CYBERPOOLS

Cybersecurity Risk Assessment

Sample Organization - POC

Assessment Date:	10/27/2025
Report Date:	10/27/2025
Conducted By:	CyberPools Assessment Team
Member Contact:	Contact Person

TEST DOCUMENT — Document doesn't look right? We'll help you out! — TEST DOCUMENT — TEST DOCUMENT — TEST DOCUMENT — Document doesn't

What is a Cyber Risk Assessment?

A cyber risk assessment is the process of identifying, evaluating, and prioritizing potential security threats to an organization's assets and infrastructure. This includes analyzing the likelihood and impact of these risks and determining the measures and controls to be put in place to mitigate them. The goal of a cyber risk assessment is to improve an organization's cybersecurity posture and prevent data breaches, unauthorized access, and other types of cyber-attacks.

Methodology

The following categories have been derived from previous version of the risk assessment which questions were influenced from previous cyber insurance claims, cybersecurity best practices, and common knowledge derived from the cybersecurity industry and as outlined by organizations such as NIST (National Institute of Standards and Technology), CISA (Cybersecurity and Infrastructure Security Agency) and CIS (Center for Internet Security).

It is recommended that organizations schedule a review meeting with appropriate district personnel to discuss identified risks and to define remediation actions.

Grading Methodology Update

As of January 2025, CyberPools has implemented a two-tier assessment model that provides complementary perspectives on your cybersecurity posture. This assessment measures both Tier I (foundation compliance with 12 core cyber insurance requirements) and Tier II (comprehensive security maturity across all control categories). The Tier II score uses a weighted calculation: 80% Tier I + 20% comprehensive controls. This heavily weighted approach ensures that foundation controls—which are critical for cyber insurance eligibility—have substantial influence on your overall assessment, while gaps in these core requirements receive immediate attention.

The 80/20 weighted methodology in Tier II strongly emphasizes the critical importance of foundation controls—the 12 risk assessment questions that map to the 7 core cyber insurance requirements. These controls represent the non-negotiable baseline for cyber insurance eligibility and protection against the most common threats. Missing even one foundation control will have substantial impact on your Tier II score. Organizations should prioritize achieving strong Tier I scores (85%+) as the primary objective before advancing to more sophisticated security controls.

> **Questions or Feedback:** For any questions about our risk assessment or grading, please reach out to cyber@cyberpools.org

Executive Summary & Assessment Results

Executive Summary

This is a Proof of Concept report demonstrating the new **dual-score model** for CyberPools Risk Assessments. The report now shows both a **Foundation Score** (based on core cyber insurance requirements) and a **Security Maturity Score** (based on comprehensive assessment).

Assessment Results

TIER I SCORE

79%

Foundation compliance based on 12 core cyber insurance requirements

12 Risk Assessment Questions (7 Insurance Requirements)

TIER II SCORE

79%

Comprehensive security maturity (80% Tier I + 20% All Controls)

9 Control Categories • 51 Security Questions

Understanding Your Tier I and Tier II Scores

This assessment provides two complementary scores that measure different aspects of your cybersecurity posture:

- **Tier I Score** measures foundation compliance using 12 detailed risk assessment questions that map to the 7 core requirements from most cyber insurance providers. This ensures your organization meets minimum baseline security requirements for cyber insurance eligibility.
- **Tier II Score** evaluates your comprehensive security maturity across all 9 control categories. This score is calculated as 80% Tier I + 20% comprehensive controls, heavily emphasizing foundation compliance while considering your overall security posture.

Detailed Score Breakdown

Risk Distribution

3	5	43
HIGH RISK	MODERATE RISK	LOW RISK

Section Scores

NO.	SECTION	SCORE
1.0	Inventory and Control of Assets	89%
2.0	Account Management	88%
3.0	Data Protection	39%
4.0	Secure Configuration of Enterprise Assets	90%
5.0	Malware Defense	75%
6.0	Data Recovery	100%
7.0	Security Awareness	86%
8.0	Vendor Management	77%
9.0	Incident Response Management	8%

1 Assessment Methodology

Rating Legend

CONTROL RATING	IMPACT RATING	RISK RATING
Fully Implemented Control(s) are fully implemented and effective at mitigating risk.	**Low (1)** Minimal disruption of operations and no sensitive data compromised or exfiltrated.	**Low (0-9)** Overall risk is low to organization
Partially Implemented Controls are partially implemented and somewhat effective in mitigating risk.	**Moderate (3)** Operational disruptions of operations but no sensitive data compromised or exfiltrated.	**Moderate (10-15)** Overall risk is moderate to organization
Not Implemented Control(s) are nonexistent.	**High (5)** Significant disruption of operations and sensitive data compromised or exfiltrated.	**High (16-25)** Overall risk is high to organization.
Not Applicable Control(s) are not necessary or applicable to the environment.	**Not Applicable (0)** No impact to your organization or environment as a result of the missing control.	**Not Applicable (0)** No risk posed as a result of the missing control.

Scoring Methodology

Raw Score Calculation

Each control is evaluated using a two-factor calculation that multiplies the implementation status by the potential impact to the organization.

Formula: Control Rating × Impact Rating

Control Rating: Indicates control implementation status.

- 1 = Fully Implemented
- 3 = Partially Implemented
- 5 = Not Implemented

Impact Rating: Reflects the level of organizational disruption if the control fails.

- 1 = Low impact (minimal disruption, no data compromise)
- 3 = Moderate impact (operational disruption, no sensitive data compromise)
- 5 = High impact (significant disruption and/or data compromise)

Score Normalization

Raw scores are normalized to a 0–100 scale to produce comparable category and overall scores across assessments.

- Ensures organizations can be measured consistently year over year.

- Maintains alignment with industry benchmarks and CyberPools grading standards.
- Keeps the model sensitive to partially implemented controls versus complete gaps.

Two-Tier Assessment Model (80/20 Weighting)

This assessment provides two complementary scores that measure different aspects of your cybersecurity posture:

Tier I Score (Foundation Compliance)

Based on 12 risk assessment questions that map to the 7 core cyber insurance requirements. These controls represent the non-negotiable baseline for cyber insurance eligibility and protection against the most common threats.

Tier II Score (Comprehensive Security Maturity)

Formula: Tier II = (80% × Tier I Score) + (20% × Comprehensive Score)

The Tier II score heavily weights your foundation compliance while also considering your performance across all 51 assessment questions and 9 control categories.

Why 80/20 weighting? This aggressive weighting ensures that foundation controls—which are critical for cyber insurance compliance—have substantial influence on your comprehensive security maturity assessment. Missing even one foundation control will have significant impact on your Tier II score. Organizations with foundation gaps will see their Tier II score appropriately reflect this critical deficiency, regardless of strengths in other areas.

Score Interpretation:

- **85%+ (Tier I or II):** Strong compliance/maturity
- **70-84%:** Adequate with room for improvement
- **Below 70%:** Critical gaps requiring immediate attention

Risk Calculation Example

Control: Multi-factor Authentication

Control Rating: Partially Implemented (3)

Impact Rating: High (5)

Raw Risk Score: 3 x 5 = 15

Result: 15 scores as moderate risk based on risk rating legend above.

Tier I: Cyber Compliance

The following table summarizes compliance with critical cybersecurity requirements identified by CyberPools. These requirements represent essential controls that significantly reduce organizational risk.

NO.	REQUIREMENT	COMPLIANCE
1.4	Has the organization adopted and implemented plans to retire or protect and segregate end-of-life software?	√ Yes
2.3	Is MFA enabled and enforced for all cloud resources, including email, document repositories, messaging or meeting platforms, and identity and access management tools?	√ Yes
2.4	Is MFA implemented for remote access to on-premises or hub networks?	✗ No
2.5	Is MFA in place for all admin or privileged user accounts to ensure enhanced protection against unauthorized access?	√ Yes
2.6	Does the organization enforce MFA for access to all critical systems and data?	√ Yes
4.3	Does the organization have a Patch Management Process to install all software patches within 30 or fewer days and critical and high-severity patches within 7 days?	√ Yes
4.7	Does the organization conduct regular external vulnerability scans?	√ Yes
5.4	Has the organization adopted and implemented endpoint detection and response (EDR) software services?	✗ No
6.3	Does the organization have an air gap or immutable backup of critical data/systems?	√ Yes
6.4	Does the organization perform bi-annual checks of the backups including testing and validation of recoverability capability?	√ Yes
7.2	Does the organization conduct phishing simulation tests and training at least quarterly?	√ Yes
7.3	Does the organization offer follow-up security training?	✗ No

Inventory and Control of Assets

89%

Overview

Inventory and Control of Assets refers to the practice of keeping track of all the devices an organization owns or uses, such as computers and servers. This enables the organization to know where everything is, who owns it, and whether there are any security issues. Having control over assets means implementing processes to manage, secure, and track them effectively, and to prevent unauthorized access. It also helps to identify unauthorized and unmanaged assets to remove or remediate them, reducing cybersecurity risks. Maintaining an inventory and control of assets is a critical component of any organization's cybersecurity program.

Importance

Having an up-to-date inventory and control of assets helps organizations identify and prioritize security risks and implement the appropriate controls to mitigate them. Many regulatory and insurance requirements may mandate that organizations maintain an inventory of their assets. Failing to do so can result in non-compliance and potential penalties and fines. Having a complete and accurate inventory of assets enables organizations to quickly determine the extent of a security incident and respond appropriately. Having an inventory and control of assets helps organizations make informed decisions about resource allocation and prioritize the protection of their most critical and valuable assets. Enterprises cannot defend what they do not know they have. Managed control of all enterprise assets also plays a critical role in security monitoring, incident response, system backup, and recovery. Having control over assets helps organizations monitor network activity and detect security threats, improving their overall security posture. In summary, having an inventory and control of enterprise assets (physical and software) is crucial for organizations to effectively manage risk, maintain compliance, and improve their overall security posture.

Controls Assessment

Control Standard: *Establish and maintain an inventory of all end-user assets with the potential to store, transmit, or change data. This often includes devices such as desktops, laptops, and mobile devices (tablets and cellphones).*

1.1 Does the organization inventory all company-owned devices?

Control Status: FULLY IMPLEMENTED (1) Impact: MODERATE (3) Risk Score: 3 - LOW

Comments:

Spreadsheets with SN and MAC address, device type, who it's assigned to. They are not asset tagged. As staff comes and goes, we update that as needed. We do not track student owned devices.

or quarantine the asset.

1.2 Does the organization have a way to identify and address any unauthorized assets from the network (wired and wireless)?

Control Status: PARTIALLY IMPLEMENTED (3) Impact: MODERATE (3) Risk Score: 9 - LOW

Comments:

> At this point, i've had issues where theres devices joined, but we don't actively monitor that. Wifi is isolated from core network. Monitor the top devices for internet activity. Ubiquity management, it gives a dashboard look, drill down to each client device, and see what's out there, how many devices. We can see irregular named devices, and that'll flag it for us. Wired ports are not disabled. DHCP pool set up, there's static address for staff and faculty. Any devices not registered will only get internet access.

Control Standard: *Establish and maintain a detailed inventory of all licensed software installed on enterprise assets. The software inventory should document important attributes such as the title, publisher, initial install/use date, and business purpose for each entry; where appropriate, include the Uniform Resource Locator (URL), app store(s), version(s), deployment mechanism, and decommission date. Review and update the software inventory bi-annually, or more frequently.*

1.3 Does the organization maintain an inventory of all licensed software installed across the organization?

Control Status: FULLY IMPLEMENTED (1) Impact: MODERATE (3) Risk Score: 3 - LOW

Comments:

> We have very few licenses. we use Adobe cloud suite, licensing managed within there. Staff can not install any application, they have to contact IT.

---

segmented, with proper controls and regular audits to ensure that the software is free of any compromises.

1.4 Has the organization adopted and implemented plans to retire or protect and segregate end-of-life software?

Control Status: FULLY IMPLEMENTED (1) Impact: HIGH (5) Risk Score: 5 - LOW

Comments:

> All of our environment are all compliant with Windows 11. Server backend is EOL 2012, currently updating to 2021.

2.0

Account Management

88%

Overview

Account management is the practice of managing user accounts and their access to an organization's systems and data. This includes creating and deleting accounts, setting permissions and access levels, and regularly reviewing and updating account information. Cybersecurity best practices recommend implementing strong password policies, multi-factor authentication, and limiting access to only what is necessary for each user's job function. Regular monitoring and auditing of account activity can help detect and respond to potential security incidents.

Importance

Effective account management is critical for managing cybersecurity risks and preventing unauthorized access, as it limits access to only authorized users and reduces insider threats. By enforcing strong password policies, regularly reviewing account activity, and promptly detecting and responding to security incidents, organizations can enhance password security and mitigate the risk of potential security incidents. Additionally, effective account management enables organizations to comply with regulations and standards, avoiding costly fines and reputational damage. In summary, a good account management process is essential for maintaining the confidentiality, integrity, and availability of an organization's systems and data.

Controls Assessment

Control Standard: *Establish and maintain an inventory of all user, administrator, and service accounts, including names, usernames, start/stop dates, and departments. Validate account authorization at least quarterly. Service accounts should follow the principle of least privilege, use complex passwords with 180-day rotations (if feasible), and undergo regular monitoring for abnormal activity.*

2.1 Does the organization have an inventory of all user accounts including users/admins/service accounts?

Control Status: FULLY IMPLEMENTED (1) Impact: MODERATE (3) Risk Score: 3 - LOW

Comments:

Active Directory, on prem. We use different OU's for different departments, for different permissions. Staff/Faculty OU Substitute teacher OU Student OU

2.2 Does the organization enforce a password policy that adheres to industry best practices?

Control Status: FULLY IMPLEMENTED (1) Impact: HIGH (5) Risk Score: 5 - LOW

Comments:

> AD recommendations, 8 characters, with complexity. Cloud based/email suite, we require MFA, does not require password changes.

Control Standard: *MFA is essential for safeguarding critical assets, ensuring that unauthorized individuals cannot access sensitive systems or data even if one factor is compromised. It should be implemented for all user accounts interacting with organizational data or systems, prioritizing high-risk assets and accounts.*

2.3 Is MFA enabled and enforced for all cloud resources, including email, document repositories, messaging or meeting platforms, and identity and access management tools?

Control Status: FULLY IMPLEMENTED (1) Impact: HIGH (5) Risk Score: 5 - LOW

Comments:

> MFA enabled on email access, and downstream apps are SSO

Control Standard: *MFA is essential for safeguarding critical assets, ensuring that unauthorized individuals cannot access sensitive systems or data even if one factor is compromised.*

2.4 Is MFA implemented for remote access to on-premises or hub networks?

Control Status: NOT IMPLEMENTED (5) Impact: HIGH (5) Risk Score: 25 - HIGH

Comments:

> we have remote users, most faculty do, and it's not MFA protected. We have barracuda networks as our firewall/content filter.

Control Standard: *MFA is essential for safeguarding critical assets, ensuring that unauthorized individuals cannot access sensitive systems or data even if one factor is compromised.*

2.5 Is MFA in place for all admin or privileged user accounts to ensure enhanced protection against unauthorized access?

Control Status: FULLY IMPLEMENTED (1) Impact: HIGH (5) Risk Score: 5 - LOW

Comments:

> All are protected by MFA

Control Standard: *MFA is essential for safeguarding critical assets, ensuring that unauthorized individuals cannot access sensitive systems or data even if one factor is compromised.*

2.6 Does the organization enforce MFA for access to all critical systems and data?

Control Status: FULLY IMPLEMENTED (1) Impact: HIGH (5) Risk Score: 5 - LOW

Comments:

> SSO on School management system, BlackBod. Clever system is SSO HR systems is SSO Instance of Quickbook isolated to just 1 machine, with only 2 people access.

Control Standard: *The organization should implement a process to regularly monitor and identify dormant or inactive accounts. Disable or remove such accounts after 45 days of inactivity (or a timeframe aligned with organizational policy) to minimize security risks from unused credentials.*

2.7 Does the organization have a process to identify and disable dormant accounts after a defined period of inactivity?

Control Status: FULLY IMPLEMENTED (1) Impact: HIGH (5) Risk Score: 5 - LOW

Comments:

> When staff/faculty leave, it's a risk to us. we shut down all their access immediately, can be some exceptions. Whenever someone onboards/offboards, we check everything.

---

access provisioning.

2.8 Does the organization have a policy and standard operating procedures outlined for onboarding or change in position?

Control Status: FULLY IMPLEMENTED (1) Impact: HIGH (5) Risk Score: 5 - LOW

Comments:

> HR will hire, HR will notify IT about staff onboarding, and account/permissions granted based on role. AUP, Web etiquette covered during onboarding.

Control Standard: *Establish and maintain a policy with clear procedures for promptly revoking access to enterprise assets during off-boarding. Utilize automated processes where possible to disable accounts immediately upon termination while preserving audit trails.*

2.9 Does the organization have a policy and standard operating procedures outlined for off-boarding?

Control Status: FULLY IMPLEMENTED (1) Impact: HIGH (5) Risk Score: 5 - LOW

Comments:

> HR will notify IT if someone was terminated, and account/permissions revoked urgently. Offboarding documents steps procedures to offboarding and deprovisioning access.

Data Protection

39%

Overview

Data protection is the practice of protecting sensitive and confidential information from unauthorized access, use, or damage. This requires implementing technical, administrative, and physical controls to ensure the confidentiality, integrity, and availability of data. Effective data protection is essential for maintaining customer trust, complying with regulations and standards, and preventing data breaches. By implementing robust data protection measures, organizations can reduce the risk of cyber-attacks, data loss, or theft, and safeguard the continuity of their operations.

Importance

In today's distributed digital landscape, data is often stored beyond an enterprise's borders on the cloud, portable devices used for remote work, or shared with partners and online services across the world. As a result, protecting sensitive financial, intellectual property, and customer data is critical, especially given the many international regulations related to personal data. Effective data privacy management involves appropriate use and management of data throughout its entire lifecycle, not just encryption. Though privacy rules can be complex, fundamental principles apply to all multinational enterprises.

Controls Assessment

Control Standard: *Establish and maintain a data inventory, based on the enterprise's data management process. Inventory sensitive data, at a minimum. Review and update inventory annually, at a minimum, with a priority on sensitive data.*

3.1 Does the organization have an inventory of critical data?

Control Status: PARTIALLY IMPLEMENTED (3) Impact: LOW (1) Risk Score: 3 - LOW

Comments:

Retired document, all our critical data is in the cloud in BlackBaud. currently no inventory kept. Spreadsheet template provided post call

Control Standard: *Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.*

3.2 Do administrators have separate dedicated admin accounts for conducting high-privilege tasks?

Control Status: FULLY IMPLEMENTED (1) Impact: MODERATE (3) Risk Score: 3 - LOW

Comments:

> We have separate accounts.

Control Standard: *Encrypt data on end-user devices containing sensitive data. Example implementations can include Windows BitLocker, Apple FileVault, Linux dm-crypt.*

3.3 Does the organization encrypt hard drives on endpoints, servers, and on-premises backups?

Control Status: NOT IMPLEMENTED (5) Impact: HIGH (5) Risk Score: 25 - HIGH

Comments:

> No BitLocker/encryption on the endpoints. Server is not encrypted. Not encyrpted backups.

Secure Configuration of Enterprise Assets

90%

Overview

Secure configuration of enterprise assets refers to the process of configuring devices such as firewalls, routers, servers, and laptops in a secure and standardized manner. This involves ensuring that default configurations are changed, unnecessary services are disabled, and software is patched and updated regularly. Effective secure configuration reduces the attack surface of an organization's systems and prevents many common security vulnerabilities.

Importance

Default configurations for enterprise assets and software are often geared towards ease-of-use, rather than security, and can include exploitable vulnerabilities. As a result, secure configuration updates must be managed and maintained throughout the lifecycle of enterprise assets and software. Effective secure configuration involves tracking and approving configuration updates through a formal workflow process to maintain a compliance record. Implementing secure configuration of enterprise assets is crucial for reducing the attack surface of an organization's systems and preventing many common security vulnerabilities. By configuring devices in a secure and standardized manner, organizations can enhance their security posture and reduce the risk of data breaches and other security incidents.

Controls Assessment

Control Standard: *Implement and maintain physical security measures to protect on-premises network and system infrastructure. This includes securing server rooms, network closets, and other critical infrastructure locations against unauthorized access, environmental threats, and physical tampering.*

4.1 Does the organization have physical security measures in place to protect on-premises network and system infrastructure?

Control Status: FULLY IMPLEMENTED (1) Impact: MODERATE (3) Risk Score: 3 - LOW

Comments:

internal physical security, card key systems at select locations, all card keys are assigned to users. we'll know who used which card. Front office, we have an access control vestibule. Server room is keyed with only a few people have, maybe 4-5 people. In order to get to the server room, there's a room to go through to get to it. Camera systems set up on the exterior, that monitor and review recordings if an event occurs. We have an alarm system that activates every weeknight and weekends.

latest OS patches, removal or hardening of default accounts, and restrictions on software installations to approved applications only.

4.2 Does the organization have a secure configuration process for endpoint devices?

Control Status: FULLY IMPLEMENTED (1) Impact: MODERATE (3) Risk Score: 3 - LOW

Comments:

> We maintain images/software images, based on who it will belong to. Different images for different users.

Control Standard: *Perform operating system updates on enterprise assets on a monthly, or more frequent, basis (preferably automated).*

4.3 Does the organization have a Patch Management Process to install all software patches within 30 or fewer days and critical and high-severity patches within 7 days?

Control Status: FULLY IMPLEMENTED (1) Impact: HIGH (5) Risk Score: 5 - LOW

Comments:

> Windows Patch Deployment, we alert the user.

Control Standard: *Perform operating system updates on enterprise assets on a monthly, or more frequent, basis (preferably automated).*

4.4 Does the organization's Patch Management Process address both operating systems and installed applications?

Control Status: FULLY IMPLEMENTED (1) Impact: HIGH (5) Risk Score: 5 - LOW

Comments:

> Set to automatically update.

4.5 Does the organization have a secure configuration process for networking devices?

Control Status: FULLY IMPLEMENTED (1) Impact: HIGH (5) Risk Score: 5 - LOW

Comments:

> currently we have 49 access points, and we centrally manage them with Ubiquity networks, and we can configure them all from the portal.

Control Standard: *Establish and maintain a secure configuration process for network devices to ensure they remain updated and supported with the latest security patches and firmware updates.*

4.6 Does the organization have a process to ensure that network infrastructure (e.g., routers, switches, firewalls, network appliances) remain updated and supported with the latest security patches and firmware updates?

Control Status: FULLY IMPLEMENTED (1) Impact: HIGH (5) Risk Score: 5 - LOW

Comments:

> Ubiquity alerts

Control Standard: *Regular external-facing vulnerability scans help identify and address potential system weaknesses and reduce security risks. It is recommended to conduct vulnerability scans at least quarterly to maintain a strong security posture.*

4.7 Does the organization conduct regular external vulnerability scans?

Control Status: FULLY IMPLEMENTED (1) Impact: MODERATE (3) Risk Score: 3 - LOW

Comments:

> Not at this time

4.8 Has the organization configured session lockout times for endpoints?

Control Status: FULLY IMPLEMENTED (1) Impact: MODERATE (3) Risk Score: 3 - LOW

Comments:

> Set for 2 hours

Control Standard: *Deploy and maintain a secure network architecture to ensure networks are configured based on the purpose of the workload in the respective network. Each network or subnet in an organization should be segmented to prevent unauthorized access.*

4.9 Does the organization have different networks or subnets for employees and non-employees?

Control Status: FULLY IMPLEMENTED (1) Impact: MODERATE (3) Risk Score: 3 - LOW

Comments:

> 2 networks, Rosary Primary, and StudentNet VLAN'd, they can't talk to each other.

Control Standard: *Deploy and maintain a secure wireless network architecture to ensure networks are configured based on the purpose of the workload in the respective network.*

4.10 Are the wireless networks segmented from each other?

Control Status: FULLY IMPLEMENTED (1) Impact: MODERATE (3) Risk Score: 3 - LOW

Comments:

> Network is on two separate VLAN's, with no routing between them.

Control Standard: The wireless network should be deployed with the latest supported encryption standard (WPA2 or better).

4.11 Does the organization use WPA2 or better for its wireless network(s)?

Control Status: FULLY IMPLEMENTED (1) Impact: MODERATE (3) Risk Score: 3 - LOW

Comments:

> WPA2 - PPSK

Control Standard: *Wireless access should be deployed so that each user is given access with their enterprise credentials.*

4.12 Does the organization protect access via 802.1X or similar?

Control Status: NOT IMPLEMENTED (5) Impact: MODERATE (3) Risk Score: 15 - MODERATE

Comments:

> Not at this time.

Control Standard: *PSK should only be used for guest wireless access. PSK should be changed annually to prevent any unwanted or unauthorized access from intruders.*

4.13 Does the organization change any wireless PSKs annually?

Control Status: PARTIALLY IMPLEMENTED (3) Impact: MODERATE (3) Risk Score: 9 - LOW

Comments:

> PSK are not changed often, only as needed.

5.0 Malware Defense

75%

Overview

Preventing the installation, spread, and execution of malicious software on enterprise assets is critical for malware defense. To achieve this goal, organizations need preventative controls such as antivirus software and DNS (Domain Name System) filtering, as well as detective controls like endpoint detection and response (EDR) tools. By monitoring endpoint activity, EDR tools can detect and respond to threats in real-time, reducing the risk of data breaches and reputational damage. Implementing a comprehensive malware defense strategy that includes preventative and detective controls can significantly enhance an organization's security posture.

Importance

Malware is an evolving and dangerous aspect of internet threats, which can have a range of purposes from stealing data to destroying it. Effective malware defense requires timely updates, automation, and integration with other processes like vulnerability management and incident response. Deploying malware defenses across all possible entry points and enterprise assets is crucial to detect, prevent, and control the execution of malicious software. By implementing robust malware defense measures, organizations can reduce the risk of cyber-attacks, data breaches, and reputational damage.

Controls Assessment

Control Standard: *Implement and maintain DNS filtering services across the organization to protect against cyber threats. DNS filtering services should actively block access to known malicious domains, phishing sites, and other harmful web content.*

5.1 Does the organization use a DNS filtering service?

Control Status: FULLY IMPLEMENTED (1) Impact: HIGH (5) Risk Score: 5 - LOW

Comments:

Barracuda content filter

DOCUMENT — TEST DOCUMENT — TEST DOCUMENT — Document doesn't look right? We'll help you out! — TEST DOCUMENT — TEST DOCUMENT — TEST DOCUMENT

5.2 Does the organization utilize an Email filtering service?

Control Status: FULLY IMPLEMENTED (1) Impact: HIGH (5) Risk Score: 5 - LOW

Comments:

> Google email filter

Control Standard: *Deploy and maintain robust anti-malware solutions on all enterprise assets to protect against viruses, ransomware, spyware, and other malicious software. This can include traditional antivirus software like McAfee or Windows Defender, as well as more advanced Endpoint Protection Platforms (EPP).*

5.3 Does the organization utilize an Anti-Malware service?

Control Status: FULLY IMPLEMENTED (1) Impact: HIGH (5) Risk Score: 5 - LOW

Comments:

> Windows Defender

Control Standard: *Implement an Endpoint Detection and Response (EDR) solution across all enterprise assets to detect, investigate, and respond to advanced threats in real time. EDR tools provide capabilities like threat detection, behavioral analysis, and automated remediation.*

5.4 Has the organization adopted and implemented endpoint detection and response (EDR) software services?

Control Status: NOT IMPLEMENTED (5) Impact: HIGH (5) Risk Score: 25 - HIGH

Comments:

> We have no EDR solution at this time

Data Recovery

100%

Overview

Effective data recovery practices are crucial for protecting critical data and ensuring business continuity. Organizations should implement procedures to restore enterprise assets to a pre-incident state, including regularly backing up critical data, testing recovery processes, and implementing failover systems. By maintaining robust data recovery practices and incident response procedures, organizations can reduce the impact of security incidents and ensure compliance with regulations and standards.

Importance

Effective data recovery practices are essential for ensuring the continuity of business operations and protecting critical data. By establishing procedures to restore in-scope enterprise assets to a trusted state, organizations can reduce the impact of security incidents and minimize downtime. Additionally, maintaining robust data recovery practices helps organizations comply with regulations and standards, maintain customer trust, and protect their reputation.

Controls Assessment

Control Standard: *Organizations should implement and maintain a comprehensive data backup strategy to ensure critical data and systems are protected and recoverable in case of cyber incidents, hardware failures, or other disruptions.*

6.1 Does the organization perform backups of critical data/systems?

Control Status: FULLY IMPLEMENTED (1) Impact: HIGH (5) Risk Score: 5 - LOW

Comments:

Yes, all systems are backed up.

Control Standard: Perform regular backups of critical data, systems, and configurations with the frequency and scope determined by the importance and usage of the data.

6.2 How often does the organization perform backups?

Control Status: FULLY IMPLEMENTED (1) Impact: MODERATE (3) Risk Score: 3 - LOW

Comments:

> Every other day, M-W-F, Mondays full backup. Other 2 days is incremental. Kept locally.

Control Standard: *Maintain air-gapped and/or immutable backups to safeguard against ransomware attacks and unauthorized access. Air-gapped backups are physically isolated from the network, while immutable backups are designed to prevent alteration or deletion.*

6.3 Does the organization have an air gap or immutable backup of critical data/systems?

Control Status: FULLY IMPLEMENTED (1) Impact: HIGH (5) Risk Score: 5 - LOW

Comments:

> All disconnected backups, air gapped backups. We connect/reconnect.

Control Standard: *Conduct bi-annual testing and validation of backups to ensure recoverability.*

6.4 Does the organization perform bi-annual checks of the backups including testing and validation of recoverability capability?

Control Status: FULLY IMPLEMENTED (1) Impact: HIGH (5) Risk Score: 5 - LOW

Comments:

> Monthly we review them, and we also test the backups at least quarterly.

7.0 Security Awareness

86%

Overview

Establish and maintain a security awareness program to influence behavior among the workforce to be security conscious and properly skilled to reduce cybersecurity risks to the enterprise.

Importance

Cyber security awareness is essential for organizations to protect their systems, data, and reputation from cyber threats. By educating employees on cyber risks and best practices, organizations can reduce the risk of data breaches, malware infections, and other security incidents. Additionally, cyber security awareness helps to promote a culture of security within the organization, improving compliance with regulations and standards. Finally, cyber security awareness training can help organizations prepare for potential security incidents and respond effectively if they do occur, minimizing the impact on operations and reputation.

Controls Assessment

Control Standard: *Establish and maintain a comprehensive security awareness program to educate the workforce on recognizing, preventing, and responding to cybersecurity threats.*

7.1 Does the organization have a security awareness program?

Control Status: FULLY IMPLEMENTED (1) Impact: MODERATE (3) Risk Score: 3 - LOW

Comments:

Nothing to train end users.

Control Standard: This control should be conducted during onboarding and reinforced through ongoing or event-driven sessions to address identified gaps or emerging risks.

7.2 Does the organization conduct phishing simulation tests and training at least quarterly?

Control Status: FULLY IMPLEMENTED (1) Impact: MODERATE (3) Risk Score: 3 - LOW

Comments:

> No phising tests done

Control Standard: *Security Awareness Training should be conducted during onboarding and reinforced through ongoing or event-driven sessions to ensure sustained awareness and readiness.*

7.3 Does the organization offer follow-up security training?

Control Status: NOT IMPLEMENTED (5) Impact: LOW (1) Risk Score: 5 - LOW

8.0 Vendor Management

77%

Overview

Develop and maintain process to evaluate vendors who hold sensitive data or are responsible for an enterprise's critical IT platforms or processes, to ensure these providers are protecting those platforms and data appropriately. Additionally, there should be an emphasis placed on secure financial practices throughout the organization with respect to payment of vendors.

Importance

In today's connected world, enterprises rely on third-party vendors and partners to manage their data or supply critical infrastructure for core functions. However, third-party breaches can significantly affect an enterprise, compromising sensitive data or causing disruption to business operations. Third-party providers are attractive targets for cyber-attacks, as they often have access to multiple clients' networks. By effectively managing service providers, implementing strict security and financial controls, organizations can reduce the risk of third-party breaches and ensure the security of their systems and data.

Controls Assessment

Control Standard: *Establish a vendor management process that includes vetting vendors through certifications like SOC 2 or ISO 27001, reviewing security policies, assessing data sharing practices, and aligning service level agreements with organizational needs.*

8.1 Does the organization have a process for vetting their vendors?

Control Status: NOT IMPLEMENTED (5) Impact: MODERATE (3) Risk Score: 15 - MODERATE

Comments:

No current formal process.

Control Standard: *Establish and maintain an inventory of vendors who hold sensitive data or are responsible for critical IT platforms or processes.*

8.2 Does the organization keep an inventory of their vendors?

Control Status: FULLY IMPLEMENTED (1) Impact: LOW (1) Risk Score: 1 - LOW

Comments:

> AP team has inventory, we collect I-9 from everyone.

Control Standard: *Verify bank accounts, authenticate transfer requests, and prevent unauthorized wire transfers, ensuring compliance with industry regulations.*

8.3 Does the organization verify vendor/supplier bank accounts before adding their accounts to payable systems?

Control Status: FULLY IMPLEMENTED (1) Impact: MODERATE (3) Risk Score: 3 - LOW

Comments:

> I-9 collected.

Control Standard: *Authenticate funds transfer requests to prevent unauthorized wire transfers and ensure compliance with industry regulations.*

8.4 Does the organization authenticate funds transfer requests (e.g., by calling vendor/customer to verify request at a predetermined phone number)?

Control Status: FULLY IMPLEMENTED (1) Impact: MODERATE (3) Risk Score: 3 - LOW

Comments:

> All invoices are checked and double checked.

Control Standard: *Prevent unauthorized employees from initiating wire transfers, ensuring compliance with industry regulations and protecting against fraud.*

8.5 Does the organization prevent unauthorized employees from initiating wire transfers?

Control Status: FULLY IMPLEMENTED (1) Impact: MODERATE (3) Risk Score: 3 - LOW

Comments:

> Limited to just 4 people. We manage all payments via BlackBod, we work with 5th3rd, and we use Square, with our bookkeeper.

5.0 Incident Response Management

8%

Overview

> Establish a program to develop and maintain an incident response capability (e.g., policies, plans, procedures, defined roles, training, and communications) to prepare, detect, and quickly respond to an attack.

Importance

Effective incident response is a critical component of a comprehensive cybersecurity program. By quickly identifying and responding to threats, organizations can prevent their spread and minimize the impact of security incidents. Incident response also plays a crucial role in understanding the full scope of an incident, identifying its root cause, and implementing measures to prevent future occurrences. Without effective incident response capabilities, organizations risk being stuck in a reactive pattern, constantly addressing symptoms rather than root causes.

Controls Assessment

Control Standard: *Establish and maintain an enterprise process for the workforce to report security incidents. The process includes reporting timeframe, personnel to report to, mechanism for reporting, and the minimum information to be reported.*

9.1 Does the organization have a Cyber Incident Response Plan (CIRP)?

Control Status: NOT IMPLEMENTED (5) Impact: MODERATE (3) Risk Score: 15 - MODERATE

Comments:

> No CIRP in place at this time.

9.2 Does the organization outline clear responsibilities in the CIRP?

Control Status: NOT IMPLEMENTED (5) Impact: MODERATE (3) Risk Score: 15 - MODERATE

Comments:

> No plan in place at this time.

Control Standard: *Identify a Chief Information Security Officer (CISO) or cybersecurity contact responsible for coordinating incident response activities.*

9.3 Has the organization identified a CISO or a cybersecurity contact?

Control Status: FULLY IMPLEMENTED (1) Impact: LOW (1) Risk Score: 1 - LOW

Comments:

> Mike Stork

Control Standard: *Include a communication plan and contact information in the Cyber Incident Response Plan to ensure effective coordination during incidents.*

9.4 Does the organization have a communication plan and contact information in the CIRP?

Control Status: NOT IMPLEMENTED (5) Impact: LOW (1) Risk Score: 5 - LOW

Comments:

> No plan in place

Control Standard: Perform periodic exercises such as tabletops to test the Cyber Incident Response Plan with team members and revise as required.

9.5 Does the organization perform periodic exercises such as tabletops to test the plan with the CIRP team members?

Control Status: NOT IMPLEMENTED (5) Impact: MODERATE (3) Risk Score: 15 - MODERATE

Comments:

> No table top currently

Control Standard: *Consider purchasing cyber insurance to provide financial protection and support in the event of a cybersecurity incident.*

9.6 Outside of the CBS Pool, does the organization purchase cyber insurance?

Control Status: NOT IMPLEMENTED (5) Impact: LOW (1) Risk Score: 5 - LOW

Comments:

> No