CYBER – WHAT YOU NEED TO KNOW

Sheri Pontolillo
Managing Principal
INTEGRO

WHAT'S IN STORE?

- States, SEC and FINRA released new requirements and guidance.
- Affects all firms, large and small.
- Includes a recommendation / directive to purchase cyber insurance. NEW!

Let's Review:

- Why and What of some of the new regulations
- Elements of Cyber Liability Insurance
- Types of cyber breaches and typical claims
- Do's and Don'ts in the event of a breach
- Question & Answer

TODAY'S TAKE-AWAYS

1. **Develop a mental picture of where you and your firm stands.**

2. **Identify areas for improvement or more research in order to prepare for implementation.**

3. **Give some thought to resources to assist, i.e. attorneys, consultants, vendors, insurance broker.**

4. **If not your area of responsibility, still valuable info. You don't want to be "that guy." Know what's up, be alert, and be *part of the solution* by understanding the need behind the new WSPs.**

HOW DID WE GET HERE?

SEC, FINRA and the States took cues from primarily three groups:

- National Institute of Standards and Technology (NIST) / non-regulatory branch of the US Dept of Commerce

  - Core Objectives (Best Practices) and Tiers of Compliance (Readiness) to be followed.

- Financial Services – Information Sharing and Analysis Center (FS-ISAC)

  - Members track, share, opine upon cyber security events.

- Office of Compliance Inspections & Examinations (OCIE)

  - February 2015 Report on sweep of 57 BDs and 49 Advisors.

HOW DID WE GET HERE?

HOW DID WE GET HERE?

OCIE Cyber Exam Sweep

57 BD's & 49 RIA's examined

- 54% of BD's and 43% of RIA's received fraudulent emails seeking to transfer client funds.
  - 26% reported losses over $5,000 but less than $75,000 (fairly small).
  - 1 firm reported loss in excess of $75,000.
- 25% of the BD's that had losses – attributable to employees/reps not following identity authentication procedures.
- 65% of BD's reported the fraudulent emails by filing a SAR but only 7% reported to law enforcement. RIA's generally did not report incidents.

HOW DID WE GET HERE?

Culminated in a new regulatory involvement

- **States**
  - Colorado – Cybersecurity regulations on BDs and IAs.
  - Vermont – Cybersecurity regulations on BDs and IAs.
  - New York – Cybersecurity regulations apply to “Insurance Brokers.”

48 states, DC, Guam, Puerto Rico and Virgin Islands have Breach/Privacy Laws

(Alabama and South Dakota are likely next).

- **FINRA** making “recommendations” citing the NIST report

HOW DID WE GET HERE? – NY Minute

DFS Cybersecurity Regs - It's a **REGULATION**, NOT Guidance.

All Covered Entities must "assess [their] specific risk profile and design a program that addresses [their] risks in a robust fashion" in order to "ensure the safety and soundness of the institution and protect its customers."

Credits to:
Kelly Geary of Integro, **Jim Stanhope** of iSecure and **Dianna McCarthy** of Winget Spadafora & Schwartzberg

HOW DID WE GET HERE? – NY Minute

- Applies to: Entities operating pursuant to a license, registration, charter, or similar authorization under NY's Banking, Insurance or Financial Services Laws
  - NYS Banks
  - Trusts
  - Budget Planners
  - Check Cashers
  - Credit Unions
  - Money Transmitters and their Holding Companies
  - Licensed Lenders
  - Mortgage Brokers and Bankers
  - Holding Companies
  - Insurance Companies and Brokers

Deadlines:

August 28, 2017

February 15, 2018

March 1, 2018

HOW DID WE GET HERE? – NY Minute

NY Compliance Components

- Cybersecurity Program
- Cybersecurity Policy
- Risk Assessment
- Chief Information Security Officer
- Penetration Testing and Vulnerability Assessments
- Audit Trail
- Access Privileges
- Application Security
- Cybersecurity Personnel
- Third Party Service Provider Security Policy
- Multi-Factor Authentication
- Limitations on Data Retention
- Training and Monitoring
- Encryption of Nonpublic Information
- Incident Response Plan


I changed all my passwords to "incorrect".
So whenever I forget, it will tell me "Your password is incorrect."
More funny pictures at WWW.JOKESPINOY.COM

National Institute of Standards and Technology

NIST SET THE STAGE WITH

THE NIST FRAMEWORK

TWO PARTS

CORE = Set of Best Practices

CORE FRAMEWORK 5 + 1

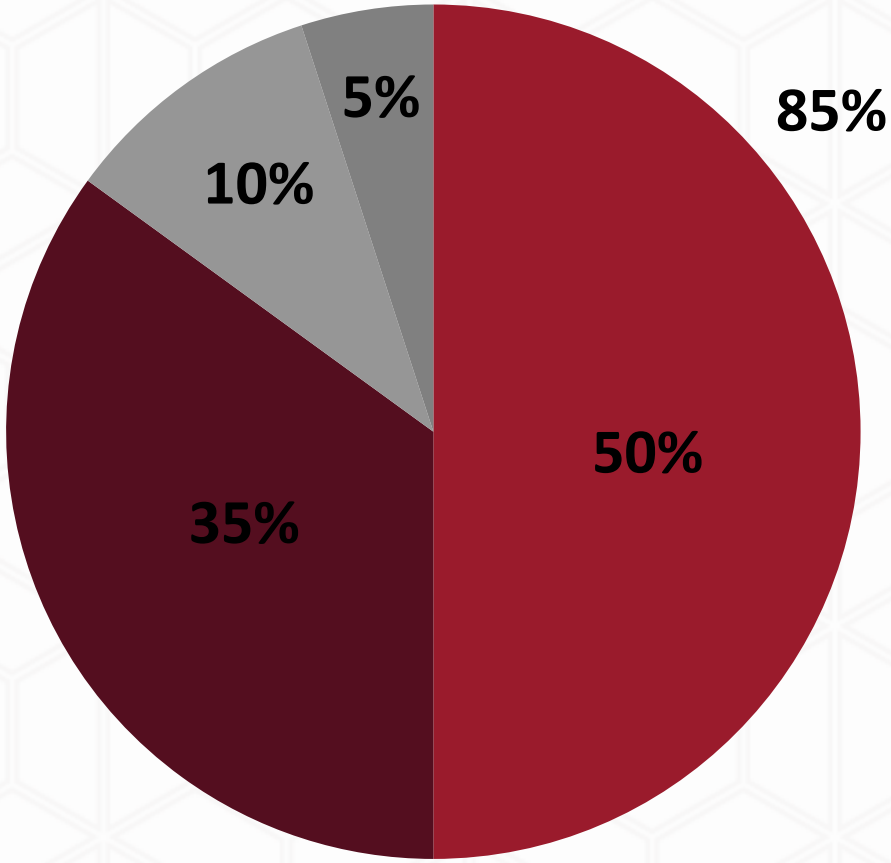
- IDENTIFY - Operational understanding
- PROTECT - Safeguards implemented
- DETECT - Identify a cyber occurrence
- RESPOND - Action upon an event
- RECOVER - Restore impaired capabilities or services
- \+ 1 Plus PAY UP - Fines and liabilities

NIST SET THE STAGE WITH

TIER = WHERE DO **YOU** STAND?

THE NIST FRAMEWORK
TWO PARTS

TIER FRAMEWORK



85%

- PARTIAL - Ad hock, reactive, inconsistent, not formal
- INFORMED - Management knows, compartmentalized
- REPEATABLE - Company-wide, formal, consistent methods ← Your Goal
- ADAPTIVE - Claim saavy, collaborate with external partners

THE RESULTING NEW REQUIREMENTS

If you want to get in the weeds, download these reports

1. SEC Cybersecurity Guidance / April 2015
2. FINRA Report on Cybersecurity Practices / February 2015
   - You can download FINRA's Cybersecurity Checklist (excel doc)

Good News:

- New regulations focused on essentially same points
- Some criteria are subjective based upon size/other characteristics of firm

Regulations Vary, and will continue to evolve, i.e. Vermont:

- Requirement for firms to pay for ID restoration
- Evidence of cyber insurance (tailored for size/scope of firm)

THE RESULTING NEW REQUIREMENTS

Key Point	Action
Cyber Security Program	Have a program to protect – 360
Cybersecurity Policy	Written cybersecurity policy
Risk Assessment	Periodic, documented, describe risk mitigation
Chief Information Security Officer-CISO	Designated, annual report, can be outsourced
Penetration Testing and Vulnerability Assessments	Monitor effectiveness
Audit Trail	Designed to detect and respond to events
Access Privileges	Limit and periodically review privileges
Application Security	Assessment of In-House and 3rd Party applications

THE RESULTING NEW REQUIREMENTS

Key Point	Action
Cybersecurity Personnel	Identified team to support CISO
Third Party Service Provider Security Policy	WSPs – information accessible or held by 3rd party
Multi-Factor Authentication	External individuals/networks accessing internal systems
Limits on Data Retention	WSPs for periodic disposal of nonpublic info
Training and Monitoring	Regular training; monitor/detect unauthorized access or use
Encryption of Non-Public Information	Control/protect NPI held or transmitted
Incident Response Plan	WSP to respond to and recover from an event

CYBER BREACHES AND CLAIMS EXPLAINED

- Social Engineering / Phishing Attacks via email / Theft of Funds
- Ransomware / Extortion
- Distributed Disruption of Service (DDOS)
- Breach of Private Personal Information (PPI)

Why?

- “Data is the new oil” – very valuable. Can be used and/or sold.
- Commercial espionage; trade secrets, pre-release financial reports, strategic plans, source code of valuable websites and applications, theft/sale of data.
- SEC / EDGAR and Equifax!!

➢Worrisome – Ransomware, Healthcare and Energy Grid attacks.

➢Pay particular attention to Terrorism Exclusions.

CYBER INSURANCE

- Cyber risk does not (yet) fit squarely within <u>any one insurance product</u>. Coverage ***may*** or ***may not*** be found in the following policies:

  - Management Liability/D&O
  - Employment Practices Liability
  - E&O/Professional Liability
  - Commercial Crime / Fidelity Bond
  - CGL/Property
  - Kidnap/Ransom
  - Cyber Insurance

Example:

Loss of 3rd party / client funds

- **Don't make assumptions - Conduct a Gap Analysis**: Identify and understand your **UNINSURED** exposure.

ELEMENTS OF CYBER INSURANCE

- **Privacy & Network Security Liability** - defense costs and settlements, if you are sued because of:
  - loss / theft of clients' or employees' personal OR business confidential information.
  - inadvertent transmission of a virus or hacking attack to a 3rd party.
- **Security Evaluation & Forensic Investigation** – expenses to investigate a breach to determine the cause and extent.
- **Privacy Regulatory Defense, Fines & Penalties** – for non-compliance with privacy laws.

ELEMENTS OF CYBER INSURANCE

- **Media Liability** – for media AND social media exposures (for example, copyright infringement, libel/slander or invasion of privacy related to your websites or blogs).
- **Data / System Restoration** – costs to restore your data / systems that are damaged.
- **Business Interruption** – your lost income during a system outage.
- **Notification & Credit Monitoring** - expenses to notify individuals whose information has been compromised, and provide credit repair services.
- **Public Relations Expenses** – to cover cost of repairing company image or name tarnished due to cyber event.

DIGGING A LITTLE DEEPER (1 of 2)

Questions to ask when buying cyber coverage:

- **what wrongful acts are covered for harming whom**
  - liability to others - Privacy, network security, media, triggered by an act by the insured.
  - 1st party coverage -data restoration, business interruption, the policy is triggered by a breach.

- **who can be the perpetrator**
  - an outside person (like a hacker or criminal),
  - a rogue employee (who intentionally causes a breach),
  - the insured's own negligence (lost device, trash bin vs shredding, etc.).

DIGGING A LITTLE DEEPER (2 of 2)

Questions to Ask:

- **Who/What can be <u>injured or damaged</u>**
  - <u>anyone</u> whose information is breached (privacy coverage).
  - only where an individual's info is breached and used to divert funds, steal identity, establish credit, commit healthcare fraud, etc.
  - a <u>3rd party</u> who is damaged by an attack emanating from the insured's.
  - the <u>insured's own damages</u>, for example, data restoration or business interruption (lost income / extra expense due to a system failure).
  - the insured's reputation.

- **<u>where</u> can the act or breach occur**
  - Does the policy cover acts occurring at the BD/RIA home office?
  - Does the policy cover acts occurring at the Advisor's office?
  - Does the policy include coverage for acts of independent contractors?

MORE QUESTIONS TO ASK

- **Would the policy apply if a rogue employee of the home office OR the rep's office committed a wrongful act?**
- **No coverage for the rogue employee, but would "Innocent Insureds" be covered?**
- **Would the policy apply if the private client information or corrupted data belonged to a third party, such as a vendor or other personal or business relationship?**
- **What if the information for which we are responsible is in the hands of a third party vendor?**
- **What if a device belonging to the home office staff OR the rep OR rep's staff was lost (such as a laptop or cell phone) and was used to retrieve private client information?**
- **Are all devices and data covered, both home office and reps' equipment? What about personal computers used for business?**

RECAP: PRE-BREACH AND POST-BREACH

- Risk Management has two categories; Pre-Breach and Post-Breach
- **Pre-Breach includes**
  - Risk Assessment of Exposures and Safeguards
  - Establish and Maintain Written Procedures
  - Train, re-train and remind associates
  - Educate clients of dangers of cyber communications
  - Leverage investment in vendors' products for added security
  - Purchase cyber insurance

Basic Best Practices

- Know **what** you need to protect – client info, proprietary models, employee records
- Know **where** it is – servers, cloud, mobile devices, etc.
- Texting an issue

RECAP: PRE-BREACH AND POST-BREACH

- **Post-Breach includes**
  - Analysis of source and scope of cyber event
  - Quantify the damages (funds, equipment, software, reputation)
  - Identify solution for damages
  - Notification to harmed parties
  - Interaction with regulators
  - Remediation of damages to people and property (yours and others')

DO'S AND DON'TS IN THE EVENT OF A CLAIM

- **Call your Breach Coach** – a lawyer
- Important to have Privileged and Confidential discussions in the early stages of exploring who did what when
- Help you prioritize next steps
- Assist you with tendering claim to Cyber insurer
- Recommend and work with additional service providers; forensic consultants, notification specialists, publicity consultants

DO'S AND DON'TS IN THE EVENT OF A CLAIM

- **Stop the bleeding**
- Mitigating damages is essential to protecting your coverage under the cyber policy
- Ascertain ASAP the source of the cyber event and who is/was affected
- Communicate the solution while identifying the problem

YOUR TAKE-AWAYS

- **Understanding of the regulators' concerns and knowing where you stand.**
- **What to expect in the future.**
- **Resources available (experts, reports, checklists).**
- **Knowledge of typical claim patterns.**
- **Mandatory cyber coverage on the horizon.**
- **New budget item / get advisors ready too.**
- **Knowledge of key coverage components.**
- **What questions to ask before purchasing cyber liability coverage.**


WEB SECURITY EXPERT
IF YOU GIVE ME LOTS OF MONEY, I WILL DO VARIOUS VAGUE THINGS TO INCREASE YOUR WEB SECURITY
Dilbert.com DilbertCartoonist@gmail.com
WOW! I WOULD HAVE BEEN HAPPY WITH JUST VARIOUS THINGS, BUT THAT VAGUE STUFF SOUNDS GREAT TOO!
9-27-12 ©2012 Scott Adams, Inc./Dist. by Universal Uclick
AND NOW HE'S MY RESPON-SIBILITY?
DON'T SCREW UP HIS VAGUE-NESS PLAN BECAUSE I THINK IT CAN WORK.

CYBER – WHAT YOU NEED TO KNOW

Questions
And
Answers