Managing the impact of breaches
Session objectives

1. Share ideas on how to manage business impact for breaches

2. Describe a recommended incident response process
Breaches are inevitable

World's Biggest Data Breaches
Selected losses greater than 30,000 records
(updated 18th May 2015)

- **Anthem**
  Second-largest health insurer in the US
  80,000,000
  Read a bit more

- **JP Morgan Chase**
  76,000,000

- **Target**
  70,000,000

- **Equifax**
  More than 99 percent of affected consumers had their Social Security numbers exposed.

- **NHS 'could have prevented' WannaCry ransomware attack in Ukraine**

- **New Charges in Huge C.I.A. Breach Known as Vault 7**

- **Cyberwarfare with Russia 'now greater threat than terrorism', warns British Army chief**
  ‘We may not have a choice about conflict with Russia,’ says Sir Nick Carter

- **New Snowden documents prove the hacked NSA files are real**

- **Source:** [http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/](http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/)
More breaches

Your enterprise will experience more breaches if you follow these practices


2. Synthetic breaches will increase in volume
1. What is the most important part of a security incident response process?

2. Which functional group is essential to breaches after Security?

Facts
Business impact
Root cause
Corrective action

Lessons Learned

Communications
We use this process for business resiliency, physical security and cyber security.

Incident response is a converged or cross-functional process.

Incident leads facilitate using subject matter experts.

Lessons learned are always harvested.

**Incidents are celebrated!**
Five steps of incident response

This is designed for communication to all stakeholders

If you were a victim of a security breach...what would you want to know?

1. What are the facts?
2. How does it impact me?
3. What went wrong? How did this happen?
4. What are you doing to fix the problem and make me whole?
5. What have you learned to avoid this from happening again?

<table>
<thead>
<tr>
<th>Five Phases</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>1</strong> Understand and Capture Facts</td>
<td>Clear and concise facts about WHAT happened, WHEN it happened, and WHERE it happened.</td>
</tr>
<tr>
<td><strong>2</strong> Business Impact</td>
<td>Defines business(es) impacted for engagement to manage the incident risk.</td>
</tr>
<tr>
<td><strong>3</strong> Identify Root Cause</td>
<td>Root cause or hypothesis of root cause.</td>
</tr>
<tr>
<td><strong>4</strong> Corrective Action</td>
<td>Defines WHAT, WHO and WHEN will be completed to address the incident near term and long term.</td>
</tr>
<tr>
<td><strong>5</strong> Lessons Learned</td>
<td>Defines opportunities to improve the environment in response and preventing future incidents.</td>
</tr>
</tbody>
</table>

One of the most important aspects of cyber-security related incidents is to learn what was compromised and how to identify methods for preventing the incident in the future.
What are examples of synthetic breaches?

1. Conducting a red team review using a specified scenario
2. Doing a pen test
3. Testing key controls
4. Automated scenario testing
We strive to create synthetic incidents using tools to automate the set up and preparation in a continuous way using simulation.

Automation reduces the work effort to set up scenario tests.
Breaches that resulted in significant changes in controls

A cyber security researcher uncovered the exposure of tens of thousands of insurance applications. It was reported as a HIPAA violation to OCR.
Breaches that resulted in significant changes in controls

Our approach

Developed a broker education and communication program

• Enforced the need for laptop encryption-HIPAA implications
• Added education to broker registration process using a pop up window
• Encouraged the encryption laptop check and download of encryption software when necessary
• Addressed the challenges of using cloud infrastructure as a service
• Recommended configuration settings for different cloud providers
• Provided a vulnerability management and incident response support plan
Aetna discovered several hundred devices with unpatched versions of operating systems and no malware protection in a recently acquired company in Thailand. Breaches that resulted in significant changes in controls

Aetna now deploys both endpoint protection software and information protection software that creates a virtual layer for the data, significantly reducing security risk.
Breaches that resulted in significant changes in controls

How many phishing emails make it into your enterprise to end users each day?

10?
100?
1,000?
Type 1 phishing emails eradicated

Type 2 phishing emails eradicated

Type 3 phishing results are misleading since these are actually type 4

This is where the problems are

79% of all phishing emails are type 3/4
Type 3/4 orchestration

- Collect phishing alerts in Splunk
- Review proxy/endpoint logs – how the end user reacted
- Apply an automated script for proxy block and reset of passwords
- Share true positive email results with selected vendors to improve and adjust controls

<table>
<thead>
<tr>
<th>Recipient Action</th>
<th>Supporting Evidence</th>
<th>CTFC Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>No click on link or attachment download.</strong> Yes? Click on link with HTTP traffic only.</td>
<td>No proxy traffic to malicious domain. No traffic within packet capture tool to domain’s IP address. No reply email to attacker. HTTP traffic able to be viewed completely with no credentials entered. Traffic blocked by proxy to malicious domain.</td>
<td>Place proxy block. No password reset required.</td>
</tr>
<tr>
<td><strong>Click on link with HTTPS traffic.</strong></td>
<td>Any HTTPS traffic to the phishing website. (AND) Unable to determine whether user entered credentials.</td>
<td>Place proxy block. Reset account password.</td>
</tr>
<tr>
<td><strong>Click on link, review of traffic determined user entered credentials.</strong></td>
<td>HTTP traffic to phishing website with credentials shown in traffic. (OR) HTTPS traffic to phishing website. (AND) Review of traffic shows a redirect to site that would suggest password was entered. (OR) Reply email to attacker from recipient without blocked traffic.</td>
<td>Place proxy block. Reset account password, open IR.</td>
</tr>
</tbody>
</table>
Different tactics require different controls

Sender

<table>
<thead>
<tr>
<th>Impostor</th>
<th>Authentic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spoof</td>
<td></td>
</tr>
<tr>
<td>Look-Alike Domain</td>
<td></td>
</tr>
<tr>
<td>Display Name Deception</td>
<td></td>
</tr>
<tr>
<td>Compromised Account</td>
<td></td>
</tr>
<tr>
<td>Account Owner</td>
<td></td>
</tr>
</tbody>
</table>

1. DMARC
2. Sinkhole newly registered domains
3. Apply domain attributes to inbound filters
4. Identity Mapping Model
Inbound email protection – Domain attributes

Using email traffic data, the system learns the unique fingerprint of all email senders into your enterprise. This durable **identity trust model** is used to stop all messages that do not prove they should be trusted.

- **29,231** servers sent email for an enterprise on a single day.
- **312** servers for the enterprise.
- **4,641** servers owned by service providers.
- **9,732** benign email forwarders.
- **14,526** malicious senders.
Inbound email protection – Type 3/4

- Identified as a type 3
- Passes DMARC
- Looks legit
Inbound email protection – Identity mapping

**Identity mapping**

Which Identity is perceived to be sending this message?

**Behavioral analytics**

Does this message match the expected behavior for that identity?

**Trust modeling**

How is the perceived Identity related to the recipient?
Inbound email protection - Identity mapping

- **Origin** – Where are messages typical sent from?
  - Servers/IPs
  - 3rd Party Services
  - Device
- **Destination** – Who are messages typical sent to?
  - Number and breadth of recipients
  - Types of recipients
  - Frequency of sending to specific recipients
- **Artifact** – What are the typical elements of the content?
  - Attachment/URL types and characteristics
  - Signature and structure of messages
- **Chronology** – When are messages typically sent?
  - Regularity/Frequency-domain signals
  - Time of day, Day of week/month/year
- **Transmission** – How are messages transmitted?
  - Usage of mailing lists and forwarders
  - Number of servers in delivery path
- **Identification** – Which identity markers are used?
  - Which email addresses/services are used?
  - Which variants of display name, signature, etc.?
Sources of incidents

1. Threat actors
2. Employee mistakes (emails sent to the wrong recipient)
3. Red Team Reviews
4. Crisis Management scenario tests
5. Pen tests
6. Vulnerability services
7. Key control testing

8. Daily risk reviews
9. Third party vulnerability reports
10. Security operations calls
11. Privacy incidents
12. Help desk calls
13. Alerts from models
14. MSP or SOC alerts

CISOs should avoid “delegating” incident response leadership
Daily threat and vulnerability assessment (TVA)

<table>
<thead>
<tr>
<th>TVA Risk Score</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Severe 5.00</td>
<td>Imminent risk of significant business disruption. Business disruption/loss anticipated.</td>
</tr>
<tr>
<td>High 4.00 – 4.99</td>
<td>High risk of business disruption. IRT incident identified and can be contained.</td>
</tr>
<tr>
<td>Elevated 3.00 – 3.99</td>
<td>Moderate risk of business disruption. Identified anomalies in environment.</td>
</tr>
<tr>
<td>Guarded 2.00 – 2.99</td>
<td>General risk of business disruption. Potential threats identified.</td>
</tr>
<tr>
<td>Low 0.00 – 1.99</td>
<td>Low risk of business disruption. No known threats identified.</td>
</tr>
</tbody>
</table>

- **Threats**
- **Vulnerabilities**

- **People**
  - Industry Trends
  - External Events
- **Process**
  - Internal Events
- **Technology**
  - Infrastructure (Client/Server/Network)
  - Applications

- Source Risk Scoring
  - Conducted via daily meeting
  - Input source results scored based on impact, likelihood and control effectiveness.
  - Consensus applied to category risk.

- Daily TVA Report
- 24 Hour Risk Calculation from Category Risk
- Categorized Input Data
- Distribution to Stakeholders

© 2018 Aetna Inc. 22
Enterprise risk score

(Impact + Likelihood)/2 = Inherent Risk * Control Effectiveness = Residual Risk

<table>
<thead>
<tr>
<th>Impact</th>
<th>Likelihood</th>
<th>Control Effectiveness</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical</td>
<td>Almost Certain</td>
<td>Mostly Ineffective</td>
</tr>
<tr>
<td>&gt;$10M loss; &gt;10% market share loss</td>
<td>&gt; 75% chance of occurring.</td>
<td>&lt; 10% of the population</td>
</tr>
<tr>
<td>Loss of executive life</td>
<td>Sophisticated adversary almost certain to initiate.</td>
<td>Rarely Effective</td>
</tr>
<tr>
<td>Severe impact on reputation/brand/member</td>
<td>Error, accident &gt; 49 times a year.</td>
<td>10-20% of the population</td>
</tr>
<tr>
<td>Severe/catastrophic harm to individuals.</td>
<td></td>
<td>Occasionally Effective</td>
</tr>
<tr>
<td>Severe degradation operational performance.</td>
<td></td>
<td>Mostly Effective</td>
</tr>
<tr>
<td>&gt; 7.5% of member accounts affected.</td>
<td></td>
<td>Highly Effective</td>
</tr>
<tr>
<td>High</td>
<td>Probable</td>
<td>Rarely Effective</td>
</tr>
<tr>
<td>$5M - $10M loss; 7-10% market share loss.</td>
<td>50-75% chance of occurring.</td>
<td>10-20% of the population</td>
</tr>
<tr>
<td>Significant impact on reputation/brand/member</td>
<td>Sophisticated adversary highly likely to initiate</td>
<td>21-50% of the population</td>
</tr>
<tr>
<td>Long-term negative media coverage.</td>
<td>Error, accident 24-49 times a year.</td>
<td>Mostly Effective</td>
</tr>
<tr>
<td>Severe/catastrophic harm to individuals.</td>
<td></td>
<td>Highly Effective</td>
</tr>
<tr>
<td>Severe degradation in mission capability.</td>
<td></td>
<td>75% of the population.</td>
</tr>
<tr>
<td>5% of member accounts affected.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Medium</td>
<td>Possible</td>
<td>Occasionally Effective</td>
</tr>
<tr>
<td>$1M - $5M loss.</td>
<td>25-50% chance of occurring.</td>
<td>21-50% of the population</td>
</tr>
<tr>
<td>Some impact on reputation/brand/member</td>
<td>Less sophisticated adversary likely to initiate</td>
<td>Mostly Effective</td>
</tr>
<tr>
<td>National short-term negative media coverage.</td>
<td>Error, accident 12-23 times a year.</td>
<td>Highly Effective</td>
</tr>
<tr>
<td>Significant harm to individuals.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Significant degradation in mission</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2.5% of overall member accounts affected.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Low</td>
<td>Unlikely</td>
<td>Unsophisticated threat actor unlikely to initiate.</td>
</tr>
<tr>
<td>$500k - $1M loss.</td>
<td>&lt;25% chance of occurring.</td>
<td>&lt;10% of the population</td>
</tr>
<tr>
<td>Limited impact on reputation/brand/member.</td>
<td>Unsophisticated threat actor unlikely to initiate.</td>
<td></td>
</tr>
<tr>
<td>Minor harm to individuals.</td>
<td>Error, accident 3-14 times a year.</td>
<td></td>
</tr>
<tr>
<td>Limited impact on operations</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1-2.5% of all member accounts affected.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Very Low</td>
<td>Rare</td>
<td>Unsophisticated threat actor unlikely to initiate.</td>
</tr>
<tr>
<td>&lt;$500k financial loss</td>
<td>&lt;5% chance of occurring.</td>
<td>&lt;1% of the population</td>
</tr>
<tr>
<td>No reputational/brand/member damage.</td>
<td>Unsophisticated threat actor unlikely to initiate.</td>
<td></td>
</tr>
<tr>
<td>Negligible adverse effect on operations.</td>
<td>Error, accident 1-2 times a year.</td>
<td></td>
</tr>
<tr>
<td>&lt;1% of all member accounts affected.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Enterprise risk score

### Event
- **Score**: 2.0
- **Adjusted Score**: 2.02

### Category
- **Score**: 2.21

<table>
<thead>
<tr>
<th>Category</th>
<th>Category Risk Level</th>
<th>Category Score</th>
<th>Adjusted Category Score</th>
<th># Active TVA Metrics</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 - Security Incidents</td>
<td>Guarded</td>
<td>66.40</td>
<td>0.20</td>
<td>42</td>
</tr>
<tr>
<td>2 - Security Operations</td>
<td>Guarded</td>
<td>7.30</td>
<td>0.23</td>
<td>4</td>
</tr>
<tr>
<td>3 - Inside - Out Analysis</td>
<td>Guarded</td>
<td>11.54</td>
<td>0.36</td>
<td>4</td>
</tr>
<tr>
<td>4 - Physical Security</td>
<td>Guarded</td>
<td>4.00</td>
<td>0.25</td>
<td>2</td>
</tr>
<tr>
<td>5 - External Trends</td>
<td>Guarded</td>
<td>15.75</td>
<td>0.18</td>
<td>11</td>
</tr>
<tr>
<td>6 - Infrastructure</td>
<td>Guarded</td>
<td>30.90</td>
<td>0.35</td>
<td>11</td>
</tr>
<tr>
<td>7 - Applications</td>
<td>Guarded</td>
<td>7.07</td>
<td>0.18</td>
<td>5</td>
</tr>
<tr>
<td>8 - Internal Composite</td>
<td>Guarded</td>
<td>24.51</td>
<td>0.28</td>
<td>11</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>167.46</strong></td>
<td><strong>2.02</strong></td>
<td><strong>90.00</strong></td>
</tr>
</tbody>
</table>

- **Daily Risk Score** is the summation of all Adjusted Category Scores.
- **Adjusted Category Score** = (Category Score / # Active TVA Metrics) / # of Categories
Questions?

routhj@aetna.com
781-943-1140

Slides available – contact Jennifer Santiago