MARSH & McLENNAN AGENCY | AIG

WORLD CLASS. LOCAL TOUCH.

# PRIVACY AND SECURITY PROTECTION AND BEST PRACTICES

OCTOBER 14, 2016

**Presented By:**

**Marsh & McLennan Agency**
Kevin McLaughlin, CPCU, MAS, Director, Professional Liability

**AIG**
Shiraz Saeed, Product Specialist-Cyber Risk
Phillip Kibler, Global Head of Cyber Risk Consulting

# New HHS Regulation on Cloud Computing and HIPAA Compliance

- HHS allows storage of information on a cloud based system.
- Data encrypting is extremely important.
- Encryption is important but does not allow availability of data during emergencies.
- Encryption along with administrative and physical safeguards.
- Must execute a Business Associate Agreement (BAA).
  - Must include a resolution agreement and corrective action plan for ePHI records of 3,000 or more.
  - The Cloud Provider must comply with all HIPAA regulations.
  - The Cloud Provider must return or destroy all PHI at the termination of the contract.

# Mobile Devices
## One of the Most Serious Potential Deficiencies in a Cloud Based System

- **From HealthIT.gov**
  - Use a password or other user ID.
  - Install and enable encryption.
  - Install and activate remote wiping and/or disabling.
  - Disable and do not install or use file sharing applications.
  - Install and enable a firewall.
  - Install and enable security software.
  - Keep your security software up to date.
  - Research mobile applications before downloading.
  - Maintain physical control – lock in a secure location, lock the screen when not in use, keep it with you at all times, don’t let others use it.
  - Use adequate security to send or receive health information over public Wi-Fi networks.
  - Delete all stored PHI before discarding or reusing the device.

# Should An Organization Allow The Use Of Mobile Devices?

- Decide whether the benefit outweighs the risk.
- Assess the threats and vulnerabilities to your health information.
- Identify your organization’s mobile device risk management strategy, including privacy and security safeguards.
- Develop, Document and Implement mobile device policies and procedures.
- Train providers and professionals on mobile device security awareness.

# Verizon Report
## 2016

- Breaches are now a Global Battle.
- A lot of Data Breaches are never reports – or even discovered.
- The insider threat is misunderstood.
- Cyber Espionage is rate but usually serious.
- Internet of things are still on the drawing board.
- Successful Data Breaches are rarely difficult.

# Experian Report
## 2016

- Vendors’ Switch to EMV Chips and PIN – Compatible payment terminals will not stop payment breaches.
- Breaches at large healthcare organizations will make headlines, but breaches of smaller organizations will cause the most damage.
- Cyber conflicts between countries will have a negative impact on consumers and businesses.
- US 2016 Presidential Campaign will be targets.
- “Hacktivism” by groups that target organizations will resurge.

# How Do We Identify Exposures?

### Do You Handle Confidential Information?

- Own company (including employees)
- Clients (confidential, personal, or commercial)
- PII, PHI, PFI,
- Corporate Confidential Information

### Where Do You Store The Information?

- Online v. Offline Information
- System Topography
- Do you operate the network yourself or outsource to a vendor?
- Security and Governance

### Do You Have A Website?

- What content is on the site?
- Can employees or third parties upload content (blog, post pictures or comments)?
- Content ownership

# 2016 Trends and Factors

Ransomware is the

#1

security issue clients are dealing with[1]

1.2M

Approximate number of new malware or variants on average each day[1]

209 days

the average time from initial infection until discovery of breach[5]

$4.3M

Average cost of a breach[3]

Cyber is the

#1, 2, or 3

risk businesses globally face[4]

Percent of businesses attacked that are small or medium in size:[2]

62%

## Healthcare is becoming one of the *most targeted industries*[1]

[1] Symantec (2016) *Internet Security Threat Report* retrieved from www.symantec.com/security-center
[2] Crowdstrike (2015) *Global Threat Report* retrieved from www.crowdstrike.com/global-threat-report-2015/
[3] IBM (2016) *Cost of a Data Breach Study* retrieved from www.ibm.com/securitydata-breach/
[4] AON (2015) *Global Risk Management Survey* retrieved from www.aon.com/2015GlobalRisk
[5] Verizon (2016) *Verizon Data Breach Incident Report* retrieved from www.verizonenterprise.com/resources/reports/rp_dbir_2016_report_en_xg.pdf

# Why Does This Keep Happening To My Organization?

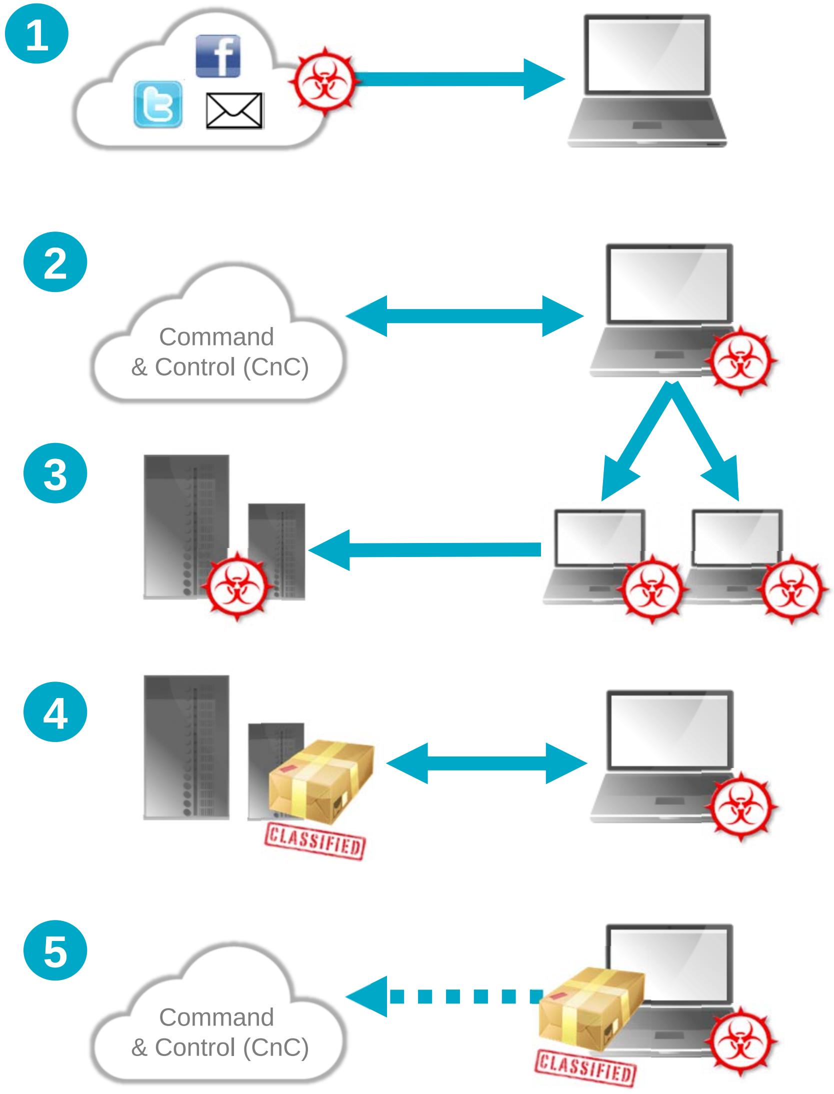
## Too Much Noise. Too Few Resources.

**End Users/Endpoints**

**Infrastructure**

**80-90% of all security incidents can be easily avoided!**

# Attackers Usually Follow this 5-State Attach Chain



**Break-in**

**Reconnaissance, spear phishing, and remote exploits to gain access**

**Latch-on**

**Malware and backdoors installed to establish a foothold**

**Expand**

**Lateral movement to increase access and maintain a presence**

**Gather**

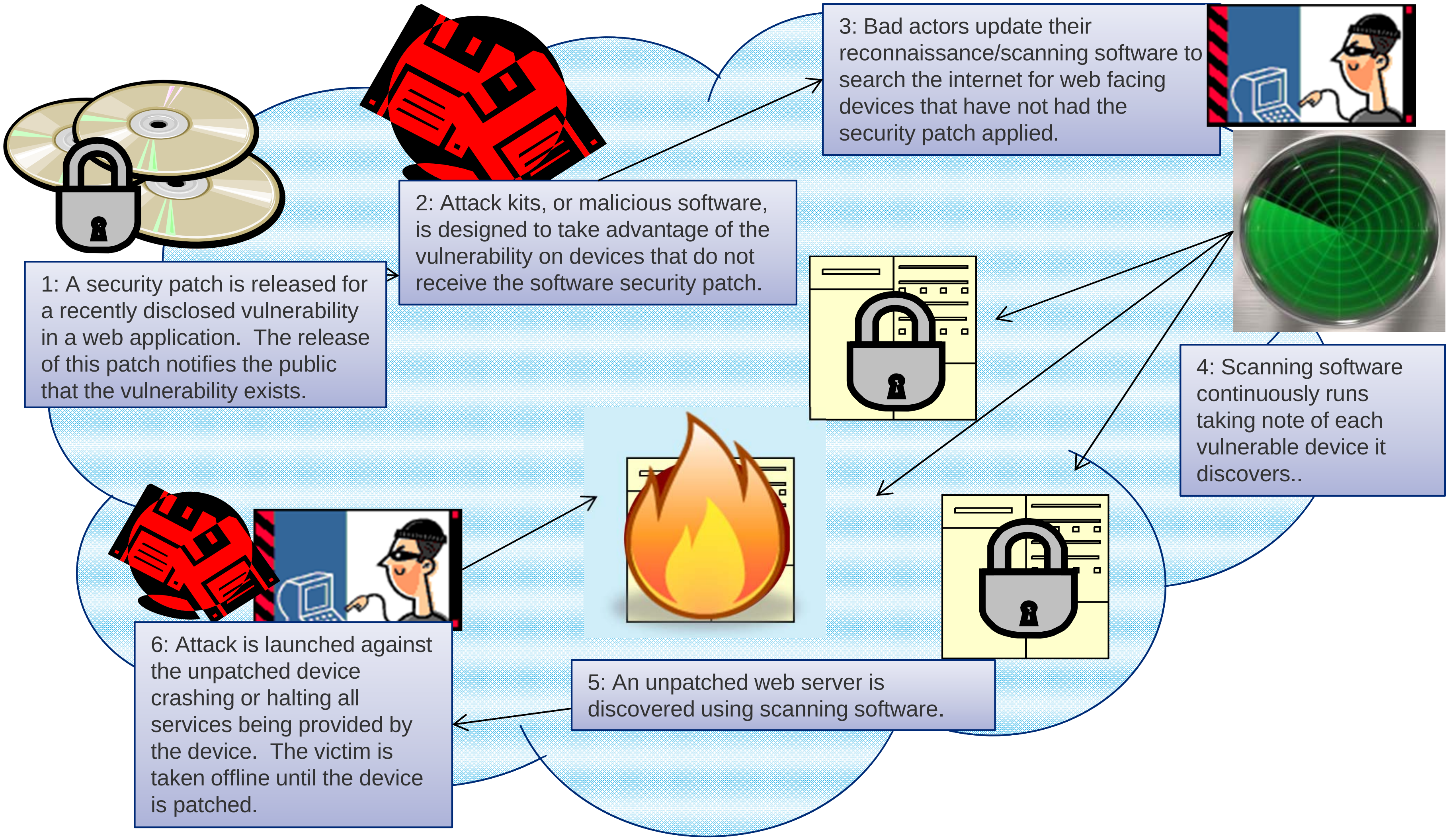
**Acquisition and aggregation of confidential data; setting up command-and-control**

**Exfiltrate**
(and **Execute**)

**Data exfiltration to external networks; and execute additional destructive attacks**

# Illustration of An Advanced Persistent Threat

The below illustration shows an example of the type of opportunistic attack that an incident response firm  has responded to, investigated, and provided findings on. To protect customer confidentiality, specific details have been revised and/or combined from different incidents.



1: A security patch is released for a recently disclosed vulnerability in a web application.  The release of this patch notifies the public that the vulnerability exists.

2: Attack kits, or malicious software, is designed to take advantage of the vulnerability on devices that do not receive the software security patch.

3: Bad actors update their reconnaissance/scanning software to search the internet for web facing devices that have not had the security patch applied.

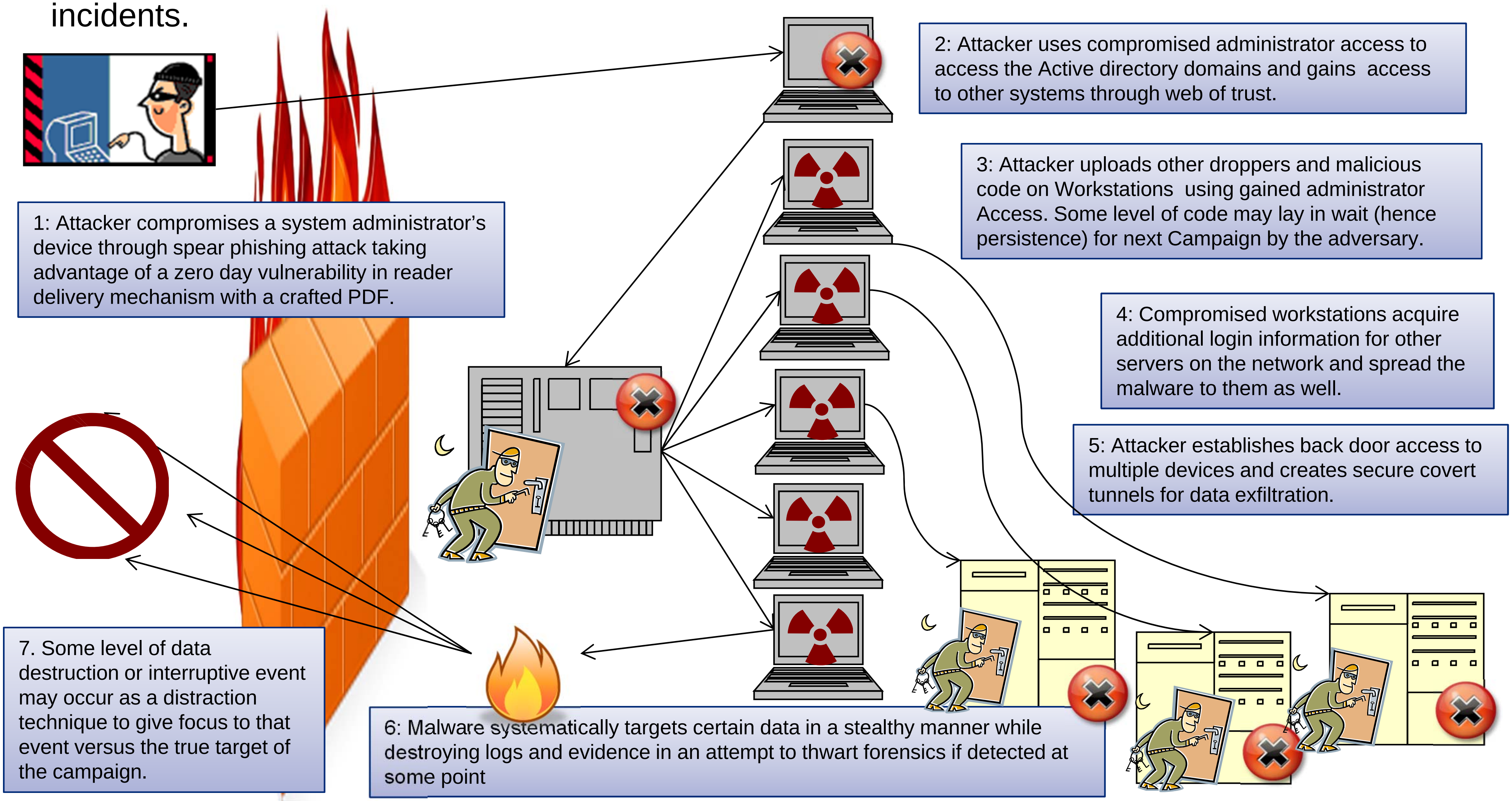
4: Scanning software continuously runs taking note of each vulnerable device it discovers..

5: An unpatched web server is discovered using scanning software.

6: Attack is launched against the unpatched device crashing or halting all services being provided by the device.  The victim is taken offline until the device is patched.

# Presentation Objectives

The below illustration shows an example of the type of sophisticated breach events that an incident response firm has responded to, investigated, and provided findings on.  To protect customer confidentiality, specific details have been revised and/or combined from different incidents.



1: Attacker compromises a system administrator's device through spear phishing attack taking advantage of a zero day vulnerability in reader delivery mechanism with a crafted PDF.

2: Attacker uses compromised administrator access to access the Active directory domains and gains  access to other systems through web of trust.

3: Attacker uploads other droppers and malicious code on Workstations  using gained administrator Access. Some level of code may lay in wait (hence persistence) for next Campaign by the adversary.

4: Compromised workstations acquire additional login information for other servers on the network and spread the malware to them as well.

5: Attacker establishes back door access to multiple devices and creates secure covert tunnels for data exfiltration.

6: Malware systematically targets certain data in a stealthy manner while destroying logs and evidence in an attempt to thwart forensics if detected at some point

7. Some level of data destruction or interruptive event may occur as a distraction technique to give focus to that event versus the true target of the campaign.

# Common Methods and Attack Surfaces

These common methods and attack surfaces are typically used during a cyber attack

## Social & Phishing

Target: **Individual Users**

Purpose:
- Pre-attack Intelligence Recon
- Build trust using fake social profiles
- Initial infection

## Malware, Zero-Day & Botnets

Target: **Endpoint Systems and Servers**

Purpose:
- Obtain access to systems
- Create backdoors
- Establish command-and-control over large network of devices

## Passwords & Configs

Target: **Endpoint Systems and Servers**

Purpose:
- Initial penetration
- Expansion of reach
- Escalation of privileges

## Distributed Denial-of-Service

Target: **Network & Application Infrastructure**

Purpose:
- Cause operational disruption
- Create diversion for other attacks

## Smart & Mobile Hacking

Target: **Mobile and Embedded Devices**

Purpose:
- New attack surface / entry point to enterprise network
- Gain access to user data through vulnerable mobile Operating System and apps

## Structured Query Language Injection

Target: **Database servers**

Purpose:
- Obtain account and user credentials
- Steal sensitive data

# Examples of Global Security Standards

**SANS 20 Controls**[6]

ISO 27002 Sections[7]

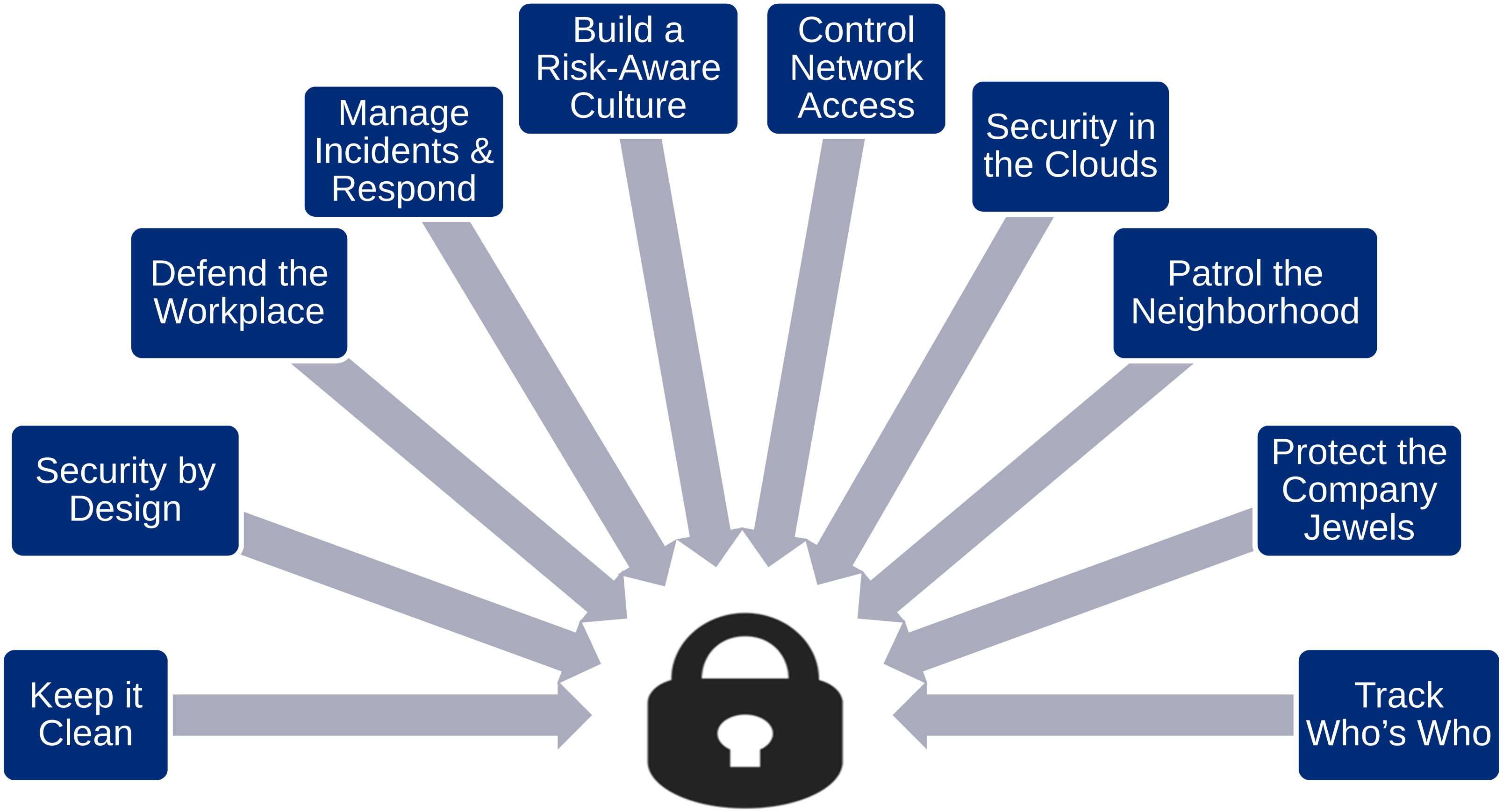
# National Institutes Standards and Technology

| Function Unique Identifier | Function | Category Unique Identifier | Category |
|---|---|---|---|
| ID | Identify | ID.AM | Asset Management |
| | | ID.BE | Business Environment |
| | | ID.GV | Governance |
| | | ID.RA | Risk Assessment |
| | | ID.RM | Risk Management Strategy |
| PR | Protect | PR.AC | Access Control |
| | | PR.AT | Awareness and Training |
| | | PR.DS | Data Security |
| | | PR.IP | Information Protection Processes and Procedures |
| | | PR.MA | Maintenance |
| | | PR.PT | Protective Technology |
| DE | Detect | DE.AE | Anomalies and Events |
| | | DE.CM | Security Continuous Monitoring |
| | | DE.DP | Detection Processes |

# National Institutes Standards and Technology (continued)

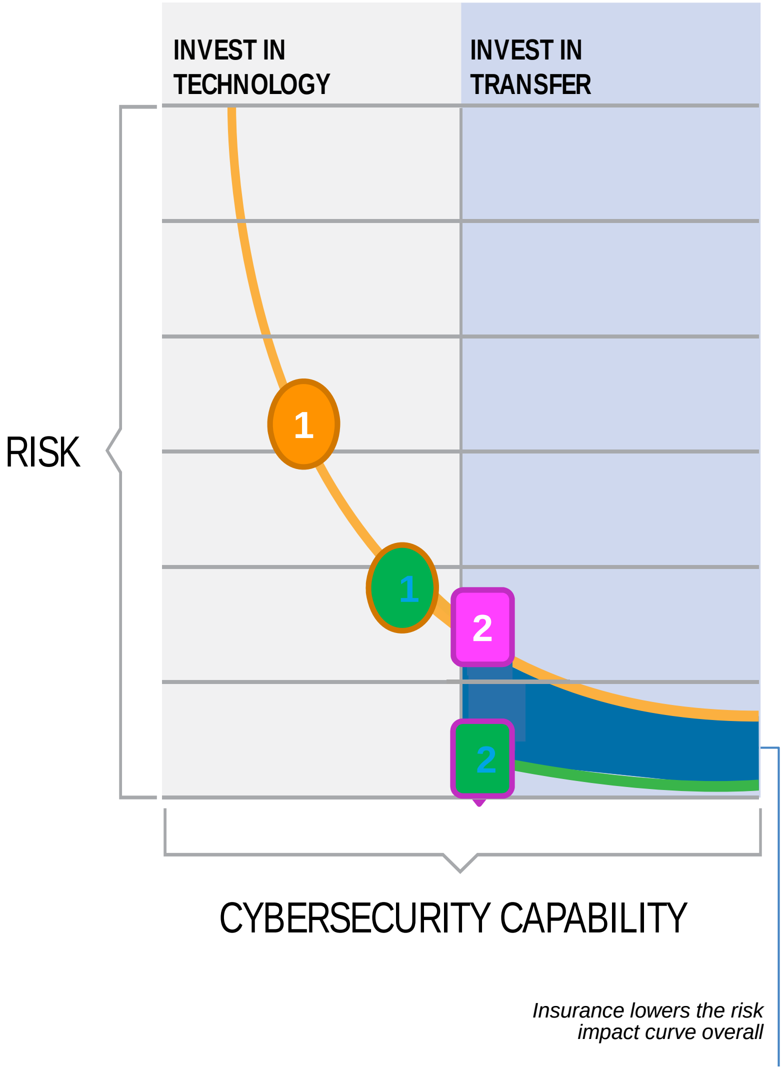
| Function Unique Identifier | Function | Category Unique Identifier | Category |
|---|---|---|---|
| RS | Respond | RS.RP | Response Planning |
| | | RS.CO | Communications |
| | | RS.AN | Analysis |
| | | RS.MI | Mitigation |
| | | RS.IM | Improvements |
| RC | Recover | RC.RP | Recovery Planning |
| | | RC.IM | Improvements |
| | | RC.CO | Communications |

# Ten Critical Security Areas
## Cybersecurity Defense In Depth



**Within each area, move from manual and reactive to automated and proactive to achieve optimized security**.

# Cyber Risk Reduction Curve
## Risk Transfer



*Insurance lowers the risk impact curve overall*

- Clients have different risk approaches for different scenarios
- For some, technology controls will present the greatest risk reduction.
- For others, insurance will present the greatest risk reduction.
- Investing in insurance reduces the impact for all.

# Protecting Against A Breach:  Basic Guidelines

## Basic Guidelines and Best Practices to Safeguard Data

- Total breach costs have grown every year since 2006, and in 2015, data breaches cost companies an average of $154-$158 per compromised record according to the 2015 Ponemon study.
- Data security expert Brian Lapidus, chief operating officer of the Fraud Solutions division of Kroll, suggests:
  - Look beyond IT security when assessing your company's data breach risks.  To eliminate threats throughout the organization, security must reach beyond the IT department. A company must evaluate employee exit strategies (HR), remote project protocol, on- and off-site data storage practices, and more – then establish and enforce new policies and procedures and physical safeguards appropriate to the findings.

*Tips to Prevent Data Breach from:  Kroll Fraud Solutions (http://krollfraudsolutions.com)*

# Protecting Against A Breach: Basic Guidelines

## Basic Guidelines and Best Practices to Safeguard Data (continued)

- Establish a comprehensive breach preparedness plan that will enable decisive action and prevent operational paralysis when a data breach occurs. Our efforts will demonstrate to consumers and regulators that your organization has taken anticipatory steps to address data security threats. Disseminate this plan throughout the management structure to ensure everyone knows what to do in the event of a breach. In preparation, consider the following:
  - Who will have a role in reviewing the policies on a predictable timetable?
  - What are the physical security elements? When and how will they be tested?
- Educate employees about appropriate handling and protection of sensitive data. The continuing saga of lost an stolen laptops containing critical information illustrates that corporate policy designed to safeguard portable data only works when employees follow the rules.

# Protecting Against A Breach:  Basic Guidelines

## Basic Guidelines and Best Practices to Safeguard Data (continued)

- Thieves can’t steal what you don’t have.  Data minimization is a powerful element of preparedness. The rules are disarmingly simple:
  - Don’t collect information that you don’t need.
  - Reduce the number of places where you retain the data.
  - Grant employees access to sensitive data on an “as needed” basis, and keep current records of who has access to the data while it is in your company’s possession.
  - Purge the data responsibly once the need for it has expired.
- Conduct a periodic risk assessment. Business models and operations change and might alter risk levels and liabilities.  Determining if you’ve acquired new areas or levels of risk can be accomplished through both internal audit and specialized external resources.

# Protecting Against A Breach: Basic Guidelines

## Basic Guidelines and Best Practices to Safeguard Data (continued)

- Provide training and technical support to mobile workers. Ensure that the same standards for data security are applied regardless of location, by providing mobile workers with the straightforward policies and procedures, ensuring security and authentication software is installed on mobile devices and kept up-to-date, and providing adequate training and technical support for mobile workers.

- Retain a third-party corporate breach and data security expert to analyze the level of risk and exposure. An evaluation performed by an objective, neutral party leads to a clear and credible picture of what's at stake, without pressuring staff who might otherwise worry that their budgets or careers are in jeopardy if a flaw is revealed.

- Don’t rely on encryption as your only method of defense. Encryption is a security best practice, but, when used alone, it can give businesses a false sense of security. Although the majority of state statutes require notification only if a breach compromises unencrypted personal information, professionals can and do break encryption codes.

# Protecting Against A Breach:  Basic Guidelines

## Basic Guidelines and Best Practices to Safeguard Data (continued)

- Keep current with security software updates (or patches). An unpatched system is, by definition, operating with a weak spot just waiting to be exploited by hackers. Admittedly, applying patches takes time and resources, so senior management must provide guidance on allocations and expectations.

- Hold vendors and partners to the same standards. It's important to define your security requirements upfront with vendors—third-party service providers may be required to maintain appropriate security measures in compliance with certain state and federal regulation. Ensure that your organization maintains control of data at all times, especially with offshore data storage or services.

# HIPAA
## Purpose

- Make healthcare delivery more efficient
- Enable more Americans to have health insurance – Title I
- Three main provisions:
  - the portability provisions
  - the tax provisions
  - the administrative simplification provisions

# Title I

- Regulates the availability of health insurance.
- Protects health coverage when workers lose or change jobs.
- Limits restrictions on pre-existing conditions.
- Long term care, vision and dental are exempt unless they are part of an overall health plan.
- Health Care Organizations (HCOs) needs to pass patient records back and forth, thus the evolution of EDI set of protocols.
- **The EDI Rule** – establishes code sets for electronic transmission of data
- **The Privacy Rule** – must "reasonably safeguard" patient data – intentional or unintentional disclosure.
- **The Security Rule** – protect against "any reasonably anticipated threats or hazards".

# Introduction of HITECH ACT

Change on 9/23/09 with the introduction of the Health Information Technology for Economic and Clinical Health Act (HITECH Act)

- Addresses security breaches of unsecured protected medical data
- Prohibits disclosure of protected information.
- Imposes penalties.
- **Requires Encryption** – data is unusable, unreadable or indecipherable to unauthorized individuals.
- Breach must be reported to the Secretary of Health and Human Services.
- If the breach affects 500 or more individuals – must notify the affected individuals and to the media.
- Less than 500 – annual report to the HHS Secretary.
- Allows the Office for Civil Rights to enforce the HIPAA Privacy Rule.

# Sample Situation
## Covered Entity:  Hospital

- **HIPAA**:  Privacy regulations that govern the healthcare industry.

- **HITECH Act**: Health Information Technology for Economic and Clinical Health Act.
  - Enacted on February 17, 2009.
  - Breach notification requirements for HIPAA covered entities + business associates.

| | |
|---|---|
| Access | Record |
| Maintain | Destroy |
| Retain | Hold |
| Modify | Use |

  - Beach notification applies to HIPAA to promote the adoption and meaningful use of health information technology.

- **Subtitle D of the HITECH Act addresses the privacy and security.**
  - Outlines the guidelines for who, what, where, when a privacy breach occurs.

# Guidelines

| If… | Then… |
|---|---|
| Breach occurs | Written notice, first class mail at last known address, as soon as practicable no later than 60 days after discovery of breach |
| Individual is deceased | Notify next of kin |
| Insufficient information for 10+ individuals | Home page of website of covered entity or major print or broadcast media |
| Urgent | Telephone |
| 500+ residents in a given state | 1. Prominent media outlet within the state<br>2. Notify the Secretary within 60 days<br>3. Secretary to post on an HHS Web site a list that identifies each covered entity involved |

# Notification Requirements
## Letters/E-Mail Typically Include:

- Description of what happened, date of the breach and the date of the discovery of the breach.
- Description of the types of unsecured PHI that were involved in the breach (i.e., full name, Social Security number, date of birth etc.).
- The steps individuals should take to protect themselves from potential harm resulting from the breach.
- Description of what the covered entity involved is doing to investigate the breach, to mitigate losses, and to protect against any further breaches.
- Contact procedures for individuals.

# Most Common Mistakes Employers Make When Dealing With HIPAA

- Failing to comply with the security rules.
  - Have you completed compliance efforts?
  - Updated Plan Documents or Business Associate Agreements.
- Disregarding FSAs or wellness programs:
  - Subject to HIPAA?
- Failing to train/retrain workers.
  - Has initial training taken place?
  - Has further training taken place?
- Ignoring State Privacy Laws.
  - Are you familiar with these laws?

# Most Common Mistakes Employers Make When Dealing With HIPAA (continued)

- Failing to update the notice of privacy practices and/or send the three year reminder.
  - Do changes in your health plan administration require an update?
  - Do you remind participants about the privacy notice and where to obtain it?
  - Does open enrollment notices count as an update?
- Failing to maintain a written procedure for investigating and resolving privacy complaints.
  - What are the appropriate corrective measures necessary to resolve HIPAA complaints?
  - Oral or written investigation?
  - Can you sanction an employee who violated these policies?

# Fines and Penalties:
## None if Corrected Within 30 Days

- Individual did not know (and by exercising reasonable diligence would not have known) that he/she violated HIPAA.
- HIPAA violation due to reasonable cause and not due to willful neglect.
- HIPAA violation due to willful neglect but violation is corrected within the required time period.
- HIPAA violation is due to willful neglect and is not corrected.

# Fines and Penalties:
## None if Corrected Within 30 Days (continued)

| HIPAA Violation | Minimum Penalty | Maximum Penalty |
|---|---|---|
| Individual did not know (and by exercising reasonable diligence would not have known) that he/she violated HIPAA | $100 per violation, with an annual maximum of $25,000 for repeat violations (Note: maximum that can be imposed by State Attorneys General regardless of the type of violation) | $50,000 per violations, with an annual maximum of $1.5 million |
| HIPAA violation due to reasonable cause and not due to willful neglect | $1,000 per violation, with an annual maximum of $100,000 for repeat violations | $50,000 per violation, with an annual maximum of $1.5 million |
| HIPAA violation due to willful neglect but violation is corrected within the required time period | $10,000 per violation, with an annual maximum of $250,000 for repeat violations | $50,000 per violation, with an annual maximum of $1.5 million |
| HIPAA violation is due to willful neglect and is not corrected | $50,000 per violation, with an annual maximum of $1.5 million | $50,000 per violation, with an annual maximum of $1.5 million |

# Email and HIPAA - The New Frontier…

## How Often is PHI Found in Outbound Email?

- One third of large organizations investigated a suspected violation of privacy or data protection regulations via email.
- In addition, more than a quarter of companies said that it is “common” or “very common” to find personal healthcare, financial or identity data that may violate privacy and data protection regulations in email leaving their organizations.
- Despite these risks, only 35.5% of responding companies said that they had deployed technology that can detect PHI in outbound mail.

# Audits

- Who can audit?
- What can you do?
- How to be proactive.
- Be Audit Ready all the time.

# What Else Can You Do?

- Obtain proper insurance.
- Use an encrypted system that follows the security measures outlined in the Federal Register.
- Complete a Security Analysis of your system.
- Replace manual systems with electronic devices/ software.
- Develop, communicate and continually refine HIPAA Best Practices to Staff.

# Privacy Protection Insurance is Typically Not Expensive and has Various Options

- Costs for legal liability from the breach.
- Defense costs.
- Regulatory action expense.
- Notification costs.
- Public relations costs.
- Identity theft (this is especially important when taking credit card information).
- Cyber extortion.
- Loss of ncome.

# Coverage Overview
## Social Media Exposures

| Coverage | Where Typically Found | Typical Exposure |
|---|---|---|
| **Security & Privacy Liability**<br>3rd Party Defense & Damages for Release of Corporate Private or Personal Private confidential information triggered by failure of computer security or wrongful release or disclosure of information by the insured, the insured's employee of another third party | Privacy Policy | Disclosure of information |
| **Privacy Regulatory Action**<br>Outside legal defense costs to defend a regulatory action/investigation | Privacy Policy<br>EPLI including Third Party | Invasion of privacy, bullying, rights violations |
| **Information Asset**<br>Reproduction of lost or corrupted data | Privacy Policy | Intentional destruction of information to hinder an investigation |
| **Business Interruption**<br>From failure of computer security or wrongful release or disclosure of information as noted above | Privacy Policy<br>Property | Disclosure of information |
| **Cyber Extortion**<br>Extortion to prevent lost, stolen, published or corrupted data | Privacy Policy<br>Crime | Cyber hacking from e-mail correspondence |

# Coverage Overview
## Social Media Exposures (continued)

| Coverage | Where Typically Found | Typical Exposure |
|---|---|---|
| **Crisis Management**<br>Covers the costs to retain public relations assistance n the event of a covered crisis. Coverage is also included for the cost to notify customers of a release of privacy information as well as costs to provide credit monitoring or other mediation services in the event of a covered incident. | Privacy Policy | Costs and assistance for public relations and any notification to the public |
| **Internet Media/Media Liability**<br>Liability for allegation such as defamation, copyright infringement or invasion of privacy arising from material published by the insured for either on-line or off-line materials or both | Privacy Policy<br>EPLI including Third Party GL<br>General Liability | Violation of intellectual property, defamation, personal publishing embarrassing photos or information company vs. non company activities |
| **Employment Practices Liability with Third Party Injury** | EPLI Policy with Third Party Liability<br>General Liability<br>Workers' Comp | Bullying, threats of violence, disparagement, harassment and discriminatory comments or pictures |

# AN EFFECTIVELY MONITORED AND ENFORCED ACCEPTABLE USE POLICY:

The Best Defense Against Potential Claim

Insurance Provides Peace Of Mind

# How Can You Protect Your Company From Social Media Risk?

- Develop acceptable use policy.
- Create a risk management program to maintain and enforce the policy.
  - Don’t have it.
  - Have it, don’t enforce it.
  - Enforce it selectively, never update it or remind employees about it.
- Have an effective response plan which will mitigate claims.
- Indicate and pre-negotiate rates with all who may be involved so that expenses can also be controlled, i.e., PR, IT, law firm.
- Obtain specialized insurance.

# Social Networking Can Be Addressed By A Combination Of Insurance Policies

- **Privacy & Network Security Coverage** – especially important as respects rogue employees.
- **Media Liability Insurance.**
- **Employment Practices Liability Insurance** – Including Third Party.
- **DIC Liability** to fill in gaps between policies.

MARSH & McLENNAN
AGENCY

**Advice and Accolades:**
Implementing continuous improvements and seeking preferred client feedback are critical parts of our commitment to providing exceptional service and results to our clients.  If there is a colleague you would like to recognize, or if there are areas you feel we can improve, kindly direct your comments to our CEO, Anthony C. Gruppo, at: AGruppoCEO@mma-ne.com.

This document and any recommendations, analysis, or advice provided by Marsh & McLennan Agency LLC (collectively, the “Marsh & McLennan Agency Analysis”) are intended solely for the entity identified as the recipient herein (“you”). This document contains proprietary, confidential information of Marsh & McLennan Agency and may not be shared with any third party, including other insurance producers, without Marsh & McLennan Agency’s prior written consent. Any statements concerning actuarial, tax, accounting, or legal matters are based solely on our experience as insurance agents or brokers and risk consultants and are not to be relied upon as actuarial, accounting, tax, or legal advice, for which you should consult your own professional advisors. Any modeling, analytics, or projections are subject to inherent uncertainty, and the Marsh & McLennan Agency Analysis could be materially affected if any underlying assumptions, conditions, information, or factors are inaccurate or incomplete or should change. The information contained herein is based on sources we believe reliable, but we make no representation or warranty as to its accuracy. Except as may be set forth in an agreement between you and Marsh & McLennan Agency, Marsh & McLennan Agency shall have no obligation to update the Marsh & McLennan Agency Analysis and shall have no liability to you or any other party with regard to the Marsh & McLennan Agency Analysis or to any services provided by a third party to you or Marsh & McLennan Agency. Marsh & McLennan Agency makes no representation or warranty concerning the application of policy wordings or the financial condition or solvency of insurers or reinsurers. Marsh & McLennan Agency makes no assurances regarding the availability, cost, or terms of insurance coverage.