Agenda

- Environment
- Assessment Overview
- Risk and Issue Score
- Issue Review
- Next Steps
Environment

<table>
<thead>
<tr>
<th>NETWORK ASSESSMENT (changes)</th>
<th># Enabled Users</th>
<th># Disabled Users</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain Controllers</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>Number of Organizational Units</td>
<td>20</td>
<td></td>
</tr>
<tr>
<td><strong>Users</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td># Enabled</td>
<td>59</td>
<td></td>
</tr>
<tr>
<td>Last Login within 30 days</td>
<td>23</td>
<td></td>
</tr>
<tr>
<td>Last Login older than 30 days</td>
<td>36</td>
<td></td>
</tr>
<tr>
<td># Disabled</td>
<td>39</td>
<td></td>
</tr>
<tr>
<td>Last Login within 30 days</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Last Login older than 30 days</td>
<td>38</td>
<td></td>
</tr>
<tr>
<td><strong>Security Group</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Groups with Users</td>
<td>50</td>
<td></td>
</tr>
<tr>
<td># Total Groups</td>
<td>106</td>
<td></td>
</tr>
<tr>
<td><strong>Computers in Domain</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Total Computers</td>
<td>88</td>
<td></td>
</tr>
<tr>
<td>Last Login within 30 days</td>
<td>58</td>
<td></td>
</tr>
<tr>
<td>Last Login older than 30 days</td>
<td>30</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th># Enabled Users</th>
<th># Disabled Users</th>
</tr>
</thead>
<tbody>
<tr>
<td>Employee - ePHI authorization</td>
<td>111</td>
<td>0</td>
</tr>
<tr>
<td>Employee - no ePHI authorization</td>
<td>2</td>
<td>0</td>
</tr>
<tr>
<td>Vendor - ePHI authorization</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Vendor - no ePHI authorization</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Former Employee</td>
<td>5</td>
<td>0</td>
</tr>
<tr>
<td>Former Vendor</td>
<td>3</td>
<td>0</td>
</tr>
</tbody>
</table>

Operating System Support

[Chart showing supported and unsupported operating systems with percentages]
Assessment Overview

The following areas were assessed. Potential issues were found in the areas highlighted in RED.

Environment
- Facility Access Controls

Users
- Information System Activity Review
- Termination Procedures
- Access Authorization
- Existing Security Measures Related to Access Controls
- Password Management
- Administrative Access Control
- Audit Controls
- Person or Entity Authentication

Servers and Local Computers
- Protection Against Malicious Software
- Applications and Data Criticality Analysis
- Business Associate Agreements

Firewall
- Access Authorization
- Protection Against Malicious Software

Email
- Applications and Data Criticality Analysis
Risk and Issue Score

Current Risk Score

High Risk

97

Low Risk

Current Issue Score

Current (1792)

448  896  1344  1792  2240
Unsupported Operating Systems (97 pts)

**Issue:** 2 computers were found using an operating system that is no longer supported. Unsupported operating systems no longer receive vital security patches and present an inherent risk.

**Recommendation:** Upgrade or replace computers with operating systems that are no longer supported.
User has not logged in in 30 days (13 pts)

**Issue:** Users that have not logged in in 30 days could be from a former employee or vendor and should be disabled or removed.

**Recommendation:** Disable or remove user accounts for users that have not logged in in 30 days.
User password set to never expire (80 pts)

**Issue:** User accounts with passwords set to never expire present a risk of use by authorized users. They are more easily compromised than passwords that are routinely changed.  

**Recommendation:** Investigate all accounts with passwords set to never expire and configure them to expire regularly.
Non-administrative generic logons have access to Network Share on system with ePHI (85 pts)

**Issue:** Generic accounts which could be in use by multiple people cannot be properly restricted and should not have access to network shares with ePHI.

**Recommendation:** Remove access to Network Shares on systems with ePHI.
**Issue Review**

**Automatic screen lock not turned on. (94 pts)**

**Issue:** Automatic screen lock prevents unauthorized access when users leave their computers. Having no screen lock enable allows authorized access to network resources.

**Recommendation:** Enable automatic screen lock on the following computers: BO-SANDBOX, CONFERENCE_ROOM, DC03, DEVKASEYA, DEVTS, DEV_2012-CORE, Ehammond-WIN7, FILE2012-1, HV01, HV02, HV03, jacob-WIN8, KjacobsASUSPC, MARKETING-1, Mmayhemon-HP, Mwest-WIN864, PITmarcus-PC, Psimpson-PC, Psimpson-WIN764, REX, SQL2012-01, Thayden-DT
**Issue Review**

*Computer with ePHI does not have object level auditing on (11 pts)*

**Issue:** Object level auditing helps identify users who have accessed files and other system resources. Object level auditing may impose an unacceptable performance impact and should be considered for use on high risk computers or environments.

**Recommendation:** Evaluate the pros and cons of enabling object level access or ensure alternative methods for breach identification are in place.
Passwords less than 6 characters allowed (75 pts)

Issue: Passwords are not required to be 6 or more characters, allowing users to pick extremely short passwords which are vulnerable to brute force attacks.

Recommendation: Enable enforcement of password length to 6 more characters.
Audit user login in not turned on (30 pts)

**Issue:** Login auditing is required for proper identification of access to computers and resources. In the event of a breach, audit logs can be used to identify unauthorized access and the severity of the breach.

**Recommendation:** Enable user login auditing.
Anti-virus not installed (94 pts)

**Issue:** Malware protection is required but not identified as being installed on computers in the network.

**Recommendation:** Install a commercial grade anti-virus program on the computers indicated in the Endpoint Security section of the Evidence of HIPAA Compliance report.
**Issue Review**

**Anti-virus not turned on (92 pts)**

**Issue:** Malware protection is required but not identified as being enabled on computers in the network.

**Recommendation:** Enable anti-virus program on the computers indicated in the Endpoint Security section of the Evidence of HIPAA Compliance report.
Anti-spyware not installed (94 pts)

**Issue:** Malware protection is required but not identified as being installed on computers in the network.

**Recommendation:** Install a commercial grade anti-spyware program on the computers indicated in the Endpoint Security section of the Evidence of HIPAA Compliance report.
Anti-spyware not turned on (92 pts)

**Issue:** Malware protection is required but not identified as being enabled on computers in the network.

**Recommendation:** Enable anti-spyware program on the computers indicated in the Endpoint Security section of the Evidence of HIPAA Compliance report.
Anti-spyware not up to date (90 pts)

**Issue:** Out-of-date definitions may not properly protect a computer from attacks by malicious software.

**Recommendation:** Ensure anti-spyware programs on the computers indicated in the Endpoint Security section of the Evidence of HIPAA Compliance report are up-to-date.
**Issue Review**

**USB drives detected in use (unencrypted) (75 pts)**

**Issue:** Theft is the most common form of data breach. Unencrypted USB drives in an environment with ePHI may allow data loss through theft.

**Recommendation:** Eliminate the use of unencrypted USB drives.
**USB drives detected in use (50 pts)**

**Issue:** The use of USB drives increase the change of data loss through theft and should be discouraged to the extent possible.

**Recommendation:** Reduce or eliminate the use of USB drives in the environment.
Workstations with ePHI not backed up (78 pts)

**Issue:** Security Center reports that computers identified as having ePHI are not backed up.

**Recommendation:** Ensure that data is properly backed up on computers with ePHI. See the Endpoint Security section of the Evidence of HIPAA Compliance for a list of computers.
Inconsistent password policy / Exceptions to password policy (68 pts)

**Issue:** Password policies are not consistently applied from one computer to the next. A consistent password policy ensure adherence to password best practices.

**Recommendation:** Eliminate inconsistencies and exceptions to the password policy.
Potential free hosted web-based email solution in use (93 pts)

**Issue:** The use of free hosted web-based email may allow transmission of ePHI outside of the company through entities that you may not have a signed Business Associate agreement.

**Recommendation:** Identify the necessity of using the free hosted email services and discontinue their use.
Company WiFi open or using insecure security (i.e., WEP) (94 pts)

*Issue:* Open or insecure WiFi protocols may allow an attacker access to the company’s network and resources.

*Recommendation:* Enabled WiFi security and use a more secure protocols such as WPA2.
**Terminated employee account enabled (96 pts)**

**Issue:** One or more accounts are still enabled for terminated employees. This poses a risk of unauthorized access.

**Recommendation:** Disable accounts for all terminated employees.
**Terminated vendor account enabled (96 pts)**

**Issue:** One or more accounts are still enabled for terminated vendors. This poses a risk of unauthorized access.

**Recommendation:** Disable accounts for all terminated vendors.
User not logged in in 90 days (not terminated) (25 pts)

**Issue:** Inactive user accounts were found that could potentially indicate terminated employees or vendors.

**Recommendation:** Investigate all inactive accounts and disable accounts from terminated employees and vendors.
Unrestricted network share with ePHI (80 pts)

**Issue:** Network shares containing ePHI were found as completely unrestricted (granting access to 'Everyone').

**Recommendation:** Investigate the network shares containing ePHI with unrestricted access. Limit access to the minimum necessary.
LOTS of Security patches missing on computers with ePHI (90 pts)

**Issue:** Security patches are missing on computers designated as having ePHI. Maintaining proper security patch levels is required by HIPAA to prevent unauthorized access and the spread of malicious software. Lots is defined as missing 3 or more patches and may be an indicator of issues with the patching system.

**Recommendation:** Address patching on computers with missing security patches.
Next Steps

- Agree on List of Issues to Resolve
- Present Project Estimates and Costs
- Establish Timelines
- Set Milestones
- Get Signoff to Begin Work