Cybersecurity Incident Response: How to Survive an Attack

Grand A/B
1:30 – 2:00

boston.healthprivacyforum.com | #hitprivacy
Learning Objectives

• **Explain** key steps in Incident Response (IR) plan
• **Describe** the process for properly investigating, containing, and recovering from an incident
• **Explain** the value in having well-defined “playbooks,” particularly for handling evidence procedures
• **Confirm** the IR maturity roadmap
• **Provide** informational resources
An effective incident response program will benefit your organization by:

- Reducing costs
- Reducing recovery time
- Improving your legal defensibility, &
- Providing a framework for continuous improvement
**SANS/CIS Top-20 Mostly Technical**

1. Inventory of Authorized and Unauthorized Devices
2. Inventory of Authorized and Unauthorized Software
3. Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers
4. **Continuous Vulnerability Assessment and Remediation**
5. Malware Defenses
6. Application Software Security
7. Wireless Device Control
8. Data Recovery Capability
9. **Security Skills Assessment and Appropriate Training to Fill Gaps**
10. Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
11. Limitation and Control of Network Ports, Protocols, and Services
12. **Controlled Use of Administrative Privileges**
13. Boundary Defense
14. Maintenance, Monitoring, and Analysis of Security Audit Logs
15. **Controlled Access Based on the Need to Know**
16. **Account Monitoring and Control**
17. Data Loss Prevention
18. **Incident Response Capability**
19. Secure Network Engineering
20. Penetration Tests and Red Team Exercises

**Gartner Administrative & Technical**

1. Governance
2. Policy
3. Awareness & Training
4. Identity Management
5. Vulnerability Management
6. **Incident Response**

**Sources:**

SANS/CIS: [https://www.cisecurity.org/critical-controls/](https://www.cisecurity.org/critical-controls/)
Gartner Research: *The Security Processes You Must Get Right*
Incident Response & Management: “Protect the organization's information, as well as its reputation, by developing and implementing an incident response infrastructure:”

- Plans
- Defined roles
- Training
- Communications
- Management oversight

...for quickly discovering an attack and then effectively containing the damage, eradicating the attacker's presence, and restoring the integrity of the network and systems.
A security maturity model is a set of characteristics, attributes, indicators, or patterns that represent capability and progression within the information security discipline. Model content typically exemplifies best practices and may incorporate standards or other codes of practice of the discipline.

Models:

A. Provide a benchmark against which an organization can evaluate the current level of capability of its:
   • Practices
   • Processes
   • Methods
B. Set goals and priorities for improvement

# Maturity Model Comparison

<table>
<thead>
<tr>
<th>Capability Maturity Model (CMM) – Dept. of Defense</th>
<th>Gartner</th>
<th>E&amp;Y</th>
<th>NIST Cybersecurity Framework</th>
</tr>
</thead>
<tbody>
<tr>
<td>Informal</td>
<td>Ad-hoc</td>
<td>Aligned</td>
<td>Partial</td>
</tr>
<tr>
<td>Planned &amp; Tracked</td>
<td>Repeatable</td>
<td>Enterprise-wide</td>
<td>Risk Informed</td>
</tr>
<tr>
<td>Well Defined</td>
<td>Defined</td>
<td>Continuous</td>
<td>Repeatable</td>
</tr>
<tr>
<td>Quantitatively Controlled</td>
<td>Optimized</td>
<td>Proactive</td>
<td>Adaptive</td>
</tr>
<tr>
<td>Continuously Improving</td>
<td>Innovating</td>
<td>Validated</td>
<td>Formal</td>
</tr>
</tbody>
</table>

- **Gartner**:
  - Informal
  - Planned & Tracked
  - Defined
  - Optimized
  - Innovating
- **E&Y**:
  - Aligned
  - Enterprise-wide
  - Continuous
  - Proactive
  - Validated
- **NIST Cybersecurity Framework**:
  - Partial
  - Risk Informed
  - Repeatable
  - Adaptive
  - Formal
## IR Capabilities

**Ranked by Maturity Level**

<table>
<thead>
<tr>
<th>Level-1 (Formal)</th>
<th>Level-2 (Planned and Tracked)</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Written Policy</td>
<td>• P&amp;P follows a standard (NIST, US-CERT, etc.)</td>
</tr>
<tr>
<td>• Written Procedure</td>
<td>• Stakeholders are kept in the loop</td>
</tr>
<tr>
<td></td>
<td>• Incidents are defined (types and severity)</td>
</tr>
<tr>
<td></td>
<td>• Teams are created</td>
</tr>
<tr>
<td></td>
<td>• Playbooks for major cyber events are created</td>
</tr>
<tr>
<td></td>
<td>• Escalation processes are defined</td>
</tr>
<tr>
<td></td>
<td>• Incidents are tracked and categorized</td>
</tr>
<tr>
<td></td>
<td>• RACI Matrix is created</td>
</tr>
</tbody>
</table>
IR Playbooks

• Based on standards like US-CERT, NIST SP800-61, SANS/CIS best practices

• IR Playbooks 5 basic phases
  1. Detection & notification of the incident
  2. Assessment of the incident
  3. Containment of the incident
  4. Eradication of the incident
  5. Follow-up of the incident
Common Playbook Scenarios

• System compromise - internal
• System compromise - cloud
• Theft of confidential information
• Theft or loss of mobile device/media
• Malware
• Phishing
• Distributed Denial of Service (DDoS)
## IR Playbooks

### Spear Phishing Incident Response Playbook

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>START</strong></td>
<td><strong>2.1 Gather Information/Analyze</strong></td>
<td><strong>3.1 ID Component(s) &amp; Location(s)/Create Containment Request</strong></td>
<td><strong>4.1 Analyze Information &amp; Determine Eradication Options</strong></td>
<td><strong>5.1 ID Restoration Requirements</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Triage Trigger Event</strong></td>
<td><strong>2.2 Classify Severity</strong></td>
<td><strong>3.2 Review &amp; Authorize Containment Request</strong></td>
<td><strong>4.2 Review &amp; Approve Eradication Plan</strong></td>
<td><strong>5.2 Execute Restoration Plan</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Incident</strong></td>
<td><strong>Yes</strong></td>
<td><strong>3.3 Contain Incident</strong></td>
<td><strong>4.3 Eradicate Incident</strong></td>
<td><strong>5.3 Validate Recovery</strong></td>
<td></td>
</tr>
<tr>
<td><strong>No</strong></td>
<td><strong>1. Detect &amp; Report</strong></td>
<td><strong>3.4 Notify Incident Coordinator of Containment Status</strong></td>
<td><strong>4.4 Notify Key Stakeholders</strong></td>
<td><strong>5.4 Notify Key Stakeholders</strong></td>
<td></td>
</tr>
<tr>
<td><strong>STOP</strong></td>
<td><strong>Engage Core I/R Team</strong></td>
<td><strong>3.5 Preserve Evidence</strong></td>
<td><strong>4.5 Preserve Evidence</strong></td>
<td><strong>5.5 Monitor Environment</strong></td>
<td></td>
</tr>
</tbody>
</table>

**Source:** tw-Security
**Playbook: Containment Phase**

**Note:** If you are a victim of Ransomware, don’t just let IT solve the problem. Require the engagement of your Privacy/Compliance Officer. You should perform a breach risk assessment. You may need to forensically prove that no data (from the infected device(s) left the organization.

**Beware:** If encryption software was able to encrypt your data, it may have been able to read and copy your data as well.

**Source:** tw-Security
# IR RACI Matrix

<table>
<thead>
<tr>
<th>Actor</th>
<th>Overall Coordination</th>
<th>Gather Logs and Analyze</th>
<th>Specialized Forensic Operations and Analysis</th>
<th>Issue, Emergency Change Management</th>
<th>Engineering and Technical Assurance</th>
<th>Staff Monitoring and Investigation</th>
<th>Law Enforcement Liaison</th>
<th>Media Messaging</th>
<th>Staff Messaging</th>
<th>Customer Messaging</th>
<th>Partner Messaging</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIO/CISO/CPO</td>
<td>A</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>AR</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IT Incident Coordinator</td>
<td>R</td>
<td>I</td>
<td>I</td>
<td></td>
<td></td>
<td></td>
<td>I</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td>C</td>
</tr>
<tr>
<td>Network Engineering / Systems Engineering</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td></td>
<td></td>
<td></td>
<td>I</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Scribe</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td></td>
<td></td>
<td></td>
<td>I</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Information Security</td>
<td>I</td>
<td>AR</td>
<td>AR</td>
<td>R</td>
<td></td>
<td></td>
<td>I</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Business IT Units</td>
<td>I</td>
<td>I</td>
<td>C</td>
<td>C</td>
<td></td>
<td></td>
<td>I</td>
<td>C</td>
<td>C</td>
<td>C</td>
<td>C</td>
</tr>
<tr>
<td>Enterprise Risk Management</td>
<td>I</td>
<td>I</td>
<td>I</td>
<td>C</td>
<td></td>
<td></td>
<td>I</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Internal Audit</td>
<td>I</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>I</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Internal Investigations</td>
<td>I</td>
<td>AR</td>
<td>AR</td>
<td>C</td>
<td>I</td>
<td></td>
<td>AR</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Forensic Services (Third-Party Provider)</td>
<td>I</td>
<td>R</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>R</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Law Department (Internal or External)</td>
<td>I</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>C</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>External Legal Counsel</td>
<td>I</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Source:** Gartner Toolkit - Security Incident Response Preparation RACI Matrix
IR Capabilities

Level-3 (Well Defined)

• Playbooks are rehearsed (tabletop)
• Threat advisories are monitored
• Validated (by a qualified 3rd party)
• Enterprise-wide
• Root cause “Lessons Learned” performed after incidents
• Incident call trees are developed
• Emergency Management defines IT events
• Cyber insurance
• Security event monitoring is managed systematically in real time
• Training for IT
• Forensic Firms - retainer in place
• FBI - Knowing who and when to contact
Tabletop Exercise Benefits

- **Practice** makes perfect - before a cyber event (or often, after...)
- **Identify** talent, process, and tools that need modification or improvement
- **Determine** the adequacy of existing training levels
- **Demonstrate** the ability to recover (a tabletop is easier, less time consuming and less expensive than a simulated technical drill or a real event.
- **Provide** a mechanism for maintaining and updating the playbooks
- **Meet** legal and audit requirements

**Note:** 3rd party tabletop facilitation and validation provides an external perspective
IR Capabilities

Level-4 (Quantitatively Controlled)

• Defined set of metrics are used
• Metrics used to drive improvement
• Training for first responders
• Hospital Incident Command System (HICS)
• Ongoing research is conducted to learn about new threats
• Enterprise is able to analyze malware and determine its purpose and characteristics
Engage Emergency Management (HICS)

Protective Services
Emergency Mgmt.

Information Security

BCM = Business Continuity Management

Source: Gartner (November 2013)
IR Capabilities

Level-5 (Continuously Improving)

- Playbooks are rehearsed (live drills – beyond tabletop)
- Ability to separate noise from the real event
- Legally defensible evidence gathering
- Forensic technicians withstand cross examination
IR Exercises Beyond Tabletop

- **Conducting** technical drills
- **Separating** real events from “noise”
- **Gathering** data in a legally defensible way
- **Withstanding** cross examination
Forensic Cheat Sheet-1

- Obtain authorization to search and seize
- Secure the area, which may be a crime scene
- Document the chain of custody of every item that was seized
- Bag, tag, and safely transport the equipment and e-evidence
- Acquire the e-evidence from the equipment by using forensically sound methods and tools to create a forensic image of the e-evidence
Forensic Cheat Sheet

- Keep the original material in a safe, secured location
- Design your review strategy of the e-evidence, including lists of keywords and search terms
- Examine and analyze forensic images of the e-evidence (never the original!) according to your strategy
- Interpret and draw inferences based on facts gathered from the e-evidence. Check your work
- Describe your analysis and findings in an easy-to-understand and clearly written report
- Give testimony under oath in a deposition or courtroom
Resources

• FEMA – Free training for emergency responders
  – https://cdp.dhs.gov/training/resident/

• NIST Special Publications
  – SP 800-61 I/R Guide
  – SP 800-66 HIPAA

• SANS/CIS
  – https://www.sans.org/critical-security-controls

• Verizon Data Breach Report
Summary

• I used a maturity model to describe the characteristics of an effective IR program – to provide an improvement roadmap
• We discussed a standards based/phased IR process
• I listed common IR planning scenarios
• We looked at a graphical representation of a playbook – designed to be read under stress
• I explained the value of tabletop and beyond tabletop exercises
• I provide information resources
Bottom Line

...A plan that has not been tested, is only a better wish!
Questions
Mark W. Dill, CISM, CRISC
Partner & Principal Consultant
tw-Security.com

boston.healthprivacyforum.com | #hitprivacy