CP
CYBERPOOLS.ORG

Cybersecurity Risk Assessment

Santa Catalina School

Assessment Date:	10/15/2025
Report Date:	10/23/2025
Conducted By:	Alex Robles
Member Contact:	Jodi Wiseley

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

Santa Catalina School achieved an overall cyber risk score of **82%**, reflecting a **strong cybersecurity foundation** with effective controls in **asset management**, **multi-factor authentication**, **vendor oversight**, and **staff awareness**.

The school demonstrates **mature practices** through **comprehensive MFA enforcement**, **air-gapped backups**, and **regular security training**, but key vulnerabilities remain in **Incident Response** and **Endpoint Security**.

Specifically, the absence of a formal **Cyber Incident Response Plan (CIRP)**, lack of **Endpoint Detection and Response (EDR)**, and limited **endpoint encryption** present elevated risks to timely detection and recovery.

Strengthening these areas by implementing a **CIRP**, deploying **EDR**, **encrypting devices** and establishing a **backup validation process** will significantly enhance the school's readiness and resilience against modern cyber threats.

Summary of Results

82%

OVERALL RISK SCORE

1

HIGH RISK

8

MODERATE RISK

42

LOW RISK

Section Scores

NO.	SECTION	SCORE
1.0	Inventory and Control of Assets	**89%**
2.0	Account Management	**88%**
3.0	Data Protection	**72%**
4.0	Secure Configuration of Enterprise Assets	**87%**
5.0	Malware Defense	**75%**
6.0	Data Recovery	**86%**
7.0	Security Awareness	**100%**
8.0	Vendor Management	**100%**
9.0	Incident Response Management	**8%**

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 (1)

Risk Score 16-25 – requires immediate attention.

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

Category: Malware Defense

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

> There is no EDR.

Moderate Risk Findings (8)

Risk Score 11-15 – schedule remediation activities.

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

Category: Account Management

Control Status: PARTIALLY IMPLEMENTED (3) Impact: HIGH (5) Risk Score: 15 - MODERATE

> We don't have an automated process yet, but we do try to regularlyy monitor at least once a year. at this time, Departed employees' accounts are currently disabled but not deleted for retention purposes.

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

Category: Account Management

Control Status: PARTIALLY IMPLEMENTED (3) Impact: HIGH (5) Risk Score: 15 - MODERATE

> We do have an onboarding process managed through a Google Form and IT ticketing, but we don't have a formalized process for position changes.

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

Category: Data Protection

Control Status: PARTIALLY IMPLEMENTED (3) Impact: HIGH (5) Risk Score: 15 - MODERATE

> Not on endpoints. Acronis is encrypted.

4.8 Has the organization configured session lockout times for endpoints?

Category: Secure Configuration of Enterprise Assets

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

> We do not have an enforced session lockout policy. Default settings apply, which appear to lock devices after approximately two minutes of inactivity.

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

Category: Data Recovery

Control Status: PARTIALLY IMPLEMENTED (3) Impact: HIGH (5) Risk Score: 15 - MODERATE

> We do test our recovery process at least annually.

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

Category: Incident Response Management

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

> No we don't, we are in the process of working on this.

9.2 Does the organization outline clear responsibilities in the CIRP?

Category: Incident Response Management

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

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

Category: Incident Response Management

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

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
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?	√ Yes
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?	✗ No
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?	√ Yes

> **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

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:

> We do have an inventory of all company-owned devices maintained in Mosyle. Windows devices are currently inventoried in the Meraki dashboard and are being transitioned into Mosyle. The inventory includes device type, serial number, MAC address, assigned user, operating system, hard drive status, Apple ID, model, and last update time. Devices generally follow a consistent naming convention based on user and model. We do use asset tags—primarily on newer equipment.

Control Standard: *Ensure a process exists to identify and address unauthorized assets frequently. This includes wireless access and wired network ports. The enterprise may choose to remove the asset from the network, deny the asset from connecting remotely to the network, 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: FULLY IMPLEMENTED (1) Impact: MODERATE (3) Risk Score: 3 - LOW

Comments:

> We do have controls in place to detect and restrict unauthorized devices. Unused wired ports are disabled or unpatched, and VLAN segmentation isolates critical networks. Wireless access uses Google OAuth authentication, requiring domain credentials to connect to faculty or student SSIDs. Guest networks are isolated, and alerting is in place for rogue access points. Local network access also requires password authentication.

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

Comments:

> We partially have an inventory of licensed software. Bulk-purchased applications are tracked, and there is a process for reassigning or removing licenses as needed. However, end users maintain local administrator rights, so software installed individually by users is not centrally inventoried.

Control Standard: *Ensure that only currently supported software is designated as authorized in the software inventory for enterprise assets. Any end-of-life (EOL) software, which is unsupported, yet necessary for the fulfillment of the enterprise's mission, should be 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:

> We do have a process to track and decommission end-of-life (EOL) applications. Alerts from vendors or internal monitoring prompt review and notification to affected users. We do have some legacy PCs running EOL software that remain in use but are noted and segmented accordingly.

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:

> We do have an inventory of user accounts in our Google admin, with different OU's for different employee groups.

Control Standard: *Ensure the organization has implemented and enforces a password policy that aligns with current best practices as outlined by leading authorities such as NIST, CISA, Microsoft, and other cybersecurity experts.*

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:

> We have a password policy requiring at least 12 characters, one number, one special character, and one capital letter. Password expiration is not enforced but resets are recommended if risks are identified.

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:

> We do have MFA enforced for all cloud resources including Google (primary data repository), Zoom (SSO), and other key platforms.

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

Comments:

> We do have MFA enforced for VPN access via Meraki protocol, though VPN usage is limited.

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:

> We do have MFA enforced for all admin and privileged accounts.

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:

> We do have MFA for critical systems, including cloud and VPN access. Blackbaud systems have MFA.

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: PARTIALLY IMPLEMENTED (3) Impact: HIGH (5) Risk Score: 15 - MODERATE

Comments:

> We don't have an automated process yet, but we do try to regularlyy monitor at least once a year. at this time, Departed employees' accounts are currently disabled but not deleted for retention purposes.

Control Standard: *Implement and maintain a policy with clear, documented procedures for granting access to enterprise assets during onboarding or role changes. This process should include automated workflows where possible to ensure timely, consistent, and secure access provisioning.*

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

Control Status: PARTIALLY IMPLEMENTED (3) Impact: HIGH (5) Risk Score: 15 - MODERATE

Comments:

> We do have an onboarding process managed through a Google Form and IT ticketing, but we don't have a formalized process for position changes.

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:

> We have an offboarding process that uses the same Google Form and Excel tracking sheet to disable accounts and wipe/collect devices.

3.0

Data Protection

72%

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

Comments:

> We do keep a spreadsheet for the sensitive data we keep and it is regularly updated as needed.

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 do use admin accounts for elevated tasks.

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: PARTIALLY IMPLEMENTED (3) Impact: HIGH (5) Risk Score: 15 - MODERATE

Comments:

> Not on endpoints. Acronis is encrypted.

4.0

Secure Configuration of Enterprise Assets

87%

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

Comments:

> We do have physical security controls in place. The vast majority of networking and system equipment is stored in lockable spaces or cabinets. Lower school sites use locked tech carts, and all classrooms are lockable. Access to network equipment requires physical keys, and security cameras are installed in key areas.

Control Standard: *Establish and maintain a secure configuration process for all enterprise assets, including end-user devices, IoT devices, servers, and software. This process should include creating a standardized "golden image" for endpoint deployment that incorporates the 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 do have a secure configuration process managed through Mosyle. Configurations are standardized

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:

> We do have a patch management process managed through Mosyle and supported by KT. Patches are monitored, tested, and deployed as needed, with attention to critical and high-severity updates.

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:

> We do have patching processes that cover both operating systems and applications. However, some Mosyle-managed apps rely on user-initiated updates rather than automatic patching.

Control Standard: *Establish and maintain a secure configuration process for network devices. This includes management of default accounts on enterprise assets and software, such as root, administrator, and other pre-configured vendor accounts.*

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:

> We do have standardized and secure configurations applied across Cisco Meraki devices, matching VLAN and security settings across the network.

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:

> KT manages firmware and security updates for all network infrastructure components.

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:

> We do not have regular external vulnerability scanning in place.

Control Standard: *Configure automatic session locking on enterprise assets after a defined period of inactivity. For general-purpose operating systems, the period should not exceed 15 minutes. For mobile end-user devices, the period should not exceed 2 minutes.*

4.8 Has the organization configured session lockout times for endpoints?

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

Comments:

> We do not have an enforced session lockout policy. Default settings apply, which appear to lock devices after approximately two minutes of inactivity.

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:

> Yes, we have separate networks, including guest, faculty/staff, shared laptop, student, and AirPlay/printer networks, as well as a residual VLAN for administrative use.

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:

> Yes, we have wireless segmentation in place. Access is controlled through VLANs and access control lists (ACLs), with no inter-VLAN routing, except for AirPrint and AirPlay functionality.

Control Standard: *The wireless network access controls should be deployed with the latest accepted encryption standards (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 personal

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

Comments:

> We do have 802.1X-equivalent protection implemented through Google OAuth authentication for wireless access.

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:

> We do not have a formal annual PSK rotation schedule. Wireless passwords are updated as needed, but not on a recurring annual basis.

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:

> DNS protection is managed through Mosyle's Device Scout, along with the Meraki firewall's content filtering and intrusion detection features.

Control Standard: *Email filtering services should detect and filter spam, phishing attempts, and emails containing malicious attachments or links, safeguarding the organization from email-based threats.*

5.2 Does the organization utilize an Email filtering service?

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

Comments:

> Email filtering is configured and enforced through google.

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:

> Webroot - Anti-Virus solution.

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:

> There is no EDR.

6.0

Data Recovery

86%

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 we use syscloud.

Control Standard: *Perform regular backups of critical data/systems to minimize potential data loss, aligning the frequency with 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:

> Continuous through the day.

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:

> Yes we do, Syscloud is our back up target which is air gapped.

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:	PARTIALLY IMPLEMENTED (3)	Impact:	HIGH (5)	Risk Score:	15 - MODERATE

Comments:

> We do test our recovery process at least annually.

7.0

Security Awareness

100%

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:

> We utilize the KnowBe4 platform for security awareness.

Control Standard: *This program should include regular phishing simulation tests conducted at least quarterly, and follow-up training 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:

> Yes. While these were not previously held on a regular cadence, we do conduct our phishing awareness trainings through KnowBe4. We have completed one so far this school year with future sessions now scheduled, including a training at the start of the school year.

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

Comments:

> Yes this is set up through KnowBe4

8.0

Vendor Management

100%

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

Comments:

> Yes, we do. Jodi leads this process. We review all contracts that the school enters into, often involving legal counsel when necessary. We use several methods to assess vendor reputability, including recommendations from the National Association of Independent Schools and other districts. We also rely on guidance from our legal counsel, who works with other independent schools, as well as referrals from our existing vendors.

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:

> Business office keeps a list of those vendor. IT also keeps its own list as well.

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:

> we do require a w9 from all vendors

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:

> we usually do a verbal verification of bank account.

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:

> Yes our banking site is a dual authorization system no one person can initiate a transfer. It requires dual authorization.

9.0

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 we don't, we are in the process of working on this.

Control Standard: *Ensure the incident response plan includes clear responsibilities for all team members.*

9.2 Does the organization outline clear responsibilities in the CIRP?

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

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

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:

> Not in a CIRP but we do have this as part of the emergency response plan.

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

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

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

Comments:

> Yes, through Lloyd's of London.

Thank You for Participating

We appreciate your commitment to strengthening your cybersecurity posture. This assessment is an important step in protecting your organization.

Questions or Feedback? Our team is here to help. Contact us at cyber@cyberpools.org

Our Services

Our comprehensive suite of cybersecurity services designed to protect pools and their members.

SERVICE	WHAT IT DOES
Vulnerability Scans	External scan of networks for vulnerabilities, prioritized report of any vulnerabilities identified during scan, and remediation guidance to safeguard against exploitation of known vulnerabilities
Risk Assessments	High-level overview of IT infrastructure to determine cyber posture, identify gaps in best practices, and provide remediation guidance
Phishing and Training Campaigns	Phishing emails sent to member staff to test and raise awareness, report of campaign outcomes, and remediation guidance to safeguard against predatory phishing
Incident Response Planning	Guidance creating a written incident response plan to help streamline response during an actual event
IT Policy Templates	Access to downloadable, customizable policies and assistance customizing selected policies to members' specific systems and resources
MFA and EDR Group Purchasing	Bulk purchasing to make multi-factor authentication (MFA) and endpoint detection and response (EDR) resources more affordable for members
vCISO Consulting	On-demand access to a virtual chief information security officer (vCISO) for cybersecurity guidance on topics such as network architecture, access control, encryption, etc.
Tabletop Exercises	Scenario exercises designed to guide you through a possible "real-life" incident in preparation for an actual event
Claims Consulting	Post-claim assistance with remediation, plus management of vendors and/or third-party claims adjusters
Education	A library of webinars, presentations, and white papers to help educate your staff, members, and clients