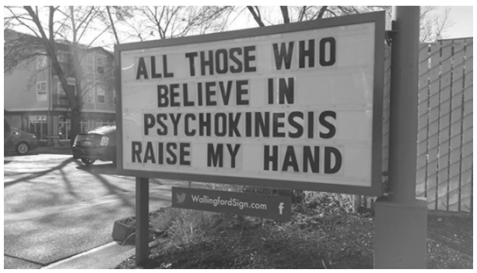
The Role of Compliance in Cybersecurity

Megan Moloney
Senior Strategy, Risk, and Compliance Manger
Federal Bureau of Investigation

Indian Hills Community Sign

I welcome audience participation



Wallingford Sign

COMPLIANCE:

Merriam Webster Definition

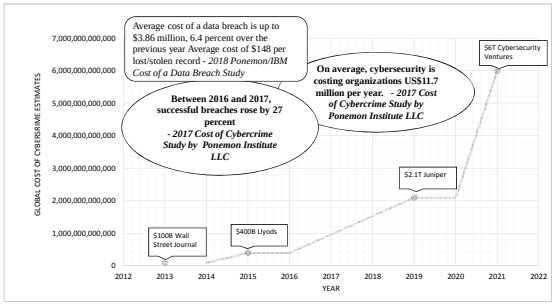
- "the act or process of complying to a desire, demand, proposal, or regimen or to coercion;
- "conformity in fulfilling official requirements;
- "a disposition to yield to others
- "the ability of an object to yield elastically when a force is applied."

CYBERSECURITY:

Merriam Webster Definition

measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack

Epidemic of Rising Cybercrime Costs



85%

Indian Hills Community Sign

So what does this have to do with *me*?

The cyber regulatory environment is maturing.
PCI DSS * HIPPA *Sarbanes-Oxley * GDPR
It's our responsibility to ensure compliance with those laws, regulations, and policies.

But even total regulatory compliance does not guarantee cybersecurity.

Compliance has a continuous role to play in preparing for, responding to, and recovering from cyber incidents.

Cybersecurity Road Map for Compliance Professionals

What questions should you be asking?

- Does the organization have an Enterprise Risk Management Strategy and does it address cyber risk?
- What is the Cybersecurity Governance Structure?
- Has the organization performed a Risk Assessment and/or Business Impact Analysis for cybersecurity risks?
- Does the organization have a Crisis Management Team for cyber events?
- Does the organization have a Crisis Response Plan for cyber events?
- What third party service provider policies and governing agreements (SLAs) are in place and are they appropriately managed and adhered to?

Indian Hills Community Sign

Enterprise Risk Management Strategy

- NIST Maturity Framework and model under NIST 800-53
- COSO *Enterprise Risk Management–Integrating with Strategy and Performance (updated 2017)* (greater emphasis on culture, business value of ERM, and role of IT)
- Cybersecurity-specific Frameworks:
  - ISO/IEC Security Control Standards (focuses on information security management systems)
  - Federal Financial Institutions Examination Council (FFICE) Cybersecurity Assessment (focuses on financial institutions)
  - SEC/OCIE Cybersecurity Initiative (focuses on Investment Firms)
  - FCC Cyber Security Planning Guide (focuses on Small Businesses)
  - NIST Cybersecurity Framework (focuses on Manufacturing)

Cybersecurity Governance Structure

- **Guidance**: ISO 27001: This is a key resource for Cybersecurity Governance processes; NIST SP 800-53 also provides a selection of controls.
- **Ways to measure meaningfulness of a Cybersecurity Governance Structure**:

- Robust Policy Framework
- Metrics (e.g. statistics on phishing email click rate, repeat offenders, intrusion attempts, training completion rates, etc.)
- Culture (transparency/ accountability)
- Budget
- Audit/Risk Committee Reporting Practices (frequency/audience)
- Internal Reporting Mechanisms (communication & escalation practices; bifurcated channels)
- Compliance Penalties/Incentives

Let's take a moment to talk about Reporting….

- How are you informed?
- Do you play any role in determining when and how to inform regulators, other government authorities, shareholders, and/or customers?

Let's take a moment to talk about Incentives….

- Sentencing Guidelines (2004 amendments)
- Opportunity to build cross-functional relationships
- Compliance can provide added value to management

- Tangible Assets
- Monetary
- On the Spot
- Publication

Take the Lead

Risk Assessments

- Four Key Aspects
  - Assets (physical assets/personnel/intellectual property/data)
  - Threats (insiders/cybercriminals/competitors/nation-states)
  - Vulnerabilities (lack of robust controls/poorly trained workforce)
  - Impact (safety/mission/business)

U.S. Navy photo by Mass Communication Specialist Seaman William P. Gatlin 2010; Wikimedia Commons

Business Impact Analysis

NIST SP 800-34 Rev. 1 provides a BIA Template, consisting of three steps:

1. Determine mission/business processes and recovery criticality (mission/business/safety)

2. Identify Resource Requirements

3. Identify Recovery Priorities for System Resources

Cyber Event Crisis Management Team

Commitment

Strategic direction

Designated Responsibility

The Crisis Management Team MUST consist of executive level professionals beyond IT

CEO; CIO; CISO; General Counsel; System Administrators/Application owners; Human Resources; Public Relations

HADLEY 1978/WIKIMEDIA COMMONS

Was someone missing from that list?

Yes. You.

Wallingford Sign

CRISIS RESPONSE PLAN

- General Steps
  1. Prevention
  2. Preparation
  3. Detection
  4. Analysis
  5. Containment
  6. Communication
  7. Eradication
  8. Recovery
  9. Post-Event Analysis

Proactive

Reactive

M. J. RICHARDSON 2007; WIKIMEDIA COMMONS

Prevention

Perhaps the step with which organizations are most familiar, but also most remiss….

- Patching
- Anti-virus
- IDS/IPS systems
- Data minimization
- Multifactor Authentication
- Encryption
- Access Control Management

Preparation

- Draft Incident Response Plan*
- Form Incident Response Team (lower level than Crisis Response Team; Must also be multi-disciplinary; Consider several for different incident types/impacted systems)
- Prepare cyber-specific Crisis Communication Plan (specific standards of procedures for communicating internally or externally, e.g. with stakeholders, governmental authorities, regulators, press, customers, etc.)*
- Create Robust Policy*
- Create Checklists
- Create Checklists
- Conduct Training (consider incentivized war games, not just tabletop exercises)*
- Testing Regimes
- Gather Threat Intelligence
- Jumpbags (Standalone Computer Essentials, Printer, Camera, Hardcopies of Checklists, Incident Response Plan, Crisis Communication Plan, etc.)
- Outsourced monitoring, auditing, penetration testing*

See, 2016 European Union Agency For Network And Information Security document "Strategies for Incident Response and Cyber Crisis Cooperation," for additional insights.

https://www.organizational-savvy-short-funny-stuff-com/funny-traffic-signs.html
Last accessed September 17, 2018

Detection

- Indicators: Logs reflecting unauthorized use of vulnerability scanners, vulnerability intelligence (public/government-issued), direct threats (Sony Entertainment), sluggish systems, unusually heavy network traffic, antivirus deactivation, bounced emails, erased logs, etc.
- Tools: Firewalls; Intrusion Detection Systems (IDSs); Intrusion Prevention Systems (IPSs); Antivirus and Anti-Spam Software; System Activity Logs; Application Activity Logs; Network Analyzers; File Integrity Check Products; System Information and Event Management Products (SIEM); and Vulnerability Scanners

Analysis

- Is it a legitimate threat (or a false positive)?
- What type of attack is it? What stage is it in?
- What impact would it have if successful?
- If it has succeeded, what systems, networks, data breached?
- What are the origins of the attack?

Attack DDoS, Jory Villa

Containment

- Isolate affected systems, hardware, etc. Shutdown not always advisable, because it may limit monitoring and attribution.

Frank Schwichtenberg

Wallingford Sign

Communication

Timely

Accurate

Honest

Rauantiques 2016, Wikimedia Commons

Note: There is no requirement for information to be ***complete.***

Do you have your privacy officer on speed dial?

You should.

Evolution of Reporting Requirements

State Laws: All 50 states have reporting laws

PCI DSS: Varies based upon merchant level

HIPAA: Covered entities must provide notification of the breach to affected individuals no later than 60 days after discovery of breach

Sarbanes Oxley: Auditing IT Infrastructure

GDPR: 72 hours after discovery of CIA breach

Wallingford Sign

Feared Consequences of Reporting….

- Reputational Damage
- Loss of Business
- Decreased Value
- Legal Liability

Wallingford Sign

Actual Consequences of Non- Reporting….

- Reputational Damage
- Loss of Business
- Decreased Value
- Legal Liability

Wallingford Sign

Recovery

*Rebuilding * Restoring * Reinstalling * Patching*

It's a marathon, not a sprint

The old adage, if it's not broke don't fix it, may help budgets and bottom lines, but also helps your adversary.

- Kevin Hiltpold, Optiv

Senior Airman Laura Turner

NIST Cyber Recovery Playbook Essentials:

- Documentation
- Communication
- Practice

Recovery presents a window of opportunity for Compliance.

http://www.pitchfordskies.com Photography by Linda Oyama Bryan. Stone and Stucco French Provincial with Hand Hewn Window Headers and Shutters on Lake Geneva.

Don't waste it.

Wallingford Sign

Third Party Risk Management

- According to Soha Systems, *Despite Record Breaches, Secure Third Party Access Still Not an IT Priority*, June14, 2016):
  - "Research has revealed that **third parties cause 63 percent** of all data breaches."
    - For example: Target/HVAC breach; Reported cost to Target was $148M (See, Rachel Abrams, ***Target Puts Data Breach Costs at $148 Million, and Forecasts Profit Drop,*** Aug. 5, 2014)
  - "Deloitte, in its Global Survey 2016 of third party risk, reported that **87 percent** of respondents had **faced a disruptive incident with third parties** in the last two to three years."
  - In May 2016, Ponemon Institute published "survey that revealed that **75 percent of IT and security professionals said the risk of a breach from a third party is serious and increasing**."
- **2018 Examples: BestBuy/Kmart/Delta/Sears; Saks Fifth Avenue/Lord & Taylor; Applebee's; Chili's; UnderArmour; My Heritage**
- **Potential Mitigations Include:**
  - Perform thorough Due Diligence (with emphasis on cyber hygiene)
  - Map your data and vendors (Determine which vendors are of highest impact; Update regularly)
  - Perform active oversight (Consider creating a Third-party Management Committee)
  - Ensure robust contractual provisions (Access; Audit; Incident Reporting; Liability; Termination)

Indian Hills Community Sign

PRIMARY TAKEAWAY:

Be engaged in your organization's cybersecurity

- Enhances your organization's resiliency posture
- Builds relational ties between compliance and other verticals
- Demonstrates value of Compliance to organization

QUESTIONS?

Wallingford Sign

Cybersecurity Resources

The following sites are an array of recognized sites/blogs that offer cybersecurity background and news

- https://krebsonsecurity.com
- https://www.privacyrights.org
- https://www.csoonline.com
- https://www.securityforum.org
- https://bankinfosecurity.com
- http://www.lawandsecurity.org
- https://darkwebnews.com
- https://thehackernews.com
- https://www.tripwire.com/state-of-security/
- https://www.schneier.com/
- https://nakedsecurity.sophos.com/
- https://www.darkreading.com/
- https://taosecurity.com/
- https://twitter.com/threatpost
- http://resources.infosecinstitute.com