The Threat Within: Corporate Ally or Corporate Enemy

Damon Stokes, Senior Manager, Security Governance
Blue Cross Blue Shield of Michigan
Why the focus on Insider Threat

• Last year the ‘Insider Threat’ eclipsed external threats as the top Cyber Security concern
• Breaches can directly influence the brand reputation
• Undetectable exfiltration tactics
Notable Incidents

• Sony
• Government (Snowden, WikiLeaks, etc)
• Morgan Stanley
• BCBSM
Evolution of Security
Evolution of Security

Initial focus was based on protecting from the outside-in
Evolution of Security

• As external threats began to become more frequent and sophisticated, spending priorities were continuously allocated to external mitigation strategies

• The unintended consequences of this approach netted being hard on the outside, but soft in the middle
Net result of security industry’s investment focus

Company Data

Interior controls

Exterior controls
Evolution of Security (cont)

Legacy IT was very operational focused and lacked a defined strategy to address internal security. Examples of this were exhibited with:

- Shared administrative passwords
- Weak passwords (accounts, applications, devices)
- Lack of system hardening (services, capabilities)
- Hyper-elevated individual user account authorization
The Insider Threat
# The Insider Threat

<table>
<thead>
<tr>
<th>Threat Type</th>
<th>Profile</th>
<th>Net Result</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malicious</td>
<td>Current or former employees/contractors deliberately misuses data in a manner that affects the security of an organizations’ data, systems, or daily business operations</td>
<td>Financial &amp; Personal Gain, Espionage or Revenge</td>
</tr>
<tr>
<td>Accidental</td>
<td>Current employees/contractors that improperly handled computer equipment and/or corporate data that affects the security of an organization</td>
<td>Emails or faxes sent to the incorrect destinations. Lost/ stolen laptops, tablets, and smart phones devices</td>
</tr>
</tbody>
</table>
The Insider Threat (Non Malicious)

- 75% of programmers use hacking tools not required for their job
- 93% of employees had sensitive data in both the cloud and on unencrypted USB
- 75% of employees use pirated applications and media
- 82% of employees exploit misconfigured web filters or blocked sites
- 14% use torrent applications to share applications/media
- 21% of employees use unapproved methods of encryption

Source: Insider Threat Study - Dawn Cappelli & Andrew Moore
The Insider Threat (Malicious)

- Responsible for 43% of all malicious attacks (internal and external)*
- 32% of employees have admitted to stealing confidential corporate information on at least one occasion*
- 31% of employees said that they would retaliate to a dismissal by deliberately stealing and/or sharing sensitive corporate data*
- Many healthcare breaches still go unreported. Breaches involving the health records of fewer than 500 individuals are not required to be publicly reported. Theft accounts for 83 percent of all large HIPAA privacy and security breaches.**

Source: *Inforworld, **HealthCare IT News,
Case Studies

➤ **Programmer Adds Code To Shut Down System**

A 30 year contract programmer at a software firm inserted code that made the systems permanently power down after a random number of restarts. When it was discovered, he was confronted about it by investigators. He stated that he had a side business and was using this opportunity to ‘come and save the day’ while earning extra income.

*Lesson Learned: Peer Code Review*

➤ **Financial Engineer Steals Company’s Trading Algorithms:**

A hedge fund financial engineer stole the companies trading algorithms, despite very tight controls around that intellectual property. He managed to bypass those controls by using two virtual machines and eventually sending the information to his personal email account and to an external hard drive. He was discovered only due to additional controls IT had installed that allowed them to notice this employee had unusually large numbers of files on his system.

*Lesson Learned: Host based controls*
Case Studies (cont)

➢ Use of File Sharing Site

Three employees at a law firm configured Dropbox to be the firm’s primary internal file sharing platform. Before quitting these employees transferred approximately 78,000 documents from their current firm to their new one. They subsequently modified confidential client information on those files and sent them back to the original employer’s document repository.

Lesson Learned: Restrict use of external file sharing sites

➢ Use of Smart Phone Cameras

From 2012 to 2014 a healthcare employees used a camera phone to take screenshots of more than 5,000 subscribers’ PHI. The stolen information was used to obtain fraudulent credit cards and purchase more than $500,000 worth of merchandise.

Lesson Learned: Create personal and corporate mobile device standards
Wrong Email Recipient

An employee at a Fortune 500 organization was working late into the night to finish the quarterly forecast. The spreadsheet she was working on contained very sensitive and proprietary information on the organization’s forecasts for production, shipping, and supplier pricing. When finished she sent to her boss; so she thought. The next morning she received an email from a very large trade magazine that said “Thank you, looks like a lot of work went into this.” The employee then realized her email client had auto-completed the writer’s address by mistake.

Other Examples of Accidental Insider Threat

- Posting sensitive data on public websites
- Clicking on suspicious link in emails
- Using ‘found’ USB drive
- Losing paper records
- Losing laptops, tablets
- Losing portable storage device (USB drive, CD)
The Insider Threat  

( cont )

<table>
<thead>
<tr>
<th></th>
<th>Situation</th>
<th>Complications</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Industry threat data suggests that the insider threat is now the greatest information security risk to organizations</td>
<td>Monitoring and controlling the activities of “trusted” insiders presents serious technical and cultural challenges</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Systems and implemented controls do not provide the visibility today to assess and manage the insider risk</td>
</tr>
<tr>
<td></td>
<td></td>
<td>The scope of the data and systems organization must protect is large and monitoring and controlling all potential insider risk is impractical</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>3</th>
<th>Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>What systems and processes are the most sensitive and present the greatest opportunity for insider threat actions</td>
</tr>
<tr>
<td></td>
<td>What steps can your organization take to protect against the risk of insider threat?</td>
</tr>
<tr>
<td></td>
<td>What initiatives can your organization take in the short, mid and long term to begin to implement processes and controls to mitigate the insider threat risk?</td>
</tr>
<tr>
<td></td>
<td>What residual risk remains that we are willing to accept?</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>4</th>
<th>On-going Strategy</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Create a multi-year strategy and roadmap that focuses on addressing the highest insider risks to your organization.</td>
</tr>
<tr>
<td></td>
<td>Prototype and implement practical short term controls to address the highest risk</td>
</tr>
<tr>
<td></td>
<td>Develop concepts and plans for mid and long term improvements and position for future year planning and budget</td>
</tr>
</tbody>
</table>

© 2016 HITRUST Alliance.
The Insider Threat Countermeasures
Insider Threat Countermeasures

**Education / Awareness:**
Promoting Insider Threat awareness training that educates employees/contractors of what is considered insider crimes, the consequence, and their responsibility to report.

- Training & awareness events
- Procedure for reporting suspected incidents

**Accountability:**
Holding employees/contractors responsible for their actions that jeopardize the confidentiality, integrity and availability of your organization’s data.

- Policies/procedures
- Security Agreements

**Audit Logging:**
Enabling electronic logs on high risk system to provide documentary evidence of the sequence of activities that have affected a record at any specific time an operation, procedure, or event occurred.

- Applications and network logs
- SIEM or other log analysis

**Detection / Prevention:**
Implementing controls that identify, alert, prevent and report real time activities that pose a risk to your organization’s data.

- IDS/IPS
- Managed Security policies and configurations

**Active Monitoring:**
Implementing security solutions to detect and report the insider attack before meaningful business impact is accomplished.

- UBA Tools
- Information Security Compliance Checklist standards
Using HITRUST to aid with Insider Threat Mitigation Strategies
B-Secure, *A Desk Assessment Program*

Designed to implement and measure the necessary operational controls to protect information assets at facilities and to educate the workforce on security awareness, polices, and procedures. Employees will learn:

- Security awareness and the personal value of it
- Secure workspace practices
- Secure data practices
- Confidential/critical data taxonomy
- How to protect company assets
B-Secure (cont.)

Assessments occur after business hours and examine the following:

- Desktop Computer Logged On
- Unsecured Mobile Devices (laptops, phones, etc)
- Password Found
- Open PHI/PII/ Confidential
- Media Found
- Trash/Rec. Bin (PHI/PII/Confidential Info)
- Printers (Documents)
Related HITRUST Controls

01.h Clear Desk and Clear Screen Policy
02.a Roles and Responsibilities
02.e Information Security Awareness, Education and Training
06.g Compliance with Security Policies and Standards
07.a Inventory of Assets
07.c Acceptable Use of Assets
07.d Information Labeling and Handling
08.c Securing Offices, Rooms, and Facilities
08.I Secure Disposal or Re-Use of Equipment
09.o Management of Removable Media
09.p Disposal of Media
09.q Information Handling Procedures
09.u Physical Media in Transit
11.a Reporting Information Security Events
The Threat Within: Corporate Ally or Corporate Enemy

Damon Stokes, dstokes2@bcbsm.com