Cyber-INV-security in 2018 and Beyond....
Fear, Uncertainty, Doubt

However,

It is Manageable

OK, Back to The Bonadio Group Standard…
We Will Cover

- Why Information Security
- Organic Risk Management
- Emerging Information Security Threats
- Regulatory Concerns
- Breach Notification Challenges
- Programs and Assessments
- What to Do Now
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
Why Information Security?

Recent News

• Cybercrime will exceed **$2 Trillion** by 2019: Top Threat to Infrastructure, Productivity and Revenue in every industry

• Cybercrime-as-a-Service (CaaS) becomes more advanced

• Artificial intelligence (AI) and machine learning (ML) will become cybercrime weapons

• New US and international regulations alter the cybersecurity landscape

• More than half of organizations surveyed were struck by ransomware in 2017, and more than 75 percent of them were running up-to-date endpoint protection

• Hacking accounted for 50% of the breaches disclosed in one month;
Why Information Security

Internet Reports

• As of the latest reports, there are now over 4.0 Billion internet users

• Savvy attackers are using increased levels of deception and, in some cases, hijacking organizations’ own infrastructure (IoT) and turning it against them

• 60 percent of all targeted attacks in 2017 struck small to medium-sized organizations. More than 50% were Not-for-profit, public services, or healthcare organizations
Organic Risk Management

• Traditional Risk Management
  o A process controlled by few
  o Limited by knowledge base of key entities such as board of directors, management
  o Frequently applied in reactionary mode
  o Focused on past but not potential strategies
  o Basic tool to discuss risks but not always focused on your unique needs
  o May lead to a false sense of conclusion surrounding reasonable assurance regarding overall achievement of control alignment to actual risk
Organic Risk Management

- Organic Risk Management
  - A “human” approach to risk management process
  - Easily understood by all entities in the organization
  - Can be applied in any strategy setting and across the enterprise
  - Designed to identify existing and potential events that may affect the entity
  - Focused on keeping you alive
  - A method that provides processes that actionably address assurance for risk management
Organic Risk Management

• What keeps you Alive?
  ✓ Regulatory Compliance
  ✓ Cybersecurity
  ✓ Data Access
  ✓ Intellectual Property
  ✓ Physical
  ✓ Vendor Management
  ✓ Reputation
  ✓ Profit
  ✓ Community
  ✓ ????
Emerging Threats

Ransomware – Not Going Away

• Ransomware exploits **human and technical** weaknesses to gain access to an organization’s technical infrastructure in order to deny the organization access to its own data by encrypting that data.
Emerging Threats

Social Engineering – Still #1

• **Phishing** – the attempt to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money), often for malicious reasons, by masquerading as a trustworthy entity in an electronic communication.

• **Spear Phishing** – an e-mail spoofing fraud attempt that targets a *specific organization and persons in that organization*, seeking unauthorized access to confidential data. Spear phishing attempts are not typically initiated by "random hackers" but are more likely to be conducted by perpetrators out for financial gain, trade secrets, or marketable information.
Emerging Threats

Internet of Things (IoT) – DDoS Botnets

There is expected to be 75 billion connected devices by 2020.
Emerging Threats

Cybercrime as a Service (CaaS)

• Cybercrime-as-a-Service has opened a wide digital door to anyone looking to score a quick, illicit buck on the internet.
• Russian DDoS boomer 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.
• Disgruntled employees can hire a CaaS to perform attacks
Emerging Threats

Not new, but ever changing

- Virus
- Malware
- Physical
- Administrative
- Technical
- Users
- IP
- Vendors
- Others?
Laws and Regulations

Data Privacy and Security

- U.S. - EU Safe Harbor
- GDPR (EU General Data Protection Regulation)
- New York State Attorney General
- Personal Health Information Protection Act

- FISMA
- The Digital Millennium Copyright Act
- The FTC Seal
- PCI DSS Compliant
- Identity Theft

- GLBA Security Standards
- 23 NYCRR 500 Cybersecurity Requirements for Financial Services Companies
HIPAA Security Rule

Recent News

Some of the Largest HIPAA Settlements:

• Advocate Health (Downers Grove, IL): $5.55 million
• New York Presbyterian Hospital and Columbia University: $4.8 million
• Cignet Health (Prince George County, MD): $4.3 million
• Triple-S (San Juan, PR): $3.5 million
• University of Mississippi (Jackson, MS): $2.75 million

In 2017, over $18,000,000.00 in HIPAA fines for non-compliance with just the Security Rule Risk Management requirements
Other Cybersecurity Headlines

Recent News

• EmblemHealth: $575k settlement to NYS (in addition to HIPAA sanctions)
  • Printed individual’s SSNs on mailing labels

• Aetna: $1.15 million settlement to NYS
  • HIV prescription information was visible through plastic window on envelope
  • Affected 2,460 New Yorkers
Breach Notification

How many records have to be breached before you report it?

1
Breach Rule Changes

• **General Definition:** The acquisition, access, use, or disclosure of protected information in a manner not permitted under the Laws or Rules, which *compromises the security or privacy* of the protected information.

  ➢ *Note:* Regulations such as HIPAA: The harm standard was removed

• **Ransomware** is now considered a reportable breach under HIPAA
Breach Rule Changes

• **Exclusions** – Normally, these are **not** considered a breach:

  ✓ Unintentional acquisition, access, or use by workforce member or person acting under authority
  ✓ Inadvertent disclosure by person authorized to access
  ✓ Disclosure to unauthorized person who would not be able to retain such information
Breach Notification

• Disclosure probability – If none of the previous exclusions apply, the disclosure is considered a breach unless you can demonstrate:

“that there is a low probability that the protected health information has been compromised based on a risk assessment…”
Breach Notification

- **Exclusion via Risk Assessment** (demonstrating low probability)

  - The nature and extent of the protected information involved, including the types of identifiers and the likelihood of re-identification

  - The unauthorized person who used the protected health information or to whom the disclosure was made

  - Whether the protected health information was actually acquired or viewed

  - The extent to which the risk to the protected health information has been mitigated
Why Breach Protection?

Internet Reports:

• As of April 2018, there are now over 4.5 Billion internet users

• Savvy attackers are using increased levels of deception and, in some cases, hijacking organizations’ own infrastructure (IoT) and turning it against them

• 60 percent of all targeted attacks struck small- and medium-sized organizations

• Organizations are not universally adopting practices like blocking certain files and screensavers, email attachments, unsecure connections
It’s A Breach – Now What?
Breach Notification

- **Perform all items in your CSIRP** (required per many laws and regulations)

- **Notification to individuals**
  - Notify each individual whose unsecured protected health information has been, or is reasonably believed to have been, accessed, acquired, used, or disclosed as a result of a breach.

- **Notification to the media**
  - Required in several instances depending on the size of the breach

- **Notification to the Attorney General and others**
Breach Notification

Notification to Individuals – *Additional Requirements Normally Include*:

- **Timeliness** – 60 days after discovery

- **Content Elements** –
  - What happened and when
  - What was information was involved (DOB, SSN, etc.)
  - Steps that individuals should take
  - *Steps that you (the Covered Entity (CE) are taking"
  - Contact procedures

- **Plain Language** – All communications must be in plain language
Breach Notification

Other Considerations:

• Law Enforcement Delay
  ✓ Law enforcement may request a delay in notification

• Burden of Proof
  ✓ The covered entity shall have the burden of demonstrating that all notifications were made as required by this subpart or that the use or disclosure did not constitute a breach, as defined at

• Document Everything!
Breach Notification

Summary:

• Provide notice no later than 60 days from detection

• Have procedures to notify all required parties (individuals, media, Secretary)

• Document, Document, Document, Document...
Cybersecurity Assurance

Programs and Assessments

• Must be tailored to the organization
• Must be evidentiary based
• Must be based on standards

HITRUST

ISO 27001

COBIT

NIST

PAGE 30
Cybersecurity Programs and Assessments

• Know the difference between:
  ➢ Vulnerability Assessment
  ➢ Penetration Test
  ➢ Social Engineering Test
  ➢ Risk Assessment
  ➢ Cybersecurity Audit
As part of the work program, know what data you have and where your data is:

• Work
• Home
• Third Parties/BA’s
• Social Networking
• Email
• Portable devices
• Mobile apps
• Websites
Assess who has access to what whether it is needed data and to perform their duties

- Include audit tools and data exfiltration controls
- Assess local admin rights and temporary download folders
- Watch out carefully for “exception lists”
• Depending on data held, may require additional testing and auditing

• Assess contracts to confirm whether they contain protection and payment clauses above the standard boilerplate language in limitation of liability clauses

• Assess both yourself and your vendor for the appropriate cyber-liability coverage
Plug Known Holes

- Technical Vulnerability Testing
- Penetration Test
- Social Engineering Test
- May be required by some standards and is highly suggested to support most Risk Assessment standards
Know *who* has access to *what* data

- Assess all controls from all IoT devices
- Confirm/Perform Security Awareness Training
- Know what is encrypted
- Vendors and Third Parties
  - **Repeat!**
Train Your Users

- Must be performed at hire and annually
- Should be focused on the audience (e.g., one training for users, another for Board…)
- Must repeated anytime there is an incident
Questions?

Thank You!