CP

CYBERPOOLS.ORG

Cybersecurity Risk Assessment

Sample Organization

Assessment Date:	11/05/2025
Report Date:	11/05/2025
Conducted By:	Assessment Team
Member Contact:	Contact Person

Introduction

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 September 2025, and in alignment with our continuous improvement practices across all Cyber Toolkit services, CyberPools has enhanced the grading formula used in this assessment. The updated methodology ensures that scores more accurately reflect implementation status across each control category and the overall assessment.

While the overall score provides a high-level benchmark, members should place greater emphasis on the control categories and the associated risk ratings (Low, Medium, High). These ratings highlight which areas carry greater weight in reducing organizational risk and therefore warrant more focused attention during remediation planning.

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

Executive Summary

[EXECUTIVE SUMMARY - CUSTOMIZED BY ACCOUNT MANAGER]

This section provides a high-level strategic overview of the assessment findings. The Account Manager reviews the detailed results and synthesizes key strengths and priority opportunities for improvement.

Sample Executive Summary:

"The organization demonstrates strong cybersecurity fundamentals with excellent performance in access management and incident response capabilities. A mature backup strategy and comprehensive security awareness program reflect the organization's commitment to operational resilience. Primary opportunity exists in implementing DNS filtering to strengthen malware defense posture. Overall, the assessment reveals a well-managed security program with focused areas for enhancement."

Note: This placeholder text will be replaced with custom content entered by the Account Manager in the CRM system. The executive summary should be 4-8 sentences highlighting strategic insights, key strengths, and priority recommendations.

Summary of Results

80%

OVERALL RISK SCORE

2

HIGH RISK

4

MODERATE RISK

44

LOW RISK

Section Scores

NO.	SECTION	SCORE
1.0	Inventory and Control of Assets	96%
2.0	Account Management	57%
3.0	Data Protection	33%
4.0	Secure Configuration of Enterprise Assets	79%
5.0	Malware Defense	83%
6.0	Data Recovery	88%
7.0	Security Awareness	106%
8.0	Vendor Management	103%
9.0	Incident Response Management	87%

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.

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.

How to Read This Report

This assessment provides a comprehensive evaluation of your organization's cybersecurity posture. Each section is designed to give you actionable insights with full context for decision-making.

Report Structure

Control Categories: Nine security focus areas covering the full spectrum of cybersecurity controls

Category Scoring: Each category receives an overall percentage score (higher is better)

Individual Questions: Detailed assessment of specific controls within each category

Understanding Category Pages

Each category section includes:

1. **Category Header**

   Category number, name, and overall score percentage with visual grade badge

2. **Category Overview**

   Brief description of what this category covers and why it matters

3 Why It Matters

Business impact and real-world risks if controls in this area fail

4 Control Assessment Questions

Detailed evaluation of individual controls (see breakdown below)

Understanding Question Blocks

Each control question provides comprehensive context:

Question Number & Text	e.g., 1.1 Does the organization inventory all devices?
Control Description	Explains what the control does and best practices
Control Status	FULLY IMPLEMENTED (1) PARTIALLY IMPLEMENTED (3) NOT IMPLEMENTED (5)
Impact	LOW (1) MODERATE (3) HIGH (5)
Risk Score	Calculated as Control Status × Impact. Higher scores indicate greater risk.
Assessment Notes	Field observations, evidence, and context from the assessment team

Using This Report

- Review the **Key Findings** section first for immediate priorities
- Use category scores to identify focus areas for improvement
- Reference Assessment Notes for specific remediation guidance
- Track progress over time by comparing scores between assessments

⚠ KEY FINDINGS

The following controls were highlighted based on their risk scores and should be reviewed with the stakeholder team.

High Risk Findings (2)

Risk Score 16-25 – requires immediate attention.

0.0 Unknown Question (ID: 21eb4c81...)

Category: Account Management

Control Status: NOT IMPLEMENTED (5) Impact: MODERATE (3) Risk Score: 25 - HIGH

> No formal offboarding process.

0.0 Unknown Question (ID: b2a06977...)

Category: Data Protection

Control Status: NOT IMPLEMENTED (5) Impact: MODERATE (3) Risk Score: 25 - HIGH

> Not enabled FileVault, we will be pushing out version 26 soon, which comes with filevault. Servers are not encrypted No encryption on backups

Moderate Risk Findings (4)

Risk Score 11-15 – schedule remediation activities.

0.0 Unknown Question (ID: 52800943...)

Category: Account Management

Control Status: PARTIALLY IMPLEMENTED (3) **Impact:** MODERATE (3)
Risk Score: 15 - MODERATE

> we're working on streamlining that process. It's a bit informal, and we just hear through the "grape vine" that someone was hired. Access is granted based on role.

0.0 Unknown Question (ID: 25922a65...)

Category: Secure Configuration of Enterprise Assets

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

> users can define that. students we have a session time of 10 minutes.

0.0 Unknown Question (ID: 5c46e5bb...)

Category: Secure Configuration of Enterprise Assets

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

> Not at this time

0.0 Unknown Question (ID: 66fb305d...)

Category: Incident Response Management

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

> No table tops ran yet.

Cyber Requirements 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

Note: Items marked "No" represent areas requiring immediate remediation to ensure compliance with cybersecurity best practices and insurance requirements.

1.0

Inventory and Control of Assets

96%

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

0.0 Unknown Question (ID: 4e256554...)

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

Comments:

> Jamf and Google Admin console, and we use Instinctive to manage Chromebook devices, we use in addition to GAM, gives us a more granular look. All devices are asset tagged, mac and sn notated.

0.0 Unknown Question (ID: 42e46a89...)

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

Comments:

> WPA2 - PPSK Meraki solution limits local area network acccess, switches and AP, and they have a built in firewall feature, allow us to implement NAC. Devices that are plugged in, are hardwired to VLAN, or connect to default network. We are not filtering by MAC addresses

---

0.0 Unknown Question (ID: 49b1fdb8...)

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

Comments:

> We began establishing a doc with our business office, that shows our vendors, expiration dates, renewal periods.

0.0 Unknown Question (ID: 2ddff9d2...)

Control Status: FULLY IMPLEMENTED (1) Impact: MODERATE (3) Risk Score: 5 - LOW

Comments:

> No EOL currently We do have AP's at our lower grade school, that are going to be EOL in 2026, and we are phasing them out.

2.0 Account Management

57%

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

0.0 Unknown Question (ID: ddc56966...)

Control Status: FULLY IMPLEMENTED (1) Impact: MODERATE (3) Risk Score: 5 - LOW

Comments:

> we don't have remote access connections, and if we do grant it, we keep those open for the amount of access they need.

0.0 Unknown Question (ID: 8864a47a...)

Control Status: FULLY IMPLEMENTED (1) Impact: MODERATE (3) Risk Score: 5 - LOW

Comments:

> All MFA

0.0 Unknown Question (ID: c3d35793...)

Control Status: FULLY IMPLEMENTED (1) Impact: MODERATE (3) Risk Score: 5 - LOW

Comments:

> MFA protected critical systems, and if they do not have MFA, they use google SSO.

0.0 Unknown Question (ID: e5c8fefc...)

Control Status: FULLY IMPLEMENTED (1) Impact: MODERATE (3) Risk Score: 5 - LOW

Comments:

> Usually at beginning of the year, we perform sweeps and remove any dormant accounts not used. Judge it based on whether or not the person is part of the district, once we get confirmed they are gone, we remove their account and associated licenses. Faculty we give them some time to close out their accounts and more relevant items. Admins get longer time, to ensure they can access sensitive info or otherwise.

0.0 Unknown Question (ID: 52800943...)

Control Status: PARTIALLY IMPLEMENTED (3) Impact: MODERATE (3) Risk Score: 15 - MODERATE

Comments:

> we're working on streamlining that process. It's a bit informal, and we just hear through the "grape vine" that someone was hired. Access is granted based on role.

0.0 Unknown Question (ID: 21eb4c81...)

Control Status: NOT IMPLEMENTED (5) Impact: MODERATE (3) Risk Score: 25 - HIGH

Comments:

> No formal offboarding process.

0.0 Unknown Question (ID: 75e0f1f6...)

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

Comments:

> AD is main repository, and Google for students. We have offloaded service accounts for Google workspace, we are able to keep service accounts active, but limited to what they can do or access, and can only use it for what they need it for.

0.0 Unknown Question (ID: 6ffb751c...)

Control Status: FULLY IMPLEMENTED (1) Impact: MODERATE (3) Risk Score: 5 - LOW

Comments:

> 8 char + with 3/4 complexity. No forced PW changes.

0.0 Unknown Question (ID: d6b5984b...)

Control Status: FULLY IMPLEMENTED (1) Impact: MODERATE (3) Risk Score: 5 - LOW

Comments:

> MFA enabled for all staff emails

3.0

Data Protection

33%

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

0.0 Unknown Question (ID: 5c1a240b...)

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

Comments:

Nothing at this time.

0.0 Unknown Question (ID: ee21191d...)

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

Comments:

> separate accounts

0.0 Unknown Question (ID: b2a06977...)

Control Status: NOT IMPLEMENTED (5) Impact: MODERATE (3) Risk Score: 25 - HIGH

Comments:

> Not enabled FileVault, we will be pushing out version 26 soon, which comes with filevault. Servers are not encrypted No encryption on backups

4.0

Secure Configuration of Enterprise Assets

79%

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

0.0 Unknown Question (ID: 71c04895...)

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

Comments:

> We have locks on all server rooms, with specific keys for cdertain people. Access controls and camera's everywhere.

0.0 Unknown Question (ID: 00be77b9...)

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

Comments:

> JAMF helps configure all Apple devices. Depends on who needs the devices and what they need, system is configured on per case basis.

0.0 Unknown Question (ID: 9782ade0...)

Control Status: FULLY IMPLEMENTED (1) Impact: MODERATE (3) Risk Score: 5 - LOW

Comments:

> JAMF and Acronis assists with patching

0.0 Unknown Question (ID: 0347bdfc...)

Control Status: FULLY IMPLEMENTED (1) Impact: MODERATE (3) Risk Score: 5 - LOW

Comments:

> Only JAMF does Apps, Acronis patches OS

0.0 Unknown Question (ID: cfc6760b...)

Control Status: FULLY IMPLEMENTED (1) Impact: MODERATE (3) Risk Score: 5 - LOW

Comments:

> We do those manually, we use a config template. We built it manually based on network doc specifics.

0.0 Unknown Question (ID: ef9e6b1d...)

Control Status: FULLY IMPLEMENTED (1) Impact: MODERATE (3) Risk Score: 5 - LOW

Comments:

> Internally handled, we have an alert system that lets us know about updates. We use third-party cloud managed solutions, Meraki, which alerts us to update. Acronis does the patching as well.

0.0 Unknown Question (ID: b8a56435...)

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

Comments:

> CyberPools

0.0 Unknown Question (ID: 25922a65...)

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

Comments:

> users can define that. students we have a session time of 10 minutes.

0.0 Unknown Question (ID: 6fa75575...)

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

Comments:

> SSIDs: 7 SSID's, actively use 3, student, staff, and CCSVIT (IT team, for overview of network, not broadcasted) and SSID for IoT, and peripherals. And a guest network, with splash screen captive portal. elementary school has a SSID, with extra security precautions, so that the health employees using that SSID, can get to their security portal.

0.0 Unknown Question (ID: 02fb049d...)

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

Comments:

> IT team can traverse all, the rest are segmented.

0.0 Unknown Question (ID: 7644e4a9...)

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

Comments:

> WPA2-PPSK

0.0 Unknown Question (ID: 5c46e5bb...)

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

Comments:

> Not at this time

0.0 Unknown Question (ID: 7a360ec9...)

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

Comments:

> PSK's are changed, last time it was changed was when we put up the new APs

5.0

Malware Defense

83%

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

0.0 Unknown Question (ID: 5a80ba2c...)

Control Status: FULLY IMPLEMENTED (1) Impact: MODERATE (3) Risk Score: 5 - LOW

Comments:

> DNS - We use LimeWize, and Firewall, GoGuardian on student devices

0.0 Unknown Question (ID: 64577c3f...)

Control Status: FULLY IMPLEMENTED (1) Impact: MODERATE (3) Risk Score: 5 - LOW

Comments:

> Google email filter, education+

0.0 Unknown Question (ID: a7bdcd9b...)

Control Status: FULLY IMPLEMENTED (1)   Impact: MODERATE (3)   Risk Score: 5 - LOW

Comments:

> Acronis EDR

0.0 Unknown Question (ID: 9215cad3...)

Control Status: FULLY IMPLEMENTED (1)   Impact: MODERATE (3)   Risk Score: 5 - LOW

Comments:

> Acronis EDR

6.0

Data Recovery

88%

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

0.0 Unknown Question (ID: feeab3b0...)

Control Status: FULLY IMPLEMENTED (1) Impact: MODERATE (3) Risk Score: 5 - LOW

Comments:

> Yes

0.0 Unknown Question (ID: ba30b5bc...)

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

Comments:

> VEEAM for backups in cloud, Nightly full backups, which is backed up to NAS (Qnap)

0.0 Unknown Question (ID: cd72f5cf...)

Control Status: FULLY IMPLEMENTED (1) Impact: MODERATE (3) Risk Score: 5 - LOW

Comments:

> Air gap VEEAM backups

0.0 Unknown Question (ID: e95173e9...)

Control Status: FULLY IMPLEMENTED (1) Impact: MODERATE (3) Risk Score: 5 - LOW

Comments:

> We usually try to them once quarter. Full recoverys

7.0

Security Awareness

106%

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

0.0 Unknown Question (ID: c57ac602...)

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

Comments:

> CyberPools phishing and awareness training. Innovative teaching coach sends out newsletters and bits of information about best practices, and what to watch for.

0.0 Unknown Question (ID: 4d15f50e...)

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

Comments:

> CP campaigns

0.0 Unknown Question (ID: acb6e426...)

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

Comments:

> Yes, when we notice some users require further education, we'll address it

8.0

Vendor Management

103%

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

0.0 Unknown Question (ID: 255e7396...)

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

Comments:

> SOPPA compliance, and no software can be downloaded without IT approval. Learn approval used to show which apps are SOPPA compliant, and at what level.

0.0 Unknown Question (ID: bd3192a9...)

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

Comments:

> Learn platform displays all of our SOPPA compliant vendors, and it's public facing on our website.

0.0 Unknown Question (ID: 4f878db9...)

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

Comments:

> w-9 collected as verification, we do not pay wires or checks.

0.0 Unknown Question (ID: 0d554ad2...)

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

Comments:

> If anything looks suspicious, we'll verify by calling a known number.

0.0 Unknown Question (ID: 7b903cea...)

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

Comments:

> No wire transfers

9.0

Incident Response Management

87%

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

0.0 Unknown Question (ID: 3fe16317...)

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

Comments:

> Built a CIRP using the template last year, could use an update

0.0 Unknown Question (ID: d626ce23...)

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

Comments:

> everyone involved knows their roles

0.0 Unknown Question (ID: 4c59c42f...)

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

Comments:

> CISO or cybersecurity contact, Rene

0.0 Unknown Question (ID: 349d6344...)

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

Comments:

> yes

0.0 Unknown Question (ID: 66fb305d...)

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

Comments:

> No table tops ran yet.