



Odyssey Discovery

Sample

Prepared for:



Odyssey Discovery – Sample

This document serves as a sample to illustrate the areas typically addressed in an Odyssey Discovery network assessment.

Each assessment is tailored to the unique needs and environment of the client.



Executive Summary

Odyssey Discovery Overview

Usherwood Office Technology performed an Odyssey Discovery on your network starting in June of 2024.

During the Odyssey Discovery, we evaluated and provided an assessment of your overall security, IT infrastructure, endpoints, licensing, active directory, patched, dark web credentials, and compliance.

The Odyssey Discovery was performed by Usherwood Office Technology Team composed of the following Individuals:

Dan Smith, Director of IT Security Engineering Services

Sean O'Connor, Senior Cyber Security Engineer

Sean Hope, Director of MPS

Dan Hernborg, Pre Sales Engineer

Chris Atwood, Senior Solutions Architect

Stewart Walts, Director, vCIO Services

Odyssey Discovery Objectives

Our objective throughout this process is to gather as much information as possible and then evaluate it against best practice, and industry standards, all while maintaining a security first mindset.

Additionally, we involve our trained engineering team from the beginning. Taking pictures and evaluating the environment in person, along with real time data gathering from our Odyssey Discover Tool, allows our team to see all of your network. When all of that data is collected, we meet with the team and work together to put forth our findings and suggestions.

We aim to provide you with a thorough breakdown of your network and a path forward based on your needs.

Executive Summary

Usherwood Office Technology follows the National Institute of Standards and Technology (NIST) and Cyber Security Framework (CSF) for compliance and will cite those controls as appropriate throughout our findings. We will cite those relevant at the bottom of the applicable page.

What is CSF?

The Cyber Security Framework (CSF) was developed by the National Institute of Standards and Technology (NIST) as a response to President Obama's Executive Order 13636 to strengthen and standardize critical Infrastructure security within the United States. It's a reference tool that provides guidance for security practitioners as they work to improve their organization's cyber security posture.

The first step in strengthening cyber security is identifying where you stand today. You have to start somewhere, and referencing the CSF for that process saves immeasurable effort and hours of research and planning. It's a little like using tax software to file taxes rather than reading the entire tax code and completing returns manually; but on a larger scale. As a framework, the CSF lets you map your current security controls and processes and identify gaps, giving you a basic measurement of organizational cyber security maturity. If your goals include complying with regulatory standards, the CSF helps you cover your bases and prioritize your biggest wins.

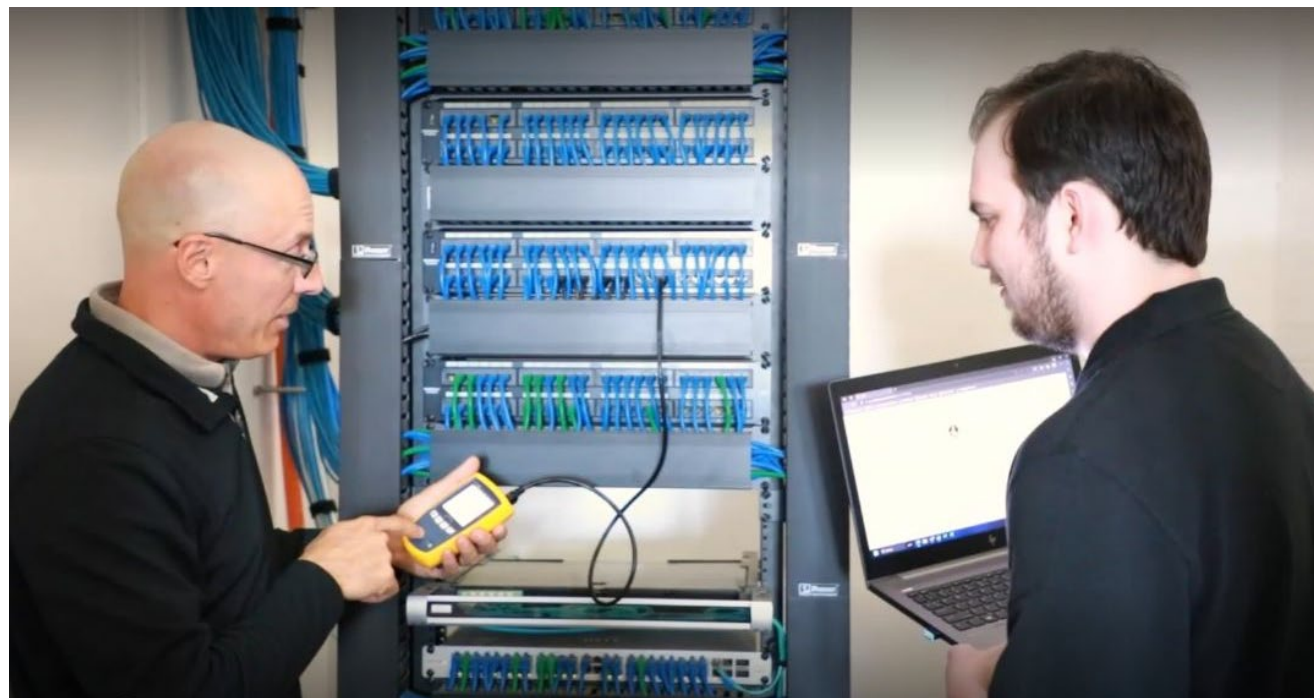
NIST Cyber Security Framework

Heavily used throughout the United States for its user-friendliness, the CSF is organized into five primary function and multiple categories:

Functions	Categories				
Identify	Asset Management	Business Environment	Governance	Risk Assessment	Risk Management Strategy
Protect	Access Control	Awareness & Training	Data Security	Information Protection Process & Procedures	Maintenance
Detect	Anomalies & Events	Security & Continuous Monitoring	Detection Processes		
Respond	Response Planning	Communications	Analysis	Mitigation	Improvements
Recovery	Recovery Planning	Improvements	Communications		

Odyssey Discovery Summary

The Odyssey Navigator report provides visibility into specific weaknesses and deficiencies in the security controls employed within or inherited by the information system. They are potential vulnerabilities if exploitable by a threat source. The findings generated provide important information that facilitates a discipline and structured approach to mitigating risks in accordance with organizational priorities.



Our Odyssey Discovery tool evaluates your network against industry standards and best practices which provides us both a high-level overview. We evaluated based on the categories below.

- Security
- Vulnerability
- Compliance
- Patch
- IT Infrastructure
- Endpoint
- Active Directory
- Licensing

Vulnerability Assessment

RATING GUIDE



Base Score

Reflects the severity of a vulnerability according to its intrinsic characteristics which are constant over time and assumes the reasonable worst case impact across different deployed environments.



Impact Score

Impact focuses on the actual outcome that an attacked can achieve as a result of exploiting the vulnerability in question. Impact metrics are comprised of three sub-metrics – Confidentiality, Integrity, and Availability.



Exploit Score

The exploitability sub-score represents metrics for Access Vector, Access Complexity, and Authentication, and measures how the vulnerability is accessed, the complexity of the attack, and the number of times an attacker must authenticate to successfully exploit a vulnerability.

NVD VULNERABILITY SEVERITY RATINGS

CVSS V3.0 RATINGS

Severity	Base Score Range
None	0.0
Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0

- The National Vulnerability Database (NVD) is a database that is maintained by NIST.
- Common Vulnerabilities and Exposure (CVE) is a list of publicly disclosed vulnerabilities and exposures that's maintained by MITRE
- The Common Vulnerability Scoring System (CVSS) is a system generally used in vulnerability management programs. It indicates the severity of information security vulnerability and is an essential part of many vulnerability scanning tools.

****First four digits in CVE represents the year the vulnerability was announced**

Vulnerability Assessment

Vulnerabilities are evaluated across hardware, software, and even policies within an organization. These are presented based on how critical they are, and in some cases are uncovered after the engineering team examination. CVSS scores are the industry standard for understanding their severity.

ASSETS

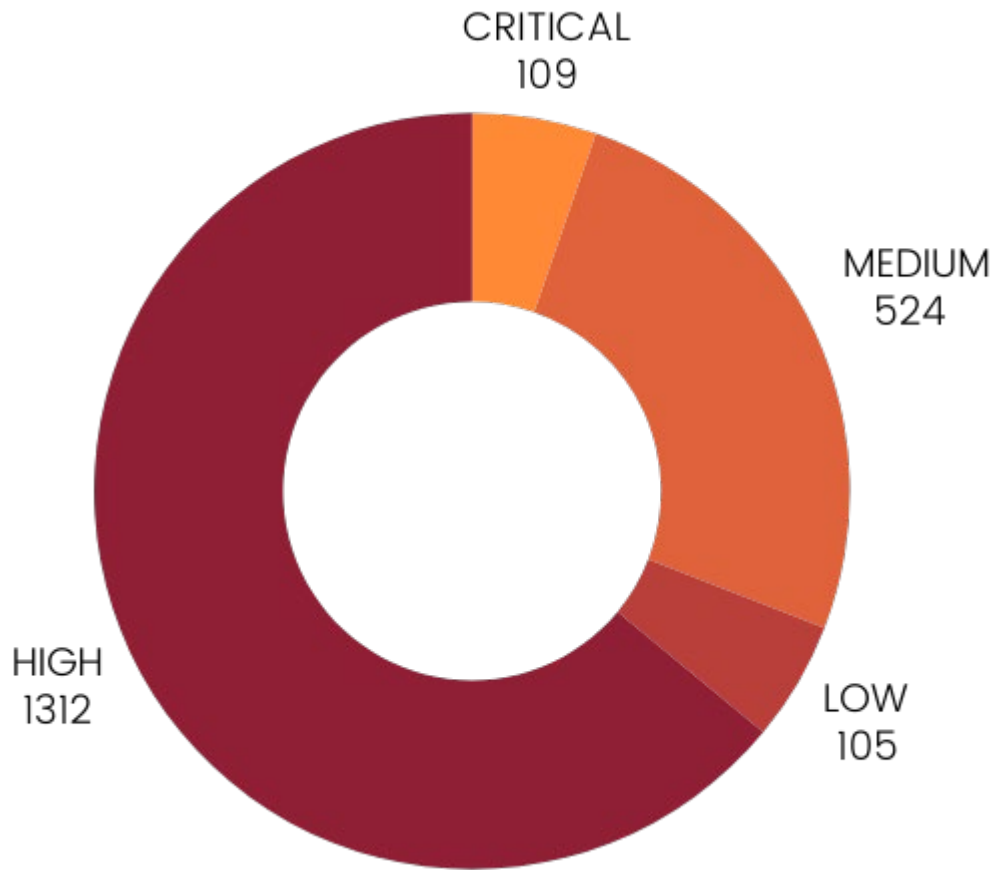
No. of Assets discovered 60

VULNERABILITIES ACROSS ASSETS

Critical Authenticated Vulnerabilities	14
High Authenticated Vulnerabilities	985
Med Authenticated Vulnerabilities	560
Low Authenticated Vulnerabilities	14
Critical Network Vulnerabilities	25
High Network Vulnerabilities	40
Medium Network Vulnerabilities	125
Low Network Vulnerabilities	38

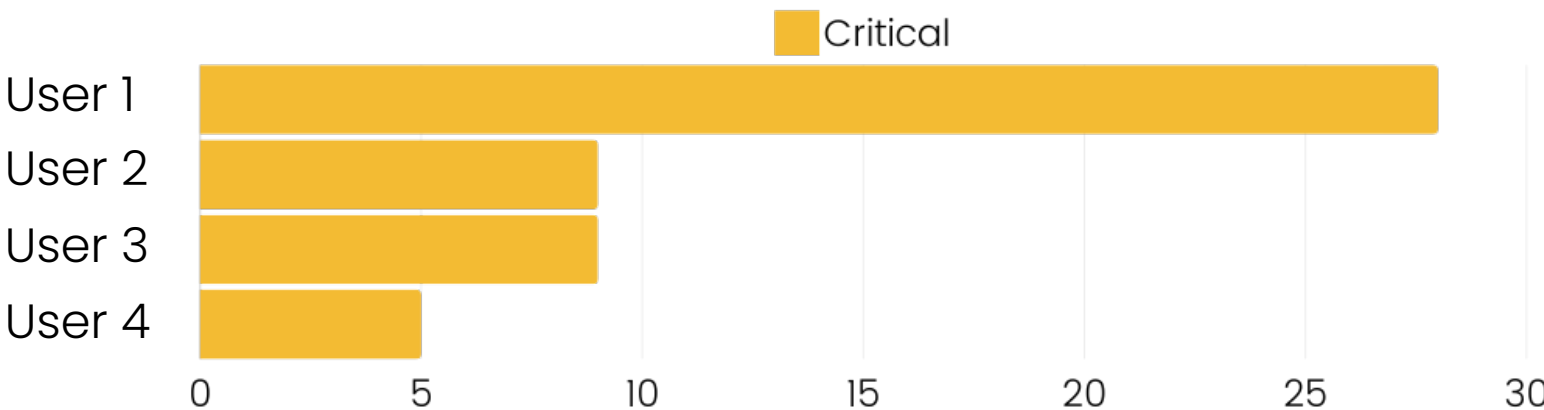
VULNERABILITY BREAKDOWN

Asset Level Vulnerabilities 1042



TOP CRITICAL ASSETS

Critical Vulnerabilities have to be patched and resolved quickly.



Compliance Assessment

Compliance is evaluated based on regional requirements for certain business segments. Compliance is typically tied to security standards and is critical to best practice for the modern workplace. These findings are based on observations of your environment measured against those standards.

LLMNR
8 Assets with LLMNR enabled

NTLMV1
4 Assets with NTLMV1 enabled

NBTNS
9 Assets with NBTNS enabled

SMBV1 Server
0 Assets with SMBV1 Server enabled

SMBV1 Client
1 Assets with SMBV1 Client enabled

SMB Signing
8 Assets with SMB Signing Disabled



Compliance Assessment

SMB v1

Server Message Block (SMB) is a protocol used primarily for sharing files, printer services, and communication between computers on a network.

Since September 2016, Microsoft has strongly encouraged that SMBv1 be disabled and no longer used on modern networks, as it is a 30-year-old design that is much more vulnerable to attacks than much newer designs such as SMBv2 and SMBv3. Recommendation from CIS is to ensure 'Configure SMB v1 server' is set to 'Disabled'. ABC Company has 2 non-compliant assets.

TITLE	DESCRIPTION
Ensure 'Configure SMB v1 server' is set to 'Disabled'	This setting configures the server-side processing of the Server Message Block version 1 (SMBv1) protocol. The recommended state for this setting is: ...
Ensure 'Configure SMB v1 client driver' is set to 'Enabled: Disable driver'	This setting configures the start type for the Server Message Block version 1 (SMBv1) client driver service (MRxSmb10), which is recommended to be dis...

LLMNR

The Link-Local Multicast Name Resolution (LLMNR) is a protocol based on the Domain Name System (DNS) packet format that allows both IPv4 and IPv6 hosts to perform name resolution for hosts on the same local link.

An attacker can listen on a network for these LLMNR (UDP/5355) or NBT-NS (UDP/137) broadcasts and respond to them, tricking the host into thinking that it knows the location of the requested system. Recommendation from CIS is to ensure 'Turn off multicast name resolution' is set to 'Enabled'. ABC Company has 15 non-compliant assets.

TITLE	DESCRIPTION
Ensure 'Turn off multicast name resolution' is set to 'Enabled'	LLMNR is a secondary name resolution protocol. With LLMNR, queries are sent using multicast over a local network link on a single subnet from a client...

Patch Assessment

Patch Assessment is the process that helps acquire, test and install multiple patches on a computer, enabling systems to stay updated on existing patches and safeguards the IT environment from vulnerability and exploit.

TOP MISSING PATCHES

VULNERABILITY	CRITICAL	HIGH	ASSET COUNT
Windows 11 Build	4	123	12
Microsoft Edge	18	0	8
Google Chrome	0	15	21
Windows 10 Build	1	4	0



42 Critical Patches

Apply patches within 30 days



36 High Patches

Apply patches within 30-60 days



71 Medium Patches

Apply patches within 60-90 days



2 Low Patches

Apply patches within 180 days

Cyber Insurance Assessment

Common Cybersecurity Requirements

Endpoint Detection and Response (EDR)

EDR is an integrated endpoint security solution designed to detect, investigate, and respond to cyber threats.

Security Awareness Training

Security awareness training is the regular training of employees on best practices for spotting and avoiding malicious content.

Multi-Factor Authentication (MFA)

MFA is a verification method that requires users to provide at least two forms of identification to access something.

Patch all High / Critical Issues

All high / critical issues must be patched in less than 30 days.

Robust Backups

Must have assets backed up.

Common Insurance Claims

Data Breach Response:

Covers the costs associated with managing and mitigating a data breach, including notifying affected parties, credit monitoring, and public relations efforts.

Cyber Extortion:

Protects against losses incurred due to extortion threats, such as ransomware attacks, where cybercriminals demand payment to restore access to data or systems.

Business Interruption:

Compensates for financial losses resulting from a disruption of normal business operations caused by a cyber event.

Cyber Insurance Assessment

Do you implement critical patches (within 2 months)? ☒ Yes ☐ No

BUSINESS EMAIL COMPROMISE

Check “Yes” next to the option below that applies to your organization’s email application:

On Premise ☐ Yes ☐ No

Hosted/Cloud Based ☐ Yes ☐ No

If Hosted/Cloud Based, which one? ☐ Yes ☐ No

If Hosted/Cloud Based, have you enabled all default logging for email, including audit logging and mailbox auditing? ☐ Yes ☐ No

If Hosted/Cloud Based, have you implemented one or more of the following email authentication standards: DMARC, DKIM, or SPF? ☐ Yes ☐ No

Do you use email to store, process, and/or transmit sensitive information including Personally Identifiable Information and/or Personal Health Information? ☐ Yes ☐ No

Do you have a formalized email retention policy? ☐ Yes ☐ No

If yes, what is the maximum duration of email retention per the policy?

Do you have any end of life or end of support software on your network? ☐ Yes ☒ No

If yes: Is the software segregated from the rest of the network? ☒ Yes ☐ No

Do you allow remote access to your network? ☒ Yes ☐ No

If yes: Do you use multi-factor authentication (MFA) to secure all remote access? ☒ Yes ☐ No

Do you require a virtual private network (VPN)? ☒ Yes ☐ No

Do you permit users remote access to web-based email (e.g., Outlook Web Access (OWA))? ☒ Yes ☐ No

Common Insurance Claim Loopholes

Coverage Denial:

Providing inaccurate information or omitting relevant details in the application may give the insurance company grounds to deny coverage. If a cyber incident occurs and the insurer discovers that the information on the application was incorrect or incomplete, they may refuse to honor the policy.

Policy Rescission:

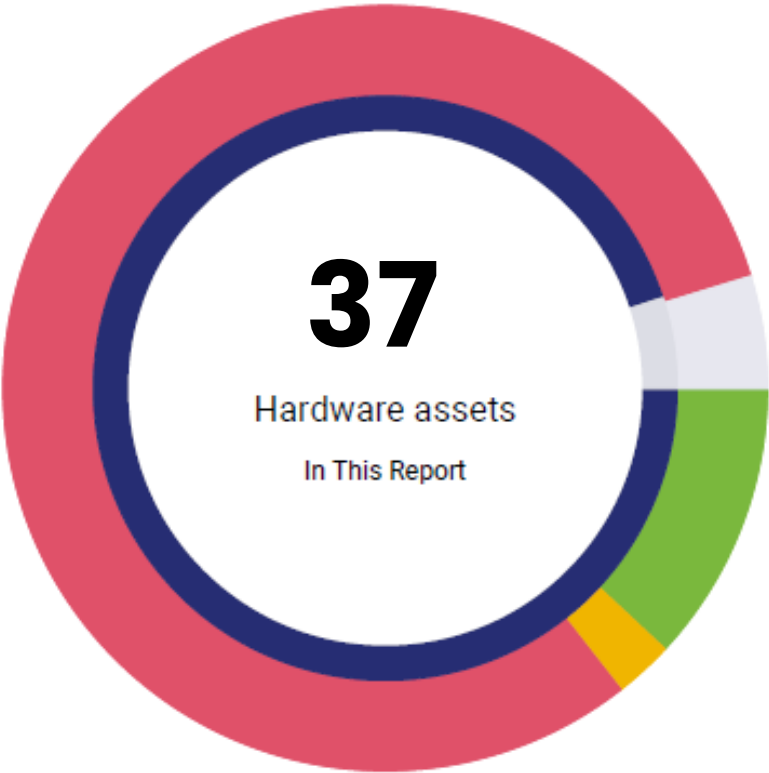
In more severe cases, the insurer may choose to rescind the policy altogether. Rescission means that the policy is considered void from its inception, as if it never existed. This could leave the policyholder without any coverage and facing potential legal consequences.

Premium Adjustments:

The premium for a cyber insurance policy is typically based on the information provided in the application. If the information is later found to be inaccurate, the insurer may adjust the premium accordingly.

Infrastructure Assessment

Asset discovery is simply the process of discovering and collecting data on the technology assets connected to a network for management and tracking purposes.



About This Report

This is an overview of known server and workstation hardware for ABC Company. A detailed breakdown starts on page 2. Please contact us with any questions and we would be pleased to discuss this report in further detail.

Replacement status:

- 7 Supported
No action required
- 2 Due soon
Due date within 90 days
- 25 Overdue
Action required
- 3 Unknown
Under review or unknown

Operating System:

- 24 OS supported
Within support period
- 3 OS unsupported
No longer maintained

Workstation	User	Make	Serial	Model	OS	Age	Purchased	Expires
ABC1234	user1	HP Inc	49573940	HP 123	Windows 11 OS	1.5	2023-01-15	2025-02-15
DEF5940	User2	HP Inc	440205839	HP 123	Windows 11 OS	2	2023-01-15	2025-02-15
GHI5940	User3	HP Inc	54808504	HP 123	Windows 11 OS	3	2023-01-15	2025-02-15
JKL590	User4	HP Inc	5473969	HP 123	Windows 11 OS	1.5	2023-01-15	2025-02-15
MNO59	User5	HP Inc	482556	HP 123	Windows 11 OS	2	2023-01-15	2025-02-15
PQR590	User6	HP Inc	5840690	HP 123	Windows 11 OS	2	2023-01-15	2025-02-15
STU5890	User7	HP Inc	435936-7	HP 123	Windows 11 OS	1	2023-01-15	2025-02-15
VWX902	User8	HP Inc	79067905	HP 123	Windows 11 OS	1	2023-01-15	2025-02-15
YZA502	User9	HP Inc	178496	HP 123	Windows 11 OS	3	2023-01-15	2025-02-15
BCD246	User10	HP Inc	693078-3	HP 123	Windows 11 OS	4	2023-01-15	2025-02-15
EFG453	User11	HP Inc	568305-670	HP 123	Windows 11 OS	6	2023-01-15	2025-02-15
HIJ0556	user12	HP Inc	3275996-06	HP 123	Windows 11 OS	8	2023-01-15	2025-02-15

Active Directory **Assessment**

While Active Directory is not the sole factor in securing a network, its current configuration may lack centralized and efficient security management practices. Organizations without Active Directory should implement alternative measures to ensure robust user authentication, access control, and overall network security. While having Active Directory is not a direct measure of security, its absence can contribute to increased security risks for several reasons:

User Authentication and Authorization:

- Risk: Without Active Directory, a company may lack a centralized and secure system for managing user accounts, authentication, and authorization.
- Impact: This makes it more challenging to enforce strong password policies, implement multi-factor authentication, and control access to resources based on user roles and permissions.

Resource Management and Tracking:

- Risk: Active Directory provides a centralized repository for managing and tracking network resources, including computers, servers, and other devices.
- Impact: Without this centralization, tracking and managing network assets become more challenging, making it harder to identify and respond to security threats, such as unauthorized devices on the network.

Centralized Security Policies:

- Risk: Active Directory allows organizations to enforce security policies across the network, such as password complexity requirements, account lockout policies, and other security configurations.
- Impact: In the absence of Active Directory, maintaining and enforcing consistent security policies becomes more difficult, increasing the likelihood of weak security practices across the organization.

Active Directory **Assessment**

Password Policy Summary

POLICY	SETTING	DOMAIN
Enforce password policy	34 passwords remembered	abccompany.com
Minimum password age	0 days	abccompany.com
Minimum password length	0 characters	abccompany.com

Password length less than 8 characters

Observation: 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.

Inconsistent password policy:

Observation: Password policies are not consistently applied from one computer to the next. A consistently applied password policy ensures adherence to password practices.

Recommendation: Eliminate inconsistencies and exceptions to the password policy.

Licensing Assessment

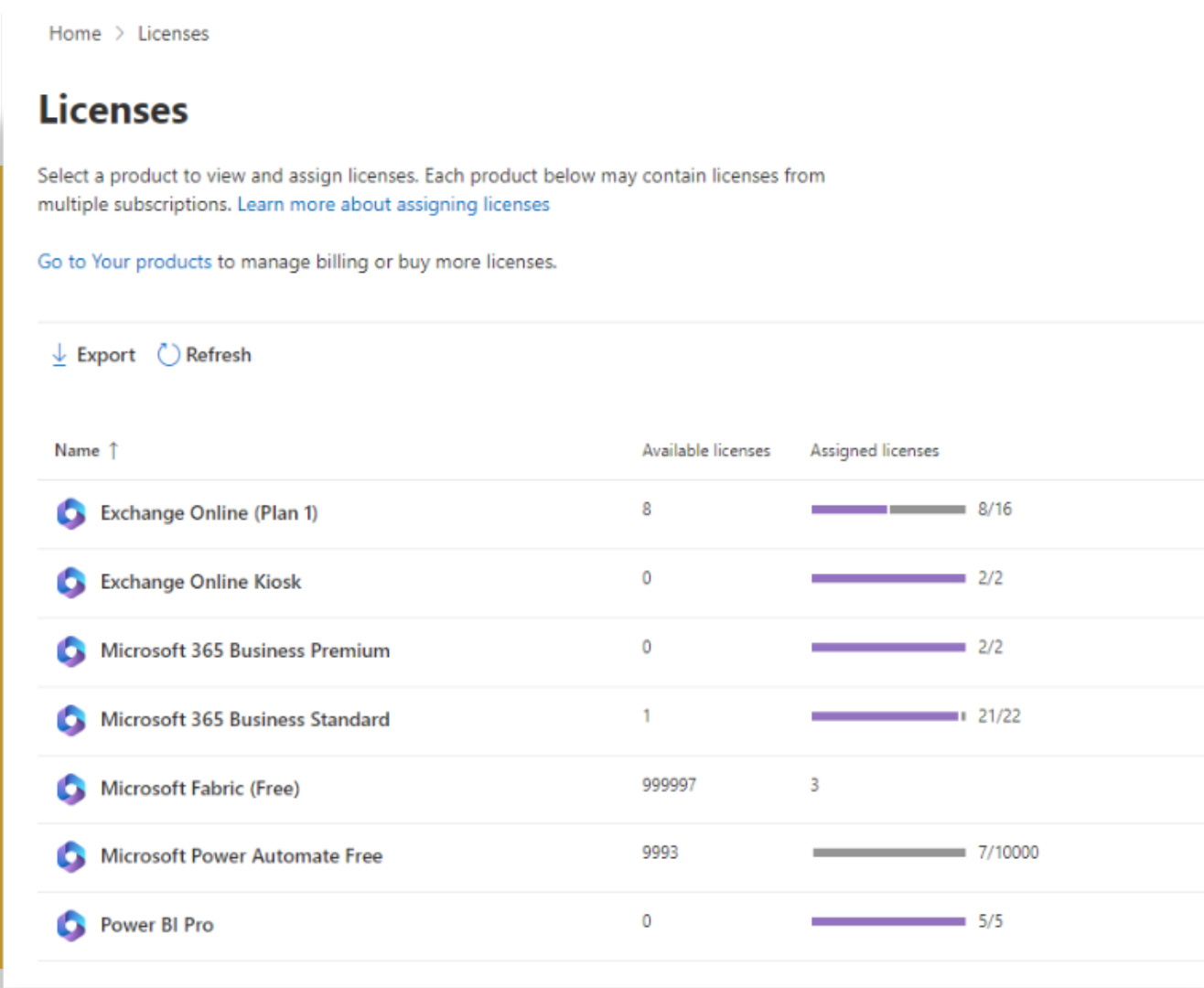
A meaningful licensing strategy will mean choosing the right license and ensuring there is enough to cover the users and devices as appropriate. We evaluate the licenses in place to ensure that there are not too much, or too little, and that desired functionality is in place and enabled








Observation

We observed a mixed Microsoft 365 licensing arrangement with MFA not enabled / configured properly. No password policy was in place.

Recommendation

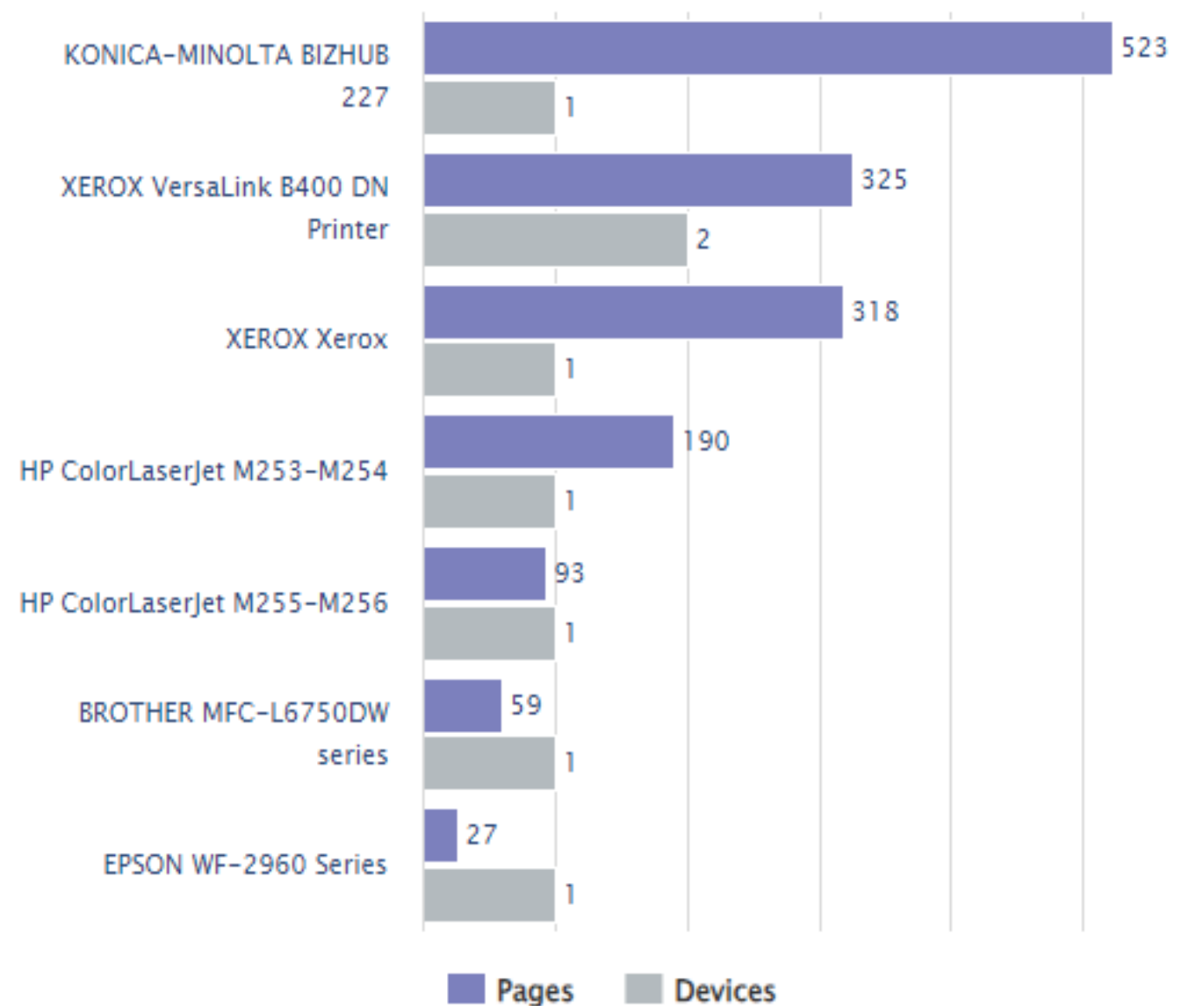
We recommend enabling multifactor authentication on all MS 365, remote access, and guest accounts. Additionally, review the licensing strategy and migrate to Business Premium licensing for further security features like Conditional Access and Advanced Threat Protection. Appropriate configuration is required to take full advantage of the solution.



Home > Licenses		
Licenses		
Select a product to view and assign licenses. Each product below may contain licenses from multiple subscriptions. Learn more about assigning licenses		
Go to Your products to manage billing or buy more licenses.		
Export Refresh		
Name ↑	Available licenses	Assigned licenses
 Exchange Online (Plan 1)	8	<div><div></div></div> 8/16
 Exchange Online Kiosk	0	<div><div></div></div> 2/2
 Microsoft 365 Business Premium	0	<div><div></div></div> 2/2
 Microsoft 365 Business Standard	1	<div><div></div></div> 21/22
 Microsoft Fabric (Free)	999997	<div><div></div></div> 3
 Microsoft Power Automate Free	9993	<div><div></div></div> 7/10000
 Power BI Pro	0	<div><div></div></div> 5/5

Print Fleet Assessment

A print fleet assessment aims to provide organizations with insights into their printing infrastructure and opportunities for improvement in terms of cost savings, efficiency, sustainability, and security.



Observation

A mixed fleet of print manufacturers are in place. Each of these devices were logged into using the default / factory administrator credentials. In some cases, the patching has never been completed.

- 1 of 2 HPs has multiple critical vulnerabilities.
- The Konica has had known vulnerabilities over the years, but we can't tell if it has been patched. The built-in security features are outdated.
- The Xerox models are all Alta Link class and have good security features

Recommendation

Follow the patching guidelines and recommendations provided by the manufacturer. They may offer specific instructions or best practices for updating their devices safely and effectively. These patches often address vulnerabilities that could be exploited by attackers. Make sure to apply these patches promptly to reduce the risk of security breaches.

IT Infrastructure **Assessment**

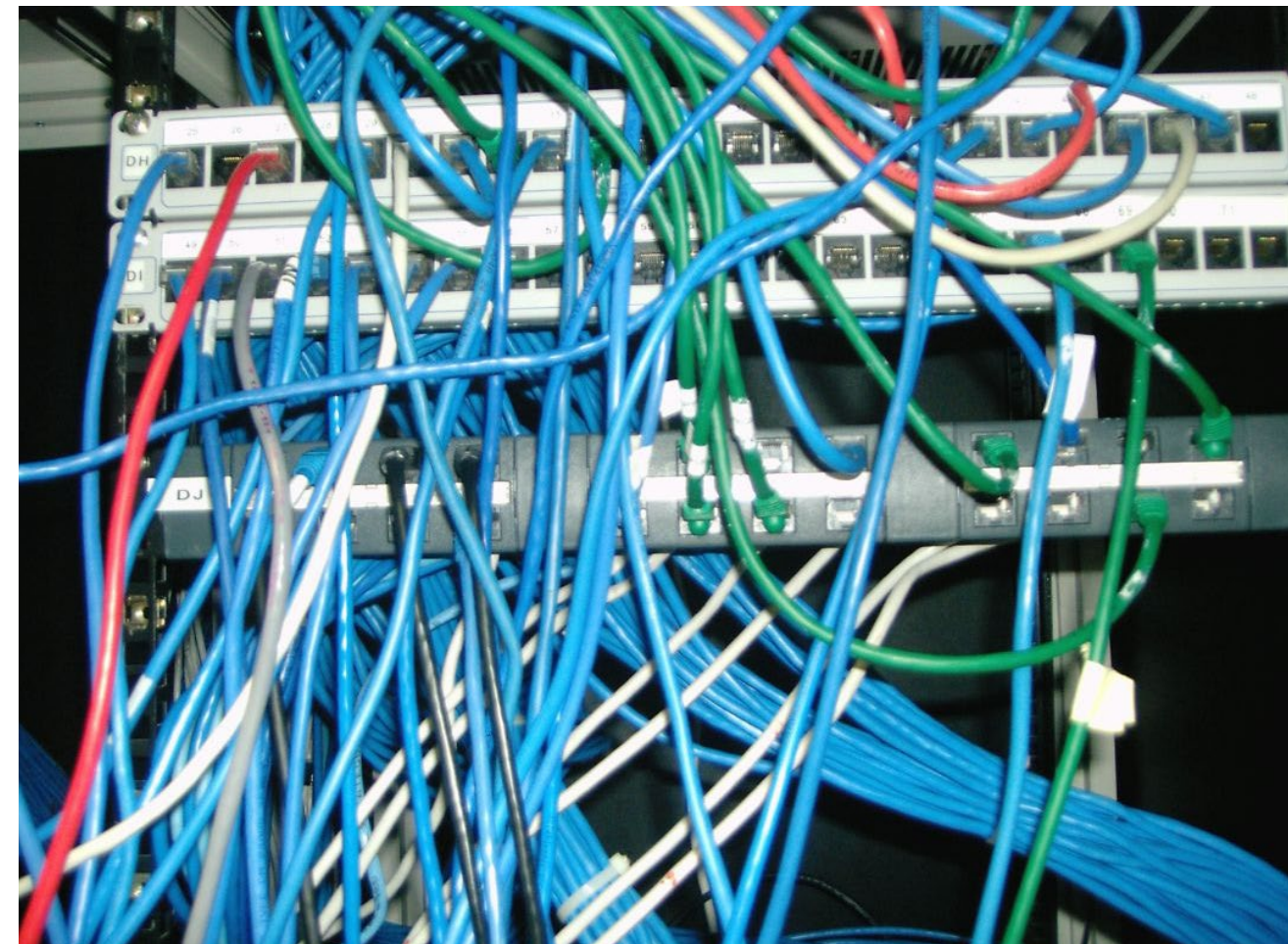
Cabling

Observation

We observed Cat5e throughout all locations with a centralized place to terminate connections. Additionally, each location has various needs for cable management.

Recommendation

We recommend using cabling management and to label as updated components are installed – clean up the cabling where cabinets are not in place and tidy up the other spots where some cable management could go a long way. For example, utilizing a patch panel that is labeled to match up with the appropriate wall plate is strongly suggested. Often using different appropriate lengths of cable can tighten up the appearance.



IT Infrastructure Assessment

Physical Security

Observation

For the main location, we observed a network rack with climate control present. Remote locations have dedicated areas for infrastructure.

Recommendation

We recommend maintaining a dedicated area for your network equipment with a lockable rack for your network equipment (modem, firewall, switching, and patch panel is strongly suggested. Additionally it is critical to maintain a climate controlled environment.



IT Infrastructure Assessment

Backup & Power

Observation

An external USB hard drive is in place to backup this QuickBooks PC. Frequency of backup is unknown. QuickBooks has a backup procedure managed by the staff.

Recommendation

We strongly recommend putting in a data protection and disaster recovery plan. Regular secure backup is vital. With everything in the cloud there needs to be regular offsite cloud backups. It is preferable that the offsite backups are in a different location altogether in the event of disaster scenarios. Evaluate any cloud provider's disaster recovery capabilities. This involves their plan to quickly recover data in case of catastrophic events like hardware failure, natural disasters, or cyberattacks.



IT Infrastructure **Assessment**

Firewall

Observation

We observed routers in place at each location with no management or patching available. A router determines the path(s) that packets should take from two different networks. While a firewall does this, it also prevents certain packets from reaching a protected network.

Recommendation

We recommend upgrading to Cisco Meraki firewalls, making sure to use Advanced Security. The Advanced Security license provides security capabilities that let us render their network effectively invisible from most of the world. Additionally, it is important to evaluate internet bandwidth and the capability of the firewall to ensure there are no bottlenecks.



IT Infrastructure **Assessment**

Switching

Observation

Switches in use at multiple locations include older models that have reached their end-of-sale or end-of-life status, meaning they are no longer supported with firmware updates or security patches. Without ongoing manufacturer support, these switches may pose security vulnerabilities and operational risks.

Recommendation

We recommend replacing these with Cisco Meraki managed switches in all locations. The ultimate goal should be to migrate towards a switching environment that provides for easier administration and automatic upgrades. The full administration in a single place, with automatic updates and 24/7 support is priceless for a business network.



IT Infrastructure **Assessment**

Wireless

Observation

The main location has sufficient wireless coverage with modern access points in place. However, the age and firmware patching schedule of these devices are unknown, creating potential risks for security and reliability.

Recommendation

We recommend planning to upgrade to the newer Cisco Meraki Access Points to compliment your firewall and switching. Network equipment from a single vendor is designed to work seamlessly together.



IT Infrastructure Assessment

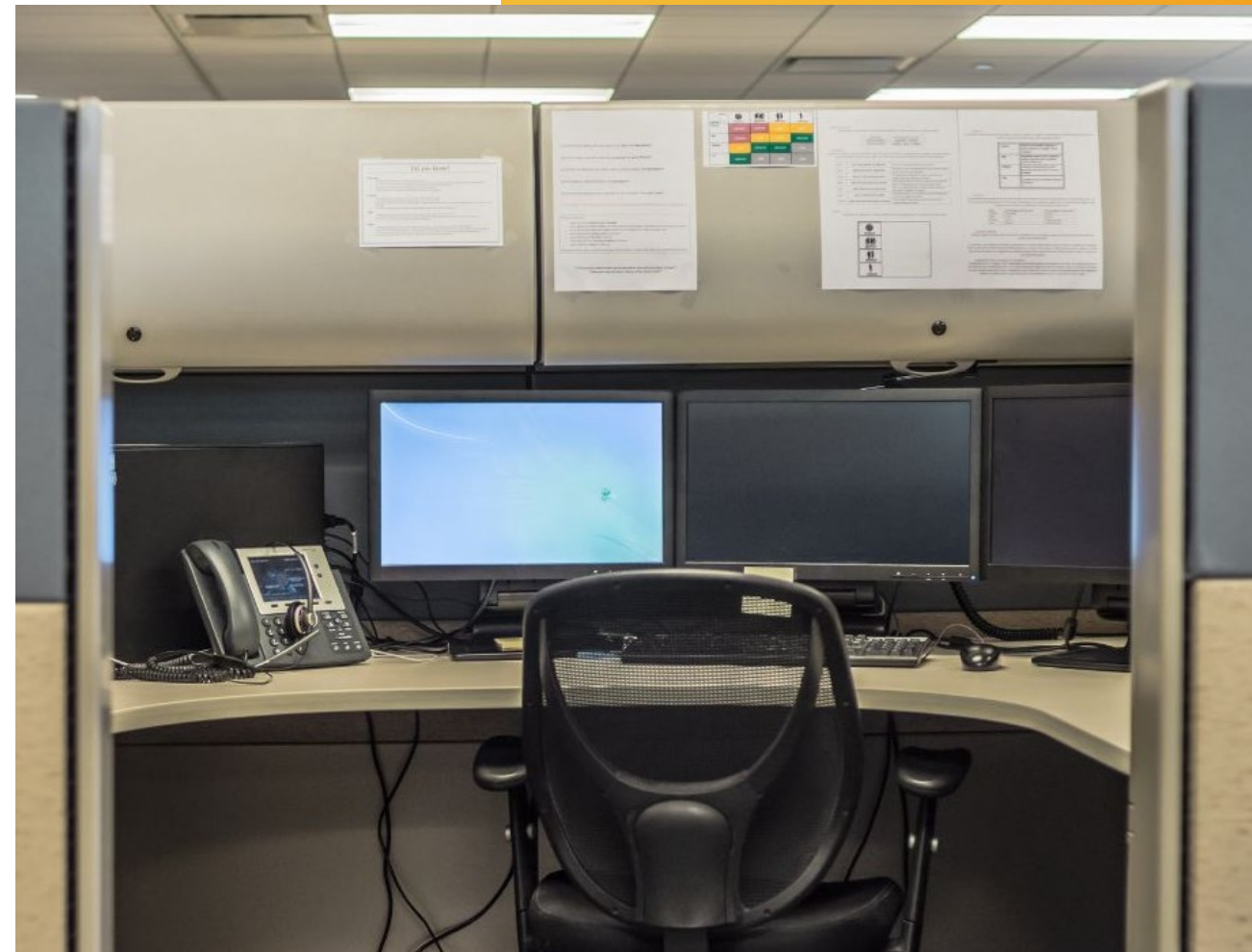
Workstations

Observation

We observed a fleet of workstations ranging from new to 5 years old. 3 of these workstations currently have an active warranty. Many of these are Windows Home Edition. Windows 7 devices are also on the network.

Recommendation

We recommend that a 3 to 5 year cycle of replacement is implemented to continue to refresh the PC's in use by the firm. This will keep users productive. Additionally, in our experience having at least 16gb of RAM is a good baseline, as well as at least gen 10 i7's (or equivalent) in place. Applications, especially for voice and video, require more and more resources. Making sure the PC's can handle added security, collaboration, and other applications will also contribute to having more productive users. We recommend that only organization supplied PC's are used to connect to the network that are verified patched and secure.



IT Infrastructure **Assessment**

Servers

Observation

The server infrastructure includes outdated hardware, including a server past end-of-life and warranty, and a workstation being used as a server, which poses reliability and security risks. Supported virtualized servers are in place with active operating systems.

Recommendation

Replace end-of-life servers and transition workstations to proper server hardware. Maintain active support agreements and ensure all servers use supported operating systems for reliability and security.



Recommendations Summary

Vulnerabilities:

A solid vulnerability mitigation program is important and recommended. This will allow the organization to reduce and eventually eliminate most of the vulnerabilities. This is an ongoing battle and one that not just patching Windows OS will resolve.

Compliance:

A SIEM/SOC solution would improve security, and cover compliance requirements. Logs will be saved, and network activity examined, which will go a long way towards improving the overall security posture of the organization.

MFA:

Multifactor authentication is a must for modern business. Cybersecurity insurance is starting to require it and it can be expected that other businesses will begin to do so as well to partner with your organization. All users need to be covered by MFA.

Passwords:

A strong and consistent password strategy is a basic building block of a good security program. This needs to be organization wide, and implemented as soon as possible.

IT Assets:

Tracking IT assets for warranty status, and OS, can help keep the organization efficient and secure. A cyclical replacement strategy means its in the budget and planned in advance. Machines shouldn't be kept until the break. The presents a higher level of risk than necessary.

Licensing:

The strategy around licensing needs to be in line with end user agreements and without risk issues with Microsoft. It should be evaluated and brought into compliance across the organization. Tracking license use also ensures the organization doesn't pay for licensing not needed.

Active Directory:

Active directory needs to be examined and cleaned up of any accounts no longer in use. All accounts should be evaluated for the level of access they have now, and will need, and then dropped to the lowest level of access necessary.

Network Hardware:

Servers need to be under warranty, preferably by the manufacturer, and kept up to date. Additionally, switches and other devices would benefit from being a set standard across the organization.

