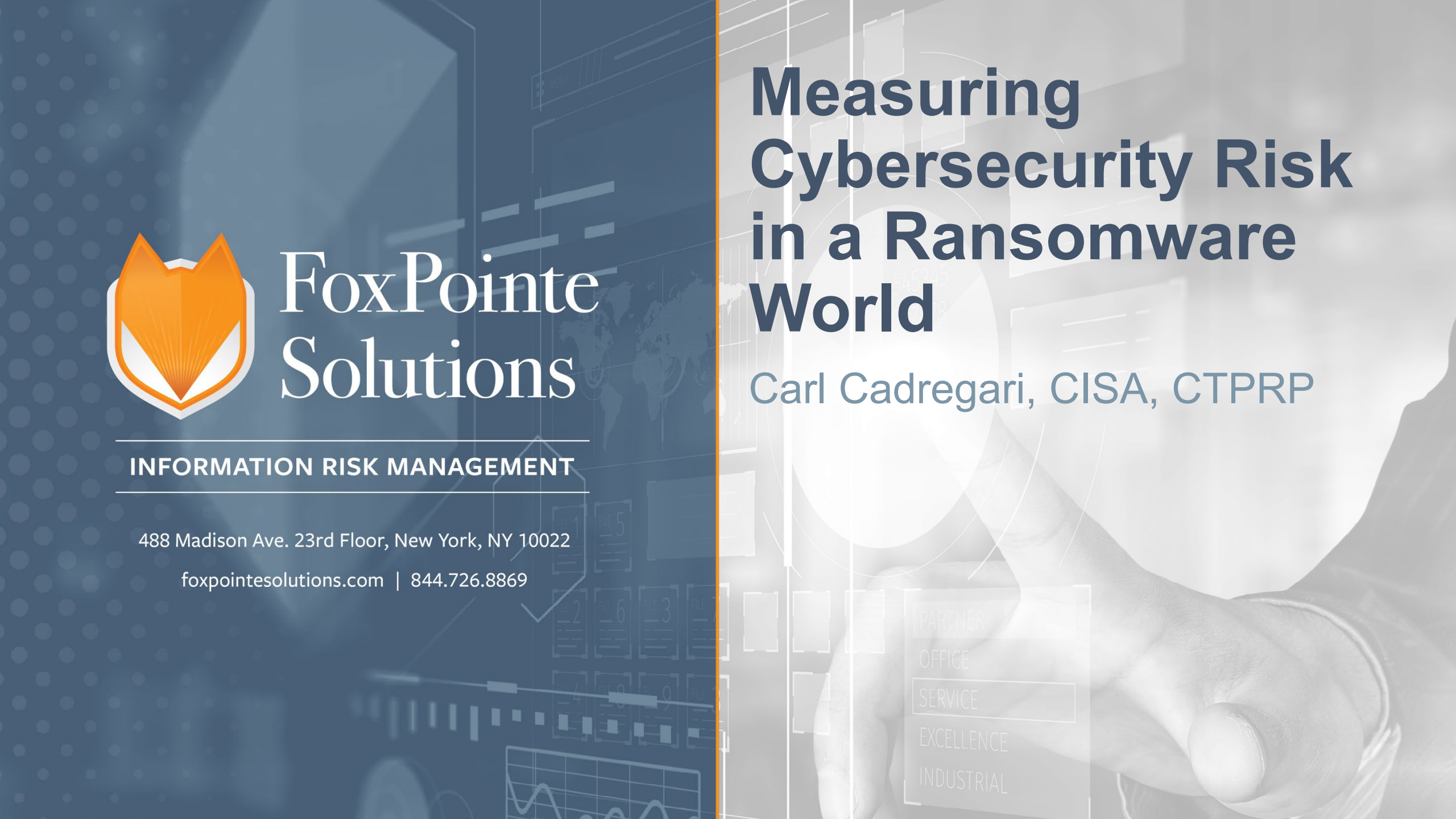


FoxPointe Solutions

INFORMATION RISK MANAGEMENT

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

foxpointesolutions.com | 844.726.8869

Measuring Cybersecurity Risk in a Ransomware World

Carl Cadregari, CISA, CTPRP


Mark LaVigne, PhD
Deputy Director
NYSAC

Carl Cadregari
Executive Vice President
FoxPointe Solutions

FoxPointe Solutions
INFORMATION RISK MANAGEMENT

THE BONADIO GROUP
CPAs, Consultants & More

We Will Cover

- Why Data Security
- Emerging Threats
- Regulatory Requirements
- Risk Assessment Controls
- Thank you

FoxPointe Solutions
INFORMATION RISK MANAGEMENT

THE BONADIO GROUP
CPAs, Consultants & More

Definitions

- NPI – Non-Public Information
- PII – Personally Identifiable Information
- PHI – Protected Health Information
- FTC – Federal Trade Commission
- ITGC – Information Technology General Controls
- ISP – Internet Service Provider
- CSIRT – Computer Security Incident Response Plan
- E-Banking – Electronic Banking
- SOC Report – Service Organization Control Report
- Cybersecurity – protections against the criminal or unauthorized use of electronic data
- VPN – Virtual Private Network
- BCP – Business Continuity Plan
- DRP – Disaster Recovery Plan
- BIA – Business Impact Analysis
- IPS – Intrusion Prevention Software/System
- IoT – Internet of Things
- BOT – Automated program that runs over the Internet
- DDoS – Distributed Denial-of-Service attack
- Phishing – email/internet “pick pocketing”
- ISP – internet service provider
- Blockchain – open, distributed ledger transactions in a verifiable and permanent way
- BA – Business Associate

FoxPointe Solutions
INFORMATION RISK MANAGEMENT

Why Data Security?

To Stay Out of the News

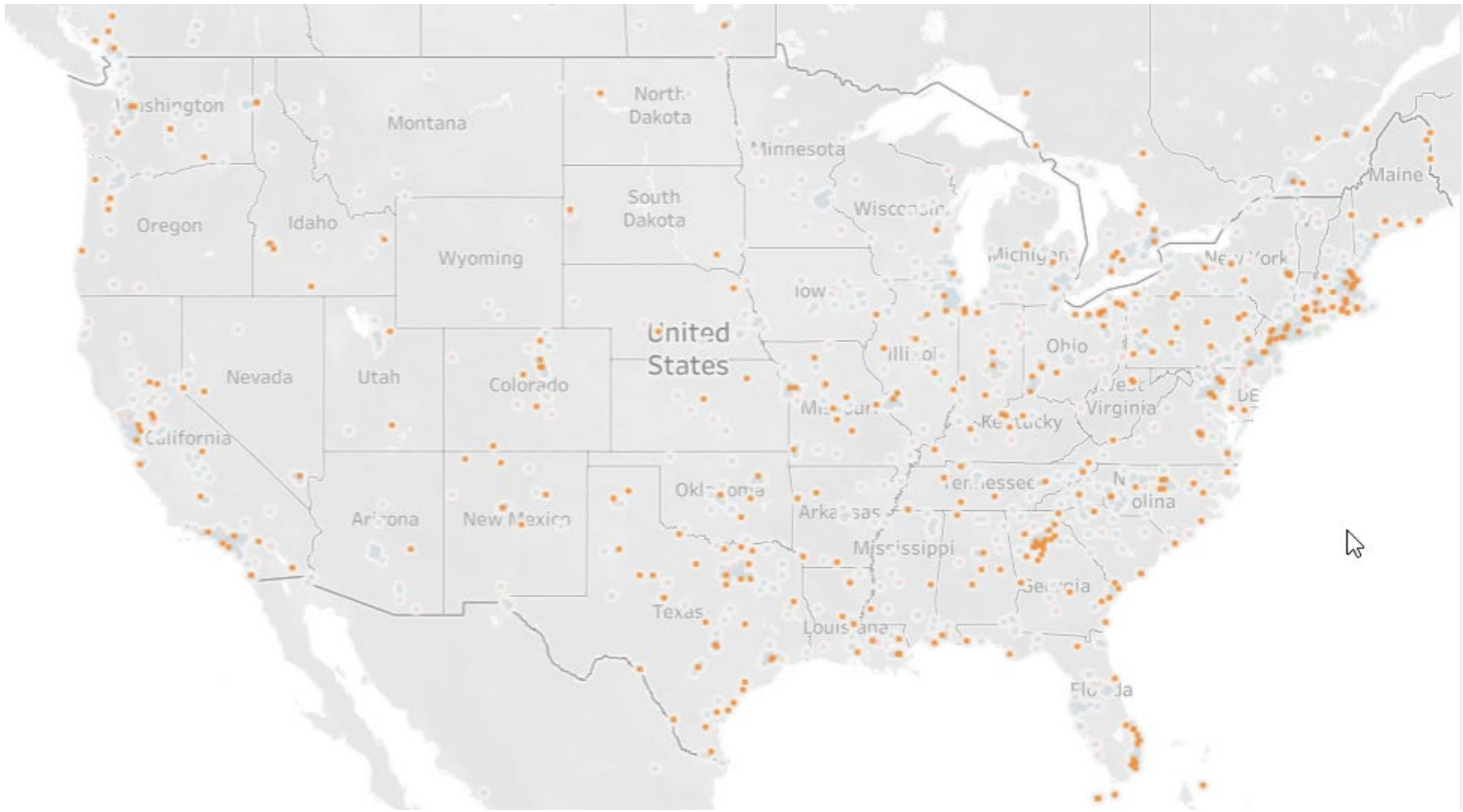
- Ransomware-as-a-service (RaaS) operation called DarkSide setting up a distributed storage system in Iran for storing data stolen from victims of its attacks
- Public housing assistance tenants in Indianapolis fear eviction, compromised bank accounts after cyber attack
- Cyberattack on Colorado state website follows Russian hacktivist threat
- City of Tucson discloses data breach affecting over 125,000 people
- Russian-speaking hackers knock US state government websites offline
- CT: Hamden mayor estimates $500,000 cost to address spring cyberattack
- Denver suburb won't cough up millions in ransomware attack that closed city hall
- GA: Former Dalton police officer sentenced to five years on probation for computer invasion of privacy and violating oath of office
- IL: Some residents' personal information possibly compromised in Quincy (IL) ransomware incident
- 4309 headlines just on Databreaches.net site

THE BONADIO GROUP
CPAs, Consultants & More

FoxPointe Solutions
INFORMATION RISK MANAGEMENT

Why Data Security?

To Stay Out of the News



THE BONADIO GROUP
CPAs, Consultants & More

FoxPointe Solutions
INFORMATION RISK MANAGEMENT

Why Data Security

Internet Reports

- As of July this year there are now 4.9 **Billion** internet users
- There are 7.26 billion unique mobile users in the world today
- Savvy attackers are using increased levels of deception and, in some cases, hijacking organizations' own infrastructure
- 60 percent of all targeted attacks struck small- and medium-sized organizations
- All 50 States now have data breach statutes.

THE BONADIO GROUP
CPAs, Consultants & More

FoxPointe Solutions
INFORMATION RISK MANAGEMENT

Emerging Threats

Ransomware

- Total **Ransomware** increased again during the first half of the year compared to the same period last year.
- Daily attacks are down but ransom requests are up
- Average downtime due to an attack: 22 days
- US average cost of a data breach: **$9.4M**
- 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.

THE BONADIO GROUP
CPAs, Consultants & More

FoxPointe Solutions
INFORMATION RISK MANAGEMENT

THE BONADIO GROUP
CPAs, Consultants & More

Emerging Threats

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

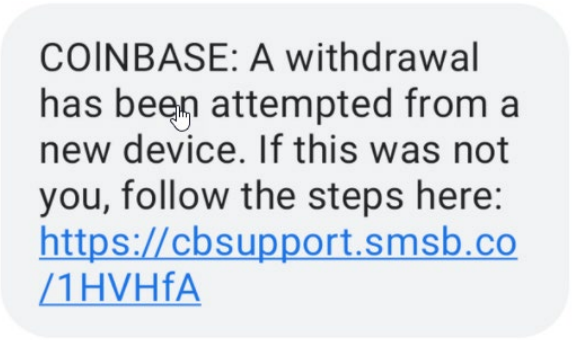
- Cybercrime-as-a-Service has opened a wide digital door to anyone looking to score a quick, illicit buck on the internet.

- 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

Emerging Threats



Smishing

- Smishing is a form of phishing that uses **mobile phones** as the attack platform. The criminal executes the attack with an intent to gather personal information. Smishing is implemented through text messages or other SMS communications.

THE BONADIO GROUP
CPAs, Consultants & More

FoxPointe Solutions
INFORMATION RISK MANAGEMENT

Emerging Threats

Not new, but ever changing

- Virus
- Malware
- Spyware
- Physical
- Administrative
- Technical
- IP
- Vendors

THE BONADIO GROUP
CPAs, Consultants & More

FoxPointe Solutions
INFORMATION RISK MANAGEMENT

Emerging Threats

Forget BYOD – how about BYODB – Bring Your Own Data Breach

- As sensors, and not just computing platforms—mobile devices susceptible to ransomware bring a new set of threats, including allowing malicious software an unparalleled look into victims' lives

There are now more Internet-connected mobile devices than people on the planet, with four out of five workers using personal mobile devices to do work

THE BONADIO GROUP
CPAs, Consultants & More

FoxPointe Solutions
INFORMATION RISK MANAGEMENT

THE BONADIO GROUP
CPAs, Consultants & More

Regulatory Requirements

HEALTH INSURANCE PORTABILITY and ACCOUNTABILITY ACT
HIPAA
ADMINISTRATIVE SIMPLIFICATION: PRIVACY, SECURITY, TRANSACTIONS

Federal and State Laws along with Standards have Risk Identification and Management Requirements

- HIPAA/HITECH
  - ✓ Required to conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate (third-party) and implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level

FoxPointe Solutions
INFORMATION RISK MANAGEMENT

THE BONADIO GROUP
CPAs, Consultants & More

Regulatory Requirements

NEW YORK Shield Act

Federal and State Laws along with Standards have Risk Identification and Management Requirements

- NY General Business Law
  - ✓ Required to identify reasonably foreseeable internal and external risks and assesses the sufficiency of safeguards in place, including third-party
- PCI DSS
  - ✓ A risk assessment, as required in the PCI DSS, is a formal process used by organizations to identify threats and vulnerabilities that could negatively impact the security of cardholder data

PCI Security Standards Council

FoxPointe Solutions
INFORMATION RISK MANAGEMENT

23 NYCRR 500
Cybersecurity Requirements for Financial Services Companies

Regulatory Requirements

Federal and State Laws along with Standards have Risk Identification and Management Requirements

- NY DFS 23NYCRR500 Cybersecurity Rule
  - ✓ Required to identify reasonably foreseeable internal and external risks and assesses the sufficiency of safeguards in place, including all third-party service providers
- GLBA
  - ✓ Expanded law has many “new” covered entities and if you have to meet NY DFS, you may be one

GLBA
Security Standards

THE BONADIO GROUP
CPAs, Consultants & More

FoxPointe Solutions
INFORMATION RISK MANAGEMENT

All That Said…

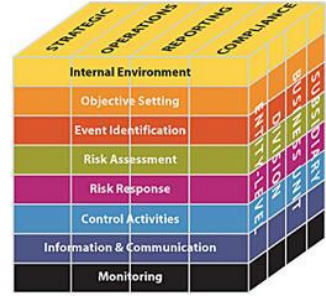
- The Sky is Falling?
- There is too much to do?
- I can't keep up?
- Where do I start?

THE BONADIO GROUP
CPAs, Consultants & More

FoxPointe Solutions
INFORMATION RISK MANAGEMENT

THE BONADIO GROUP
CPAs, Consultants & More

Your Assurance Framework



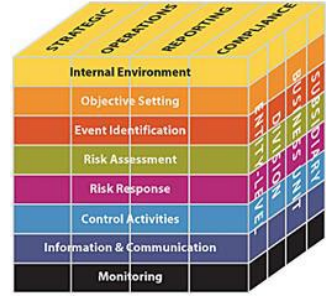
Risk Assessment as a Key Control

- Identify the:
  - ✓ 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; and
  - ✓ Risk model/framework and analytic approaches (i.e., assessment and analysis approaches) to be employed during the assessment
  - ✓ Documenting the assessment is mandatory

FoxPointe Solutions
INFORMATION RISK MANAGEMENT

THE BONADIO GROUP
CPAs, Consultants & More

Your Assurance Framework

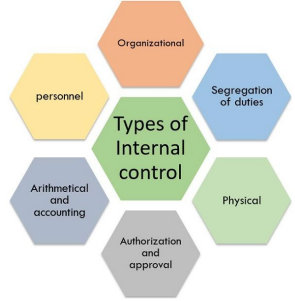


Risk Model/Framework

- Risk framing identifies, for example, organizational information regarding policies and requirements for conducting risk assessments, specific assessment methodologies to be employed, procedures for selecting risk factors to be considered, scope of the assessments, rigor of analyses, degree of formality, and requirements that facilitate consistent and repeatable risk determinations across the organization
- NIST SP800-30r1, NIST CSF, COSO, CoBIT, Regulatory Specific

FoxPointe Solutions
INFORMATION RISK MANAGEMENT

Your Assurance Framework



Control Sets

- Control sets are a catalog of security and privacy controls for information systems and organizations
- They are designed and implemented to protect organizational operations and assets from a diverse set of threats and risks
- Controls are meant to be flexible and customizable and implemented as part of an organization-wide process to manage risk and need to address diverse requirements derived from mission and business needs, laws, executive orders, directives, regulations, policies, standards, and guidelines
- NIST SP800-53R5, PCI DSS

THE BONADIO GROUP
CPAs, Consultants & More

FoxPointe Solutions
INFORMATION RISK MANAGEMENT

Your Assurance Framework

Risk Assessment Steps

- Identify the:
  - ✓ Threat Sources: Identify and characterize threat sources of concern, including capability, intent, and targeting characteristics for adversarial threats and range of effects for non-adversarial threats
  - ✓ Threat Events: Identify potential threat events, relevance of the events
  - ✓ Vulnerabilities And Predisposing Conditions: Identify vulnerabilities and predisposing conditions (i.e. data regulations, uses, third party, etc.) that affect the likelihood that threat events of concern result in adverse impacts

THE BONADIO GROUP
CPAs, Consultants & More

FoxPointe Solutions
INFORMATION RISK MANAGEMENT

Your Assurance Framework

Risk Assessment: Likelihood

- Determine the likelihood that threat events of concern result in adverse impacts, considering the:
  - Characteristics of the threat sources that could initiate the events;
  - Vulnerabilities/predisposing conditions identified; and
  - Organizational susceptibility reflecting the safeguards/countermeasures planned or implemented to impede such events

THE BONADIO GROUP
CPAs, Consultants & More

FoxPointe Solutions
INFORMATION RISK MANAGEMENT

THE BONADIO GROUP
CPAs, Consultants & More

Your Assurance Framework

Risk Assessment: Impact

- Determine the adverse impacts from threat events of concern considering:
  - The potential harm, loss, interruption, unavailability, reputational damage, etc. caused to organizational data, operations and assets, individuals, to or from other organizations
  - Where the threat event occurs
  - The assets or potential targets of threat sources, including malicious actors, internal staff, outside people, processes, administration, physical, supply chain, environmental, information resources, information systems, applications, communications links, which could be affected by the exploitation of a threat event

FoxPointe Solutions
INFORMATION RISK MANAGEMENT

Your Assurance Framework

Risk Assessment: Compliance

- Based on the applicable rule (law, regulation and/or contractual requirement, etc.):
  - Will the control meet the applicable rule
  - What is the likelihood and impact to the organization for non-compliance

HEALTH INSURANCE PORTABILITY and ACCOUNTABILITY ACT
HIPAA
ADMINISTRATIVE SIMPLIFICATION: PRIVACY, SECURITY, TRANSACTIONS

23 NYCRR 500
Cybersecurity Requirements for Financial Services Companies

GLBA
Security Standards

PCI DSS

FISMA

FACTA

THE BONADIO GROUP
CPAs, Consultants & More

FoxPointe Solutions
INFORMATION RISK MANAGEMENT

Your Assurance Framework

Overall Risk Measurement

		Likelihood					
		Remote	Highly Unlikely	Unlikely	Possible	Likely	Almost Certain
		(<1% chance of occurrence)	(1% to 10% chance of occurrence)	(10% to 25% chance of occurrence)	(25% to 70% chance of occurrence)	(70% to 99% chance of occurrence)	(>99% chance of occurrence)
Impact	Catastrophic	MODERATE	HIGH	HIGH	SEVERE	EXTREME	EXTREME
	Critical	MODERATE	MODERATE	HIGH	SEVERE	SEVERE	EXTREME
	Major	LOW	MODERATE	HIGH	HIGH	SEVERE	SEVERE
	Moderate	LOW	LOW	MODERATE	HIGH	HIGH	HIGH
	Minor	LOW	LOW	MODERATE	MODERATE	MODERATE	HIGH
	Insignificant	LOW	LOW	LOW	LOW	MODERATE	MODERATE

Impact Rating	Damage/Service Impact	Financial/Reputational Impact
Catastrophic	Nearly unrecoverable damage or service impact	Financial and reputational damage too severe to continue business
Critical	Critical, long-term damage or service impact	Financial and reputational damage could be enough to ruin the business
Major	Major damage or service impact	Extensive reputational and financial impact, but not enough to ruin the business
Moderate	Noticeable damage or service impact	Harmful reputational and financial impact, but not enough to ruin the business
Minor	Localized or minimal damage or service impact	Minor reputational and financial impact
Insignificant	Little to no damage or service impact	No reputational or financial impact

THE BONADIO GROUP
CPAs, Consultants & More

FoxPointe Solutions
INFORMATION RISK MANAGEMENT

Risk Assessment Scenario #1

Large County Run Nursing Home

- ✓ Purpose of the assessment
  - ➢ Required for HIPAA
- ✓ Scope of the assessment
  - ➢ All Nursing Home assets
- ✓ Assumptions and constraints associated with the assessment
  - ➢ The Nursing Home including cloud EMR and billing applications

THE BONADIO GROUP
CPAs, Consultants & More

FoxPointe Solutions
INFORMATION RISK MANAGEMENT

Risk Assessment Scenario #1

- ✓ Sources of information to be used as inputs to the assessment
  - ➢ Policies and procedures, IT Team, Management, Third-Party Service provider
- ✓ Risk model/framework and analytic approaches (i.e., assessment and analysis approaches) to be employed during the assessment
  - ➢ HIPAA/HITECH, NIST CSF, SHIELD Act

THE BONADIO GROUP
CPAs, Consultants & More

FoxPointe Solutions
INFORMATION RISK MANAGEMENT

THE BONADIO GROUP
CPAs, Consultants & More

Risk Assessment Scenario #1

- ✓ Control Requirement: HIPAA law requires documented information security incident response procedures that include reasonably designed and implement policies and procedures that:
  - ➢ Identify and respond to suspected or known security incidents
  - ➢ Mitigate, to the extent practicable, harmful effects of security incidents that are known or suspected to the covered entity or business associate
  - ➢ Document and report security incidents and their outcomes

HEALTH INSURANCE PORTABILITY and ACCOUNTABILITY ACT
HIPAA
ADMINISTRATIVE SIMPLIFICATION: PRIVACY, SECURITY, TRANSACTIONS

FoxPointe Solutions
INFORMATION RISK MANAGEMENT

THE BONADIO GROUP
CPAs, Consultants & More

Risk Assessment Scenario #1

- ✓ Observation: Procedures for responding to a security breach or suspected security breach are not documented but IT knows they must respond but are unsure what should be reported to internal or external entities, no user training is done on how to report an incident
- ✓ A comprehensive and documented Information Security Incident Response Plan is not in place and no testing is performed
- ✓ Only AV and AM is installed on desktop/server assets and no mobile device management or MFA is in place

FoxPointe Solutions
INFORMATION RISK MANAGEMENT

Risk Assessment Scenario #1

- ✓ Likelihood: How reasonable is it that an event may go unreported or under-reported?
- ✓ Impact: What are the probable outcomes of an unreported or under-reported incident?
- ✓ Compliance: Does the policy and implementation of the control meet the expectations of the law?

		Likelihood					
		Remote	Highly Unlikely	Unlikely	Possible	Likely	Almost Certain
		(<1% chance of occurrence)	(1% to 10% chance of occurrence)	(10% to 25% chance of occurrence)	(25% to 70% chance of occurrence)	(70% to 99% chance of occurrence)	(>99% chance of occurrence)
Impact	Catastrophic	MODERATE	HIGH	HIGH	SEVERE	EXTREME	EXTREME
	Critical	MODERATE	MODERATE	HIGH	SEVERE	SEVERE	EXTREME
	Major	LOW	MODERATE	HIGH	HIGH	SEVERE	SEVERE
	Moderate	LOW	LOW	MODERATE	HIGH	HIGH	HIGH
	Minor	LOW	LOW	MODERATE	MODERATE	MODERATE	HIGH
	Insignificant	LOW	LOW	LOW	LOW	MODERATE	MODERATE

Overall Risk: High to Severe

THE BONADIO GROUP
CPAs, Consultants & More

FoxPointe Solutions
INFORMATION RISK MANAGEMENT

THE BONADIO GROUP
CPAs, Consultants & More

Risk Assessment Scenario #2

Town IT Department (Outsourced IT)

- ✓ Purpose of the assessment
  - ➢ General risk management, 3rd Party Vendor Management, SHIELD Act
- ✓ Scope of the assessment
  - ➢ All IT and outsourced IT Company
- ✓ Assumptions and constraints associated with the assessment
  - ➢ Limited internal staff

FoxPointe Solutions
INFORMATION RISK MANAGEMENT

THE BONADIO GROUP
CPAs, Consultants & More

Risk Assessment Scenario #2

- ✓ Sources of information to be used as inputs to the assessment
  - ➢ Policies, TSP Contract, Independent reports, interviews
- ✓ Risk model/framework and analytic approaches (i.e., assessment and analysis approaches) to be employed during the assessment
  - ➢ SHIELD Act, NIST SP800-53r5

NEW YORK Shield Act

NIST National Institute of Standards and Technology U.S. Department of Commerce

FoxPointe Solutions
INFORMATION RISK MANAGEMENT

THE BONADIO GROUP
CPAs, Consultants & More

Risk Assessment Scenario #2

- ✓ Control Requirement: NY SHIELD Act law requires any entity (not just those in NY) with computerized data which includes private information of a resident of New York shall:
  - ➢ Develop, implement and maintain reasonable safeguards to protect the security, confidentiality and integrity of the private information
  - ➢ Document procedures that include reasonably designed and implement policies and procedures
  - ➢ Select service providers capable of maintaining appropriate safeguards, and requires those safeguards by contract

FoxPointe Solutions
INFORMATION RISK MANAGEMENT

THE BONADIO GROUP
CPAs, Consultants & More

Risk Assessment Scenario #2

- ✓ Observation: The Town has a documented and annually reviewed vendor risk management policy and 3rd and 4th party RA reported to Senior Management at least annually and at every material change
- ✓ The program collects and reviews the SOC 2, Type 2 from the outsourced 3rd party and (when available) from all other in scope vendors
- ✓ Written contracts are in place that detail the vendors requirement to meet all laws and regulations applicable to the Town
- ✓ All other in scope vendors who do not have an independent report are given a data and information security questionnaire that must be competed annually and returned and reviewed by Management

FoxPointe Solutions
INFORMATION RISK MANAGEMENT

Risk Assessment Scenario #2

- ✓ Likelihood: How reasonable is it that an event may go un or under-reported?
- ✓ Impact: What are the probable outcomes of an unreported or under-reported incident?
- ✓ Compliance: Does the policy and implementation of the control meet the expectations of the law?

		Likelihood					
		Remote	Highly Unlikely	Unlikely	Possible	Likely	Almost Certain
		(<1% chance of occurrence)	(1% to 10% chance of occurrence)	(10% to 25% chance of occurrence)	(25% to 70% chance of occurrence)	(70% to 99% chance of occurrence)	(>99% chance of occurrence)
Impact	Catastrophic	MODERATE	HIGH	HIGH	SEVERE	EXTREME	EXTREME
	Critical	MODERATE	MODERATE	HIGH	SEVERE	SEVERE	EXTREME
	Major	LOW	MODERATE	HIGH	HIGH	SEVERE	SEVERE
	Moderate	LOW	LOW	MODERATE	HIGH	HIGH	HIGH
	Minor	LOW	LOW	MODERATE	MODERATE	MODERATE	HIGH
	Insignificant	LOW	LOW	LOW	LOW	MODERATE	MODERATE

Overall Risk: Low to Moderate

THE BONADIO GROUP
CPAs, Consultants & More

FoxPointe Solutions
INFORMATION RISK MANAGEMENT

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!

THE BONADIO GROUP
CPAs, Consultants & More

Thank You!

Carl Cadregari
Executive Vice President
FoxPointe Solutions

ccadregari@foxpointesolutions.com
(585) 249-2779

Big firm capability. Small firm personality.

THE BONADIO GROUP
CPAs, Consultants & More

FoxPointe Solutions
INFORMATION RISK MANAGEMENT