Save the Day:
Build an Incident Response Program Now

Steve Winterfeld
Advisory CSIO
Pillars to Build Program On

1. Governance
   ii. Base it on established framework or regulation (makes it audit friendly)
   iii. Coordinated across partner programs (Resiliency, Disaster Recovery, Business Continuity and Public Relations)

2. Plan
   i. Plan – address remediation, impact analysis and communications
   ii. Playbook(s) – separate from plan that go into specifics

3. Validation
   i. Testing Plans
   ii. Exercises
Defining Incident / Breach

- Will it be based on
  - Disruption of customer access
  - Public coverage (brand)
  - Loss (revenue/data)
  - Safety
  - Compliance

- Depending on size of event you will need levels based on scope / volume
- Defining when to declare a ‘breach” starts the clock for notifications
- Issue with use of term “breach”
Scenarios

These basic scenarios will exercise all aspect of the plan:

- Data Loss (Malicious/Criminal and Unintentional)
- Third Party Data Loss (Malicious/Criminal and Unintentional)
- Merger & Acquisition (M&A)
- Loss of Availability (ie Ransomware or DDoS)
  - This would be tied to Business Continuity / Disaster Recovery plans

Need to be consistent

- Attach method vs impact (ie Insider/Hacker vs Data Loss)
- Use a industry format like CIA (impact to Confidentiality, Integrity or Availability)
Responsible, Accountable, Consulted, Informed

- Detect incident and declare incident (based on impact analysis)
- Stand up response team and contact support vendors (forensics, legal, PR)
- Conduct investigation, implement remediation
- Communication with: LEA, regulators, board, customers and partners
- Holds authority to confiscate or disconnect equipment
- Handoff and escalation points in the incident management process

<table>
<thead>
<tr>
<th>Decide on what to do with ring</th>
<th>Frodo</th>
<th>Sam</th>
<th>Gandalf</th>
<th>Aragorn</th>
<th>Head of Elves (Elrond)</th>
</tr>
</thead>
<tbody>
<tr>
<td>C</td>
<td>I</td>
<td>A</td>
<td>C</td>
<td>R</td>
<td>R</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Create Fellowship</th>
<th>Frodo</th>
<th>Sam</th>
<th>Gandalf</th>
<th>Aragorn</th>
<th>Head of Elves (Elrond)</th>
</tr>
</thead>
<tbody>
<tr>
<td>R</td>
<td>C</td>
<td>A</td>
<td>A</td>
<td>C</td>
<td>R</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Get the ring to Mt Doom</th>
<th>Frodo</th>
<th>Sam</th>
<th>Gandalf</th>
<th>Aragorn</th>
<th>Head of Elves (Elrond)</th>
</tr>
</thead>
<tbody>
<tr>
<td>R</td>
<td>C</td>
<td>A</td>
<td>A</td>
<td>C</td>
<td>I</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Distract and defeat enemies</th>
<th>Frodo</th>
<th>Sam</th>
<th>Gandalf</th>
<th>Aragorn</th>
<th>Head of Elves (Elrond)</th>
</tr>
</thead>
<tbody>
<tr>
<td>I</td>
<td>R</td>
<td>C</td>
<td>R</td>
<td>I</td>
<td>I</td>
</tr>
</tbody>
</table>
Policy (NIST Format)

Statement of management commitment

- Purpose and objectives of the policy
- Scope of the policy (to whom and what it applies and under what circumstances)
- Definition of computer security incidents and related terms
- Organizational structure, definition of roles, responsibilities, levels of authority
- Prioritization or severity ratings of incidents
- Performance measures
- Reporting and contact forms
Plan (NIST Format)

1. Mission statement
2. Strategies and Goals
3. Senior management approval (signed off on)
4. Organizational approach to incident response
5. How the IR team will communicate with the rest of the organization(s)
6. Metrics for measuring the incident response capability and its effectiveness
7. Roadmap for maturing the incident response capability
8. How the program fits into the overall organization
Definition for Incident Response

The documentation of a predefined set of instructions or procedures to detect, respond to, and limit consequences of a malicious cyber attacks against an organization’s information system(s).

CNSSI 4009-2015 / NIST SP 800-34 Rev. 1
Compliance References

- National Institute of Standards and Technology (NIST)
- North American Electric Reliability Corporation (NERC - Critical Infrastructure Protection (CIP))
- Payment Card Industry (CIP) Data Security Standard (DSS)
- Federal Financial Institutions Examination Council (FFIEC)
- Health Insurance Portability and Accountability Act (HIPPA)
- Audit frameworks - ISO/IEC, COBIT or CIS
- Cloud - CSA Cloud Controls Matrix or FedRAMP
The Team

• Incident Commander
• Leadership (CEO, CISO, CIO, CFO)
• Legal (Kovel agreement)
• Compliance / Privacy / Audit / Risk committee
• Public Relations / Communications
• Information Technology (IT)
• Security Operations Center (SOC) / Forensics
• External SME (Forensics, Communication and Legal)
• Vendor management (Third Parties)
• Client Support (call centers)
• Business Continuity / Disaster Recovery
NIST IR Process

NIST Special Pub 800-61 Incident Handling Guide
Detection (Subprocess)

- Event - Log (Evidence)
- SIEM - Alert (Correlation)
- SOC - Incident (Impact Analysis and Mitigation)
- Response - Recovery (Management and Investigation)
- Tools:
  - Security Information and Event Management (SIEM)
  - Security Orchestration, Automation, and Response (SOAR)
  - Security Operations and Analytics Platform Architecture (SOAPA)
SANS IR Process

Great for SOC

Preparation

Lessons Learned

Identification

Recovery

Containment

Eradication

Lessons Learned
MITRE ATT&CK for validation
Adversarial Tactics Techniques and Common Knowledge

Pen Test use: Common Attack Pattern Enumeration and Classification (CAPEC)
Sample Processes

- Evidence management
- Investigation
- Notify insurance, regulators, board, public, LEA
- Containment, coordination, remediation, lessons learned
- Third party management
- Business continuity / Disaster recovery collaboration
- Testing / Exercises (Validation)
Testing / Exercises Format

Exercise: Tech, Table Top, Simulation (There are third party hosted options)

Logistics: Facilitator, Scribe, Facility, Timeline, Technically feasible / realistic

Objective: Validate the plan annually

Scenarios: Data loss, Third party, Ransomware, M&A

Sample Injects: timeline - from suspicious to determination of breach, LEA notification of data found on dark web, receive ransomware/DDoS/data stolen blackmail note, physical impact (attack elevator/power or bomb threat), reporters call and ask about breach, grey hat hacker asking for payment on vulnerability, call center flooded with calls, social media blowing up, hacktivist released sensitive documents, web site defaced, insider threat
Next Steps

1. Develop roadmap to resource the program
2. Build the framework and get leadership sign off
3. Develop the plan
4. Exercise the plan
Resources

- NIST Cybersecurity Framework (800-53)
- Cybersecurity and Infrastructure Security Agency (CISA) / US Cert – Documentation and reports (ICS section)
- DHS – Documentation and programs
- Fusion cells / E-ISAC – Membership and templates
- MITRE ATT&CK and CAPEC – Program frameworks
- SANS PICERL – SOC IR program framework
Build an Incident Response Program Today
Before You Have to Build it During a Crisis