



1

We Will Cover

- Setting the Table
- Regulatory Updates
- Role of the Board
- Current Trends in Cyber and A.I.
- Key Questions for the Management Team
- Continuous Education and Awareness
- Tips for Effective Oversight
- Conclusion and Q&A



The slide has a light gray background with a faint, abstract geometric pattern. On the right side, there is a photograph of a modern, high-tech boardroom with a large circular table and several people seated around it. The room is filled with large digital screens displaying various data and charts. At the bottom right, the FoxPointe Solutions logo is displayed, consisting of an orange fox head icon and the text "FoxPointe Solutions" in a serif font, with "INFORMATION RISK MANAGEMENT" in a smaller sans-serif font below it.

2

NCUA Cybersecurity Memo

- Sent in October 2024 to Board members and CEOs
- Escalating Cyber Threats Require Board Level Attention
- Third-Party Vendors Are a Major Risk Vector
- Board members Must be Informed and Engaged, Not Technical Experts
- Proactive Incident Response and Resilience Planning Are critical



3

Why Data Security for the Board?

- What Are Your Biggest Threats?
 - “We have an IT Guy”
 - “We get a report every year”
- SolarWinds Malicious Code Attack
 - Board issue: SEC alleged material misleading statements were made and that passive oversight from the Board was unacceptable
- MGM Phishing Ransomware Attack
 - Board issue: The incident exposed weaknesses in human-factor defenses and raised questions about the board's role in ensuring comprehensive cybersecurity training and response planning.
- First American Financial Breach
 - Board issue: Internal security alerts were reportedly issued long before the board was informed. The SEC later reprimanded the company for inadequate disclosure controls, highlighting a failure in governance and communication.



4

Purpose – Why Data Security for the Board?

- Transparency
- Stay-in-the-know
- Meaningful decision making
- Regulatory expectations increasing
- Stay ahead of the curve with technology and innovation



5

Regulatory Updates

- Heavy emphasis on Governance, Board, and Management responsibility
- New requirements for Asset Inventorying and the policies and procedures that support the program.
- Multifactor authentication for all accounts accessing sensitive information.
- New reporting requirements for extortion payments and ransomware events.



6

Role of Board

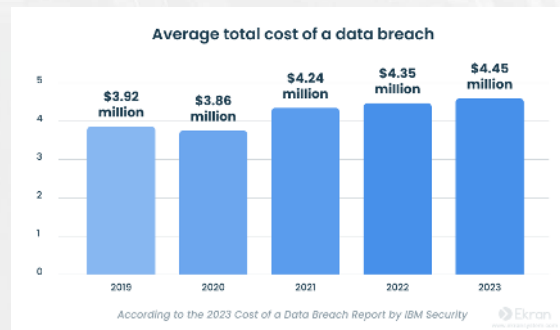
- Ensure compliance with NCUA, NYS DFS, and GLBA
- Reaffirm the Information Security Program
- Review the status of customer information security
- Review reports of the effectiveness of security initiatives
- Key interface and liaison with cyber and IT personnel
- Provide strategic direction and oversight



7

Current Trends in Cybersecurity

- Average cost of a data breach in 2023: \$4.45 million (IBM).
- 79% of organizations experienced a significant cyber event in the past year.
- Growth of AI in cybersecurity: Market expected to reach \$38.2 billion by 2026.

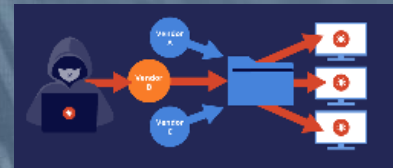


8

Current Trends

Supply Chain Threats

- The loss of critical dependent third-party technology and services may be even more wide-ranging and disruptive to patient care than when hospitals are attacked directly.
- UnitedHealth Group's Change Healthcare was attacked by the Russian ransomware group ALPHV BlackCat, impacting every hospital in the country.
- In 2024, 39.5% of data breaches in the healthcare sector occurred at business associates. This indicates a significant portion of breaches still involve third-party vendors, although the percentage is lower than the previous year.



9

Current Trends

Geopolitical Threats

- Critical infrastructure is increasingly targeted by state-sponsored threat actors.
- FBI and CISA have both recognized this as a critical issue.

Key Threats

- Russian Threat Actors: Compromised Microsoft email systems.
- Chinese Threat Actors: Compromised nine telecommunications companies in the United States.
- Volt Typhoon: Uses 'Living Off the Land' techniques to remain undetected and disrupt systems.

Mitigation Strategies

- Patching
- Multi-Factor Authentication (MFA)
- Logging
- 'End of Life' Management



10

Current Trends – Cont.

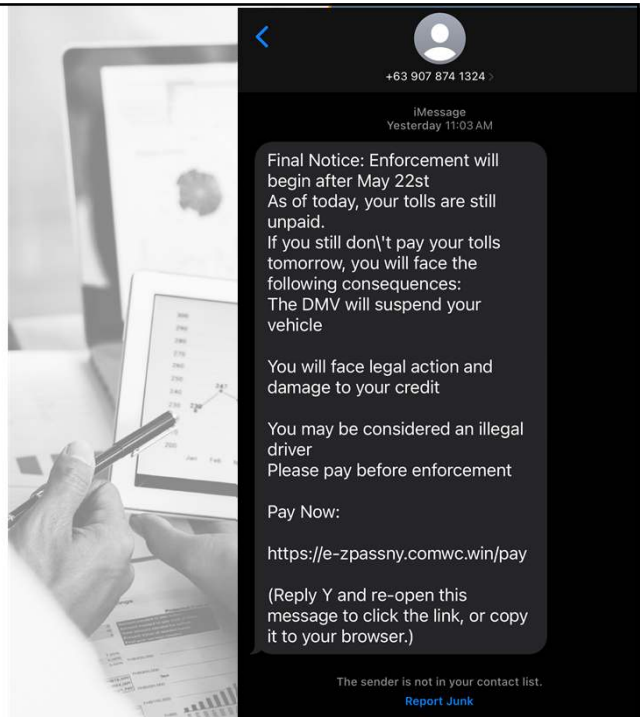
- Patelco Credit Union hit with ransomware attack that locked its 450,000 members out of their accounts in June resulted in a data breach involving sensitive personal information.
 - Hackers had unauthorized access to Patelco's databases for over 1 month before the ransomware was discovered.
 - Some customers went weeks without regaining full access to their accounts.
 - Communication from the Credit Union was slow to roll out.



11

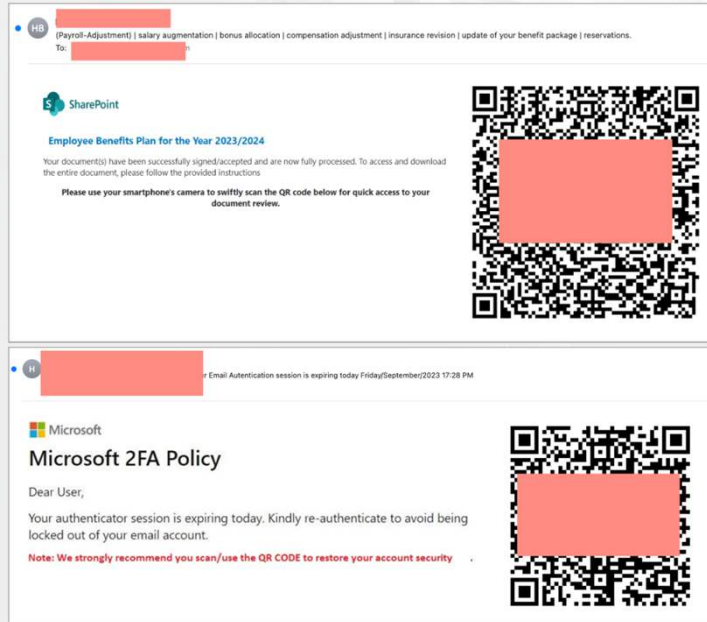
Current Trends – Cont.

- 68% increase of data breaches that originate via third parties.
- Lessons learned from the MOVEit breach
 - Communication is key
 - Vendor due diligence
- Approximately 3.4 billion phishing emails are sent each day.
- In 74% of data breaches, human factors played a role, encompassing social engineering tactics, mistakes, or misuse.



12

Scams with QR Codes



- 2022 – 1% of attacks
- 2023 – 25% of attacks
- Can bypass many filters
- Treat it just like a potential phishing. Look for red flags.
- Barracuda Impersonation Protection



13

Emerging Threats

ChatGPT and Other Artificial Intelligence (AI) Applications

- The increase in utilization of AI applications have improved efficiency and productivity.
 - However, new risks regarding information privacy and security have been introduced as a result.
- Develop an organizational policy.
 - Do not share sensitive data.
 - Define its business utility.
 - Since these are for the most part publicly accessible tools, proprietary information shared can be accessed by others.
 - AI-generated content should be classified as such.
 - Talk to your vendors about A.I. – Update your contracts!



14

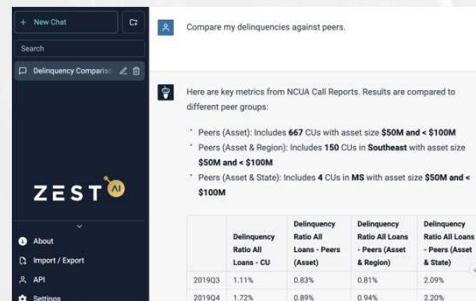
A.I. - Industry Use Cases

“Comerica says its AI bot performs work of six IT help desk agents”

As regional banks continue to face pressure to reduce operating costs, they are focusing potential cost-saving generative AI efforts to areas that aren't customer-facing or revenue-generating.

“Tennessee credit union uses generative AI tool Zest AI to foster fair lending”

- The tool is kept separate from underwriting models for regulatory compliance
- Trained initially from historical customer data and public sources such as NCUA call reports and Home Mortgage Disclosure Act filings.



15

Artificial Intelligence – This is why we can't have nice things



Man behind viral Tom Cruise deepfake videos calls the technology 'morally neutral'

Actor Miles Fisher, who has impersonated Tom Cruise in a series of uncanny deepfakes, says the positive of the technology outweighs the negative as it continues to develop.

World / Asia

Finance worker pays out \$25 million after video call with deepfake 'chief financial officer'

By Heather Chen and Kathleen Magrino, CNN
2 minute read · Published 2:31 AM EST, Sun February 4, 2024



- A.I. driven social engineering algorithms to identify ideal targets
- Deep Fakes
 - Deep Fake \$25 million loss in Hong Kong
 - AI Voice Cloning Pushes 91% of Banks to Rethink Verification



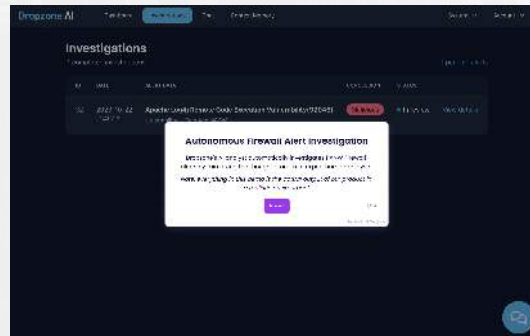
16

A.I. - Scaling and Tailoring for Smaller Institutions

Microsoft Security Copilot, Amazon Codewhisperer, Dropzone

These tools for example can look at a phishing alert and take responsive action, with no code, and you don't have to write any playbooks.

Institutions without resources for a full scale SOC team are going to be able to keep up and leverage.



17

Weighing Optimism and Risks

- 69% of Financial Service professionals say that criminals are more advanced at using AI for financial crime than banks are at using AI to fight financial crime.
- 51% of organizations lost between \$5 million and \$25 million to AI based attacks in 2023.
- AI Voice Cloning Pushes 91% of Banks to Rethink Verification
- Despite continued investment in technologies and resources to combat financial crime and fraud – threat actors are finding ways to circumvent these prevention measures.
- Study: GPT-4 Agent Can Exploit Unpatched Vulnerabilities

Report: BioCatch: 2024 AI, Fraud, and Financial Crime Survey



18

Considering the use of AI?

Step	Details
Define Objectives and Scope	<ul style="list-style-type: none"> - Identify Business Goals - Define the scope of AI Implementation
Assess Current Capabilities	<ul style="list-style-type: none"> - Technology Assessment - Skill Assessment
Develop an AI Strategy	<ul style="list-style-type: none"> - Roadmap Creation - Budgeting
Select AI Technologies and Partners	<ul style="list-style-type: none"> - Technology Selection - Partner with Vendors
Data Management and Governance	<ul style="list-style-type: none"> - Data Acquisition and Preparation - Establish Governance Policies
Develop or Acquire AI Models	<ul style="list-style-type: none"> - In-house Development - Outsource Development
Training and Testing	<ul style="list-style-type: none"> - Employee Training - Model Testing
Implementation and Integration	<ul style="list-style-type: none"> - Deployment - Integration with Existing Systems
Monitoring and Continuous Improvement	<ul style="list-style-type: none"> - Performance Tracking - Iterative Improvement
Scale and Expand	<ul style="list-style-type: none"> - Scaling AI Use - Iterative Learning
Ethical Considerations and Compliance	<ul style="list-style-type: none"> - Ethical AI Design and Use - Regulatory Compliance
Retirement or Evolution	<ul style="list-style-type: none"> - Discontinue, Evolve

This table provides a structured overview of suggested steps involved in adopting AI, from initial planning to ethical considerations and compliance.



19

Key Questions for the Management Team

- **Third Party Due Dilligence**
 - Can you walk us through how we assess and monitor our third-party vendors' cybersecurity practices, and how we ensure that our contracts include enforceable clauses for incident notification and data protection?
- **Culture of Cybersecurity**
 - How are we ensuring that cybersecurity awareness and operational resilience are integrated into employee training, performance metrics, and decision-making processes across all departments?



20

Key Questions for the Management Team

- **Resources**
 - How are we aligning our cybersecurity budget and staffing levels with our current risk profile, and do we have access to the external expertise needed to stay ahead of emerging threats?
- **Vulnerability and Threat Intelligence**
 - How are we ensuring timely patching of critical vulnerabilities, and are we actively leveraging free government threat intelligence resources to stay ahead?



21

Key Questions for the Management Team

- **Cybersecurity Preparedness**
 - What is our incident response Plan? Is it tested?
 - What is our role in a cyber incident?
 - How often are we conducting audits and assessments?



22

Key Questions – Cont.

- IT Governance
 - How do we ensure compliance with laws and regulations such as NYS DFS Part 500?
 - What steps are being taken to mitigate risks such as third-party?
- A.I. Oversight
 - Help define objectives and scope
 - Ensure the ethical use of A.I.
 - Establish an A.I. committee if necessary



23

Audits and Assessments

- Types of Audits
 - IT Audits
 - IT Risk Assessments
 - Vulnerability Scanning
 - Internal and External Penetration Testing
- Reporting and Oversight
 - Frequency and format of audit reports
 - Review and approval of the reports, workpapers and audit plan
 - Remediation of audit findings



24

Continuous Education and Awareness

- Year-Round Briefings
 - Importance of regular updates from the IT and cybersecurity teams.
 - Keeping the Board informed about new regulations and threats.
- Training Opportunities
 - Ongoing training for Board members on cybersecurity and IT trends.




25

Effective Oversight

- Establish a Cybersecurity Committee
 - Role and responsibilities.
- Promote a Culture of Cybersecurity
 - Encourage open communication and incident reporting.
- Stay Informed
 - Leverage resources from industry bodies (e.g., FFIEC, NCUA).
- Get an independent look!



26



FoxPointe Solutions

INFORMATION RISK MANAGEMENT

488 Madison Ave. 23rd Floor, New York, NY 10022

foxpointesolutions.com | 844.726.8869

Questions?

Christopher Salone –
csalone@foxpointesolutions.com

