Triage Incident Response

What to do before picking up the phone
Topics

• Making News – Notable Incidents
• Scenario
• What Answers You Should Already Have
• Quick Wins
• Next Steps to Prepare for and Respond to Cybersecurity Incidents
MAKING NEWS
Equi-Hacks!

T-Mobile

2 Million Accounts Hacked!

https://www.databreachtoday.com/false-alarm-phishing-attack-against-dnc-was-just-test-a-11414
PRESENT STATE
Relevancy

• Why does this apply to me?
• Nobody wants what I have?
• Who cares?
• But I only have access to…
Breach Stats

**Figure 1.** Threat actors within breaches over time

- External
- Internal
- Partner
- Multiple

**Figure 2.** Threat actor motives within breaches over time

- Financial
- Espionage
- Fun
- Other
- Grudge

Cyberespionage remains a major concern—espionage was a motive for 44% of breaches. Attacks usually involve phishing, installations and the use of backdoors or C2 channels. But it’s not just state secrets being targeted—the personal data you hold on citizens and employees is also at risk.
Who are the victims?

- 24% of breaches affected healthcare organizations
- 15% of breaches involved accommodation and food services
- 14% were breaches of public sector entities
- 58% of victims are categorized as small businesses

What are other commonalities?

- 49% of non-POS malware was installed via malicious email
- 76% of breaches were financially motivated
- 13% of breaches were motivated by the gain of strategic advantage (espionage)
- 68% of breaches took months or longer to discover
Thinking About Costs...

Figure 25. Cost framework for cyber crime

Internal cost activity centers
- Detection
- Investigation & escalation
- Containment
- Recovery
- Ex-post response

Direct, indirect and opportunity costs associated with cyber crimes

External consequences and costs
- Information loss or theft
- Business disruption
- Equipment damage
- Revenue loss
How do you know?

Prevention is ideal, but detection is a must!
SCENARIO
“Does this look odd to you?”
Answers You May Already Have
Show me the Data

• What devices do you have?

• What applications do you have?
Vulnerability Management
Vulnerabilities

• A ‘known vulnerability’ is a vulnerability in software that the vendor is aware of. Typically they have also created a patch or update that solves the problem. Scanning tools scan for known vulnerabilities.

• ‘Zero day vulnerabilities’ are vulnerabilities that vendors are unaware of. Vulnerability scanners have no way to detect zero day vulnerabilities.
Vulnerability Mgmt.

- Identify Active Devices/In-Scope
- Asset Identification
- Vulnerability Scan
- Remediate & Response
- Evaluate Vulnerability
- Determine Impact
- Action Plan
- Risk Acceptance Approval
- Review & Follow-up
- Identify Open Ports & Services
- OS Fingerprinting
- Vulnerability Identification
- Security Asmt.
- Corrective Action Plan
- Establish Controls
- Identify Threats
- Assess Exploits
<table>
<thead>
<tr>
<th>Assessment Type</th>
<th>Security Audit</th>
<th>Vulnerability Assessment</th>
<th>Penetration Test</th>
<th>Social Engineering</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Purpose</strong></td>
<td>Evaluation of how various security processes are designed and implemented.</td>
<td>Comprehensive identification and evaluation of known vulnerabilities in the computing environment typically involving a combination of the use of scanning tools, network diagram reviews, and reviews of device configurations.</td>
<td>Seeking to mimic the actions of a hacker – looking for any way to circumvent security controls to gain unauthorized access, typically without being detected.</td>
<td>Performing phishing, vishing and other techniques often used by hackers to deceive users into compromising their own security.</td>
</tr>
<tr>
<td><strong>What is Accomplished?</strong></td>
<td>Recommendations for enhancements to fix security management processes.</td>
<td>Identification of known technical vulnerabilities in networks, operating systems, databases and applications. Tests the adequacy of the vulnerability management process.</td>
<td>Narrow identification of known vulnerabilities based on the techniques used by the pen tester. Determine the exploitability of identified known vulnerabilities. Tests effectiveness of incident identification, response procedures.</td>
<td>Tests the effectiveness of the organization’s security awareness training program. Social engineering tactics are often used to deceive users into divulging their logon credentials or to get a user to download malware. May test effectiveness of incident identification, response procedures.</td>
</tr>
<tr>
<td><strong>What is Not Accomplished?</strong></td>
<td>Typically not able to assess effectiveness of incident identification or response procedures. May not get good visibility into technical system vulnerabilities.</td>
<td>Root cause of why known vulnerabilities exist in the environment. Unsure exactly how exploitable known vulnerabilities are. Unable to assess effectiveness of incident identification or response procedures. Won’t catch 0 day vulnerabilities.</td>
<td>Typically don’t have a comprehensive understanding of all known vulnerabilities. Will not involve 0 day vulnerabilities.</td>
<td>Doesn’t comprehensively evaluate the design and effectiveness of security management processes and doesn’t identify technical vulnerabilities.</td>
</tr>
</tbody>
</table>
Vulnerability Mgmt.

• SWOT Analysis – Known Weaknesses
• Managed Exceptions
  – Someone reviewed and signed off on these right?
• Vulnerable vs False Positives
Show Me the Log Data

What do you have?
- Servers, Firewalls, Workstations (Laptops/Desktops)

Is it the right stuff?
- Failed log on attempt (Success?)

Where is it?
- Centralized vs Local

How far back does it go?
- Is that far enough to answer your questions?
- Who has access to it?
SIEM

IDS

Firewall

Proxy

Web server

SIEM

Critical alert
Logging to SIEM

Windows
- Registry
- Event logs
- File system
- sysinternals

Linux/Unix
- Configurations
- syslog
- File system
- ps, iostat, top

Virtualization And Cloud
- Hypervisor
- Guest OS, Apps
- Cloud

Applications
- Web logs
- Log4J, JMS, JMX
- .NET events
- Code and scripts

Databases
- Configurations
- Audit/query logs
- Tables
- Schemas

Networking
- syslog
- SNMP
- Netflow
- IDS

http://coverall.splunk.com/web_assets/developers/devguide/WhatSplunkCanIndex.jpg
The system time was changed.

Event ID: 4616
Do you have the Time?

• Do you know how time is kept on all of your devices?
• Are they all set the same?
• Do you have devices in different time zones?
  – What about roaming laptops?
  – Disaster Recovery (DR) site?
• Cloud Resources?
• When in doubt UTC/GMT
What Else Can You Do?
3 Quick Wins

1. Know What You Have
   - Inventory of Data & Systems

2. Gather Ye Rosebuds
   - Check that you’re gathering the information needed to answer reasonable questions

3. Do You Have The Time
   - Set everything to UTC or have a documented plan
• **Baseline – Know Normal**
  – Devices (What do we have?)
  – Ports/Services (What do we keep open?)
  – Network Traffic (Who talks to who regularly?)
  – Encryption (Security vs disguise?)

• **Segmentation**
  – Where are the critical pieces?
  – How far did it get? How far could it get?
Planning

- Mentality – when not if
- Vulnerability management program
- Reducing the time to detect
- Implement effective monitoring
- Develop an incident response plan that includes...
  - Cyber resilience plan
  - Pre-engaging the right people
- Table top exercises
State of Mind

- When not if!
- There are two kinds of organizations – those that have been breached... and those that know they’ve been breached!
Frameworks for Success

CYBER RESILIENCY

• Asset Management
• Controls Management
• Configuration and Change Management
• Vulnerability Management
• **Incident Management**
• Service Continuity Management
• Risk Management
• **External Dependency Management**
• Training and Awareness
• **Situational Awareness**

*Source: https://www.us-cert.gov/ccubedvp/self-service-crr*
<table>
<thead>
<tr>
<th>Action</th>
<th>Completed</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Detection and Analysis</strong></td>
<td></td>
</tr>
<tr>
<td>1. Determine whether an incident has occurred</td>
<td></td>
</tr>
<tr>
<td>1.1 Analyze the precursors and indicators</td>
<td></td>
</tr>
<tr>
<td>1.2 Look for correlating information</td>
<td></td>
</tr>
<tr>
<td>1.3 Perform research (e.g., search engines, knowledge base)</td>
<td></td>
</tr>
<tr>
<td>1.4 As soon as the handler believes an incident has occurred, begin documenting the investigation and gathering evidence</td>
<td></td>
</tr>
<tr>
<td>2. Prioritize handling the incident based on the relevant factors (functional impact, information impact, recoverability effort, etc.)</td>
<td></td>
</tr>
<tr>
<td>3. Report the incident to the appropriate internal personnel and external organizations</td>
<td></td>
</tr>
<tr>
<td><strong>Containment, Eradication, and Recovery</strong></td>
<td></td>
</tr>
<tr>
<td>4. Acquire, preserve, secure, and document evidence</td>
<td></td>
</tr>
<tr>
<td>5. Contain the incident</td>
<td></td>
</tr>
<tr>
<td>6. Eradicate the incident</td>
<td></td>
</tr>
<tr>
<td>6.1 Identify and mitigate all vulnerabilities that were exploited</td>
<td></td>
</tr>
<tr>
<td>6.2 Remove malware, inappropriate materials, and other components</td>
<td></td>
</tr>
<tr>
<td>6.3 If more affected hosts are discovered (e.g., new malware infections), repeat the Detection and Analysis steps (1.1, 1.2) to identify all other affected hosts, then contain (5) and eradicate (6) the incident for them</td>
<td></td>
</tr>
<tr>
<td>7. Recover from the incident</td>
<td></td>
</tr>
<tr>
<td>7.1 Return affected systems to an operationally ready state</td>
<td></td>
</tr>
<tr>
<td>7.2 Confirm that the affected systems are functioning normally</td>
<td></td>
</tr>
<tr>
<td>7.3 If necessary, implement additional monitoring to look for future related activity</td>
<td></td>
</tr>
<tr>
<td><strong>Post-Incident Activity</strong></td>
<td></td>
</tr>
<tr>
<td>8. Create a follow-up report</td>
<td></td>
</tr>
<tr>
<td>9. Hold a lessons learned meeting (mandatory for major incidents, optional otherwise)</td>
<td></td>
</tr>
</tbody>
</table>
The Center for Internet Security (CIS) critical security controls are the core of the NIST cybersecurity framework.

Source: www.sans.org
Controls 1-5 will eliminate the majority of vulnerabilities.

All 20 controls secure an organization against the most pervasive threats.

1. Inventory of Authorized and Unauthorized Devices
2. Inventory of Authorized and Unauthorized Software
3. Secure Configurations for Hardware and Software
4. Continuous Vulnerability Assessment and Remediation
5. Controlled Use of Administrative Privileges

6. Maintenance, Monitoring, and Analysis of Audit Logs
7. Email and Web Browser Protections
8. Malware Defenses
9. Limitation and Control of Network Ports
10. Data Recovery Capability
11. Secure Configurations for Network Devices
12. Boundary Defense
13. Data Protection
14. Controlled Access Based on the Need to Know
15. Wireless Access Control
16. Account Monitoring and Control
17. Security Skills Assessment & Appropriate Training to Fill Gaps
18. Application Software Security
19. Incident Response and Management
20. Penetration Tests and Red Team Exercises

Source: www.cisssecurity.org
The National Institute of Standards and Technology Cybersecurity Framework (NIST-CSF) serves as a benchmark for coverage across numerous processes.

<table>
<thead>
<tr>
<th>IDENTIFY</th>
<th>PROTECT</th>
<th>DETECT</th>
<th>RESPOND</th>
<th>RECOVER</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Asset management</td>
<td>• Access control</td>
<td>• Anomalies and events</td>
<td>• Response planning</td>
<td>• Recovery planning</td>
</tr>
<tr>
<td>• Business environment</td>
<td>• Awareness and training</td>
<td>• Security continuous monitoring</td>
<td>• Communications</td>
<td>• Improvements</td>
</tr>
<tr>
<td>• Governance</td>
<td>• Data security</td>
<td>• Detection process</td>
<td>• Analysis</td>
<td>• Communications</td>
</tr>
<tr>
<td>• Risk assessment</td>
<td>• Information protection and procedures</td>
<td></td>
<td>• Mitigation</td>
<td></td>
</tr>
<tr>
<td>• Risk management strategy</td>
<td>• Maintenance</td>
<td></td>
<td>• Improvements</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Protective technology</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

NIST-CSF references other frameworks like NIST SP 800-53, COBIT 5, and ISO 27001 for added detail on how to implement specific controls and processes. This allows the NIST-CSF framework to provide a concise but complete evaluation baseline.
Know Who to Contact

- Before you have a situation, know what lawyers you would work with
- Pre-identify computer forensic consultants who can help with an investigation
- Ensure you have a cyber liability policy

**LAW FIRMS BEST AT CYBERSECURITY**

BTI Consulting Group found that seven firms are leading the charge on cybersecurity and privacy issues, according to top legal decision-makers. These firms are proactively reaching out to help prepare clients for future threats.

<table>
<thead>
<tr>
<th>Law Firm</th>
<th>Law Firm</th>
</tr>
</thead>
<tbody>
<tr>
<td>Baker McKenzie</td>
<td>Jones Day</td>
</tr>
<tr>
<td>Dentons</td>
<td>Latham &amp; Watkins</td>
</tr>
<tr>
<td>DLA Piper</td>
<td>Skadden</td>
</tr>
<tr>
<td>Gibson Dunn</td>
<td></td>
</tr>
</tbody>
</table>

**LEADING CYBERSECURITY LAW FIRMS**

Twenty-three additional law firms also stand out for their cybersecurity practices, according to BTI.

<table>
<thead>
<tr>
<th>Law Firm</th>
<th>Law Firm</th>
</tr>
</thead>
<tbody>
<tr>
<td>BakerHostetler</td>
<td>Greenberg Traurig</td>
</tr>
<tr>
<td>Cleary Gottlieb</td>
<td>Hogan Lovells</td>
</tr>
<tr>
<td>Cooley</td>
<td>Hunton &amp; Williams</td>
</tr>
<tr>
<td>Covington</td>
<td>K&amp;L Gates</td>
</tr>
<tr>
<td>Cravath Swaine</td>
<td>Kirkland &amp; Ellis</td>
</tr>
<tr>
<td>Davis Polk</td>
<td>Locke Lord</td>
</tr>
<tr>
<td>Dechert</td>
<td>McGuireWoods</td>
</tr>
<tr>
<td>Fried Frank</td>
<td>Paul Hastings</td>
</tr>
</tbody>
</table>

*As of Feb. 1, Sutherland Asbill & Brennan combined with Eversheds to form Eversheds Sutherland.

Source: BTI Consulting Group
SHALL WE PLAY A GAME?
Cybersecurity Breach Notification Compliance Heat Map
Resources

- Texas DIR

- Fed Guidelines for Incident Handling
  - [https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf](https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf)

- Feeling Strong?
Questions?

Brittany George, CISA, PCI-QSA | Senior Manager, IT Advisory Services
972.448.9299 | brittany.george@weaver.com

Trip Hillman, CISSP, CISA, CEH, GPEN, GCFE, GSNA | Senior Manager, IT Advisory Services
972.448.9276 | trip.hillman@weaver.com