AMS NETWORKS
AGILE | MODERN | SECURE

Technical Review

Technical Risk Analysis

Table of Contents

Technical Risk Analysis Overview

The Technical Risk Analysis aggregates risk analysis from multiple assessments performed on the network, providing you with a high-level overview of the health and security of the network.

The report details the scan tasks undertaken to discover security issues. In addition to the overall Risk Score, the report also presents separate risk scores for all IT assessments (Network, Security) performed on the network environment. This includes a summary of individual issues, as well as their severity and weighting within the risk analysis.

At the end of the report, you can find a summary of the assets discovered on the network, in addition to other useful information organized by assessment type.

Risk analysis and risk management are not one-time activities. Risk analysis and risk management are dynamic processes that must be periodically reviewed and updated in response to changes in the environment. The risk analysis will identify new risks or update existing risk levels resulting from environmental or operational changes. The output of the updated risk analysis will be an input to the risk management process to reduce newly identified or updated risk levels to reasonable and appropriate levels.

Technical Risk Analysis Discovery Tasks

The following discovery tasks were performed.

	TASK	DESCRIPTION
Network		
✓	Detect Domain Controllers	Identifies domain controllers and online status.
✓	FSMO Role Analysis	Enumerates FSMO roles at the site.
✓	Enumerate Organization Units and Security Groups	Lists the organizational units and security groups (with members).
✓	User Analysis	Lists the users in AD, status, and last login/use, which helps identify potential security risks.
✓	Detect Local Mail Servers	Detects mail server(s) on the network.
✓	Detect Time Servers	Detects server(s) on the network.
✓	Discover Network Shares	Discovers the network shares by server.
✓	Detect Major Applications	Detects all major apps / versions and counts the number of installations.
✓	Detailed Domain Controller Event Log Analysis	Lists the event log entries from the past 24 hours for the directory service, DNS server and file replication service event logs.
✓	Web Server Discovery and Identification	Lists the web servers and type.
✓	Network Discovery for Non-A/D Devices	Lists the non-Active Directory devices responding to network requests.
✓	Internet Access and Speed Test	Tests Internet access and performance.
✓	SQL Server Analysis	Lists the SQL Servers and associated database(s).
✗	Internet Domain Analysis	Queries company domain(s) via a WHOIS lookup.
✓	Missing Security Updates	Identifies computers missing security updates.
✓	System by System Event Log Analysis	Discovers the five system and app event log errors for servers.
Security		

	TASK	DESCRIPTION
✓	Detect System Protocol Leakage	Detects outbound protocols that should not be allowed.
✓	Detect Unrestricted Protocols	Detects system controls for protocols that should be allowed but restricted.
✓	Detect User Controls	Determines if controls are in place for user web browsing.
✘	Detect Wireless Access	Detects and determines if wireless networks are available and secured.
✓	External Security Vulnerabilities	Performs a detailed External Vulnerability Scan. Lists and categorizes external security threats.
✓	Network Share Permissions	Documents access to file system shares.
✓	Domain Security Policy	Documents domain computer and domain controller security policies.
✓	Local Security Policy	Documents and assesses consistency of local security policies.

Risk Score

The Risk Score is a value from 0 to 100, where 100 represents significant risk and potential issues. The score is risk associated with the highest risk issue.

Several critical issues were identified. Identified issues should be investigated and addressed according to the Technical Risk Analysis.

ISSUE TYPE	RISK SCORE
Network	
Security	
Data Security	

Issue Graph

This section contains a summary of issues detected during the Technical Review process, and is based on industry-wide best practices for network health, performance, and security. The Overall Issue Score grades the level of issues in the environment. An Overall Issue score of zero (0) means no issues were detected in the environment. It may not always be possible to achieve a zero score in all environments due to specific circumstances.

Issue Graph

Weighted Score: Risk Score x Number of Incidents = Total points: Total percent (%)

Network Issue Graph

Security Issue Graph

Data Security Issue Graph

Issue Summary

Network Issue Summary

770 Significantly high number of Domain Administrators (35 pts each)

Current Score: 35 pts x 22 = 770: 27.27%

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.

600 User password set to never expire (30 pts each)

Current Score: 30 pts x 20 = 600: 21.25%

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.

375 Few Security patches missing on computers. (75 pts each)

Current Score: 75 pts x 5 = 375: 11.97%

Issue: Security patches are missing on computers. Maintaining proper security patch levels helps prevent unauthorized access and the spread of malicious software. Few is defined as missing 3 or less patches.

Recommendation: Address patching on computers missing 1-3 security patches.

299 User has not logged on to domain in 30 days (13 pts each)

Current Score: 13 pts x 23 = 299: 10.59%

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.

194 Unsupported operating systems (97 pts each)

Current Score: 97 pts x 2 = 194: 6.87%

Issue: 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.

180 Inactive computers (15 pts each)

Current Score: 15 pts x 12 = 180: 6.37%

Issue: Computers have not checked in during the past 30 days

Recommendation: Investigate the list of inactive computers and determine if they should be removed from Active Directory, rejoined to the network, logged into by authorized users, or powered on.

180 Anti-virus not up to date (90 pts each)

Current Score: 90 pts x 2 = 180: 6.37%

Issue: Up to date anti-virus definitions are required to properly prevent the spread of malicious software. Some anti-virus definitions were found to not be up to date.

Recommendation: Ensure anti-virus definitions are up to date on specified computers.

180 Anti-spyware not up to date (90 pts each)

Current Score: 90 pts x 2 = 180: 6.37%

Issue: Up to date anti-spyware definitions are required to properly prevent the spread of malicious software. Some anti-spyware definitions were found to not be up to date.

Recommendation: Ensure anti-spyware definitions are up to date on specified computers.

136 **Potential disk space issue (68 pts each)**

Current Score: 68 pts x 2 = 136: 4.82%

Issue: 2 computers were found with significantly low free disk space.

Recommendation: Free or add additional disk space for the specified drives.

60 **Operating system in Extended Support (20 pts each)**

Current Score: 20 pts x 3 = 60: 2.12%

Issue: Computers are using an operating system that is in Extended Support. Extended Support is a warning period before an operating system is no longer supported by the manufacturer and will no longer receive support or patches.

Recommendation: Upgrade computers that have operating systems in Extended Support before end of life.

Security Issue Summary

872 **Automatic screen lock not turned on (72 pts each)**

Current Score: 72 pts x 12 = 872: 95.61%

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.

77 **Account lockout is not enabled for some computers. (77 pts each)**

Current Score: 77 pts x 1 = 77: 2.22%

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.

95 Critical External Vulnerabilities Detected (95 pts each)

Current Score: 95 pts x 1 = 95: 9.06%

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.

Data Security Issue Summary

9396 User marked as not "Not Authorized" detected on computer containing ePHI (87 pts each)

Current Score: 87 pts x 108 = 9396: 51.70%

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

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

8778 User marked as not "Not Authorized" detected on computer containing PII (87 pts each)

Current Score: 87 pts x 101 = 8778: 48.30%

Issue: One or more users who are marked as "Not Authorized" have been detected as attempting to or logging into a system that contains PII.

Recommendation: Access by users marked as "Not Authorized" who have attempted to or successfully logged into a computer with PII should be investigated to see if a breach has occurred.

468 Computer with PII not backed up (78 pts each)

Current Score: 78 pts x 6 = 468: 2.58%

Issue: Computers identified as having PII are documented as not having a backup agent installed.

Recommendation: Ensure that data is properly backed up on computers with PII. See the Asset Inventory Worksheet for a list of computers that are documented as not having a backup agent installed.

450 Computer storing PII does not use disk encryption (75 pts each)

Current Score: 75 pts x 6 = 450: 2.48%

Issue: Theft is the most common form of data breach. Unencrypted computer drives storing PII may allow data loss through theft.

Recommendation: Implement disk encryption on computers storing PII.

444 Former Third Parties with Enabled Accounts (74 pts each)

Current Score: 74 pts x 6 = 444: 2.44%

Issue: Terminated third parties should have their accounts disabled to prevent potential unauthorized access to Personal Data. The following active accounts designated as former third parties were identified. These accounts should be disabled or removed.

Recommendation: Disable or remove accounts for third parties.

400 PII on computer not authorized to store data (80 pts each)

Current Score: 80 pts x 5 = 400: 2.2%

Issue: PII data has been detected as stored on a computer not authorized to store PII.

Recommendation: Investigate the unauthorized computers storing PII. PII should be stored on computers in accordance with organization policy.

312 Computer with ePHI not backed up (78 pts each)

Current Score: 78 pts x 4 = 312: 1.72%

Issue: Computers identified as having ePHI are documented as not having a backup agent installed.

Recommendation: Ensure that data is properly backed up on computers with ePHI. See the Asset Inventory Worksheet for a list of computers that are documented as not having a backup agent installed.

300 Computer storing ePHI does not use disk encryption (75 pts each)

Current Score: 75 pts x 4 = 300: 1.65%

Issue: Theft is the most common form of data breach. Unencrypted computer drives storing ePHI may allow data loss through theft.

Recommendation: Implement disk encryption on computers storing ePHI.

261 User marked as not "Not Authorized" detected on computer containing PCI Cardholder Data (87 pts each)

Current Score: 87 pts x 3 = 261: 1.44%

Issue: One or more users who are marked as "Not Authorized" have been detected as attempting to or logging into a system that contains PCI Cardholder Data.

Recommendation: Access by users marked as "Not Authorized" who have attempted to or successfully logged into a computer with PCI Cardholder Data should be investigated to see if a breach has occurred.

240 Access to a network share authorized to store Sensitive Data is unrestricted (80 pts each)

Current Score: 80 pts x 3 = 240: 1.32%

Issue: Network shares authorized to store Sensitive Data were found as completely unrestricted (granting access to 'Everyone').

Recommendation: Investigate the network shares authorized to store Sensitive Data with unrestricted access. Limit access to the minimum necessary.

240 ePHI on computer not authorized to store data (80 pts each)

Current Score: 80 pts x 3 = 240: 1.32%

Issue: ePHI data has been detected as stored on a computer not authorized to store ePHI.

Recommendation: Investigate the unauthorized computers storing ePHI. ePHI should be stored on computers in accordance with organization policy.

80 GDPR Personal Data on computer not authorized to store data (80 pts each)

Current Score: 80 pts x 1 = 80: 0.44%

Issue: GDPR Personal Data has been detected as stored on a computer not authorized to store Personal Data.

Recommendation: Investigate the unauthorized computers storing GDPR Personal Data. Personal Data should be stored on computers in accordance with organization policy.

78 Computer with GDPR Personal Data not backed up (78 pts each)

Current Score: 78 pts x 1 = 78: 0.43%

Issue: Computers identified as having GDPR Personal Data are documented as not having a backup agent installed.

Recommendation: Ensure that data is properly backed up on computers with GDPR Personal Data. See the Asset Inventory Worksheet for a list of computers that are documented as not having a backup agent installed.

75 Computer storing GDPR Personal Data does not use disk encryption (75 pts each)

Current Score: 75 pts x 1 = 75: 0.41%

Issue: Theft is the most common form of data breach. Unencrypted computer drives storing GDPR Personal Data may allow data loss through theft.

Recommendation: Implement disk encryption on computers storing GDPR Personal Data.