What do Carnegie Hall and Good Security Incident Response Plans Have in Common: To get there you have to practice, practice, practice!

Presented by:
Sheryl Vacca  Joe Dickinson
SVP/Chief Risk Officer  Partner

Agenda

1 The Incident Response Plan
2 Planning the Exercise
3 Preparing for the Exercise
4 Practicing Incident Response
5 Wrap-up
### 6 Ps of Incident Response Planning

<table>
<thead>
<tr>
<th></th>
<th>Purpose of the Plan</th>
<th>Process</th>
<th>People</th>
<th>Preparation</th>
<th>Practice</th>
<th>Post Exercise Debrief</th>
</tr>
</thead>
</table>

#### Purpose of the Incident Response Plan

(Visual representation of purpose)
Regulations - HIPAA Security Rule

- 45 CFR 164.308(a)(7)(i) Contingency plan
  - Requires P & Ps to respond to an emergency or other occurrence that damages a system containing ePHI including
    - Data back-up plan (R)
    - Disaster recovery plan (R)
    - Emergency mode operation plan (R)
    - Testing and revision procedures (A)
    - Application and data criticality analysis (A)

NIST 800-61 R2 Computer Security Incident Handling Guide

- The process starts with a policy
- Developing the plan
  - Get senior leadership approval (not just CIO/CISO)
  - Think beyond IT when you consider who should be on the Incident Response team
  - Think through the communications plan both internally and externally
  - Assure the players understand when to bring legal counsel into the mix.
Healthcare is a Target

- Cybercrime damage costs will hit $6 trillion annually by 2021 – Cybersecurity Ventures

- Employee negligence was the root cause for 81 percent of healthcare cybersecurity incidents. - CSO Online

- The healthcare industry was the victim of 88 percent of all ransomware attacks in U.S. industries in 2016. – Becker’s Hospital Review

- 70 percent of businesses that experienced a ransomware attack paid to have their stolen data returned – IBM Survey

---

Defense Alone is Not Enough

- 99.7% of web applications Trustwave application scanning services tested in 2016 included at least one vulnerability. – 2017 Trustwave Global Security Report

- 78% of people claim to be aware of the risks of unknown links in emails. And yet they click anyway. - Friedrich-Alexander University (FAU)

- 19% of organizations have not conducted security testing in the past six months. - Security Testing Practices and Priorities: An Osterman Research Survey Report
Breaches Will Happen

- 65% of respondents feel pressure to roll out IT projects before they undergo the necessary security checks and repairs. - 2017 Security Pressures Report

- 52% of organizations that suffered successful cyber attacks in 2016 aren't making any changes to their security in 2017 - Barkly, December 2016, Security Confidence Headed Into 2017

- 59% of organizations have experienced a malware infiltration in the past six months. - Security Testing Practices and Priorities: An Osterman Research Survey Report

- 30% of organizations experienced a successful ransomware attack over the past year. - Best Practices For Dealing With Phishing and Ransomware

Incident Response is Preparation

- The median number of days from an intrusion to containment of a breach was 62 days in 2016, virtually equal to 2015. – 2017 Trustwave Global Security Report

- The healthcare industry invests less than 6% of its budget to cybersecurity. – Security Scorecard

- In the past two years, 89% of healthcare organizations were breached. – Ponemon Institute
Know some of the key factors for planning and preparing

• The vocabulary of incident response
• Understanding communication under the incident response plan
• Must emphasize that an incident does not become a breach and is not referred to as a breach until the party designated to determine if a breach has occurred has done so.
• Train EVERYONE
  - Don’t use the term breach and incident or breach and event interchangeably
    o Especially NOT in any written document
• This is more than just an Information Technology or Information Security question.
• Drafting the plan is not enough
• Testing and improving the plan will make it a meaningful when you need to actually use it

Who should be involved in Incidence Response?

• The players need to represent multiple business units
  • There may be core members of the team that will be involved for every incident
  • There may be ad hoc members depending on the nature of the incident
  • Core members include CIO, CCO, CPO, CISO, general counsel/outside counsel, public relations, HR, risk, compliance
Stages of Incident Response Planning

• Plan and prepare
• Detect and Report
• Assess and Decide
• Respond
• Post-incident activity

Definitions

➤ **Event** - An observable occurrence of a computer or network activity causing a negative impact
  - Examples:
    o A system is down or slow
    o Server running out of disk space
    o Dead power supply on a critical system

➤ **Incident** - An event that violates the policy including an event that has potential to lead to data loss, reputation loss, loss of IP, loss of funds or an outage affecting the ability of the firm to do business
  - Examples
    o Misplaced laptop
    o Social engineered transfer of funds to 3rd party
    o Email outage

➤ **Breach** - An incident that has resulted in the confirmed data loss or exposure
  - Examples
    o Stolen or unaccounted for unencrypted removable media
    o Compromise of a system with resulting in ex-filtration of data
    o The willful improper use of data by an employee
Detect and Report

- Have in place a process that allows for detection of an incident
  - SOC
  - Flag for unusual activity in the network
  - Hotline/Helpline calls
- Assure users know how and to whom to report incidents
  - What are the possible reporting lines and does everyone involved know how to respond?

Assess and Decide

- Does the plan take in to account and address who can assess the severity of the threat and
- Decide how to proceed.
- The inability to reach the right person(s) can cost the organization
  - Loss in the ability to contain the issue
  - Increase in the downtime related to the incident
  - Increase in the recovery time
Respond

• Does the organization have the right resources/tools to respond?
  – Hardware/devices
  – Software
  – External support
    o Vendors for forensics
    o Vendors for breach notification assistance
    o Legal expertise
    o General staffing support to maintain reasonable level of operations

Post Incident Recovery

• Getting systems back online in a safe manner
• Conducting an assessment for breach notification
• Update IRP, Policies, Procedures
What to do in preparation for an IR table top exercise?

• Have an incident exercise check list
  – Review P & Ps
  – Understand the communication process
    o Who
    o What and when
    o Review the escalation process

If you fail to plan, you are planning to fail!

~ Benjamin Franklin
Incidence Response Exercise - Introduction and Overview

- What is a Table Top Exercise?
  - What is your level understanding/experience?
  - Draft Our IR Team

- Actual Exercise
  - Abbreviated from our 2½ hour session

- Debrief

- See appendix for detail of a table top exercise

Post Exercise Debrief – Questions to ask

1. Other groups that could be involved in the incident response exercise?
2. Differences if the incident happened after hours or during holidays?
3. What can be done to improve the incident response process?
4. What might be different if users were working off site from locations like home or airport?
5. What tools will be needed for incident handling? Do you pre-deploy for faster response?
6. How will external notification be handled by marketing, GC, relationship partner, and senior IT management.
   - What information can or cannot be provided?
7. Tools to consider ahead of time?
8. Training and development of staff
9. Incident response is a fluid process, what you planned for 2 years ago is different from what you plan for today or will plan for a year from now.
10. Remember the 6 Ps
    - Purpose, Process, People, Plan Practice, Post debrief
What are key areas to watch for in Incident Response Process

- Lack of leadership buy-in
- Involvement of non-IT/IS personnel in planning and execution
- Testing of the incident response plan
- Up-to-date communication planning
  - Not current contact tree
  - Contact tree is not assessable
  - All players not identified with back-ups
  - No escalation communication process

Thank You!
We look forward to working together!

Questions?

Joe Dickinson
Partner, Smith Anderson
jedickinson@smithlaw.com
919-821-6782

Sheryl Vacca
SVP/Chief Risk Officer
Sheryl.Vacca@providence.org
949-204-2980
Appendix

Table Top Exercise - example
Inject 1 – Day 1 – Thursday 4:15 pm

- The IT Helpdesk starts to see an increase in tickets related to users who are unable to log in and who report that the self-help application to allow them to change their password is not working.
- IT operations also identifies that the CPU usage for various systems has exceeded the capacity set by the alert parameters.
- The organization’s Security Operations Center is seeing an increase in data being exfiltrated from the network.

Inject 1 – Day 1 – Thursday 5:00 pm

- Your IS Helpdesk sends word that you have a malware infection. The type of malware and the full functionality has not been determined. File names are being changed and senior level executives passwords have changed.
- The CEO is unable to login and cannot access his email. Assume that all systems have been compromised.
- The Oncology Department chair complains that the treatment tracking system is not accessible.
Inject 2 – Day 1 – Thursday 7:00 pm

- The Security Team determines that there are at least 2 different malware sources. Ransomware and an as yet unidentified malware that is attempting to take control of file servers and appears to have targeted senior leaders accounts including senior leaders’ personal computers and known home networks
- In addition, the accounting systems are being targeted and there is a concern that EMR file servers are being accessed which means that PHI could be at risk.

Inject 3 – Day 2 - Friday 11:30 am

- Reviewing the information gathered to date, you learn that health plan data, ERISA data, trade secret information and senior leadership credentials have been compromised. You don’t yet know the extent of the data encrypted by ransomware and data copied from your systems. Senior Leaders home networks are encrypted.
- Firewall and security logs from various sources show that data was exfiltrated via secure file transfer protocol (SFTP) to 46.30.45.39 and 185.43.205.98 in Eastern Europe and the current backups are being accessed to attempt a recovery.