



Incident Response Management

Controlled Escalation, Not a Fire Drill

Overview

- Disclaimer
- Let's conduct a Poll.
- Do we really need incident response management?
- The language of incident response - definitions
- Risk appropriate response
- Reporting and response framework
- Best practices/lessons learned

Disclaimer

Potential Unauthorized Exposure of PII and/or PHI

Business Disruptions

Not Our Topic

Scans/Probes and Attempted Access

Audit Log Analysis

Malicious Code

DoS Attacks

Help Desk Tickets

Natural Disasters

PS/IDS Alerts

Data Corruption

Disclaimer

- Although a security incident generally encompasses any compromise of an asset's Confidentiality, Integrity, or Availability, this talk considers the response process from the point in which there is a potential compromise to the Confidentiality of Personally Identifiable Information (PII) or Protected Health Information (PHI).
- The day-to-day handling of software-defined alerts and the common scans/attacks that are handled automatically by security information and event management (SIEM) products are Not considered in this talk until analysis reveals the potential compromise to the Confidentiality of PII/PHI.

Incident Definition – IDS/IPS?

The Global State of Information Security® Survey 2015










The total number of security incidents detected showed an **increase of 48%** over 2013.










Let's Take a Poll. Thumbs Ready?



Thumbs Up or Thumbs Down

1. Having a documented incident response process is optional for most organizations. 
2. An incident management process is a decision support aid, not a decision making tool. 
3. Establishing an Incident Response Team before an incident occurs will positively influence how incidents are handled. 
4. Most security experts say it's not a matter of if your organization's data will be breached, but when. 
5. There are two kinds of organizations, the ones that have been breached and know it, and the ones that don't know it. 
6. Speed of response is all that really matters when dealing with a data breach. 
7. Data breaches, isn't that why we have cyber insurance? 

Thumbs Up or Thumbs Down

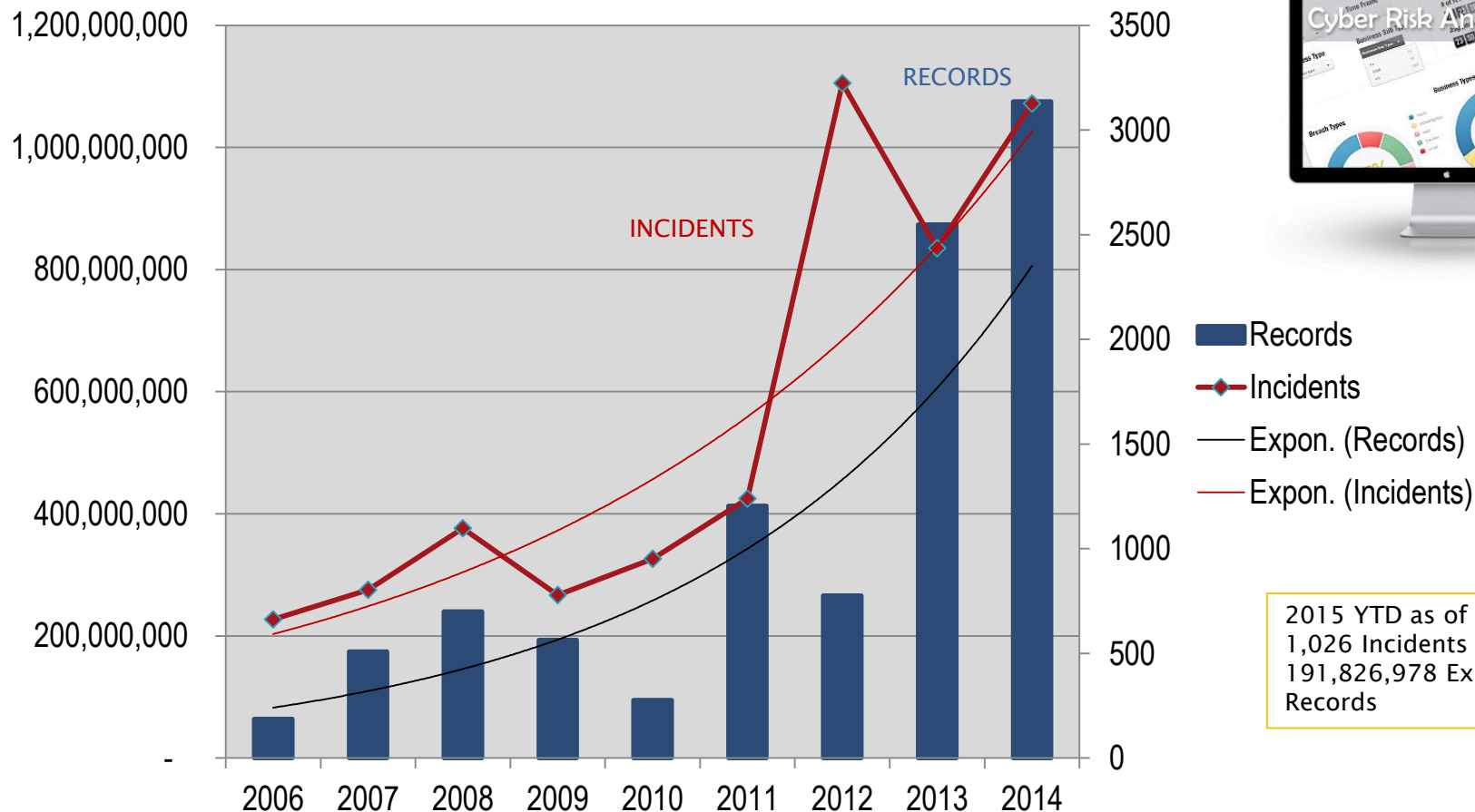
8. Prevention seems to be a losing battle, we may be better off focusing some money on detection, response, and recovery. 
9. Preparing for something that may never happen is a waste of money. 
10. Incident management can impact the level of risk to your business, brand, and reputation. 
11. The goal of incident response is to handle the situation in a way that limits damage and reduces recovery time and costs. 
12. Standard definitions of data breach terms have been applied across all industries. 
13. The nature and severity of unauthorized access to data should determine the response. 
14. An organization can be too quick to notify regarding a data breach. 



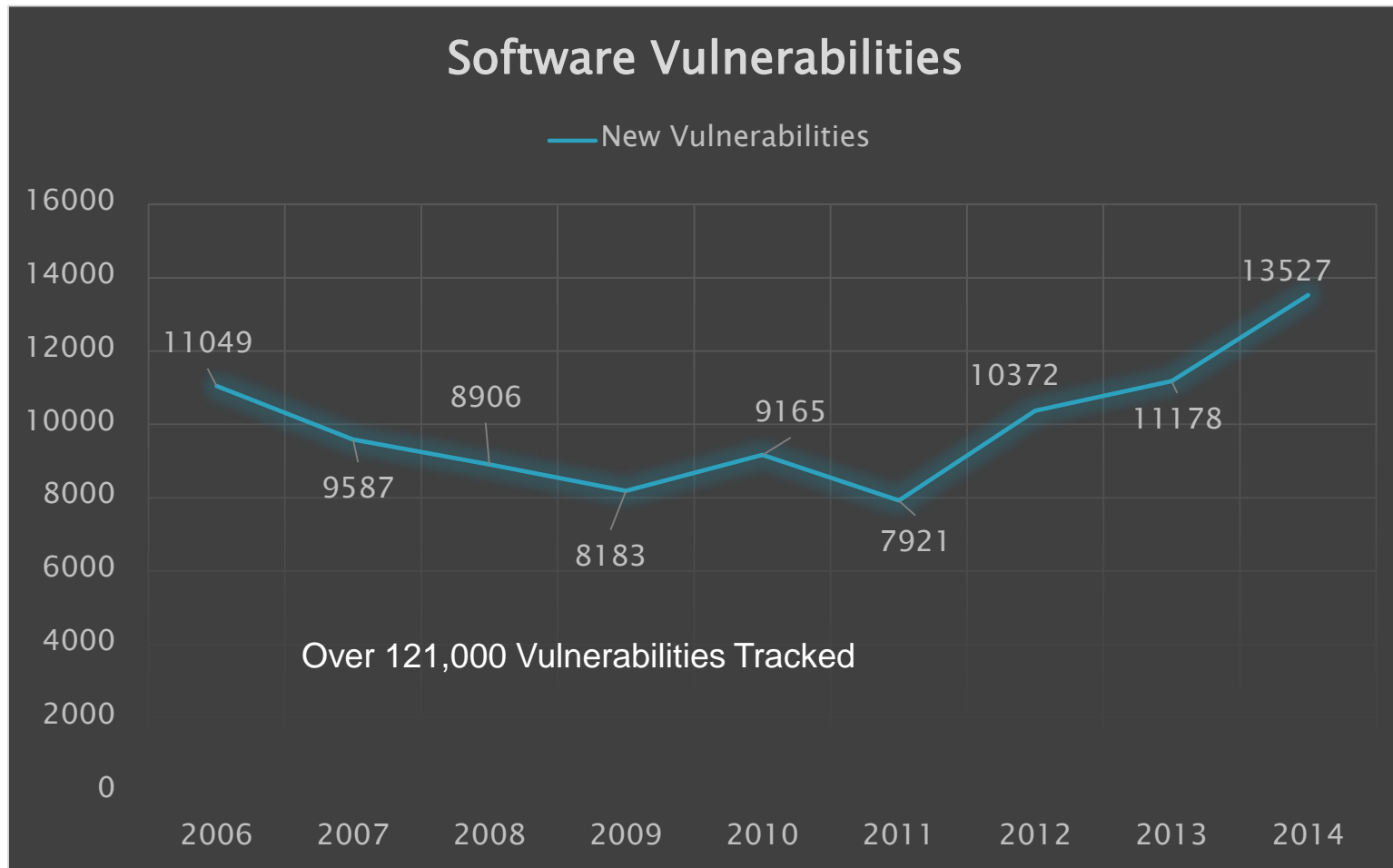
But, Do I Really Need to Be Concerned
With Incident Management?

Not just security, the right security.

Today's Reality – Data Breaches



Today's Reality – New Exploits



Regulations/Standards Demand It

- HIPAA
- HITECH
- GLBA
- FFIEC
- ISO 20000
- ISO 27002
- ISO 31000
- ISO 22301:2012
- NIST SP 800-61
- Federal Trade Commission (FTC)
- FISMA

HIPAA
HITECH
COMPLIANT



NIST
National Institute of
Standards and Technology



- The Personal Information Protection and Electronic Documents Act
- EU General Data Protection Regulation
- PCI DSS
- COBIT
- ITIL
- States' Data Breach Notification Laws
- 12 CFR 748 – Appendix B
- Office of Civil Rights



Regulator Activity

- Department of Health and Human Services' Office for Civil Rights (OCR) and the Federal Trade Commission (FTC) grew the scope of cyber regulatory investigations and penalties levied in 2014.
- OCR announced its largest fine ever in 2014, \$4.8 million, levied against a hospital for a HIPAA violation affecting 6,800 individuals.
- Many cyber regulators focus as much time on how an organization prepared for and responded to an event as they do on the circumstances that allowed the event to occur.
- Regulators are beginning to view cyber insurance as an indicator of an organization's cyber risk maturity and as reassurance that sufficient assets and expertise will be brought to bear should an incident occur.

March 30, 2015 | CFO.com | US

Regulator Activity

- The FTC announced its 50th data-breach settlement in 2014 - intends to actively investigate and penalize corporations for data breaches;
- California Department of Public Health announced a record 22 settlements in 2014, 2015 is on pace to set new record, (8) so far;
- The FTC announced a \$10 million fine in 2014 against two regional telecoms for not properly securing customer information; and
- The Federal Financial Institutions Examination Council launched a pilot audit program in 2014 to review the cyber security of more than 500 banks and credit unions. 12 CFR 748 – Appendix B

March 30, 2015 | CFO.com | US

Convinced Yet?





Some Common Definitions

Not just security, the right security.

Defining Incident Response

- The activities that address the short-term, direct effects of an incident and may also support short-term recovery. NIST SP 800-53
- Capability to effectively manage unexpected disruptive events with the objective of minimizing impacts and maintaining or restoring normal operations within defined time limits. ISACA
- The management and coordination of activities associated with an actual or potential occurrence of an event that may result in adverse consequences to information or information systems. NCSD Glossary

Definitions for Response Escalation



Some Definitions of “Event”

- An information security event is an identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant. **AN/NZS ISO/IEC 18044:2006**
- An event that results in the unauthorized disclosure, misuse, alteration or destruction of member information or member information systems. (**NCUA, Part 748, Appendix A**)
- Event - Any occurrence which is not part of the standard operation of a service and which may cause an interruption to, or a reduction in the quality of that service. (**ITIL**)

Some Definitions of “Event”

- Event – Occurrence or change of a particular set of circumstances.
 - Can be one or more occurrences, and can have several causes.
 - Can consist of something not happening.
 - Can sometimes be referred to as an “incident” or “accident”.
 - Events without consequence may be referred to as a “near Miss”, “incident”, “near hit”, or “close Call”. **(ISO 22301:2012)**

Some Definitions of “Vulnerability”

- The existence of a weakness, design, or implementation error that can lead to an unexpected, undesirable event compromising the security of the computer system, network, application, or protocol involved.
- A weakness which allows an attacker to reduce a system's information assurance.
- The intersection of three elements: a system susceptibility or flaw, attacker access to the flaw, and attacker capability to exploit the flaw.
- A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy.
- A flaw or weakness in hardware, software or process that exposes a system to compromise.

Some Definitions of “Incident”

- An incident is the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. (**HIPAA**)
- Incident – Situation that might be, or could lead to, a disruption, loss, emergency or crisis. (**ISO 22301:2012**)
- An information security incident is a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security. (**AN/NZS ISO/IEC 18044:2006**)
- An incident can be thought of as a violation or imminent threat of violation of information security policies, acceptable use policies, or standard security practices. (**NIST SP 800-61**)
- Incident - Any event which causes an interruption to, or a reduction in the quality of that service. (**ITIL**)

Some Definitions of “Breach”

- The unauthorized movement or disclosure of sensitive information to a party, usually outside the organization, that is not authorized to have or see the information. NIST SP 800-53
- A breach of security, is the unauthorized acquisition or unauthorized use of unencrypted data or, encrypted electronic data and the confidential process or key that is capable of compromising the security, confidentiality, or integrity of personal information, maintained by a person or agency that creates a substantial risk of identity theft or fraud against a resident of the commonwealth. (201 CMR 17)
- The term breach means the unlawful and unauthorized acquisition of computerized data that materially compromises the security, confidentiality, or integrity of personal information maintained by the person.
(Florida Stat. § 817.5681)

Management Friendly Definitions

Event - Occurrence that, has not yet been classified OR after analysis, is not considered a Vulnerability, Incident or Breach to information security.

Vulnerability - Event that, after analysis, did NOT result in an exposure to PII/PHI, but a weakness was discovered that could have compromised information security.

Incident - Vulnerability that, after analysis, HAS resulted in the reasonable probability of exposing PII/PHI, BUT the Risk-of-Harm to an individual has NOT occurred and is NOT considered reasonably likely.

Breach - Incident that, after analysis, HAS resulted in the reasonable probability that PII/PHI has been subject to unauthorized access AND the misuse of this information HAS occurred or the Risk-of-Harm to an individual(s) is reasonably likely.

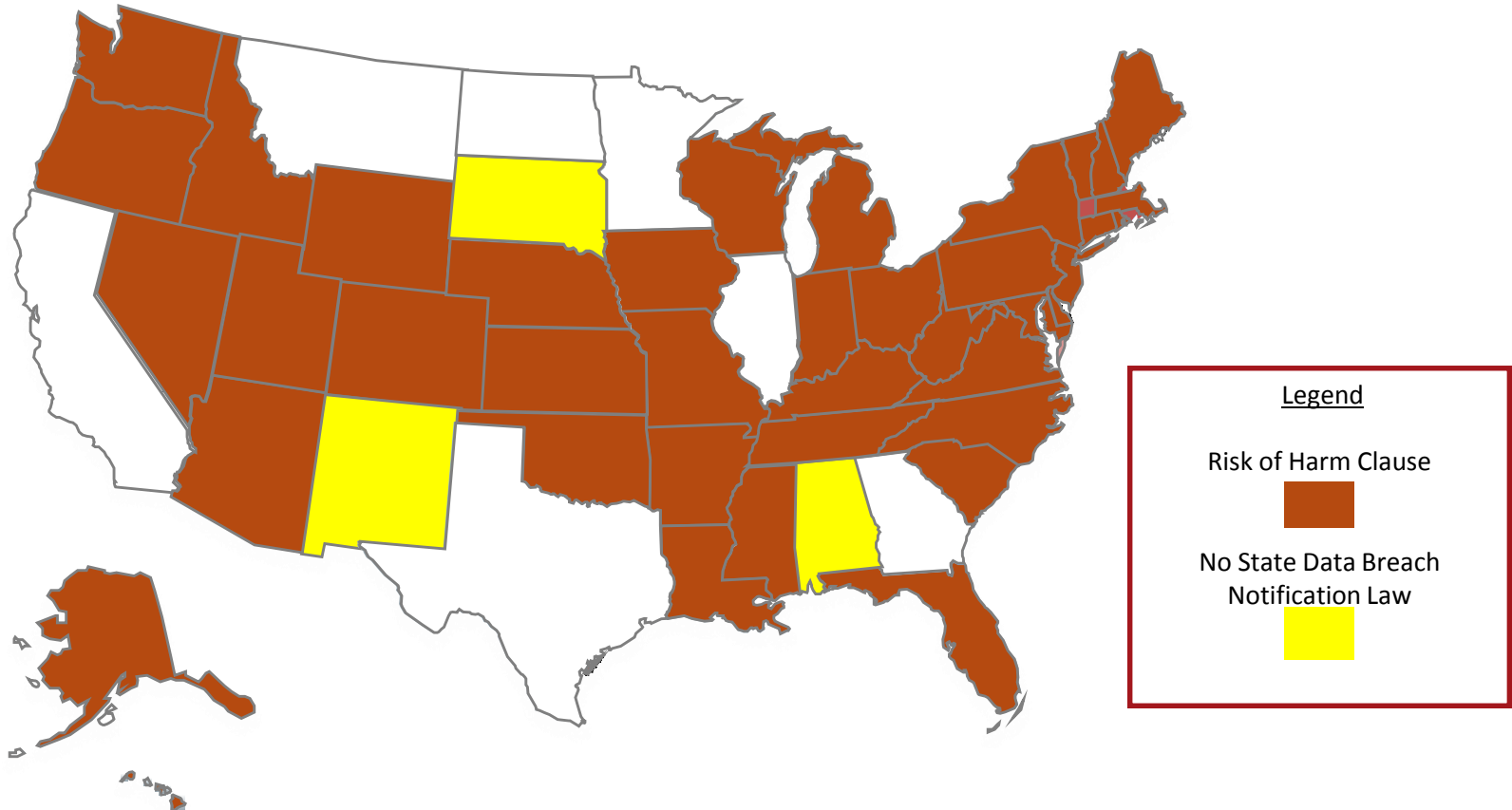
Do You Agree Risk-of-Harm Has a Role?



40 of 47 States Agree

- Notification required only if the individual or entity reasonably believes the breach has caused or will cause identity theft or other fraud to any resident of this State. (West Virginia)
- Notification is not required if the acquisition of personal information does not create a material risk of identity theft or fraud to the subject of the personal information. (Wisconsin)
- Notification required if the entity reasonably believes that such a breach has caused or will cause identity theft or other fraud to any resident of the Commonwealth. (Virginia)
- Notification under this section is not required if, after a reasonable investigation, the person or business determines that there is no reasonable likelihood of harm to customers. (Arkansas)
- Notification required if misuse of personal information for identity theft or fraud purposes has occurred, or is reasonably likely to occur. (Utah)

US States with a Risk of Harm Clause



US Department of Health and Human Services Agrees

- Considering the type of PHI involved in the impermissible use or disclosure will help entities determine the probability that the PHI could be used by an unauthorized recipient in a manner adverse to the individual or otherwise used to further the unauthorized recipient's own interests.

HIPAA Security Rule - 45 CFR Part 164

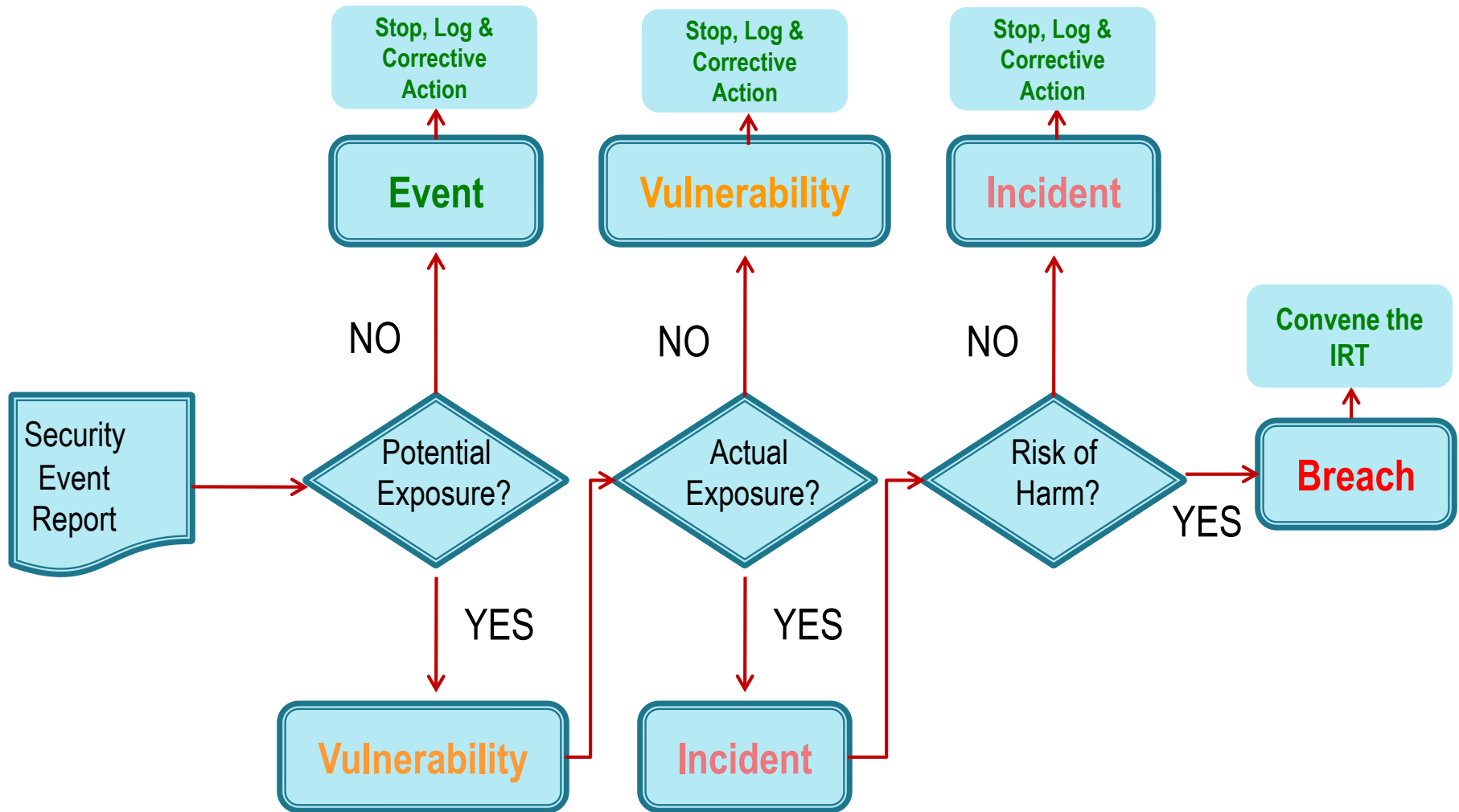
- HIPAA's objective risk assessment contains at least the following factors:
 - I. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
 - II. The unauthorized person who used the PHI or to whom the disclosure was made;
 - III. Whether the PHI was actually acquired or viewed; and
 - IV. The extent to which the risk to the PHI has been mitigated.



Risk-of-Harm

Not just security, the right security.

Risk-of-Harm Decision Tree



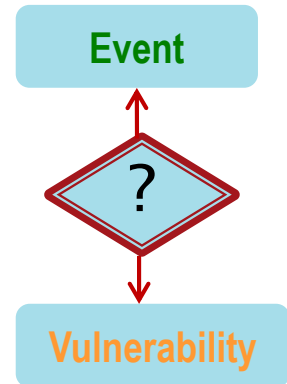
Security Event Report

Security Event Report

- All employees, contractors, owners of monitoring and alert services and third party users of information systems and services should be required to report any observed or suspected information security weaknesses or policy violations.
- Users should cease working with the compromised system, network or equipment or in the area of the suspected weakness or possible information security event.
- Information security events should be easy to submit and be responded to through appropriate management channels as quickly as possible.
- An active security event reporting process is always part of a mature information security program.

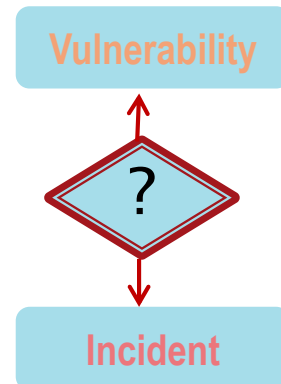
Potential Exposure? - Analyzing the Event

- Considerations:
 - Investigate the reported observations
 - Isolate the affected system to prevent further release
 - Review/activate auditing software
 - Preserve pertinent system logs
 - Make back-up copies of altered files to be kept secure
 - Identify systems that connect to the affected system
 - Conduct forensic investigation if needed
- Is there reason to believe Confidential information (PII/PHI) could have been exposed?
- If Yes, we have a **Vulnerability**, but maybe more.



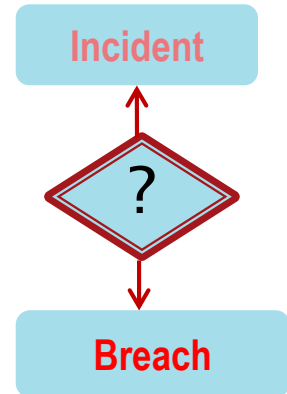
Actual Exposure? – Analyzing the Vulnerability

- Considerations:
 - Interview system/data users
 - Analyze affected system
 - Retain an external forensic expert to assist
 - Document conversations/activities/evidence
 - Analyze results of auditing software/log reviews
 - Analyze connected systems
- Is there reason to believe Confidential information (PII/PHI) HAS been exposed, BUT the Risk-of-Harm to an individual has NOT occurred and is NOT considered reasonably likely?
- If Yes, we have an **Incident**, but maybe more.



Risk-of-Harm? – Analyzing the Incident

- Considerations:
 - Deeper interviews with system/data users
 - Deeper analysis of affected and connected systems
 - Forensic experts if needed
 - Contact with external parties
 - Deeper review of auditing software/logs
 - Full documentation of conversations/activities/evidence
- Is there reason to believe Confidential information (PII/PHI) has been subject to unauthorized access AND the misuse of the information HAS occurred or the Risk-of-Harm to an individual is reasonably likely?
- If Yes, we have a **Breach**.









You Have a Breach - Now What?

- Assemble the Incident Response Team
 - CIO, CTO, CSO, CRO, CFO, CEO
 - Subject Matter Experts
 - Human Resources
 - Business Unit
 - Operations
 - Media Relations
 - Client Relations
 - In House Counsel
 - Out side Counsel
- Brief the IRT
 - Background and Description of the Event
 - Information Exposed - Analysis and Findings to date
 - Initial Assessment of Severity and Impact
 - Initial Risk-of-Harm Findings
 - Initial Notification Recommendations
 - Recommended Next Steps



In Summary - Escalation Steps

Escalation Level	Unknown	No Exposure	Potential to Expose	Exposure, but No Risk of Harm	Risk of Harm Exists	Harm has Occurred	Action(s)
Event							Log
Vulnerability							Log, Corrective Action
Incident							Log, Corrective Action, Communicate
Breach							Log, Corrective Action, Communicate, Notification

Right Out of the Headlines – Heartland Payment Systems

- Items are missing from Heartland's Santa Ana, California offices on May 8.
 - What do we have at this point? **EVENT**
- Among the items missing were TVs, LCD panels and 11 password protected desktop computers.
 - What do we have at this point? **VULNERABILITY**
- Heartland suspects that four computers contained personally identifiable information (PII), Social Security Numbers and / or banking information.
- Heartland statement: "We have seen no evidence suggesting that the data has been accessed on the stolen computers or used in any way, and we have no reason to believe any such use will occur." Anyone buying that?
 - What do we have at this point? **BREACH**
 - What would have made it an Incident?

Heartland Back Story

- In 2008 Heartland reported one of the world's first major data breaches that exposed 130 million U.S. credit and debit cards. (#7 All Time)
- Heartland sent a breach notification letter to 2,200 individuals saying their personal information may have been affected by the burglary and offering one year of credit monitoring from Kroll to those affected by the incident.
- The office that had the theft was a former Ovation Payroll location and was in the process of being fully integrated into Heartland's information and physical security systems and the data on the stolen systems was not encrypted, as they had not been fully merged with existing processes.

Heartland Payment Systems acquired Ovation Payroll January 18, 2013

Heartland Notification Letter

Heartland Payment Systems, Inc. was notified on May 8, 2015 that your personal information may have been compromised.

An incident occurred at our office in Santa Ana, California. Many items, including password protected computers belonging to Heartland were stolen.

One of these computers may have stored your Social Security number and/or bank account information processed for your employer.

We have seen no evidence suggesting that the data has been accessed on the stolen computers or used in any way, and we have no reason to believe any such use will occur.

We have involved state and federal regulatory and law enforcement agencies to assist us in determining how to proceed with the matter at hand.

Heartland continues to monitor the situation carefully and has increased its internal security and review procedures to watch for any unusual activity.

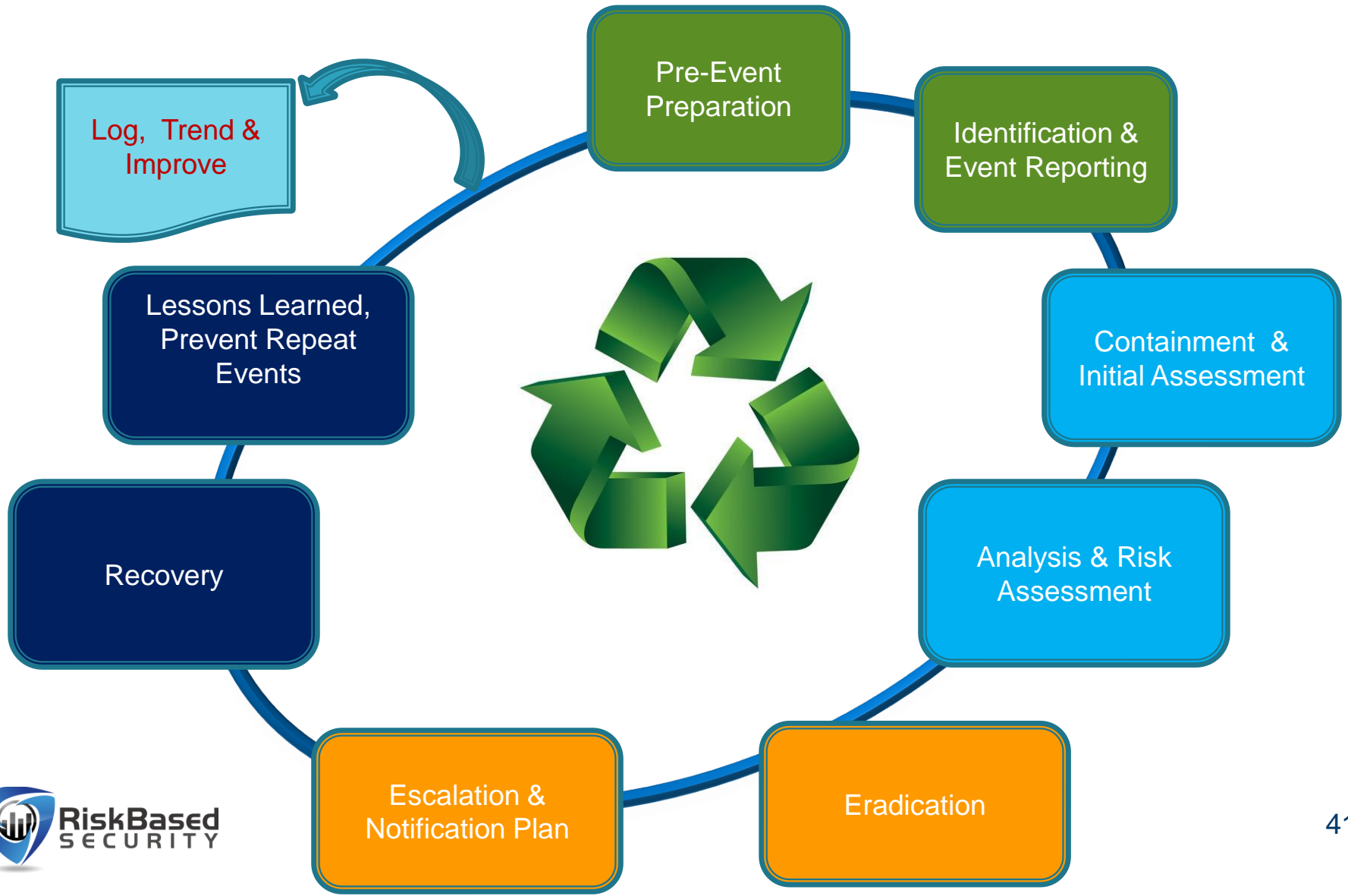
We are providing this notice to you out of an abundance of caution so that you can take steps to help protect your information from unauthorized use, such as the steps detailed in the enclosed state notification requirements.



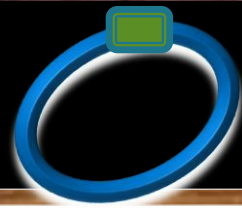
Event Response Cycle

Not just security, the right security.

Incident Event Response Cycle



Pre-Event Preparation

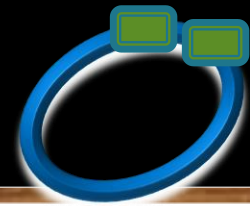


Pre-Event Preparation

‘Preparation, training and practice improve outcome’

- Publish a Security Incident Management Policy
- Name a Point Person (CISO)
- Establish an Incident Response Team
- Establish a Contact List (Internal and External)
- Define a Communication Plan (What, By Whom, To Whom, When & How)
- Train IRT Members in Roles and Responsibilities
- Conduct Incident Response Exercises
- Establish Senior Management Point of Contact

Event Reporting



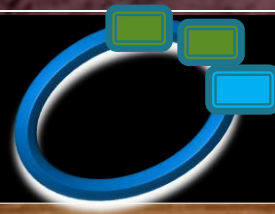
Event Reporting

‘Timely, accurate reporting of suspected events’

- Policy to Report Observations
- Employee Awareness Training
- Multiple Defined Reporting Channels
- Defined Security Point of Contact
- Centralized Coordination
- Standard Report Format



Containment & Initial Assessment



Containment & Initial Assessment

‘Immediate common sense steps to limit the event’

- Appoint a leader to launch the Risk-of-Harm Decision Tree.
- Determine the need to assemble the Incident Response Team.
- Assure internal notifications are made as appropriate per Plan.
- Safeguard evidence for future investigations and determining the root cause and appropriate corrective action.
- Maintain appropriate records including the steps taken to rectify the situation and the decisions made.



Analysis & Risk Assessment

‘Evaluate the Risk-of-Harm associated with the event’

- What, if any, confidential information is involved?
- What is the context of the information?
- Establish the cause and extent of the event.
 - Risk of ongoing breaches or further exposure?
 - Evidence of theft?
 - Information adequately encrypted, anonymous or otherwise not easily accessible?
 - Systemic problem or an isolated incident?
 - How many individuals affected?
- Assess the risk of harm that could result to individuals.
- Identify what other impact or risks could arise.

Eradication



Eradication

‘Eliminate or mitigate the cause’

- Stop or kill all active attack processes;
- Save a copy then delete all the fake files created by the attacker;
- Eliminate all the backdoors and malicious programs;
- Inoculate any virus from all infected systems and media;
- Apply patches and fixes to vulnerabilities found on all systems/devices;
- Correct any mis-configuration in firewalls and routers;
- Assure backups are clean to prevent re-infection;
- Use security scanning tools to detect any vulnerabilities;
- Update login accounts and passwords that may have been exposed; and
- If needed, reformat all the infected media and reinstall from backup.

Escalation & Notification Plan



Escalation & Notification Plan

‘The challenge is to determine if, what and when notification is appropriate’

- Each event needs to be considered on a case-by-case basis
- What is the risk of serious harm to the individual?
- Take into account the ability of the individual to take specific steps to mitigate any harm.
- Consider the legal and contractual obligations to inform other third parties about the event, such as regulators, police or other bodies.
- What are the consequences of failing to notify affected individuals?
- A direct method of notification is preferred - by phone, letter, email or in person.
- Use standard notification letter content.

Notification Letter

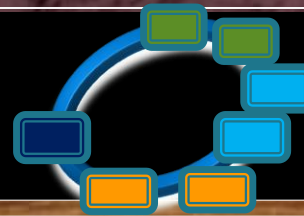


Notification Letter

‘Notification should be limited to those members whose information has been or is potentially subject to misuse.’ - Appendix B to Part 12 CFR 748

- a. Clearly describe the breach in general terms along with actions taken to contain further unauthorized access;
- b. The notice should include:
 - a. Recommendation to review financial statements and report suspicious activity;
 - b. Explanation of a fraud alert and how to place it in the individual's consumer report;
 - c. Recommendation to periodically obtain credit reports;
 - d. Explanation of how the individual may obtain a free credit report; and
 - e. Information about the FTC's online guidance regarding how to protect against identity theft.

Recovery

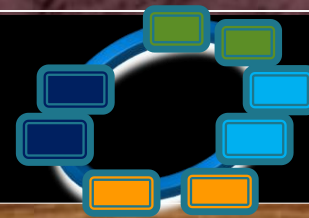


Recovery

‘The goal is to restore the system to its normal operation’

- Perform damage assessment;
- Re-install the deleted/damaged files from the trusted source;
- Restore functions/services in a controlled manner and in order of demand;
- Verify a successful restore and the system is back to normal operation;
- Provide prior notification to all interested related parties on resumption of system operation; and
- Keep records of all actions performed.

Prevent Future Events

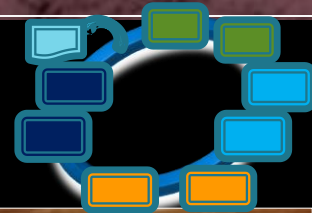


Prevent Future Events

‘Define the corrective and preventive actions which are proportionate to the significance of the event’

- Determine root cause – not just the symptoms.
- Correct the specific findings; implement actions to prevent recurrence.
- Conduct follow-up at the end of the process to ensure the prevention plan has been fully implemented.
- Review policies, procedures, employee selection and training. practices and service delivery partners for changes to reflect the lessons learned from the investigation.
- Improve your breach response plan to assist in a quick response and greater potential for mitigating harm.

Improvement Actions



Log,
Trend &
Improve

‘Decrease the number of events and reduce the impact of the events that do occur’

- Maintain log of all reported events.
- Perform analysis of types, causes and findings.
- Summarize report to senior management.
- Improve appropriate breach response plans.
- Conduct breach response exercises/test simulations.



Lessons Learned

Not just security, the right security.

Lessons Learned

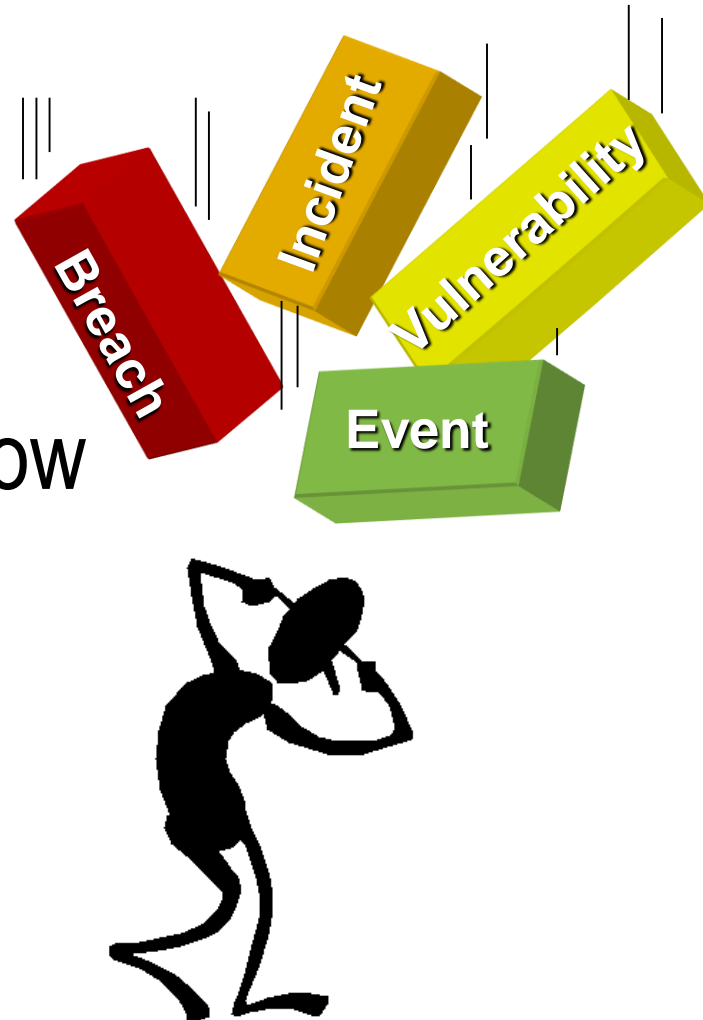
- Know Your Data Breach Notification Requirements (State Laws/Regulations)
- Publish Incident Response Policy/Procedure
 - Establish Common Terms & Definitions
 - Responsibility to report suspected security events
 - Risk-of-Harm Decision Tree
 - Central Coordination
 - List of Contacts with Authorities
 - Communication Plan (What, When, How, By Whom, To Whom)

Lessons Learned

- Define a Media Relations plan and assign a designated spokesperson;
- Conduct Employee/Management Awareness Training
- Pre-arrange Relationship with Forensics Experts, Breach Notification Company and Law Firm;
- Consider Buying Cyber Liability Insurance
- Conduct Data Breach Simulation Exercises

Most Important Lesson ...

Expect a data breach.
Document and practice how
you will respond.





Thank you for your attention

Barry L. Kouns
Risk Based Security, Inc.
Email: barry@riskbasedsecurity.com