HIPAA Assessment

Prepared For:

My Client's Company

Prepared By

Your Company

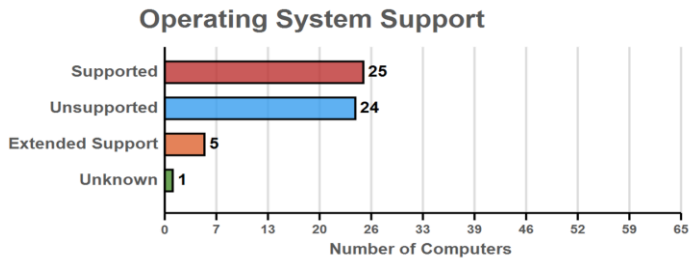
Agenda

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

Environment

Domain	
Domain Controllers	4
Number of Organizational Units	13
Users	
# Enabled	46
Last Login within 30 days	24
Last Login older than 30 days	22
# Disabled	28
Last Login within 30 days	0
Last Login older than 30 days	28
Security Group	
Groups with Users	31
# Total Groups	60
Computers in Domain	
Total Computers	155
Last Login within 30 days	54
Last Login older than 30 days	101

	# Enabled Users	# Disabled Users
Employee - ePHI authorization	3	0
Employee - no ePHI authorization	35	0
Vendor - ePHI authorization	0	0
Vendor - no ePHI authorization	1	0
Former Employee	0	0
Former Vendor	0	0



Assessment Overview

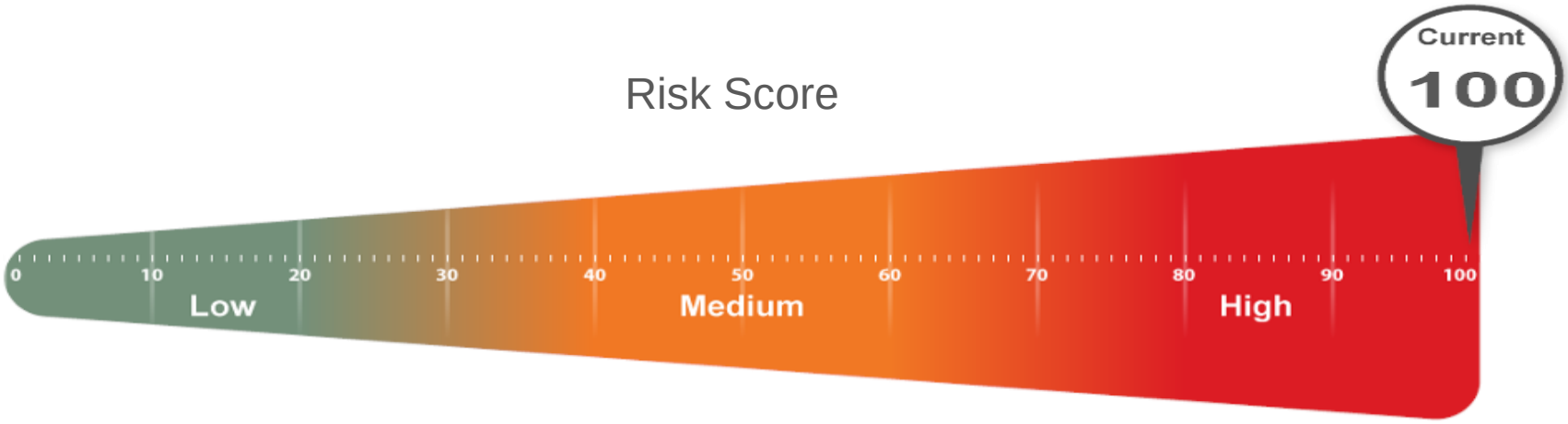
The following areas were assessed. Potential issues were found in the areas highlighted in **RED**.

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

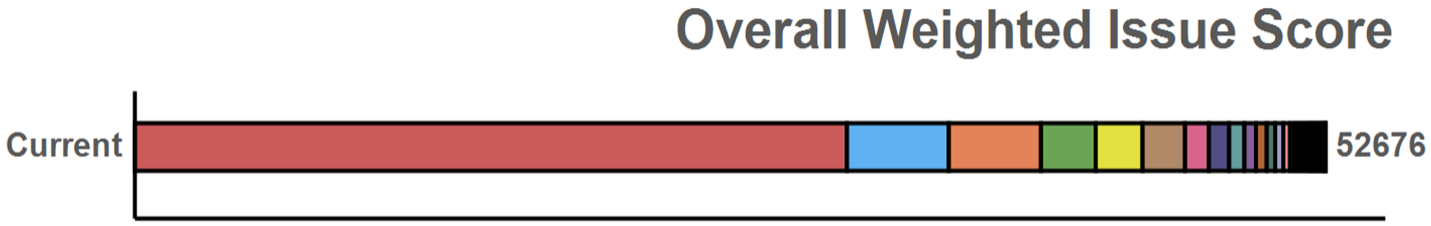
Servers and Local Computers
-Protection Against Malicious Software
-Environment
-Business Associate Agreements
Firewall
-Access Authorization
-Protection Against Malicious Software

Risk and Issue Score

Risk Score



Issue Score



Issue Review

Business Associate won't sign agreement for eFax Receiving Service (100 pts)

Issue: eFax receiving services may advertently or inadvertently be used to transmit ePHI and should sign Business Associate agreements.

Recommendation: Acquire Business Associate agreement from the company providing the eFax Receiving Service.

Issue Review

Business Associate won't sign agreement for eFax Sending Service. (100 pts)

Issue: eFax sending services may advertently or inadvertently be used to transmit ePHI and should sign Business Associate agreements.

Recommendation: Acquire Business Associate agreement from the company providing the eFax Sending Service.

Issue Review

Unsupported operating systems (97 pts)
Issue: 24 computers Computers 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.

Issue Review

Critical External Vulnerabilities Detected (95 pts)
Issue: Critical external vulnerabilities may potentially allow malicious attacks from outside your network and should be addressed as soon as possible. External vulnerabilities are considered potential security holes that can allow hackers access to your network and information.
Recommendation: Assess the risk of each vulnerability and remediate all external vulnerabilities as prescribed.

Issue Review

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.

Issue Review

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 protocol such as WPA2.

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 enabled allows unauthorized access to network resources.
Recommendation: Enable automatic screen lock on the specified computers.

Issue Review

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

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.

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.~~
Exception Explanation: See Security Exception Worksheet

Issue Review

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.~~
Exception Explanation: See Security Exception Worksheet

Issue Review

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.~~
Exception Explanation: See Security Exception Worksheet

Issue Review

Lots of Security patches missing on computers (90 pts)
Issue: Security patches are missing, 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 missing 4+ security patches.

Issue Review

Anti-virus 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-virus programs on the computers indicated in the Endpoint Security section of the Evidence of HIPAA Compliance report are up-to-date.~~
Exception Explanation: See Security Exception Worksheet

Issue Review

Firewall does not support IPS (88 pts)
Issue: Firewalls without an Intrusion Prevention System (IPS) may not adequately protect the environment against malicious external attacks.
Recommendation: Enable IPS on firewalls or investigate putting in place a firewall with IPS capabilities.

Issue Review

User marked as not requiring ePHI login detected on computer containing ePHI (87 pts)

Issue: One more users who are marked as not requiring ePHI have been detected as attempting to or logging into a system that contains ePHI.

Recommendation: Access by users marked as not requiring ePHI who have attempted to or successfully logged into a computer with ePHI should be investigated to see if a breach has occurred.

Issue Review

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

User marked as not requiring ePHI has access to network share with ePHI (85 pts)
Issue: Network shares that contain ePHI should not allow read or write permissions to users that are marked as not having ePHI access.
Recommendation: Remove access to network shares identified as having ePHI from users marked as not requiring ePHI access.

Issue Review

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.

Issue Review

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.

Issue Review

Account lockout disabled (77 pts)
Issue: Account lockout (disabling an account after a number of failed attempts) significantly reduces the risk of an attacker acquiring a password through a brute force attack.
Recommendation: Enable account lockout for all users.

Issue Review

Password complexity not enabled (75 pts)
Issue: Enforcing password complexity limits the ability of an attacker to acquire a password through brute force.
Recommendation: Enable password complexity to assure that network user account passwords are secure.

Issue Review

Passwords less than 8 characters allowed (75 pts)
Issue: Passwords are not required to be 8 or more characters, allowing users to pick extremely short passwords which are vulnerable to brute force attacks.
Recommendation: Enable enforcement of password length to more than 8 characters.

Issue Review

Medium External Vulnerabilities Detected (75 pts)
Issue: Medium severity external vulnerabilities may potentially allow malicious attacks from outside your network and should be addressed as soon as possible. External vulnerabilities are considered potential security holes that can allow hackers access to your network and information.
Recommendation: Assess the risk of each vulnerability and remediate all external vulnerabilities as prescribed.

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.

Issue Review

Password history not remembered for at least six passwords (72 pts)

Issue: Short password histories allow users to rotate through a known set of passwords, thus reducing the effectiveness of a good password management policy.

Recommendation: Increase password history to remember at least six passwords.

Issue Review

Remote Access Cloud Services could potentially expose ePHI either visually or through data transmission. (~~65 pts~~)
Issue: Remote Access Cloud Services are in use and may pose potential ePHI risk.
Recommendation: ~~It is recommended to not use third-party remote access services on systems that could potentially display or access ePHI.~~
Exception Explanation: See Security Exception Worksheet

Issue Review

USB drives detected in use (50 pts)
Issue: The use of USB drives increases the chance 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.

Issue Review

Significantly high number of Domain Administrators (35 pts)
Issue: More than 30% of the users are in the Domain Administrator group and have unfettered access to files and system resources. Compromised Domain Administrator accounts pose a higher threat than typical users and may lead to a breach.
Recommendation: Evaluate the need to have more than 30% of users in the Domain Administrator group and limit administrative access to the minimum necessary.

Issue Review

User password set to never expire (30 pts)
Issue: User accounts with passwords set to never expire present a risk of use by unauthorized 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.

Issue Review

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.

Issue Review

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: Disable or remove user accounts for users that have not logged on to active directory in 90 days.

Issue Review

Firewall does not have malware filtering (14 pts)
Issue: Firewall malware filtering is recommended for increase protection against malicious software.
Recommendation: Enable malware filtering on firewalls or investigate putting in place a firewall with malware filtering services.

Issue Review

User has not logged on to domain in 30 days (13 pts)
Issue: Users have not logged on to domain in 30 days. A user that has not logged in for an extended period of time could be a former employee or vendor.
Recommendation: Disable or remove user accounts for users that have not logged on to active directory in 30 days.

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.

Issue Review

Use of generic logins (1 pts)
Issue: While not inherently a risk, the use of generic logins (logins used by more than one person or anonymous individuals) should be discouraged.
Recommendation: Evaluate the necessity of generic logins and reduce their use when possible.

Next Steps

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