We’ve been hacked – now what?

Cybersecurity for the Public Sector
Overview of today’s discussion

• We’ve been hacked!
  • Incident Response Triage – Where do we start?
  • Incident Evaluation – How did this happen?
  • Incident Prevention – How do we protect our organization?
Incident lifecycle

- **Incident Closure**: Postmortem Analysis; Management Report
- **Planning & Preparation**: Policies; R&D; Checklists; Communication Plan & Awareness
- **Post Incident Assessment**: Postmortem – What, How, When; Corrective Actions; Lessons Learned
- **Detection, Triage**: Defining; Detecting; Prioritizing; Implementing; Awareness
- **Containment, Analysis, Tracking**: Containment; Recovery/BCP; Source of Incident
- **Investigation and Image**: Analysis; Forensic
<table>
<thead>
<tr>
<th>2017</th>
<th>Statistics</th>
</tr>
</thead>
<tbody>
<tr>
<td>$225</td>
<td><strong>Average cost per record</strong> <em>(Ponemon Institute: 2017 US Data Breach Study)</em></td>
</tr>
<tr>
<td>$7.35 mil</td>
<td><strong>Average total cost per organization</strong> <em>(Ponemon Institute: 2017 US Data Breach Study)</em></td>
</tr>
<tr>
<td>$.69 mil</td>
<td><strong>Average customer notification cost</strong> <em>(Ponemon Institute: 2017 US Data Breach Study)</em></td>
</tr>
<tr>
<td>206 days</td>
<td><strong>Average time to detection</strong> <em>(Ponemon Institute: 2017 US Data Breach Study)</em></td>
</tr>
<tr>
<td>55 days</td>
<td><strong>Average time to address a breach</strong> <em>(Ponemon Institute: 2017 US Data Breach Study)</em></td>
</tr>
<tr>
<td>82%</td>
<td><strong>Breaches detected by outsiders</strong> <em>(Verizon: 2017 Data Breach Report)</em></td>
</tr>
<tr>
<td>78%</td>
<td><strong>Initial intrusions rated as low complexity</strong> <em>(Verizon: 2017 Data Breach Report)</em></td>
</tr>
</tbody>
</table>
Incident Response Triage
Where do we start?
How would your organization react?

A. RUN
   may be you can escape the issue

B. IGNORE
   it might go away

C. STAY CALM
   you have a response plan

D. BLAME
   the IT guy or gal
Step 1: Isolate Risk
Step 2: Assess damage

• Initial Entry Point
  ▪ Email – Other recipients?
  ▪ Compromised credentials – access to other systems?

• Breadth of Impacted Systems
  ▪ Efficient log review process
  ▪ OR
    ▪ Compromised unless proven otherwise?

• Continue Isolating Risk
Step 2: Assess damage

- Availability
  - DDoS
  - Ransomware
- Integrity
  - Data Falsification
- Confidentiality
  - Data Loss
What are Hackers After?

- Social Security Numbers
- Credit Card Numbers
- Banking Information
- Usernames and Passwords
- Address, Birthdate, other Personally Identifiable Information
- Email Lists

- ANY data the organization would consider confidential
Step 3: Notifications

- IT/Information Security
- Marketing/Public Relations
- Client-Facing Staff
- Legal
- Executives/Board
- Law Enforcement – Evidence maintained appropriately?
- Vendors
Incident Evaluation

How did this happen?
Levels of detection

• Employees
  ▪ Notify immediately or fear consequences
Levels of detection

- System Logs
  - Firewall, IDS, network, application, DLP, etc.
Levels of detection

- Correlate Logs
  - SIEM solution
Key Questions to Answer

- Can you confirm the intrusion has ended?
- What was accessed?
- How much did this cost us financially and reputation?
- Was this something you trained or prepped for?
- What Lessons did you learn
- How did it happen....
How did this happen?

• Social Engineering

Most attacks begin socially. Employees are your greatest asset, but often your weakest link to security. Hackers know this, and have developed social scams by the thousands, hoping but one will fall victim
How did this happen?

• Mobile Device Management
How did this happen?

• Weaknesses in Software
How did this happen?

- Weak Passwords
How did this happen?

• Third Party Security
How did this happen?

- Misconfigurations
  - Device hardening
  - Segmentation – Internet facing confidential server
Incident Prevention

How do we protect our organization?
Compliance ≠ Security

No regulation or standard alone will keep your organization safe!
Planning

A defined response framework is important!

Prepare
- IRP ownership/team
- User awareness
- Asset management
- Vendor management

Identify
- Active methods
- Passive methods

Contain
- Connectivity
- Service
- System

Investigate
- Internal team
- Forensic support
- Legal support

Eradicate
- Disinfection strategy
- Rebuild strategy
- Other

Recover
- Functionality restore
- Containment removal
- DRP/BCP
- Other

Lessons Learned

Documentation | Reporting | Continued Communications
Who’s responsible?

Information security is not an IT issue
Building around People, Process, and Technology

Identify what you have

Protect what you identify

Detect direct and indirect attacks

Respond accordingly (IRP)

Recover appropriately (BCP/DRP)
Identify What You Have

- Asset Inventory
- Application Inventory
- Access Needs – Logical and Physical
- Vendor Inventory
Protect What You Identify

- End User Training
- Network Segmentation
- Patch Management
- Access Management
- Mobile Device Management
- Vendor Management
- Information Security Program
Detect Direct and Indirect Attacks

• Event Logging
  ▪ Firewall
  ▪ IDS/IPS
  ▪ Network
  ▪ Application

• Activity Reviews
  ▪ Alerts and Reports
  ▪ Independent
  ▪ Baselines
Respond Accordingly

- Incident Response Plan
  - Vendor/Regulator Communications
  - Senior Management Communications
- Cybersecurity Insurance
- Plan Training and Testing
Recover Appropriately

• Disaster Recovery Plan
  ▪ Data Recovery
  ▪ Redundant Connectivity
  ▪ Vendor Failover

• Business Continuity Plan
  ▪ Business Process Workarounds
  ▪ Recover Normal Operations

• Plan Training and Testing
Where Do We Focus Efforts

Risk Based Decisions

- Compliance
- Continuity
- Internal Technical Breach
- External Technical Breach
- Theft/Loss of Corporate Assets

Legend:
- Controlled Risk
- Residual Risk
Incident lifecycle