Incident Reporting and Response

"It's not a matter of if…"

Tom Walsh, CISSP

tw-Security

Overland Park, KS

tw Security
Healthcare Information Security

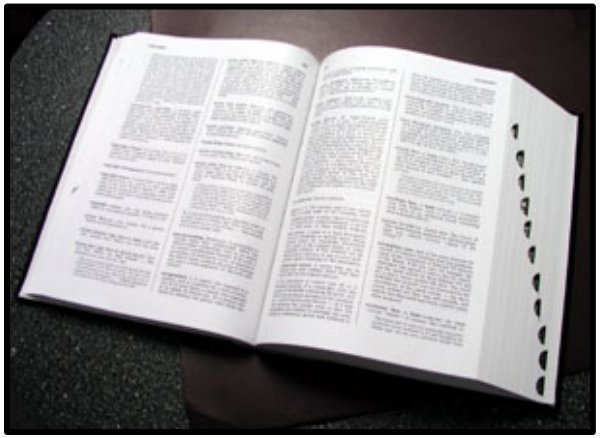
Objectives

- Explain the benefits of an incident response handling capability
- Provide an overview of incident response and incident response teams (soft skills)
- Explain the value in having an incident flow diagram
- Describe why conducting a tabletop exercise is a necessity
- Provide an opportunity to ask questions

Introduction – Tom Walsh

- **Certified Information Systems Security Professional (CISSP)**
- **14 years – tw-Security** (formerly: Tom Walsh Consulting, LLC)
- **Co-authored four books on healthcare security**
  - Published by AMA, AHIMA, and HIMSS (two books)
- **Former information security manager for large healthcare system in Kansas City metro area**
- **Started working in information security in 1992**
- **A little nerdy, but overall, a nice guy ☺**

Terminology



Terminology

- **Security Incident – Security incident means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.**

  Source: HIPAA Security Rule, § 164.304 Definitions

- **Information Security Incident – An adverse event whereby some aspect of computer security could be threatened: loss of data confidentiality, disruption of data or system integrity, or disruption or denial of availability.**

  Source: NIST Special Pub 800-61 *Computer Security Incident Handling Guide*

Information Security Incidents

Examples of security incidents include:

- Phishing and ransomware
- Theft or loss of devices or media
- Unencrypted email with PHI from an outside entity (either in the email or as an attachment)
- Unauthorized use of user passwords
- Policy violations
- Unplanned downtimes

Terminology

- **Breach – An "unauthorized acquisition, access, use or disclosure of PHI which compromises the security or privacy of the PHI, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information."**

  Source: *The Health Information Technology for Economic and Clinical Health (HITECH) Act*

- **Breach – An unauthorized act that circumvents or bypasses network (perimeter) security controls**

  Source: Experience in working with IT staff

Incident Response – Compliance

- **Health Insurance Portability and Accountability Act (HIPAA) of 1996; HIPAA Security Rule [§ 164.308(a)(6)(i) and § 164.308(a)(6)(ii)]**
- **Payment Card Industry (PCI) Data Security Standard [12.5.3]**
- ***Breach Notification for Unsecured Protected Health Information* (45 CFR Parts 160 and 164)**

Benefits of Incident Response

Incident and Breach Response

An effective incident response program will benefit your organization by:

- Reducing recovery time
- Protect the organization's reputation
- Improving your legal defensibility
- Providing a framework for continuous improvement
- Reducing costs

100% security does not exist. Organizations that are prepared with a measured and practiced incident response procedure have the best possible means to remediate and recover.

Incident and Breach Response

How important is incident and breach response?

(Jan 2017) The OCR fined Presence Health, a large health care network in Illinois, $475,000 and issued a corrective action plan (CAP) for being too slow in reporting a breach!

It's not the event, but your reaction to the event that matters the most!

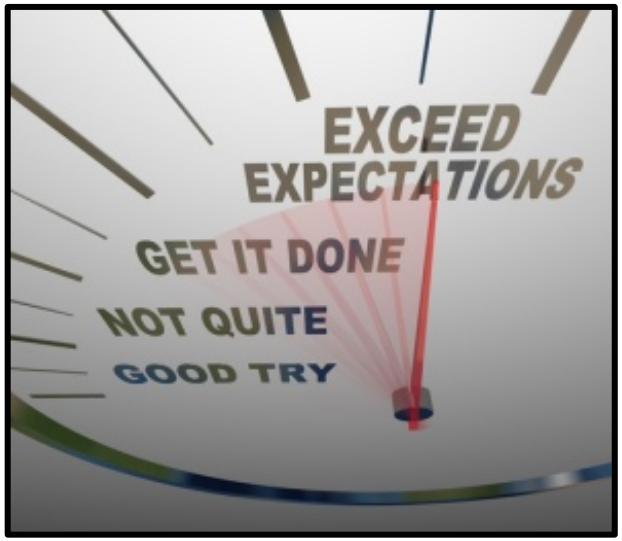
Audience Participation

What is the deadline for reporting a breach?

Incident Response Phases

Incident response is a skill developed over time

Practice makes perfect



Incident Response Phases

1. Detection

2. Analysis

3. Containment

4. Eradication

5. Recovery

6. Post Incident Activities

Incident Response

- **Incidents are a "when" not "if" occurrence**

  Does your staff know what to do?

  – Conduct a data breach tabletop exercise or drill
- **Incident response tools**
  – Incident response flow diagrams are helpful
  – Playbooks should be created and used to outline detailed procedures to follow
- **Gartner findings:**
  – Technical competence does not imply incident response competence

Categorizing Incidents

Two criteria used for categorizing incidents:

1. Type *(some examples were previously provided*)
2. Severity or potential impact to the organization
   - The classification of severity is important to assure that the appropriate resources are used during the response process
   - Incidents should be handled at the lowest escalation level capable of responding to the incident to reduce resource requirements and maintain control.

Tip of the Iceberg

- **Some incidents are like an iceberg**
  - **There may be more to it than you initially think**
  - **Only after a thorough investigation is conducted can the full depth and impact be understood**

Therefore, the severity of an incident may change as the investigation progresses

Challenges with IT Staff

- It staff like to “fix things” and get things back to normal as quickly as possible
- Unfortunately, IT staff may delete valuable forensic evidence needed to make a determination if a breach of PHI has occurred

Ransomware:
Breach or no Breach of PHI?

Breach or No Breach?

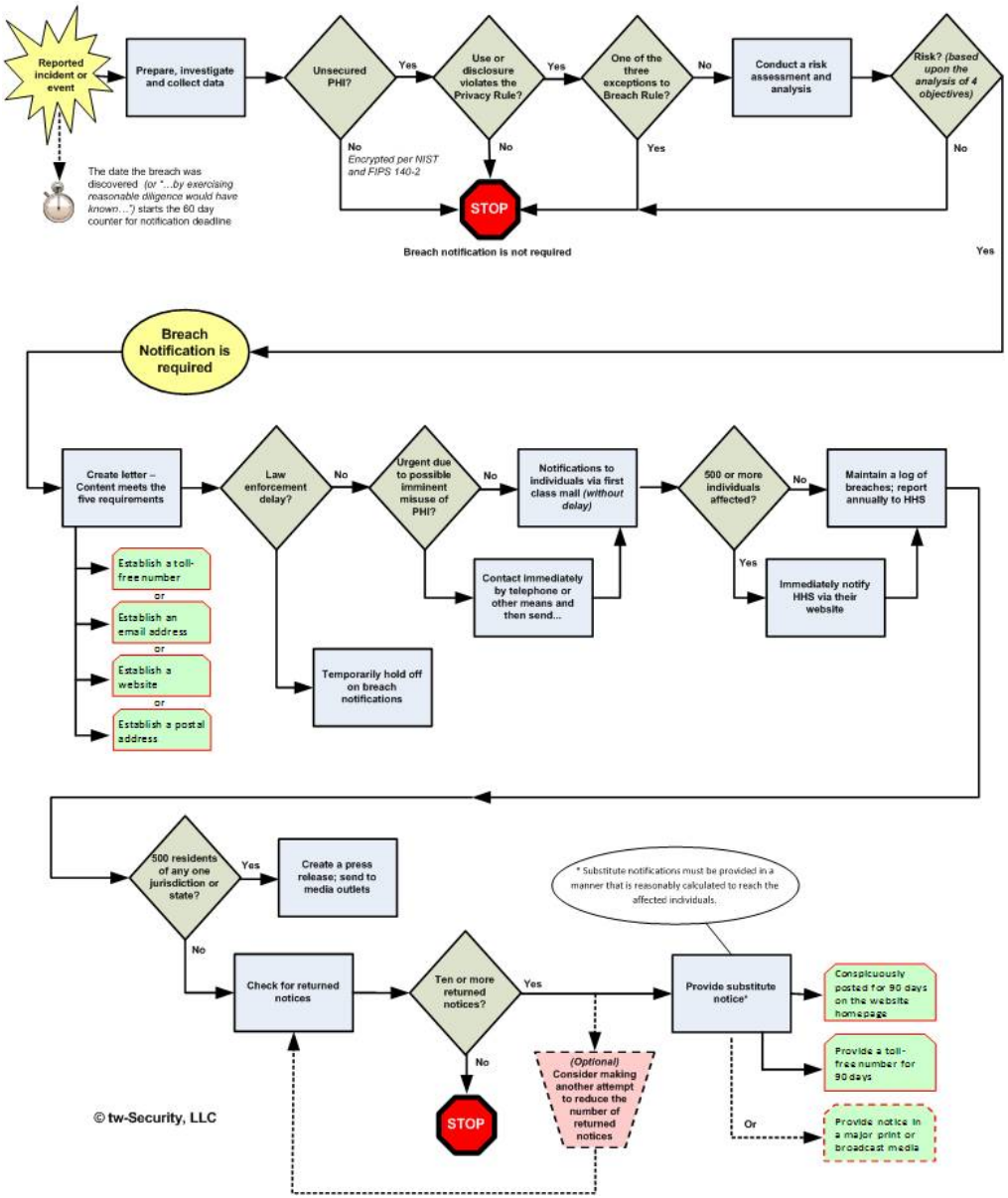
“It depends…”

- Was protected health information (PHI) involved?
- If ransomware was able to encrypt your data, could it have read and copied your data as well?
- Only after a risk analysis has been performed can it be determined if a data breach occurred
- Forensic data is needed to prove that no data from the infected device(s) left the organization
- Was the PHI encrypted prior to the incident?
  - If no, presume that PHI has been compromised and notification is necessary unless risk assessment concludes that there is a low probability of compromise

Breach Rule – Four Factors

1. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
2. The unauthorized person who used the PHI or to whom the disclosure was made;
3. Whether the PHI was actually acquired or viewed; and
4. The extent to which the risk to the PHI has been mitigated.

Breach Notification Process



Incident Response and the Incident Response Team (IRT)

Soft skills

IRT Membership (core)

The Incident Response Team (IRT) is typically:

- **Information Security Officer**
- **IT subject matter experts**
- **Director of IT Services or CIO**

Other IRT Members

Occasionally, the response team may include:

- **Privacy Officer**
- **Risk Management /Legal (internal)**
- **Human Resources**
- **COO and/or other members of Administration**

Outside resources may include:

- **Specialized legal counsel**
- **Computer forensic services**
- **Law enforcement**

Specifics of IRT Meetings

- Conducting discussions
  - Establishing team meeting location
    - "War Room" with in-person participants
    - Remote participants
  - Communication methods
    - Phone calls
    - Conference lines
    - Email
    - Instant Messaging

Sometimes, out of band communications are necessary

  - Agenda is driven by type of incident and playbook

Incident Response Documentation

- Written procedures ensure consistency
- Repeatable process
- Cleaner command lead hand-offs
- Recall of past events
- Better defensible position in litigation

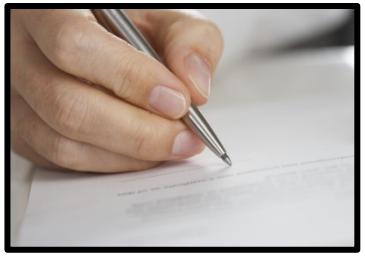
Capturing the right information in the right ways for optimal incident management and recall

Incident and/or Breach Report Form

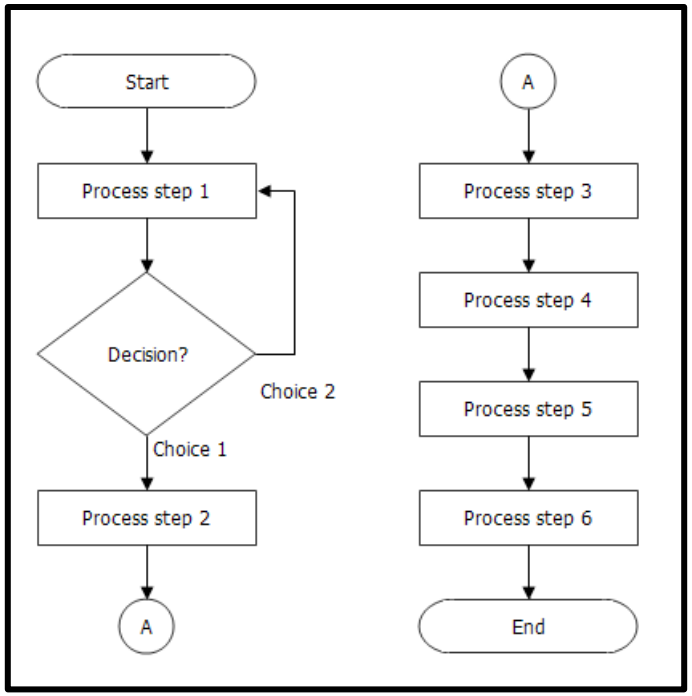
Date of discovery:	**Date and time of occurrence:**
Location of incident:	**Incident first reported to:**
Persons involved: *(Names, job titles, departments, phone numbers of the responsible staff)*	**Type of data involved:**
Number of individuals affected: *(Estimate if unsure)*	**Application or system involved:**
Description of incident: *(Explain the circumstances)*	
Type of incident: ☐ Unauthorized access ☐ Written disclosure of PHI ☐ Verbal disclosure of PHI ☐ Electronic disclosure of information ☐ Security breach of PHI (failure to secure or lost/stolen PHI) ☐ Improper destruction/disposal of PHI ☐ Other: _____	
Description of what steps were taken to contain or remediate the incident:	
Author of incident report:	**Author's contact information:**
The rest of this form is to be completed by the Privacy Officer	
Was the PHI encrypted using a FIPS 140-2 certified method? ☐ Yes ☐ No ☐ Unknown ☐ Other: _____	
Was the PHI actually acquired or viewed? ☐ Yes ☐ No ☐ Unknown ☐ Other: _____	

Taking Notes

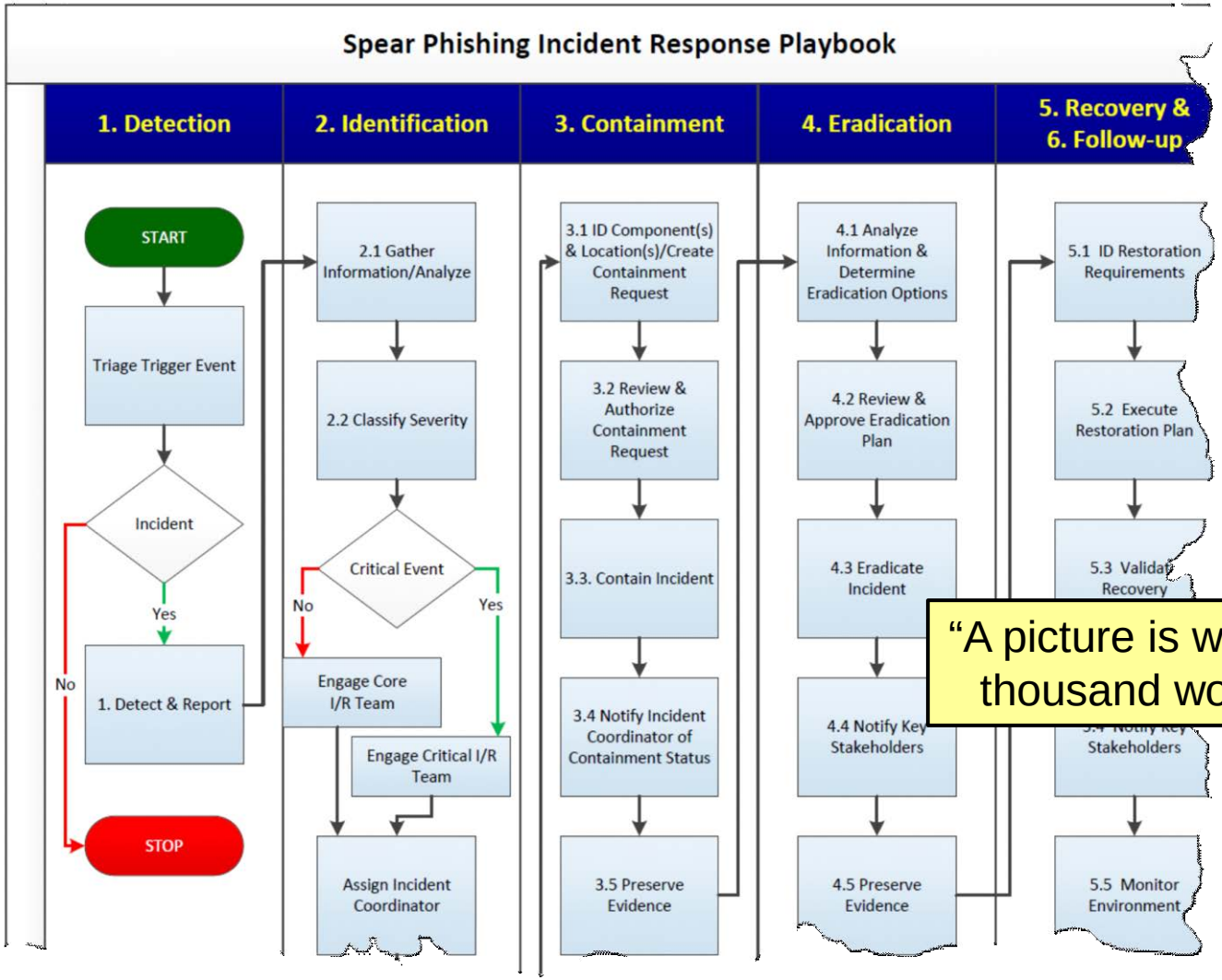
- **Capture facts – not opinions**
- **Establish standards for making data entries**
  - Maintain consistency of recording dates and times
  - Denote ~~mistakes~~ with strikethrough
- **Consider your notes being read in court**
- **Transcribe from a digital recording**
  - Delete recording after it has been transcribed



Incident Response Flow Diagram



Incident Response Flow Diagram



"A picture is worth a thousand words"

Playbooks

Common incident response playbook scenarios

- Theft or loss of mobile device/media containing confidential information
- Phishing and ransomware
- System compromise - internal
- System compromise - cloud
- Distributed Denial of Service (DDoS)

In 2016 the majority of the breaches (over 500 individuals) reported to HHS were caused by "theft"

Remind employees…

- Only an authorized spokesperson is allowed to communicate with the news media (reporters)
- Do not post to social media / networking sites

The Baltimore Sun is reporting that the cyber attack on MedStar Health is a ransomware incident, based on ransom demands that the newspaper says it has obtained.

The FBI and MedStar still have not officially confirmed a ransomware event. However, the Sun has interviewed several employees and physicians who have stated that the attack involves ransom demands. Documents obtained by the newspaper include a demand for $18,500.

MedStar personnel also have confirmed ransomware to the local Fox News affiliate.

Tabletop Exercise

Tabletop Exercise – Benefits

- Practice makes perfect
- Identify talent, process, and tools that are needed
- Determine the adequacy of existing training levels
- Demonstrate the ability to recover
- Provide a mechanism for maintaining and updating the playbooks
- Meet legal and audit requirements
- Consider combining a cybersecurity tabletop with a disaster recovery tabletop

Resources

- **NIST Special Publications**
  - SP 800-61 *Computer Security Incident Handling Guide*
- **HHS FACT SHEET: Ransomware and HIPAA**
  - https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf
- **Verizon Data Breach Report**
  - http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/
- **Department of Homeland Security (DHS)**
  - https://www.dhs.gov/cyber-incident-response

Summary

During this session, we…

- Explained the benefits of an incident response capability
- Explained the six incident response phases and how a systematic approach ensures consistency
- Identified incident response team membership, along with soft skills, tools, and documentation tips
  - Flow diagrams supported by well-defined playbooks
- Described why conducting a tabletop exercise is a necessity

Recipe for a damaged reputation

1. **Take too much confidential data**
2. **Add one part inadvertent human error or carelessness**

   Note: *You may substitute either a disgruntled employee or a dishonest employee for human error or carelessness*
3. **Mix in too little security, lack of awareness, and/or no accountability**
4. **Allow time for an incident to arise**
5. **Bake under pressure from a public disclosure**
6. **Remove responsible individuals from their jobs**

Congratulations – *Your company's reputation has been ruined and will become the prime example for other companies on what not to do!*

Questions?

Tom Walsh, CISSP

tw-Security

Overland Park, KS

www.tw-Security.com

tom.walsh@tw-Security.com

913-696-1573

tw-Security, a nationally recognized healthcare IT security consulting firm is dedicated to helping healthcare organizations protect their information resources with hands-on experience in creating and managing information security programs.