HIMSS18 The leading health information and technology conference

WHERE **THE WORLD** CONNECTS FOR HEALTH

Conference & Exhibition | March 5–9, 2018

Las Vegas | Venetian – Palazzo – Sands Expo Center

Incident Response Lessons From the Front Lines

Session 276, March 8, 2018

Nolan Garrett, CISO, Children's Hospital Los Angeles

ENGAGED

www.himssconference.org

#HIMSS18

Conflict of Interest

Nolan Garrett

Has no real or apparent conflicts of interest to report.

Agenda

- What is an Incident Response Plan?
- Incident Response and Compliance, Security Frameworks
- Policy, Plans and Process
- Real World Examples and Lessons Learned

Learning Objectives

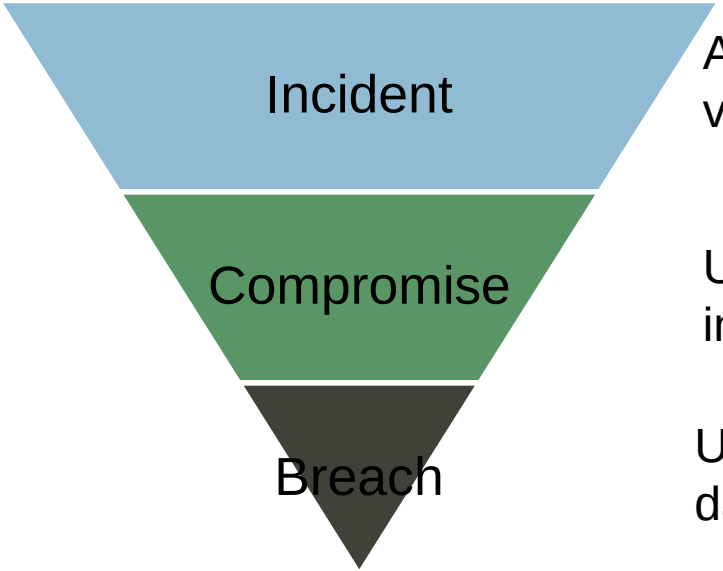
- Recognize the importance of incident response planning in relation to maintaining a state of security
- Employ standard processes for developing, maintaining and testing an incident response plan
- Demonstrate an understanding of incident response concepts and technical requirements

Why Plan for Incident Response?

- It's not a matter of if an incident will occur…
- Per-record costs for healthcare data breaches have surpassed **$400 per record**, compared to world wide averages of $158
- Costs are on average **37% higher** if detection took longer than 100 days
- Costs are additionally **68.7% higher** if containment of an identified incident took more than 30 days
- Average cost per breach across all industries surveyed reached $4M

* Source: Ponemon Institute 2016 Cost of Data Breach Study

Describing Security Events



An event that has the potential to violate security policies or controls

Unauthorized access to system(s) or infrastructure was achieved

Unauthorized access to non-public data was achieved

What is an Incident Response Plan?

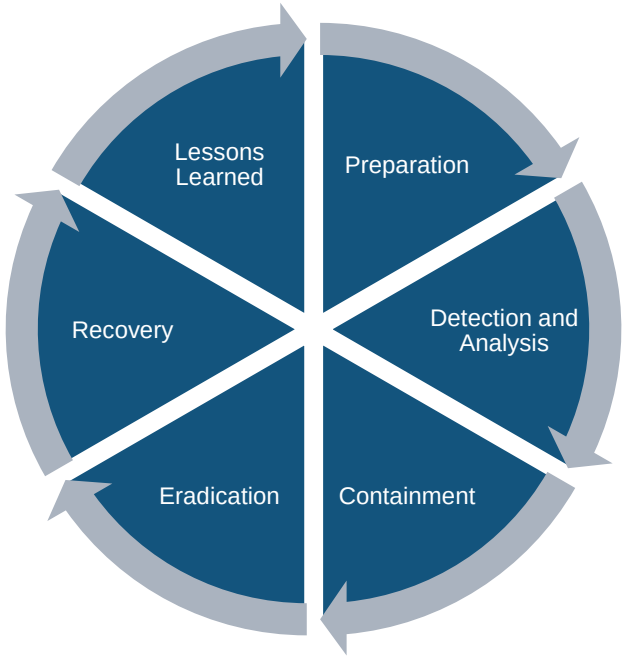
- Primary Purpose: Provide an organized, approved structure for responding to and documenting incidents in a forensically sound manner
- Defines the team structure and process that the organization will follow when an incident occurs
- Outlines executive support and oversight of the process, as well as key stakeholders
- Aims to reduce the costs of incidents and the associated response through a well organized strategy for managing the event

Incident Response and HIPAA

- 45 CFR § 164.304 defines security incident as the **attempted** or **successful** unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.
- § 164.308(a)(6)(i) **requires a covered entity to implement policies and procedures** to address security incidents. The associated implementation specification for response and reporting at § 164.308(a)(6)(ii) requires a covered entity to **identify and respond to suspected or known security incidents**, mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity, and document security incidents and their outcomes.

IR and HIPAA - Distilled

Plan Components



Preparation - Team

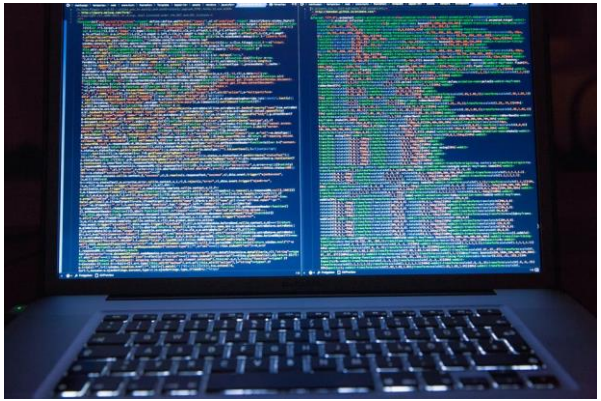
- Select a Team Model
  - Central
  - Distributed
  - Coordinating
- Select a Staffing Model
  - Employees
  - Partially Outsourced
  - Fully Outsourced

Considerations Regarding Models

- Resource Availability
- Staff and Outsourcer Expertise
- Impact on Morale
- Costs

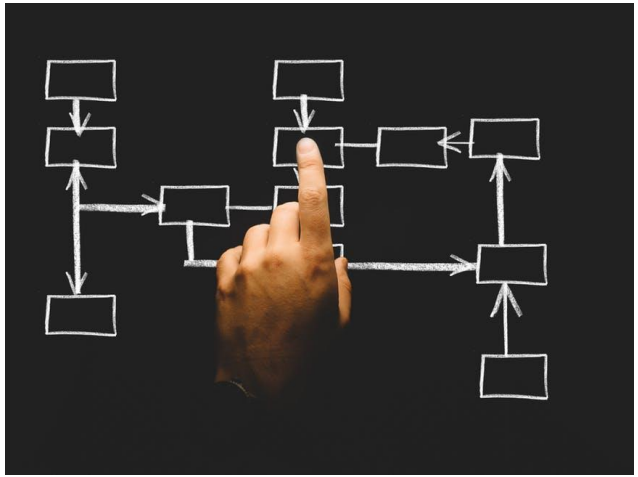
Team Skills

- Team IR Leader should be experienced in incident response, possessing both strong technical skills as well as technical and executive communication skills
- Additional skills required for successful teams:
  - Forensic analysts
  - Memory analysts
  - Malware analysts
  - Threat intelligence experts
  - Technical documentation specialists



Teams – Other Resources

- Executive Leadership
- Information Security / Assurance
- Information Technology
- Legal and Compliance
- Human Resources
- Media / Public Relations / Marketing
- Physical Security and Facilities
- External Vendors, Consultants



Preparation – Tools

- Team contact information
- Incident reporting mechanisms
- Secure communications software
- War room
- Secure storage facility
- Digital forensics software and hardware
- Dedicated analysis hardware
- See NIST SP800-61 R2, section 3.1.1

Preparation – Processes

- Risk assessment
- Network and host hardening
- End-user awareness training

Goal:

Reduce the number of events to protect the IR team from becoming overwhelmed

Detection and Analysis

- Detection is arguably the most difficult single component of incident response, taking an average of 191 days*
- Once an incident has been reported (or otherwise identified), the plan is activated and analysis begins
- Mature Incident Response Plans include an evaluation of the incident's severity or priority
- The resulting incident's severity drives further decisions about additional team members to engage and to whom to communicate within the organization
  - This should be agreed upon prior to an event occuring

* Source: Ponemon Institute 2016 Cost of Data Breach Study

Containment

- Goals:
  - Block further access or damage to systems
  - Collect evidence for use in both the response and potential legal proceedings
  - Gather details on the attack vector and actions taken to allow effective eradication
- Strategies may greatly vary depending upon the incident type

Containment

- Pre-define “playbooks” for common or major incident types such as:
  - Ransomware
  - Malware outbreak
  - Social engineering
  - Insider threat
- Refer to your risk assessment!

Eradication

- Not all incident types require eradication, but many do
- Short or medium-term steps are applied to eliminate all signs and symptoms of the incident
- Usually a series of high value quick fixes or protections that temporarily increase the security of the organization while a long-term recovery plan can be formulated

Recovery

- Goal: return to normal operations
- Recovery may take weeks or months, sometimes even longer
- Actions required to recover the affected resources are implemented
- Resources that require changes to prevent incident reoccurrence are reconfigured, updated, tested and redeployed

Lessons Learned

- Often the most frequently skipped portion of the Incident Response lifecycle
- Acts as your input to a revised IR plan, risk assessment and other organizational policies and procedures
- Looks to **document answers** to the following questions:
  - What exactly happened, and when?
  - How well did our team perform? Was our plan adequate?
  - What improvements could be made to increase the speed of execution?
  - What other corrective actions could be applied to prevent future events?

Lessons Learned

- What indicators can we watch to detect future potential events?
- Were any additional tools, staff, or external resources identified that may assist with future protection or response activities?

Test!

- Setup regular incident response plan testing
- Quarterly is a good test frequency
- Real incidents count as a test
- Use external resources to generate real-world scenarios and challenge the assumptions of your plan
- Include the outcome of your testing in IT/Information Security KPIs and reports

Real World Scenarios

A. Lost Laptop
B. Ransomware Outbreak
C. External Website Compromise

Scenario A: Lost Laptop

Adhoc Incident Response:

- Reported on Thursday afternoon to IT helpdesk
- Technician determines that standard practice is to encrypt laptops
- Ticket closed, replacement laptop ordered
- 4 months later, contacted by OCR
- Internal investigation begins
  - User remembers that the device may have been encrypted
  - Cloud management tools no longer show the device asset history, as they are only kept for 90 days
- Organization unable to positively attest that device was encrypted at time of loss

Scenario A: Lost Laptop

Planned Incident Response:

- Reported on Thursday afternoon to IT helpdesk, escalated immediately to IR team
- Asset management checklists were blank under “Device Encryption” section
- IR team utilizes Incident Response Playbook and immediately accesses reporting tools to validate laptop is reporting encrypted
- Device validated as encrypted at time of loss, remote wipe command sent to device
- Incident closed, but reported to Compliance for awareness
- Lessons Learned analysis determines that further technician training is required regarding completion of all checklist actions

Scenario B: Ransomware Outbreak

Adhoc Incident Response:

- Ransomware is identified on a critical server in the environment via an antimalware alert
- Technician responds to alert, immediately removes the malware
- This action triggers previously unidentified infections across 132 servers to immediately encrypt all data on all compromised devices, including the EMR
- Attackers demand $10,000 per encrypted device
- Organization is effectively disabled for 9 days while each system is restored from backup

Scenario B: Ransomware Outbreak

Planned Incident Response:

- Ransomware is identified on a critical server in the environment via an antimalware alert
- Technician responds to alert, following IR playbook, and advises the IR team
- IR team determines that this particular malware is a Command and Control malware
- As the team does not employ a full time malware analyst, retained consultants are engaged to evaluate the malware and identify the extent of the infection
- The internal IT, IR Team and Consultants execute a strategy to progressively remove the malware without triggering encryption

Scenario C: Website Compromise

Adhoc Incident Response:

- Your organization is notified by a patient that their web browser has warned them to avoid your website, as it is malicious
- An IT staff member reviews the site and determines that this scenario has occurred before, and asks their external marketing firm to restore the site from backup
- The marketing firm does as requested, unaware of the security incident
- The website continues to be infected and follow a cycle of infection and restoration
- Your organization's site is removed from Google search listings

Scenario C: Website Compromise

Planned Incident Response:

- Your organization is notified by a patient that their web browser has warned them to avoid your website, as it is malicious
- An IT staff member reviews the site and determines that the IR team should be contacted
- The IR team identifies the cause of the infection, and requests a restoration of the website followed by the appropriate security updates to resolve the issue
- The IR team utilizes the root cause and lessons learned analysis to enable the Information Security team's security scanners to proactively identify this kind of compromise on all current and future organization websites

Summary

- Incidents will occur – how you prepare and respond will determine the cost and survivability of your organization
- The primary purpose of an Incident Response Plan is to provide an organized, approved structure for responding to and documenting incidents in a forensically sound manner
- The most effective method to ensuring your plan is up to date is to perform regular tabletop and real world testing
- Most incidents are not reported to law enforcement, and while many breaches are, in most cases law enforcement does not actively review evidence collected unless the breach is financially sizeable
- Predefining your team and use of internal and external resources is critical to executing a timely, effective response

Recommended Reading

- NIST Special Publication 800-61 R2
  - http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf
- NIST CyberSecurity Framework (CSF)
  - https://www.nist.gov/cybersecurity-framework

Questions

Email: Nolan.Garrett@intrinium.com
LinkedIn: https://www.linkedin.com/in/nolangarrett/
Twitter: @Nolan_Garrett

Please complete the online session evaluation!