Breach; Cyber-related Account Takeover

Cyber Threats by the Numbers

Verizon Data Breach Investigation Report 2024
Financial Industry Results

3,348	1,115	Types of Compromises	Top Threat Patterns
❖ Number of reported incidents in 2023 ❖ Industry ranked 3rd overall	❖ Number of confirmed breaches/data disclosure in 2023 ❖ Industry ranked 4th overall	❖ Personal data (75%) ❖ Institution data (27%) ❖ Credentials (22%)	❖ System Intrusion ❖ Misc. Errors (Misdelivery, Misconfiguration) ❖ Social Engineering

Do you think your organization is providing an appropriate level of cybersecurity training?

What's Trending?

2023

- Direct data theft and extortion incidents are outpacing ransomware incidents
- Vast majority of data breaches involve data stored in the cloud
- AI and automation are reducing cost and minimizing time to identify and contain a breach
- Hackers are using AI to create phishing emails
- Employee training has a direct impact on reducing the cost of a breach

2024

- Proliferation of ransomware attacks
- More restrictive cyber insurance policies
- Legal trends causing a heightened focus on data privacy and transparency
- Integrating cybersecurity in corporate culture
- Using blockchain to enhance data security
- Integration of artificial intelligence (AI) and machine learning (ML) into cybersecurity practices

Artificial Intelligence on the Rise

Benefits

- Analyze large volumes of data to identify and mitigate cyber threats
- Assist in automating incident management and breach response
- Provide continuous monitoring to detect cyber attacks in real time and automate initial containment
- Internal access controls - identify anomalous behavior patterns and flag suspicious login attempts

Threats

- Increased speed and complexity of cyber attacks
- Create convincing social engineering attacks, both phishing and pretext calls (GenAI)
- ChatGPT is being used to write malicious code (e.g., malware, trojans, bots, ransomware)
- Reduced control over software development that uses AI
- Supply Chain/Third-Party vulnerabilities

NY Department of Financial Services Industry Letter

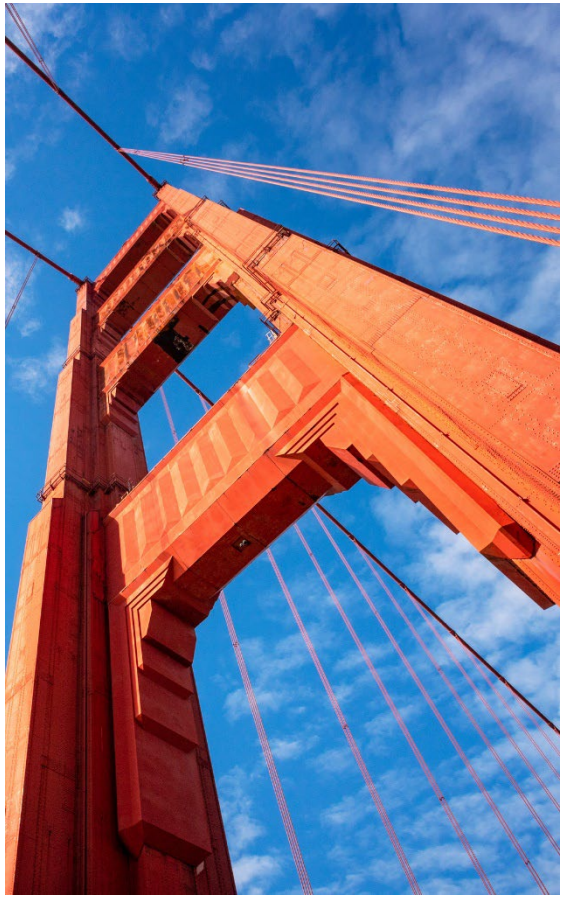
- Risk assessments – address AI-related risks
- Third-party management – understand use of AI and AI-enabled products and services
- Access controls – NY requiring multi-factor authentication to access NPI by November 2025
- Cybersecurity training – incorporate AI-related risks into regular training
- Monitoring – continuous monitoring to detect unauthorized access and unusual behaviors
- Data management – minimize NPI data and maintain up-to-date inventories

Source: https://www.dfs.ny.gov/industry-guidance/industry-letters/il20241016-cyber-risks-ai-and-strategies-combat-related-risks

What are your organization's current concerns with regard to AI?

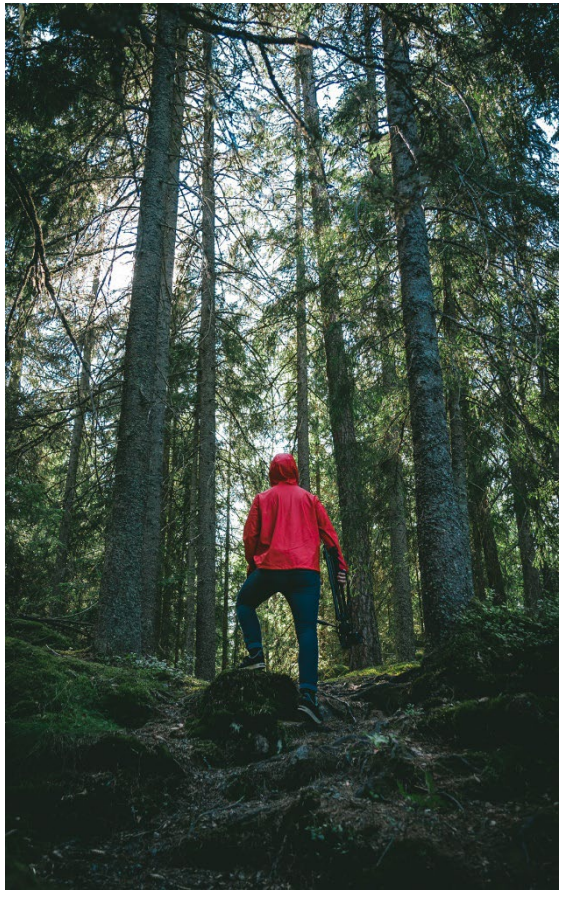
AI Trends and Use Cases

- Patch management
- Business Continuity Management and Incident Response Management testing
- Cyber incident response
- Fraud prevention
- Analyzing loan agreements
- Compliance and internal audit
- Automate repetitive manual tasks



A Look Ahead

- Emergence of generative AI (GenAI) as a mainstream capability
- Gap between security-talent supply and demand will increase
- Increasing regulatory obligations and government oversight of cybersecurity, privacy and data localization
- Use and sophistication of AI-powered cyber attacks increases
- Zero-Trust Architecture becomes the norm



Sources: Gartner.com; SecurityBoulevard.com; Medium.com

A Look Ahead

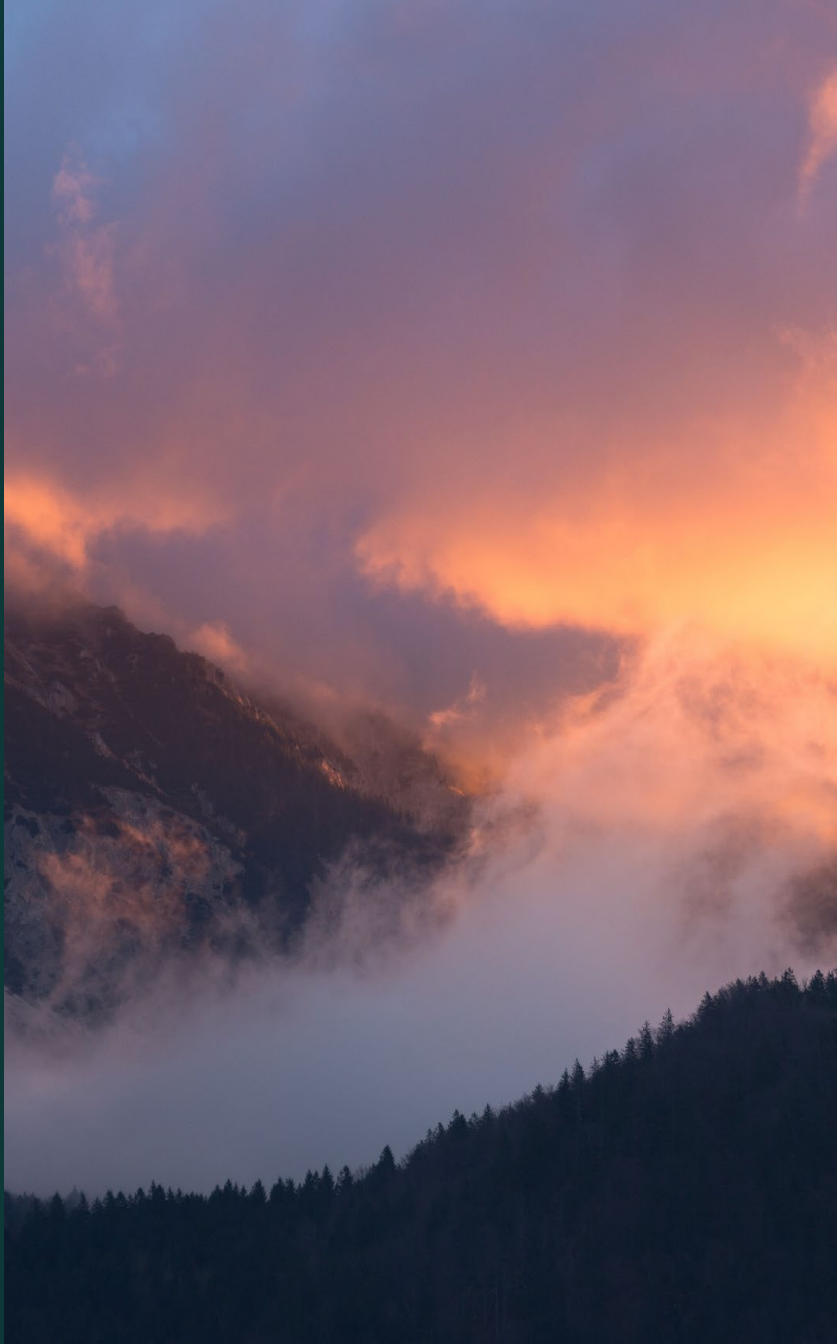
- By 2025, 60% of organizations will use cybersecurity risk as the primary determinant in conducting third-party transactions and business relationships.
- The percentage of states that enact laws regulating ransomware payments, fines and negotiations will increase to 30% by the end of 2025.
- By 2026, 70% of boards will include one member with cybersecurity expertise who will oversee a dedicated cybersecurity committee.
- The ability to efficiently mitigate cybersecurity risks will become a performance requirement for at least 50% of C-level executives by 2026.

Source: Gartner.com

Questions?

Chris Wetzel, Director
(509) 777-0168
Chris.Wetzel@mossadams.com

Thank you!



The material appearing in this presentation is for informational purposes only and should not be construed as advice of any kind, including, without limitation, legal, accounting, or investment advice. This information is not intended to create, and receipt does not constitute, a legal relationship, including, but not limited to, an accountant-client relationship. Although this information may have been prepared by professionals, it should not be used as a substitute for professional services. If legal, accounting, investment, or other professional advice is required, the services of a professional should be sought.

Praxity does not practice the profession of public accountancy or provide audit, tax, consulting or other professional services. Services are delivered by member firms, which are independent separate legal entities. The Alliance does not constitute a joint venture, partnership or network between participating firms and Praxity does not guarantee the services or the quality of services provided by participating firms. Praxity is not a 'network' within the meaning of the IESBA Code of Ethics. Praxity is organised as an international not-for-profit entity under Belgian law with its registered office in Belgium. Praxity has its registered administrative office at Suite 2, Beechwood, 57 Church Street, Epsom, Surrey KT17 4PX, UK. which is operated under Praxity - Global Alliance Limited (company number: 07873027), a limited by guarantee company registered in England and Wales.

Assurance, tax, and consulting offered through Moss Adams LLP. ISO/IEC 27001 services offered through Moss Adams Certifications LLC. Investment advisory offered through Moss Adams Wealth Advisors LLC.

THANK YOU