FoxPointe Solutions

CYBERSECURITY • IT CONSULTING • COMPLIANCE

• A Division of The Bonadio Group •

foxpointesolutions.com | 844.726.8869

Strengthen Your Cybersecurity Strategy

Brandon Agostinelli, CISA, Director

Christopher Salone, CISA, Director

May 2, 2025

We Will Cover

- Why Data Security
- Emerging Information Security Threats
- Regulatory Updates
- Governance and Control
- Data Protection
- Thank you

FoxPointe Solutions
INFORMATION RISK MANAGEMENT
• A Division of The Bonadio Group •

Do You Want To Be in the Headlines?

- To date, OCR settled or imposed a civil money penalty in a total dollar amount of **$142,528,772.00**.
- March 2025 - Mission, Texas expects ransomware impact to last months
- March 2025- Texas Man Convicted of Sabotaging his Employer's Computer Systems and Deleting Data
- Louisiana Accounting Firm Breach Impacts More Than 127K Customers.
- Accounting firm hit with class action over data breach affecting 1M+
- HHS' Office for Civil Rights Settles HIPAA Security Rule Investigation with Health Fitness Corporation; $227k monetary penalty plus corrective action plan
- Texas county says 47,000 had SSNs, medical treatment info leaked during May cyberattack
- Change Healthcare says 190 million people in America affected by data breach
- Breach notifications needed to be made faster in 2024. Instead, they were made more slowly.

FoxPointe Solutions
INFORMATION RISK MANAGEMENT

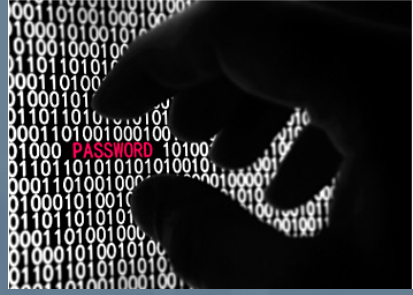
Why Data Security

Internet Reports

- As of today, there are 5.35 **billion** internet users.
- There are 7.26 billion unique mobile users in the world today.
- Over 90% of breaches in the last year involved the “human error” element (Use of stolen credentials, Phishing, Misuse, or simply an Error).
- 83% of stolen credentials resulted in a breach last year.
- All 50 States now have data breach statutes.

FoxPointe Solutions
INFORMATION RISK MANAGEMENT
• A Division of The Bonadio Group •

Why Data Security



Ransomware

- Total **Ransomware** increased again in 2024
- Ransomware was present in almost 70% of malware breaches this year.
- In 2024, 49% of ransomware attacks on financial services resulted in data encryption, a significant drop from 81% in 2023
- US average cost of a data breach in 2024: **$9.36M**
- 8 to 14% of data will not be recovered.
- Threat actors are now releasing PII/PHI/NPI up to two years **AFTER** the attack when you don't pay or try to negotiate the ransom.
- "Mal-vertising"

FoxPointe Solutions
INFORMATION RISK MANAGEMENT
• A Division of The Bonadio Group •

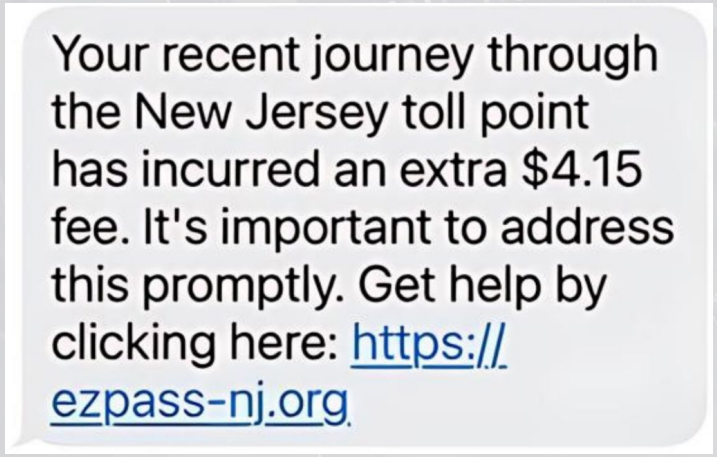
Why Data Security

Cybercrime as a Service (CaaS)/Ransomware as a Service (RaaS)

- Cybercrime-as-a-Service has opened a wide digital door to anyone looking to score a quick, illicit buck on the internet.
- Russian DDoS booter rental: $60/day, $400/week and orders over $500 qualify for 10 percent discounts.
- Ransomware kit – monthly rentals are available for $1,000 and prospective customers can test drive the product for 48 hours to see whether they like it.

FoxPointe Solutions
INFORMATION RISK MANAGEMENT
• A Division of The Bonadio Group •

Smishing – Always evolving



Think multifactor authentication. Double check with another source if you think the message might be legit

- **Website**
- **Phone call**

FoxPointe Solutions
INFORMATION RISK MANAGEMENT
• A Division of The Bonadio Group •

Why Data Security

ChatGPT, CoPilot 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 including "**Deep Fakes**".
- 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.
  - ChatGPT and similar applications are not bound by confidentiality or legal agreements, as a vendor or employee would be.

FoxPointe Solutions
INFORMATION RISK MANAGEMENT
• A Division of The Bonadio Group •

Considering the use of AI?

Step	Details
Define Objectives and Scope	- **Identify Business Goals** - **Define the scope of AI implementation**
Assess Current Capabilities	- **Technology Assessment** - **Skill Assessment**
Develop an AI Strategy	- **Roadmap Creation** - **Budgeting**
Select AI Technologies and Partners	- **Technology Selection** - **Partner with Vendors**
Data Management and Governance	- Data Acquisition and Preparation - Establish Governance Policies
Develop or Acquire AI Models	- In-house Development - Outsource Development
Training and Testing	- Employee Training - Model Testing
Implementation and Integration	- Deployment - Integration with Existing Systems
Monitoring and Continuous Improvement	- Performance Tracking - Iterative Improvement
Scale and Expand	- Scaling AI Use - Iterative Learning
Ethical Considerations and Compliance	- Ethical AI Design and Use - Regulatory Compliance
Retirement or Evolution	- Discontinue, Evolve

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

FoxPointe Solutions
INFORMATION RISK MANAGEMENT
• A Division of The Bonadio Group •

NEWS

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 Magramo, CNN

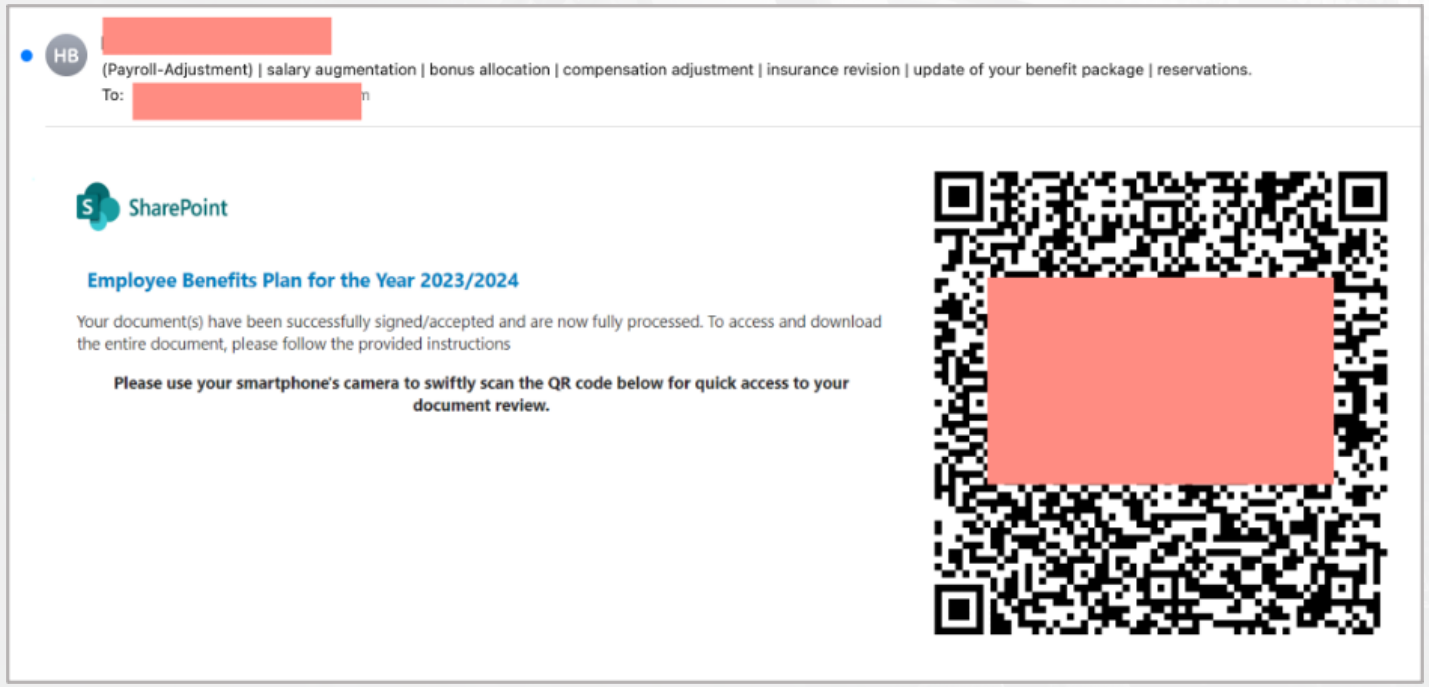
2 minute read · Published 2:31 AM EST, Sun February 4, 2024

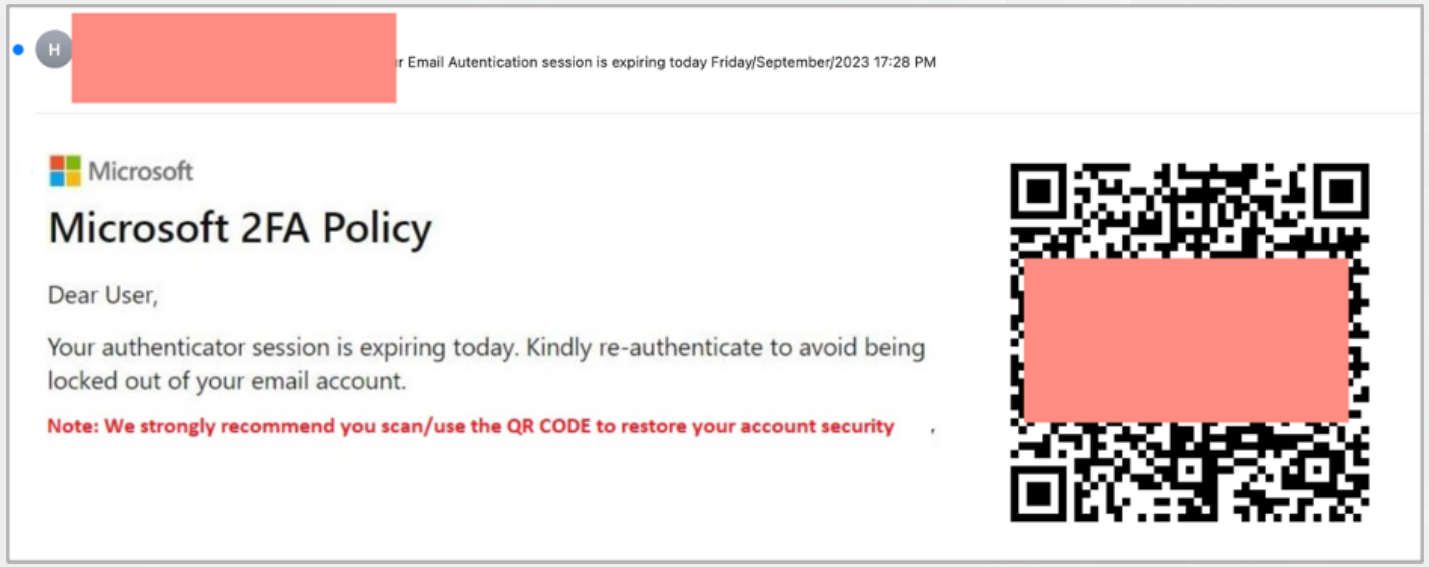
Artificial Intelligence – This is why we can’t have nice things

- 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

FoxPointe Solutions
INFORMATION RISK MANAGEMENT

Scams with QR Codes





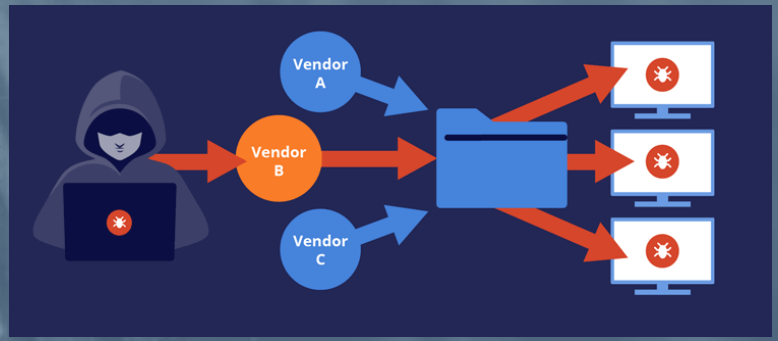
- 2022 – 1% of attacks
- 2023 – 25% of attacks
- Can bypass many filters
- Treat it just like a potential phish. Look for red flags.
- Barracuda Impersonation Protection

FoxPointe Solutions
INFORMATION RISK MANAGEMENT

Why Data Security

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.



FoxPointe Solutions
INFORMATION RISK MANAGEMENT
• A Division of The Bonadio Group •

Why Data Security

Geopolitical Threats – Texas Department of Banking

- 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

FoxPointe Solutions
INFORMATION RISK MANAGEMENT
• A Division of The Bonadio Group •

Regulatory Requirements

Changes to Laws, along with Standards, have Risk Identification, Reporting, and Breach Management Requirements

- Texas Cybersecurity Act – HB8 (2017)
- Texas Data Privacy and Security Act – HB4 (2024)
- Texas Privacy Protection Act – HB 4390 (2019)
- Federal Trade Commission GLBA (2023 Updates)
- Pending:
  - What will come of the Change Healthcare Breach (HIPAA NPRM)?

HIPAA

GLBA
Gramm-Leach-Bliley Act

FoxPointe Solutions
INFORMATION RISK MANAGEMENT
• A Division of The Bonadio Group •

Cyber Incident Reporting Requirements

If your Organization is obligated to comply with multiple cyber regulations, make sure your Incident Response Plan includes the needed notification requirements

- **HIPAA**
  - Timeframe: Within 60 days of discovering the breach.
  - Affected Individuals: All individuals whose unsecured protected health information (PHI) has been compromised.
  - Reporting: Notify the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) and affected individuals. If the breach affects 500 or more individuals, media outlets must also be notified
- **Texas Cybersecurity Act**
  - Timeframe: Within 48 hours of determining a cybersecurity incident has occurred.
  - Affected Individuals: Not specified, but any suspected breach or unauthorized disclosure must be reported.
  - Reporting: Notify the Texas Cybersecurity Coordinator

FoxPointe Solutions
INFORMATION RISK MANAGEMENT
• A Division of The Bonadio Group •

Cyber Incident Reporting Requirements (Cont.)

- **Texas Data Privacy Protection Act**
  - Timeframe: Within 60 days following the determination
  - Affected Individuals: 250 or more Texans.
  - Reporting: Notify affected individuals and the Texas Attorney General
- **Federal Trade Commission (FTC) Gramm-Leach-Bliley Act (GLBA)**
  - Timeframe: Within 30 days of discovering a breach
  - Affected Individuals: 500 or more
  - Reporting: Notify the FTC

FoxPointe Solutions
INFORMATION RISK MANAGEMENT
• A Division of The Bonadio Group •

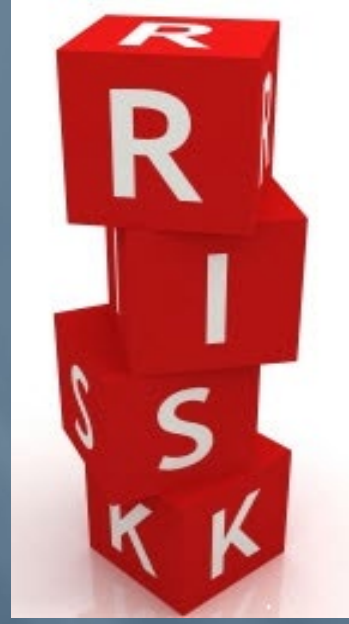
All That Said…

- **There is too much to do?**
- **I can’t keep up?**
- **Where do I start?**

FoxPointe Solutions
INFORMATION RISK MANAGEMENT
• A Division of The Bonadio Group •

Your Assurance Framework

Risk Assessment as a Key Control



- Must be an accurate and thorough assessment of all protected data, no matter where it is interacted with
- Identify the following:
  - Purpose of the assessment.
  - Scope of the assessment.
  - Assumptions and constraints associated with the assessment.
  - Sources of information to be used as inputs to the assessment.
  - Risk model/framework and analytic approaches (NIST SP800-30r1, NIST CSF, CIS, Regulatory Specific) to be employed during the assessment.
  - Repeated annually **and** at any material change

FoxPointe Solutions
INFORMATION RISK MANAGEMENT
• A Division of The Bonadio Group •

Governance and Control

- Chief Information Security Officer – Key Role/Expectations
  - Needs to be focused on monitoring, auditing and reporting, NOT implementing
  - Require a named and dedicated individual
  - Need a specific job description
  - Need to at least annually report to the Board/Audit Committee
  - Needs to have the appropriate training and certifications

FoxPointe Solutions
INFORMATION RISK MANAGEMENT
• A Division of The Bonadio Group •

Governance and Control

- Virtual Chief Information Security Officer – Key Role/Expectations
  - Everything above, based on a contracted, detailed scope of work
  - Can perform other actions (pentesting, vulnerability testing, vendor risk management, policy authoring, breach investigations, etc.)
  - Contracts must state that Management retains all responsibilities

FoxPointe Solutions
INFORMATION RISK MANAGEMENT
• A Division of The Bonadio Group •

Governance and Control

- Audit Policy
  - Commensurate with regulatory expectations
  - Must be approved on a defined schedule and frequency by your Audit Committee
- Scope is determined by a documented audit risk assessment
  - The identification/evaluation of multiple IT aspects within your ecosystem whereby risks are identified and evaluated for use in guiding the audit procedures.
- Deliverables
  - Report to the Board

FoxPointe Solutions
INFORMATION RISK MANAGEMENT
• A Division of The Bonadio Group •

Governance and Control

- Annual (minimum) report in writing to the board of directors or equivalent governing body
- Report is to include cybersecurity program and material cybersecurity risks:
  - Confidentiality, integrity and security of Nonpublic Information
  - Cybersecurity policies and procedures changes
  - Material cybersecurity risks
  - Overall effectiveness of the cybersecurity program
  - Material Cybersecurity Events for the period
  - Other items as needed

FoxPointe Solutions
INFORMATION RISK MANAGEMENT
• A Division of The Bonadio Group •

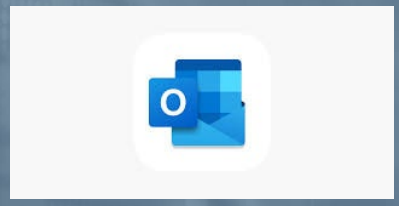
Data Protection Tools

- Acceptable Use
  - What can users do?
  - What shouldn’t they do?
  - Must be acknowledged annually.

FoxPointe Solutions
INFORMATION RISK MANAGEMENT
• A Division of The Bonadio Group •

Data Protection Tools

- Email
  - Don’t use the free version – they are not secure or compliant with any data security law.
  - Make sure any “rules” are reviewed.
  - Use the “App” vs the “Browser” version.



FoxPointe Solutions
INFORMATION RISK MANAGEMENT
• A Division of The Bonadio Group •

Data Protection Tools

- Access Controls
  - Least Rights!
  - No generic accounts.
  - Unique longer passwords.
  - Password expiration has changed.
  - Multi-Factor Authentication is a must.
  - Timely access removal.
  - Annual access review.
  - Domain needs to be stronger than user.
  - Access must be auditable and reviewed.
  - On premises and remote access controls.

FoxPointe Solutions
INFORMATION RISK MANAGEMENT
• A Division of The Bonadio Group •

Data Protection Tools

- Security Awareness Training
  - Make sure it is documented in policy.
  - Require completion at hire and at least annually.
  - Additional training after every incident.
  - **All** workforce (staff, BOD, etc.) need to be included.

FoxPointe Solutions
INFORMATION RISK MANAGEMENT
• A Division of The Bonadio Group •

Data Protection Tools

- Data Inventory, Retention, and Destruction
  - Who, What, How is information protected.
  - Data governance documented in policies.
  - Ensure organizational applicability, and meeting laws and standards.
  - Electronic and hardcopy documents.
- Audit all file locations, File shares, Applications, Portable devices (BYOD Too!), Third Party
- Interview SME's
- Interview IT
- Cross reference data type to Laws and Retention

FoxPointe Solutions
INFORMATION RISK MANAGEMENT
• A Division of The Bonadio Group •

Data Protection Tools

- Encryption
  - On all computers
  - On all portable devices (and BYOD!)
  - On email
  - Backups

Remember! Deleting a file name does NOT delete the file. It can be easily recovered with off the shelf tools!

FoxPointe Solutions
INFORMATION RISK MANAGEMENT
• A Division of The Bonadio Group •

Data Protection Tools

- End point protection past AV/AM
  - High risk devices should have endpoint detection, management and response tools
  - Web filtering
  - Spam filtering
  - Whitelisting

FoxPointe Solutions
INFORMATION RISK MANAGEMENT
• A Division of The Bonadio Group •

Data Protection Tools

- Documented Vendor Management Program
  - VM Policy
  - Vendor Risk Ranking
  - Roles and Responsibilities
  - Acceptable third–party assessments
- Risk Assessments
- Appropriate vendor contract language
- Onboarding and Annual Due Diligence Audits
- Service Level Agreement Compliance

4th party too!

FoxPointe Solutions
INFORMATION RISK MANAGEMENT
• A Division of The Bonadio Group •

Data Protection Tools

- Incident Response Plan
  - Have a documented plan
  - Use experts when in doubt
  - Have an Attorney available
  - Test the plan at least annually
  - Require 3rd parties to have a plan
  - Breach reporting should be included in your annual IRP testing

FoxPointe Solutions
INFORMATION RISK MANAGEMENT
• A Division of The Bonadio Group •

Data Protection Tools

- Patch and Change Management
  - Security Updates happen daily – they must be added.
  - Material changes need to follow a “circular” process.
  - Key for outsourced vendors too.

FoxPointe Solutions
INFORMATION RISK MANAGEMENT
• A Division of The Bonadio Group •

Data Protection Tools

- Vulnerability Assessments
  - Credentialed
  - Remediation schedule and tracker mapped to the policy
  - Vulnerability Assessment is not a Pen Test

FoxPointe Solutions
INFORMATION RISK MANAGEMENT
• A Division of The Bonadio Group •

Data Protection Tools

- Internal, External, Web, and Physical Penetration Testing
  - Qualified Personnel
  - At least annually and when significant changes to the environment occur
  - Required by contract for all 3rd party's
- Phishing
  - Smishing (cellphone)
  - Vishing (voice calling)
  - Spear (targeted)

FoxPointe Solutions
INFORMATION RISK MANAGEMENT
• A Division of The Bonadio Group •

Data Protection Tools

- Cyber Liability Coverage
  - You should have a policy
  - Make 100% certain what is covered
  - Your key vendors should have one too and you should be named on them
- Obtaining Coverage
  - Applying for and maintaining cyber liability coverage has become more difficult than ever. Many carriers are requiring security controls such as:
    - ✓ MFA
    - ✓ Security awareness training
    - ✓ Backup plans and redundancy
    - ✓ Vulnerability / endpoint management

FoxPointe Solutions
INFORMATION RISK MANAGEMENT
• A Division of The Bonadio Group •

Data Protection Tools

- Others
  - IT Asset Management Standards
  - Firewall Policy
  - Application Security Standards
  - Assurance and Testing Standards
  - Cloud Computing Policy
  - Mobile Device Program Policy
  - Instant Messaging Procedures
  - Service Requests and Problem Reporting Procedures

FoxPointe Solutions
INFORMATION RISK MANAGEMENT
• A Division of The Bonadio Group •

Key Items

- Be skeptical
- Be aware of your online presence
- Inspect
- Don’t click links
- Be smart with your passwords
- Keep your software updated
- Be an active part of your security strategy
- Risk assessment is NOT a one and done!

FoxPointe Solutions
INFORMATION RISK MANAGEMENT
• A Division of The Bonadio Group •

Thank you!

Brandon Agostinelli
bagostinelli@foxpointesolutions.com

Christopher Salone
csalone@foxpointesolutions.com

FoxPointe Solutions
INFORMATION RISK MANAGEMENT
• A Division of The Bonadio Group •