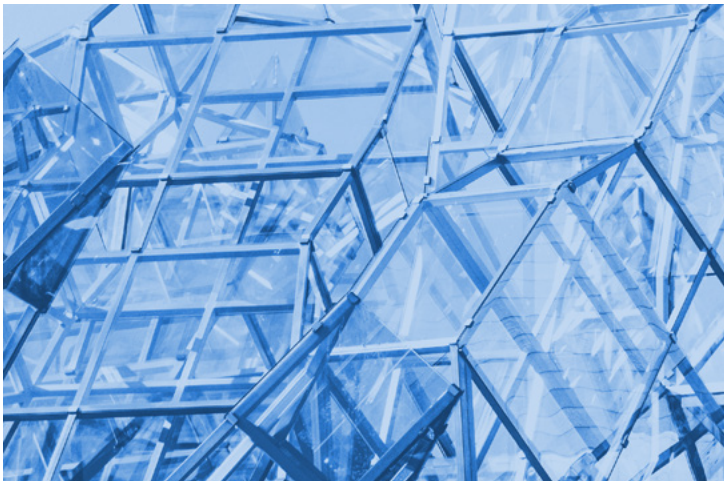
ESSENTIAL
CYBERSECURITY PRACTICES FOR K12

Produced by METL (Michigan Education Technology Leaders), an MAISA affiliated Organization.

Created for Michigan schools, by Michigan technology experts.



FOR MORE INFORMATION | MISECURE.ORG

misen Michigan Statewide Educational Network

MAISA MICHIGAN ASSOCIATION OF INTERMEDIATE SCHOOL ADMINISTRATORS SUPPORTING REGIONAL EDUCATION SERVICE AGENCIES

merit

ESSENTIAL CYBERSECURITY PRACTICES FOR K12

FIRST REVISION

For all the links listed
here and a PDF version
of this document visit:
misecure.org

Produced by METL (Michigan Education Technology Leaders),
an MAISA affiliated Organization and made possible by the efforts
of the following organizations:

misen
Michigan Statewide Educational Network

MAISA
MICHIGAN ASSOCIATION OF INTERMEDIATE SCHOOL ADMINISTRATORS
SUPPORTING REGIONAL EDUCATION SERVICE AGENCIES

merit

Contents

Introduction

Technology is a double-edged sword. Our school districts have embraced technology in order to educate students, improve educational outcomes and reduce overall costs for instruction. Unfortunately, all of this technology comes with a hidden cost. If not managed correctly, our new technology can expose us to significant financial loss, reputation damage and legal risk. Consequently, the need for properly managing cybersecurity is greater today than ever before in public education.

The reality is that cyber attacks are very likely to be local and extremely personal. In one case, a student was able to access their principal's Social Security Number and gladly shared it on social media for the world to see. In another, an employee opened a malicious email which caused all of the district's data files to be held in ransom, crippling the ability to instruct and do business. Threats like these are just a few examples of why cybersecurity must be a priority for educational leadership.

Unfortunately, cybersecurity is not a simple task that can be achieved by simply doing one thing. It is a lot like being a homeowner - your roof, HVAC, plumbing, electrical, and landscaping are just a few things you need to work on and balance in order to have a safe and comfortable home. Similarly, cybersecurity involves many components that all need to be balanced in order to keep your sensitive data away from prying eyes and your computer systems up and functioning. Cybersecurity is an ongoing process.

Thankfully, there is guidance available to help manage this large landscape of cybersecurity. The Center for Internet Security has created the "Top 20 Security Controls" - a comprehensive framework of specific and actionable things that organizations need to do to fortify their security posture against very real cybersecurity threats. This guide applies these twenty security concepts that, when implemented, substantially reduce risk and allow technology to properly do the job it is supposed to: help us educate our students.

This guide was developed and written by IT staff working at school systems across the state of Michigan, with the goal of translating these security controls into actions that make the most sense for K12 environments. Our aim is to convey to district leadership how each of these security controls affects daily operations, showcase easy and inexpensive actions that leadership and IT staff can accomplish, and give tips and next steps on how to get started.

It is our collective responsibility to protect the information we have about our students, as well as ensure our computer systems are resilient from active threats. We are excited to present this guide as the first step towards ensuring that our schools can not only accomplish this goal, but also to set an example of how cybersecurity can be performed in the educational space.

1 - Inventory and Control of Hardware Assets

MATT McMAHON
ASSOCIATE SUPERINTENDENT
FOR TECHNOLOGY
GRATIOT-ISABELLA RESD

Executive Summary

Schools need to make access to their network convenient but also secure. IT staff need to know what devices are on the network and where they are. Students and staff expect schools to support mobile personal devices, wireless networks and remote access. Any device on the network has potential to create a security issue. District IT staff should have an accurate inventory of all District owned devices and be able to locate and control access to devices connected to the District network.

Potential Solutions

It is common to find a mixture of devices in schools including Windows and OSX computers, mobile devices such as iPads, and Chromebooks. To keep inventory of these devices, most districts use multiple solutions. For computers, System Center Configuration Manager (SCCM) provides inventory and control. For mobile devices, a Mobile Device Manager (MDM) is typically used. Chromebooks are managed by the G Suite for Education console. Using these three solutions, most schools can **keep an accurate inventory** of district owned devices.

Network managers must be able to **quickly locate and control** any device attached to the school network. One way to do this is by referencing the live data within switches and routers, wireless controllers and DHCP logs. This provides inventory and control of the devices currently attached to the network. More sophisticated services such as “LanTopoLog” and “Netdisco” are designed to maintain historical records of device access.

Networks should be subnetted to **limit access** between guest and district-maintained hardware. Network access controls such as 802.1x should be implemented to ensure that only authorized users can access protected networks. Hot ports - those which are patched but unused - should be removed or moved to the guest network. Wireless controllers typically allow for multiple wireless networks to be created so that guest and district devices can be segregated.

Case Study

All users at Sunnyside Schools connect to a single, flat network. A user configuring their personal device, statically assigns the device the IP address of the network gateway which breaks Internet access for everyone. Using "show ip arp" on the router, the network administrator is able to locate the MAC address of the user. Using "show mac-address" on the switch, they are able to locate the specific port the user is connected to and disable it.

GETTING STARTED

Netdisco[1]

LanTopoLog[2]

Locating a device on your network[3]

NEOLA Policy 5136:
Wireless Communication Devices

NEOLA Policy 7543:
Remote Access To The District's Network

GETTING STARTED

CIS Control 2 Information [3 & 4]

Michigan Government General Retention Schedule, #800 - Technology Inventory (Page 26) [5]

NEOLA 7540:

Computer Technology and Networks

NEOLA 7540 .06:

Computer Hardware and Software Management

2 - Inventory and Control of Software Assets

JOSH HAYES
DIRECTOR OF THE ETA
EDUCATIONAL TECHNOLOGY ASSOCIATION

Executive Summary

Management of software assets is one of the best ways to harden school systems. Proper software management enables schools to keep an active inventory of all approved software on end user devices, enabling IT staff to easily know when certain devices need to be updated, patched, or replaced.

Keeping software up-to-date is vital for security, as attackers will attempt to use vulnerabilities in old software to compromise computer systems. By managing your software and the ways computers can run it, you can limit risk and place your district into an excellent security posture.

Potential Solutions

IT staff should **maintain a software inventory system**, keeping it up to date and routinely audited. An asset inventory system can be an open source platform (such as Spiceworks), a paid for solution (such as WASP), integrated into currently used enterprise management solution (such as Microsoft SCCM), or a simple spreadsheet.

Ultimately, the best way to stop malware is to **disable the ability** for staff to install their own software. The software employees need to perform their jobs should come pre-loaded on their computers, with IT staff taking requests to install non-standard software. By vetting and approving these exceptions, IT staff can maintain their inventory list and quickly respond to additional requests to install non-standard software.

In addition to using anti-virus software to detect and stop threats, **using application whitelisting** via built-in tools can easily monitor and manage software. This prevents malware from running even without permanently installing itself, as it would not be on the "approved" list of programs permitted to run. IT staff can prepopulate the approved whitelist with software, making deployment across your district manageable and obtainable.

Case Study

At Sunnyside Schools, endpoints infected by ransomware were remediated but the virus kept coming back. IT staff reviewed network logs and device/software inventory to try to trace where the virus may be originating from. After some further investigation, IT staff discovered traffic from a particular IP within the local network. IT eventually found the PC that had the IP address of the ransomware traffic. IT determined the PC was not in the hardware or software inventory system and wasn't managed with updates, therefore IT was unable to track it or apply software updates to it since it was not included with the rest of the managed PCs. Not having a software asset/inventory asset management system led to a vulnerability for the organization.

3 - Continuous Vulnerability Management

SAM LUTGRING
ASSISTANT SUPERINTENDENT
CALHOUN ISD

Executive Summary

New and updated vulnerabilities are constantly being discovered and published, which makes it hard for K-12 administrators to stay ahead of these discoveries. It is critical to monitor and mitigate both new and old vulnerabilities; this means ensuring that all applications and operating systems are patched to current levels and actively monitored for critical vulnerabilities. In some cases, it even becomes necessary to temporarily mitigate application vulnerabilities until software vendors can write updates to address the issue.

Potential Solutions

Many vendors provide automated software updates or notifications when new patches are released. Districts should not block these updates on machines as this can leave them exposed to attack. Instead, it is recommended that districts **develop a patch management process** for operating systems and major applications.

As part of this process, IT staff should **monitor for newly released patches** and vulnerabilities, and test these patches in a test or sandbox environment so they can be vetted before applied to primary IT systems.

When applying patches to IT systems, **designate maintenance windows** where systems can be offline for these security updates. This should occur after a designated time and frequency for mitigation review to ensure all appropriate patches have been applied to all systems.

In addition to staying current with published updates, districts should **monitor for initial vulnerabilities** that may not yet be patched and take appropriate actions to mitigate. There are multiple sources for this information available, including free mailing lists and security communities.

To confirm that all security patches and appropriate configuration is in place, **use a vulnerability scanner** on your network to automatically detect remaining issues and present them to IT staff via a report which contains actionable instructions on how to resolve remaining issues.

Case Study

Sunnyside School District utilizes SCCM to manage all Windows patches and updates. Utilizing this method, IT staff push out a CRITICAL Windows update to all servers, believing that all servers are now patched and up to date. Two weeks later, during a routine security patch level review, it is determined that one of the servers was missed. The update is quickly applied and the server is brought into compliance.

GETTING STARTED

US-CERT - Weekly Vulnerability Summary:

Previous Bulletins plus subscription information

Department of Homeland Security:

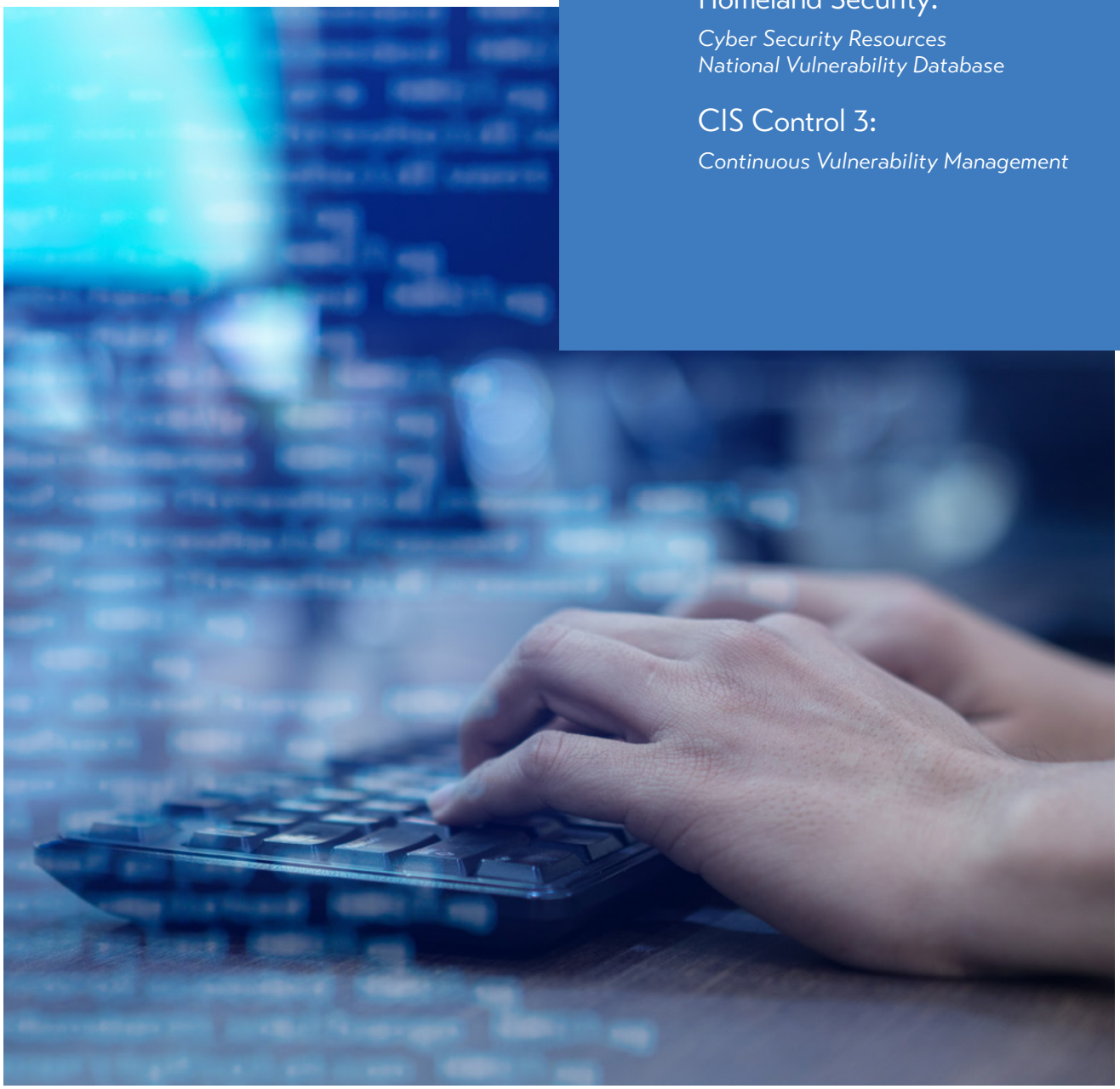
US-CERT Resources

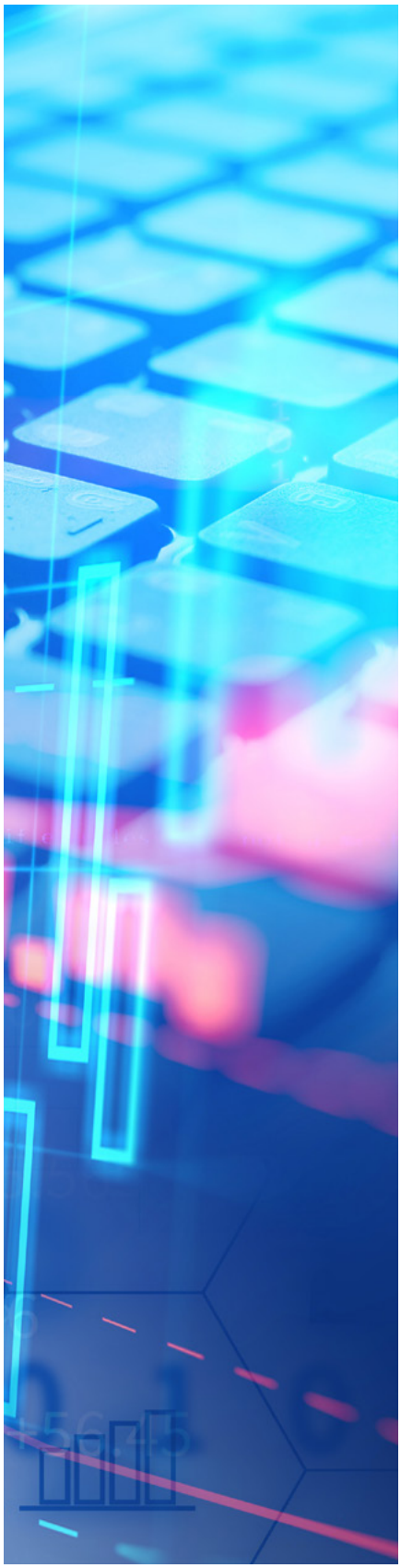
Department of Homeland Security:

Cyber Security Resources
National Vulnerability Database

CIS Control 3:

Continuous Vulnerability Management





4 - Controlled Use of Administrative Privileges

ALEX HARGROVE
SENIOR SYSTEMS ENGINEER
CLARE GLADWIN RESD

Executive Summary

Every computer and network device has a privileged Administrator account which is used to make system-level changes. These accounts are the "keys to the kingdom", and are especially targeted by attackers as it allows them full control the system, including the ability to hide their tracks. Browsing websites or opening a malicious email message while logged in as an Administrator on a local computer creates an avenue for malware and keyloggers to be installed without the user's knowledge, leading to credential theft.

Potential Solutions

IT staff should **maintain an inventory** of administrator accounts on all district systems, including any external systems such as Domain Name registration and hosted cloud solutions. This list should be **audited periodically** to ensure there are no errant entries or access.

Administrator passwords should always be **changed from their defaults**, as attackers can easily guess passwords that are still set by the manufacturer. They should also be unique for every service, never reused, and be randomly generated while following established best practices regarding length and complexity.

Administrative tasks should be performed using a dedicated account from a dedicated computer which does not have email or general Internet access; this prevents common web or email attacks from gaining a foothold on an Administrator account. For normal day-to-day computing activities, a regular account should be used on a workstation that can be reinstalled at any time in the event of a malware attack.

To fully protect Administrative accounts, **multi-factor authentication** should be used whenever possible to ensure that only authorized users - and not attackers - are using these accounts. Additionally, a Privileged Access Management (PAM) solution can not only securely share passwords amongst IT staff, but also **quickly change passwords** in the event of an incident or departure of a disgruntled employee.

Case Study

Sunnyside School District had to dismiss a system administrator who had privileged access to all servers, network devices, and workstations. Manually changing the passwords on each system was an extreme burden to the remaining staff members. The decision to implement a Privileged Access Manager (PAM) was made. This allowed system passwords to be brought under managed control with automatic scheduled rotation. Additionally, the business office was able to move away from a shared spreadsheet containing account information. This spreadsheet contained confidential passwords for paying bills and accessing payroll information. These passwords were transferred to a private section of the PAM which was only accessible to business office staff. Finally, a "break glass" procedure was created utilizing a complex master password stored in a vault accessible by the Superintendent and Business Manager, allowing them to access all password information in the event of an emergency.

GETTING STARTED

US CERT Choosing and Protecting Passwords [6]

CIS Control #4 [7]

How to enable Multi-factor authentication for various online services [8]

Microsoft LAPS [9]

GETTING STARTED

CIS Control #5 [10]

CIS Benchmarks [11]

Security Technical Implementation Guides [12]

5 - Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers

BOB HODGES
NETWORK ENGINEER
WAYNE RESA

Executive Summary

Default manufacturer settings on devices and software frequently come with default account passwords and outdated security protocols enabled. It is important for schools to create secure configurations and remove unnecessary software to reduce exposure and eliminate avenues of attack.

Potential Solutions

To securely manage laptops and workstations, school IT staff should **create operating system images** containing only the software needed by staff and students. The latest software and OS patches must be installed, default settings changed, and administrative access restricted to authorized users. Using **OS deployment tools**, the IT staff can then quickly load the image onto all school laptops and workstations and track any deviation from this image.

To secure the configuration of servers, schools must identify each server's job and determine which services and protocols are required to perform that job. To minimize the server's attack surface, **only required services and protocols should be enabled**. CIS provides guidelines for hardening servers, so reviewing their benchmark documents is a good place to start.

A Mobile Device Manager (MDM) can be used to manage and **secure iOS and Android devices**. The MDM allows schools to enforce security policies, deploy updates, and restrict device functionality to only allow features and apps needed by students and staff.

6 - Maintenance, Monitoring and Analysis of Audit Logs

DAVID LARSON
NETWORK ENGINEER
LIVINGSTON ESA

Executive Summary

Logs, as records of system events, are the eyes of your network. Without them you are essentially blind to any attacks which may be taking place. Most equipment has limited storage for logs, so a central log server is the best way to collect and maintain historical data. Besides troubleshooting issues, logs are the only method for detecting or proving an attack has taken place. For these reasons, maintaining a proper logging and audit system is key for any district.

Potential Solutions

In order to troubleshoot issues or investigate security incidents, **detailed logging should be enabled** on all servers, systems, and applications in the district. By including information such as timestamps, addresses, usernames, and event types, IT staff can quickly respond to most scenarios. Important logs to collect include DHCP messages to track network access, firewall logs to track visitors to malicious Internet sites, and workstation logs to track usage of individual computers.

Logs should be **sent to a centralized logging server** so they can be stored and analyzed in a single location. Free logging server applications available that are easy to set up and maintain; "Syslog-ng" and "Graylog" are both great options that are easy to use. The logging server should be installed separate from your main environment, as your logging server should remain available in case of failure of your primary environment.

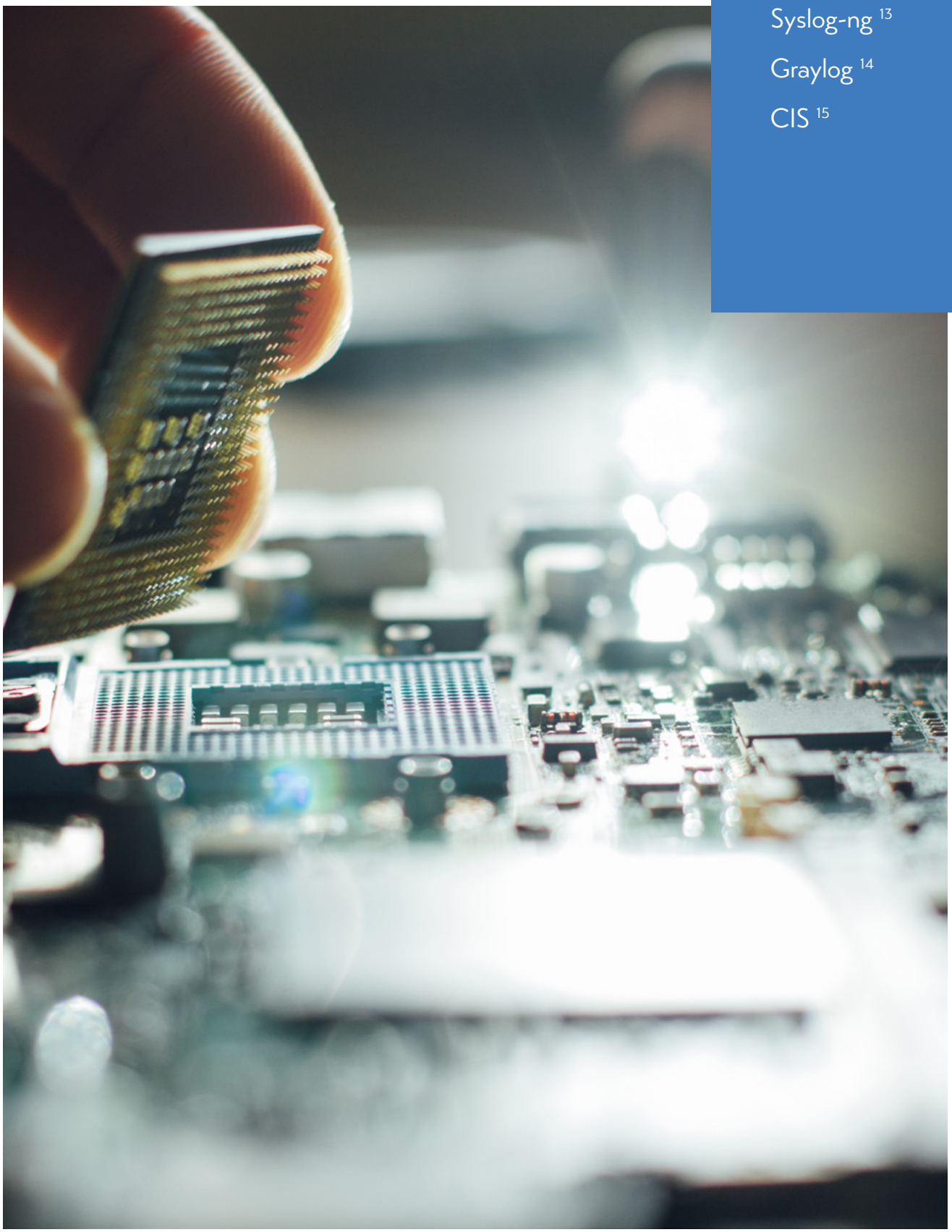
When a high priority security event occurs, the logging server should **notify the appropriate staff**, typically via an email or text message; this ensures that critical events are seen and act on quickly. Examples of such events include off-hours usage of systems and the creation of administrator accounts where they are not expected. Just as important, summaries or scheduled reports of log information should be **reviewed on a regular basis** for abnormalities.

GETTING STARTED

Syslog-ng [13]

Graylog [14]

CIS [15]



7 - Email and Web Browser Protections

MATT MCMAHON
ASSOCIATE SUPERINTENDENT
FOR TECHNOLOGY
GRATIOT-ISABELLA RESD

Executive Summary

Reading email and browsing the web are the most common end-user computer activities - and also the most dangerous. Most computer and network security incidents such as malware attacks or phishing attempts originate through email or Internet browsing. Schools need to make sure that proper tools are in place and being maintained to protect against these threats.

Potential Solutions

Protecting against web browsing attacks involves **installing a web-filtering solution** that often includes components on both the network as well as individual computers. This is especially important as most schools participate in E-rate, and are therefore required to filter for "obscene or harmful content" by the "Children's Internet Protection Act" (CIPA). Filtering products nearly always include **filtering of websites**, including pornography, adult topics, phishing and malware sites.

Network filtering devices are usually tied into a firewall strategy and include products such as "iBoss", "LightSpeed", "Sophos" and "Fortinet". Software that is installed on devices is usually purchased or licensed on a per-device or per-student basis and managed centrally, with common solutions including "GoGuardian" and "Securly". All filtering components should **log website requests** for review in the event of a security incident.

Web browsing software on computers must be **kept up to date**, including any plugins or extensions. Attackers commonly target web browsers by installing malware on the Internet and waiting for people to browse their malicious websites.

Email protection is often included as part of your email service; Google for Education and Microsoft each offer spam, phishing and malware monitoring. If a school manages their own email, or if the email provider's solution is inadequate, the school might **purchase a spam filtering solution** such as those offered by Barracuda Networks.

Case Study

Sunnyvale Public Schools is connected to Regional RESD using a fiber network. Its traffic, along with all other district traffic, goes through an iBoss content filter located at the RESD before it goes to the Internet. The content filter is configured to block "phishing", "malware", "spam", and other categories in order to protect users. All email sent to Sunnyvale Public Schools' staff goes to their Google for Education email accounts. Google scans email for virus and phishing attempts.

GETTING STARTED

CIPA [16]

iBoss [17]

Barracuda [18]

NEOLA Policy 7540:
Computer Technology And Networks

NEOLA Policy 8305 A:
Information Security Responsibilities

8 - Malware Defenses

ANDREW HAHN
SUPERVISOR, TECHNOLOGY AND DATA SERVICES
WASHTENAW ISD

RYAN GOYETTE
TECHNOLOGY SECURITY SPECIALIST
WASHTENAW ISD

Executive Summary

Defending against malware is typically difficult due to the many entry points in any given environment. End-user devices, email attachments, online downloads, malicious websites, and removable media are just some of the ways that malware can enter an organization. While a standard anti-virus solution will stop some malware in its tracks, many different malware types can bypass anti-virus solutions, necessitating a comprehensive approach to stopping malware from compromising the district.

Potential Solutions

Proper malware defense still begins with **installing antimalware software** on all desktops, laptops, and servers in the district. This software should have updated definition files - this allows the anti-malware software to detect the latest and most critical malware and viruses applicable today. Anti-malware software should be configured to **scan removable devices** such as USB sticks when they are plugged in; these are still common ways for malware to spread.

The log files from anti-malware should be **centrally logged** so that IT staff can report on the level of compliance of district computers, as well as quickly respond as soon as any infection is detected.

Modern operating systems (such as Windows 10) include imbedded features to help fight malware. These **anti-exploitation features should be enabled** as they can help prevent attacks where no known signatures files exist for antimalware software.

Case Study

Sunnydale Schools was the recipient of Emotet malware via an email phishing attack. While the initial infected computers were caught quickly, the virus spread rapidly due to not having an organization-wide antimalware solution in place. While learning on the fly, it became apparent that the virus could not hop networks, and could be brought under control using basic Microsoft Forefront Protection. The solution scanned twice a day and reported which computers were infected with specific viruses. This helped by narrowing down and tracking infected endpoints for manual reimaging, manual removal of the virus, and tracking down other infected endpoints.

GETTING STARTED

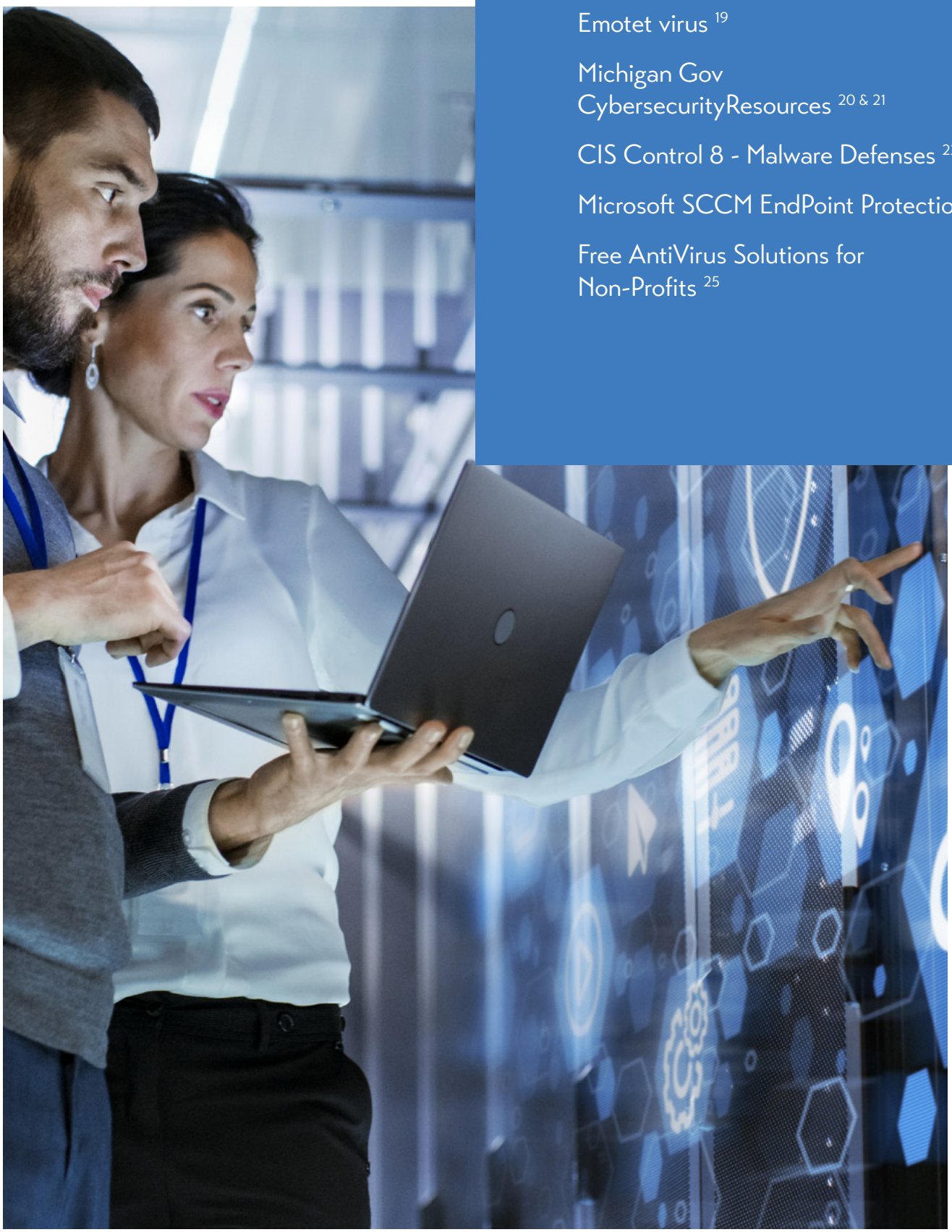
Emotet virus [19]

Michigan Gov CybersecurityResources [20 & 21]

CIS Control 8 - Malware Defenses [22 & 23]

Microsoft SCCM EndPoint Protection [24]

Free AntiVirus Solutions for Non-Profits [25]



GETTING STARTED

CIS Control #9
Application Software Security

Rapid7:
Limitation and Control of Ports Protocols and Services

Shodan [26]

MxToolbox [27]

Nmap [28]
Schedule daily Nmap scans with a script [29]

Disabling older protocols [30]

9 - Limitation and Control of Network Ports, Protocols and Services

ALEX HARGROVE
SENIOR SYSTEMS ENGINEER
CLARE GLADWIN RESD

Executive Summary

In order for a school network to be useful, it must provide access to computing services such as file and print sharing, DNS, and web filtering. School IT staff must ensure that only authorized users are accessing these services, and to prevent attackers from abusing the services to steal sensitive information or to compromise computer systems. Limiting the computers that can access district IT services along with disabling unnecessary services altogether can help stop this threat.

Potential Solutions

Only services **intended for public use** should be directly exposed to the Internet; attackers are continuously scanning the Internet looking for vulnerable systems, so reducing this footprint as much as possible is critical. Internal systems, including remote administration tools such as Remote Desktop, VNC, and SSH should be accessible only from the district network.

Internally to the district, IT staff should **disable legacy protocols** on network servers and hardware wherever possible. **Enabling workstation firewalls** with default "Block" rules will also stop attacks from spreading within your protected network. These actions dramatically reduce your risk in the event an attacker obtains a foothold inside your network via other means, such as phishing email attack.

To support employees accessing district resources remotely, require the **use of a Virtual Private Network (VPN)** with two-factor authentication. This ensures that the users of your IT services are legitimate employees and not attackers with stolen passwords.

Free tools such as "nmap" and "zenmap" can be used to internally **validate these secure changes** and make sure your security footprint is as small as possible. Additionally, using online tools such as "Shodan" and "MxToolbox" allow you to **check your network for misconfigurations** which could potentially be seen and exploited by attackers on the Internet.

Case Study

Sunnyside Schools deployed a new web filtering solution which listened for requests from clients on port 8080. After a few days, the proxy became very sluggish, and both the hardware resources on the proxy and its Internet connection were maxed out. It was discovered that while port 8080 was listening on the internal network, it was also listening on the public Internet-facing side as well. The proxy had been discovered by automated scripts called "bots" scouring the Internet for misconfigurations such as this, and was being used to proxy network traffic from unauthorized people all over the world. Once the proxy was reconfigured to only allow connections from the internal network, performance returned to normal.

10 - Data Recovery Capabilities

DAVID LARSON
NETWORK ENGINEER
LIVINGSTON ESA

Executive Summary

Despite all of our efforts, it is a hard truth that network and security controls can fail. When this happens, attackers can compromise district systems, shut down critical systems, and alter or delete data stored on district systems. Ensuring that data and system backups are in place and tested thoroughly is the only way you can trust the integrity of your data and fully recover from these attacks.

Potential Solutions

Your district should **use a comprehensive backup strategy** that ensures that all critical files, databases, and documents are backed up on a regular basis. Full backups should be performed at minimum on a weekly basis, with more frequent backup operations happening for modified or critical files. These backups should also **include configuration files** of your infrastructure devices such as switches, routers, and firewalls, as their operation is critical for your district. Backups should **use encryption** in order to protect confidential and student data; attackers frequently search for backup files as they commonly have less security protection.

As part of your strategy, the "3-2-1" backup method will help ensure you have copies of data, even in unexpected situations. This involves having three copies of district data (including the original), using two different types of storage, and keeping one copy off-site.

All backups should be **tested and verified** on a regular basis; it is extremely common for backup procedures to be incorrect or ineffectual. If you do not test backups, then you don't have backups.

Depending on your IT architecture, it may be advantageous to **backup entire computer systems**, instead of just specific data files. This can decrease the time it takes to restore service in the case of serious compromise, as in many cases it is the only way to be completely sure that all malware and attacker activity is gone.

Case Study

Network equipment configurations are saved using open-source software onto a VM. All VMs are backed up using paid software onto a physically separate system from the main servers. These backups are then copied to an off-site location at the ISD/ESA or onto cloud storage.

GETTING STARTED

Data Recovery Capability [31]

CIS Critical Control 10 [32]

Data Backup Options [33]

GETTING STARTED

Rapid7 Blog - CIS Control 11

CISecurity.org - CIS Control 11

NIST Guide for Security-Focused Config Management of Information Systems

11 - Secure Configuration for Network Devices

TROY CALGARO
MANAGER/NETWORK OPERATIONS
OTTAWA AREA ISD

Executive Summary

Just like computers, the infrastructure devices that run your district's network can be attacked and exploited. These devices - switches, routers, and firewalls - are especially important as successful attackers could gain access to private networks, redirect traffic, intercept information while in transmission, and other nefarious actions. Because these infrastructure devices are not your typical computer workstation, special care must be undertaken to secure them from harm.

Potential Solutions

The most important aspect of securing infrastructure devices is to **maintain a secure and standard configuration template** which can be reused throughout the district. By default, most devices are not configured securely and must be modified to change things such as default passwords, user accounts, and who can manage the device itself. Infrastructure devices should **utilize two-factor authentication** wherever possible in order to ensure that they are not being changed by attackers with stolen credentials. Additionally, devices should be **managed via a private, out-of-band management network** which only IT staff have access to; this prevents unauthorized staff or students from even attempting to attack the infrastructure. Numerous free examples of these configurations exist for use, and IT staff can easily modify them to best suit their needs.

Once standard configurations are implemented, automated tools should be used to **detect changes** to the configuration files and alert on any unauthorized modifications. Configuration files should be documented, reviewed, and approved by an organization change control process, with any deviations clearly documented and approved.

It is important for both security and business continuity to **document firewall rules**; the specific business reason for each rule should be outlined, along with a specific individual's name responsible for that business need, and an expected duration of the need.

Finally, IT staff must **apply security patches** regularly to infrastructure devices. Although this is commonly overlooked, these devices are just as vulnerable as standard computers. Security advisories concerning infrastructure devices should be reviewed, with IT staff properly classifying any risk and subsequently deciding schedules for applying security patches.

12 - Boundary Defense

BOB HODGES
NETWORK ENGINEER
WAYNE RESA

Executive Summary

Attackers are constantly probing school networks for weaknesses, so it is important that schools implement effective boundary defense controls to protect the flow of information as it enters and exits your private network. Firewalls exist at network boundary points and can identify, detect, and prevent attacks. Schools should ensure they have a perimeter firewall in place to reduce the chances of successful attacks reaching internal networks.

Potential Solutions

School districts should **install a firewall** at the boundary between the Internet and internal networks to protect against Internet-based attacks and to limit the exposure of internal systems. The firewall should be configured to only permit traffic that is explicitly approved by the district and have an integrated intrusion prevention system (IPS) module or support the installation of an IPS module so that it can analyze, identify, and stop known attacks.

An effective defense strategy for schools is to **segment the internal network** into multiple networks and to control the flow of data between those networks. Once segmented, a firewall can control and protect the data flowing between networks. If a firewall is unavailable, access control lists (ACLs) can be configured on network routers to permit or deny traffic between networks.

The best defense against unauthorized remote access connections is to require employees to **use a VPN connection** to access your school district's private network while offsite. VPN connections should require two-factor authentication to prevent attackers from using compromised employee credentials to gain unauthorized access. Connections to remote access tools like VNC, TeamViewer, and Remote Desktop should not be allowed from offsite locations.

GETTING STARTED

CIS Control #12 [34]

Rapid 7 Blog [35]

NEOLA Policy 7543:
Remote Access to the District's Network

GETTING STARTED

Sudent Privacy White Paper [36]

FERPA [37]

NEOLA Policy 8305:
Information Security

NEOLA Policy 8330:
Student Records

13 - Data Protection

MATT MCMAHON
ASSOCIATE SUPERINTENDENT
FOR TECHNOLOGY
GRATIOT-ISABELLA RESD

Executive Summary

Many schools underestimate the responsibility they carry to securely manage and protect student and staff data. This protection means identifying and regularly monitoring existing data, limiting access to and use of that data, and understanding and adhering to applicable laws such as FERPA, HIPAA, and COPPA.

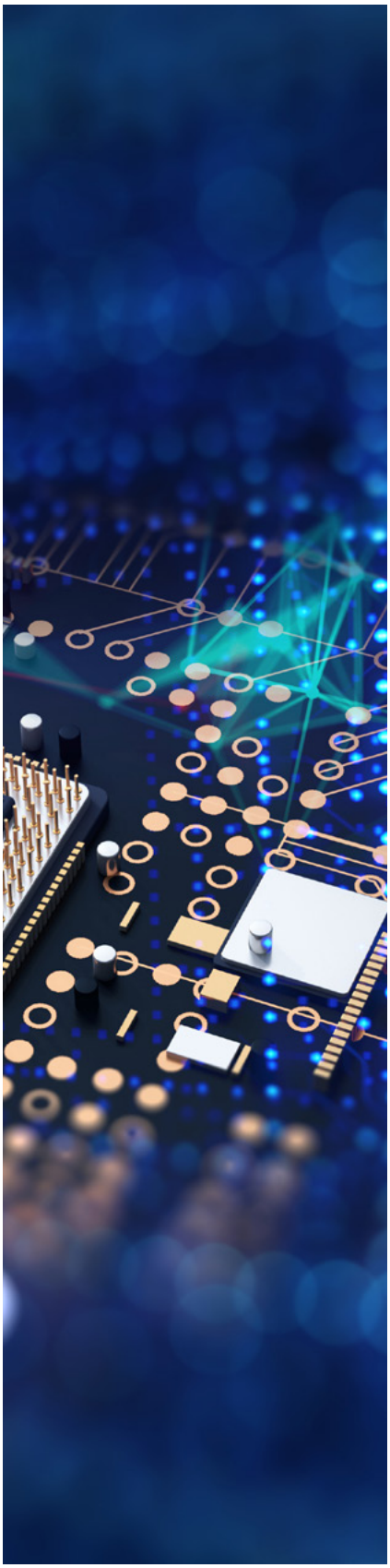
Potential Solutions

To begin with, school districts must maintain an accurate **sensitive data inventory** identifying where any sensitive, confidential, or protected data is stored. This can be a simple spreadsheet identifying the location, data owner, business purpose, and data elements which are being stored. This inventory should be updated regularly by soliciting district leadership for input and feedback, and any data storage systems no longer under sanctioned use should be removed.

Implementing data protection practices often results in making it harder to share data. For instance, rather than a school working from a single shared folder, users may have to consider each file's contents, who should (and shouldn't) have access to that file, and make sure it is **saved in an appropriate, secured location**.

Sending or transmitting data is also a large concern; while sending a file via unencrypted email may be convenient and quick, copies will linger in mailboxes for years to come. Sharing files using flash drives will avoid passing files through the Internet, but that data - even after it's deleted - can linger on the flash drive indefinitely. Software to easily **encrypt and decrypt files** and messages alleviates many of these problems, and is often required for data protected under Federal law.

Federal and state legislation is becoming more aggressive in protecting electronic data and privacy. Districts should **review their requirements** on compliance with cybersecurity and privacy legislation with their legal counsel, including the Family Educational Rights and Privacy Act (FERPA), the Health Insurance Portability and Accountability Act (HIPAA), and the Children's Online Privacy Protection Act (COPPA).



14 - Controlled Access Based on the Need to Know

ALEX HARGROVE
SENIOR SYSTEMS ENGINEER
CLARE GLADWIN RESD

Executive Summary

The ability to securely store and retrieve data is a core function of a school network. While not all data is confidential, more and more sensitive information is being stored electronically every day. Therefore, it is important to ensure that only those users who are supposed to access this information are able to do so, while keeping the data secure from prying eyes.

Potential Solutions

Most modern computer networks offer the ability to limit access to data and resources based on Access Control Lists, or ACLs. On network servers and cloud-based solutions alike, it is important to ensure that users have a so-called Home Directory which only they have access to, and a shared space to collaborate with other users. Permissions should be strict and only the **minimum set of rights necessary** to perform a given job function should be granted to each user or group of users. This is especially important to manage in the software that manages school and district functions, such as purchasing, payroll, HR, and student records.

Attackers may silently move between workstations and servers, accessing one after another until they find a high-value target with access to critical information. This lateral movement can be easily blocked by implementing **host-based firewalls** and ACLs.

Full-disk encryption should be deployed to mobile devices such as laptops so that in the event of loss or theft, the data contained on the hard drive is not accessible to anyone without the proper credentials. Additionally, volume-level encryption can be enabled on district-owned servers.

Case Study

Sunnyside Public Schools wanted to increase the security of their network, which was initially designed as a "flat" network where all devices were able to communicate directly with all other devices. After careful planning, the network was redesigned into a segmented structure where devices were logically grouped based on function, and ACLs based on least-privilege were implemented:

- Student workstations
- Teacher workstations
- Administrative staff workstations
- Internal Servers
- DMZ Servers
- Printers
- Network Management

GETTING STARTED

IP Addressing and VLAN Planning Document [38]

NetIQ eDirectory Permissions [39]

MicroFocus Open Enterprise Server File System Permissions [40]

Microsoft Active Directory Security [41]

Windows Server File System Permissions [42]

Google Drive Permissions [43]

Protect access to data and services in Office 365 [44]

Securing Privileged Access [45]

Avenues Of Lateral Movement [46]

MicroFocus ZENworks Full Disk Encryption [47]

Microsoft Bitlocker Disk Encryption [48]

VeraCrypt Disk Encryption [49]

15 - Wireless Access Control

BILL PATTERSON
NETWORK SECURITY ANALYST
INGHAM ISD

Executive Summary

Wireless networks are pervasive everywhere, and that also means that a threat can come from anywhere. Improperly configured or controlled wireless networks could allow unauthorized devices to access internal resources or infect the network. Because physical access to district buildings is often not required, attackers can be virtually invisible and access your wireless networks from nearby parking lots or sidewalks. Proper care must be placed into the design and operation of wireless networks in order to minimize the risk that they pose.

Potential Solutions

Your district should have an **inventory of approved wireless access points** that are managed by your IT staff, and they should check regularly to make sure there are no **rogue devices** impersonating the district network. This can usually be handled by an existing Wireless Intrusion Detection System (WIDS) that would alert if unauthorized access points are detected, however a physical audit where IT staff walks around with a wireless sensor to confirm these findings is strongly recommended.

It is vital to use modern and **strong encryption** such as "WPA2" when connecting to wireless networks; not doing so may result in attachers listening in to other people's network traffic. While strong and secret passwords may be used to connect, changing them frequently across the district may be a challenge. The preferred connection method uses **individual usernames and passwords** via a system like RADIUS; this allows the maximum amount of security and flexibility.

Your district should disable wireless features on clients that are not required, and **limit the systems** that your wireless networks can access. Any wireless networks or SSIDs available to the public should be isolated from all internal networks and not provide a path your sensitive internal resources.

GETTING STARTED

Microsoft Guide on Network Policy Servers (NPS) and RADIUS Authentication [50]

US-CERT Security Tip: Securing Enterprise Wireless Networks [51]

SANS Institute: A Secure Approach to Deploying Wireless Networks [52]

GETTING STARTED

Account Monitoring and Control [53]

Rapid7: Account Monitoring and Control [54]

16 - Account Monitoring and Control

BOB HODGES
NETWORK ENGINEER
WAYNE RESA

Executive Summary

Network account monitoring and control is often overlooked by school districts. Attackers use inactive accounts to impersonate legitimate users and gain access to school resources while remaining undetected. Schools can implement policies to audit, disable, and remove inactive accounts to prevent such attacks. By integrating these policies into the enrollment and employee hiring workflows, schools can better maintain control of network accounts. Schools can further protect themselves by requiring multi-factor authentication when accessing email, VPN, and other services accessible from the Internet.

Potential Solutions

Account Management:

School Districts should identify and **maintain an inventory** of each authentication system including directory services, email, and any system that accepts user authentication. The accounts on each of these systems need to be **periodically audited** to identify those that should be disabled or removed. It's beneficial to schools to centralize the points of authentication whenever possible to reduce the number of authentication systems to audit and control.

Account Lifecycle:

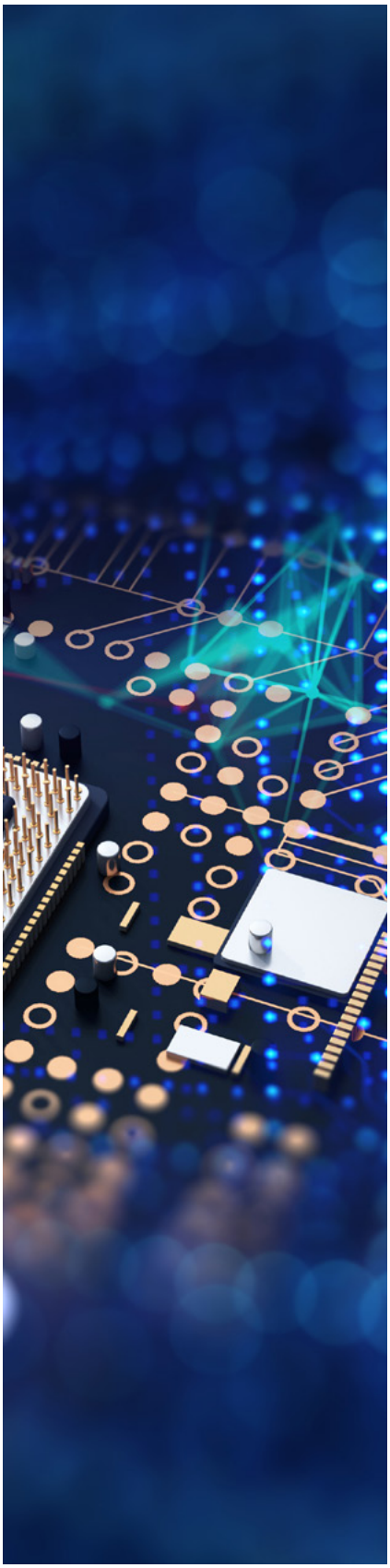
By involving HR and enrollment staff, schools can create processes to quickly identify students and employees as they enter or leave the district, ensuring that computer accounts are created and removed when no longer required. It is common for schools to automate these processes, but it's still important to audit the accounts periodically.

Multi-factor Authentication:

Schools can greatly reduce the chance of existing accounts becoming compromised by **enforcing Multi-factor Authentication (MFA)**. MFA options are built-in to many of the popular services used by schools, such as G-Suite for Education and Microsoft Office 365. MFA options are usually disabled by default so they must be enabled and enforced by the system administrator.

Event Management:

To identify compromised accounts, your district must be able to analyze authentication events. Analyzing events from each authentication system separately would be an overwhelming process, so automation is important. Control #6 assists greatly in this matter.



17 - Security Awareness and Training Program

BILL PATTERSON
NETWORK SECURITY ANALYST
INGHAM ISD

Executive Summary

Humans will always be the weakest link in cybersecurity. While our technical implementations make it harder for attackers to succeed, people always seem to find a way around them. People in every role of an organization have an active part in the overall cyber health of your district, and must be trained to understand risks, threats, and their role in cybersecurity. Without active participation by your employees in the cybersecurity process, these threats cannot possibly be contained.

Potential Solutions

Regular and measurable training should be implemented across all levels of the organization. This training should be tailored to fit different roles in the organization, i.e. teachers, finance, and administration may all have different topics and intensity of training based on how they interact with technology. The best way for this training to be adopted is to ensure **management buy-in** is made clear, with district leaders setting the example in taking and promoting security training. Employees must understand the importance and urgency in taking advantage of these training programs.

Training should be **updated regularly** to adjust for new threat vectors and current employee understanding level, and should be accompanied by a **metric** to measure how well the information is being understood by employees. This can consist of a simple quiz or freeform responses regarding how prepared employees are in understanding and responding to typical threats. These metrics should be reviewed regularly to ensure that the training is meeting the needs of the organization.

Case Study

Sunnyside Schools employs a paid service to curate and deliver individualized content via short, web-based, interactive training modules to each employee based on roles in the organization. These trainings adjust at the individual level to redeliver content the employee struggled with and also provide metrics and reports for administrative purposes to gauge the overall organizational training status.

GETTING STARTED

Cybersecurity: Everyone's Responsibility (by Cisco) [55]

The Importance of Security Awareness Training (SANS Institute) [56]

It's Everyone's Job to Ensure Online Safety at Work (CSIAC) [57]

GETTING STARTED

CIS Control #18

Application Software Security

Rapid7

Breaking Down the Control
Chaos of Application Software Security

18 - Application Software Security

KEN WEST
SOLUTIONS AND SECURITY SUPERVISOR
GENESEE ISD

Executive Summary

Software runs our schools, whether it is for collaborating, billing, attendance, communication, or any other aspect of your district. Unfortunately, outdated or misconfigured software is a highly sought-after target by attackers; with it, they can gain a foothold in your systems and potentially exfiltrate data. Because schools host a wide variety of software applications to support the needs of students and staff, it is important to know common security practices relating to software in order to stay secure and to prevent a data breach.

Potential Solutions

Much of the software applications used in K12 education are from third party vendors, such as Microsoft and Apple. Vulnerabilities in third party applications are found on a regular basis and security patches are developed to mitigate these potential threats. It is critical that these software packages be kept up to date; a challenge in K12 environments due to them being used by so many people, at times without the knowledge of the IT department.

By centrally managing a l**ist of approved software**, your district can keep programs updated with the latest security patches, and more importantly, validate whether or not the responsible vendor is continually supporting the product. Unsupported products do not receive security patches, which is a significant risk.

Using an **asset management system** can significantly aid in keeping your installed software up to date and in line with your approved software list. These systems allow your district to maintain an active list of installed software, prohibit installation of unapproved software, and push security updates as needed across your network - all with relatively minimal effort.

Finally, it is also important to regularly **review configurations** of all third party applications to verify they are not inadvertently exposing student, staff, and organizational data. You can identify risks by utilizing vulnerability and web application scanners which test application software security after deployment or other major changes in the environment.

Not all software is purchased or downloaded; many times we have to create our own to suit our custom needs. Security must be at the forefront of internal software development; developers must properly gather requirements and understand the sensitivity of the data and systems they are impacting. **Formalizing a Software Development Life Cycle (SDLC)** is important in maintaining secure application software code and fostering an environment that supports proper security controls. Peer review of code and proper unit testing can catch many common security flaws during the coding and development process.

Secure coding can be a challenge even to seasoned professionals, however **Developer Security Awareness Training** teaches your developers the security concepts needed to build your applications with security as a priority rather than an afterthought. In addition to this training, **separate test and production environments** are necessary to isolate issues and alleviate potential data leaks and data breaches.

19 - Incident Response and Management

MATT STARK
SEN PROJECT MANAGER
MICHIGAN STATEWIDE EDUCATION NETWORK

Executive Summary

Like all organizations, your school district will likely be victim to a cybersecurity attack at some point. To minimize the impact and loss when this happens, a proper Incident Response Plan (IRP) should be created so that district staff know their roles, how to respond, and ultimately how to recover and resume business and teaching operations in the event of a cybersecurity incident.

Potential Solutions

An **Incident Response Plan** is a high-level policy document that establishes several necessary components, including how to report a security incident, what different incident severity levels exist, and the different district employee or contractor roles which would be assisting in any efforts during a security incident.

The most important role is the Incident Handler, who is the primary manager of reported cybersecurity incidents. This person is typically the most senior IT employee at a district, and has the crucial job of validating security incidents, classifying them based on their severity, managing the incident through containment, remediation, and recovery, and ultimately bringing in additional employees or resources to aid in these efforts.

During significant cybersecurity incidents, all members identified inside the Incident Response Plan take part. This group is the **Cyber Security Incident Response Team (CSIRT)** and consists of senior leaders and practitioners from IT, Administration, Legal, HR, and Public Relations. The CSIRT follows the Incident Response Plan to ensure that responses and actions are appropriate, planned, and not impulsive.

Many examples of Incident Response Plans exist for use by your district, and it is important to customize them based on your organizational structure and capabilities. Your CSIRT should meet a few times a year to walk through the IRP and ensure it is still fully applicable, running through a couple example incidents. Additionally, the CSIRT should be involved in reviewing the Post-Mortem report of any verified security incident, building in improvements and lessons learned back into the IRP.

Case Study

https://www.kennasecurity.com/k-12-schools-facing-new-cybersecurity-threats-data-breaches/

GETTING STARTED

National Incident Management System [58]

NEOLA Policy 8305: *Information Security* [59]

GETTING STARTED

Penetration Tests and Red Team Exercises [60]

Penetration Testing Methodologies [61]

Penetration Testing Guidence [62]

20 - Penetration Tests & Red Team Exercises

BOB HODGES
NETWORK ENGINEER
WAYNE RESA

Executive Summary

School districts should test the effectiveness of security controls by performing penetration tests and "Red Team" exercises. During a **penetration test**, one or more security professionals attempt to penetrate the school's defenses by safely replicating real-world cyber-attacks. Complimentary to this are **Red Team exercises** - ongoing efforts by internal staff to hunt for and identify vulnerabilities that could be exploited. In both cases, testers work closely with the technology department staff to provide feedback on the school's defensive strengths and weaknesses. Schools should use this feedback to better strengthen their security posture.

Potential Solutions

Before a penetration test is performed, schools should have a good understanding of the existing security components that make up their defense strategy. Schools will be expected to identify the scope of the engagement, which includes applications and networks to be tested, and the duration of the testing. A typical **penetration test** might include the external and internal network infrastructure and web applications hosted by the school district. When choosing a vendor to perform a penetration test, ensure they have prior experience testing schools of similar size and scope. Once complete, the vendor should provide all test results, including remediation recommendations for identified vulnerabilities. Schools should remediate issues identified in the report and have those remediations retested to ensure they are effective.

Red Team exercises are a great way to **engage a district's top student talent** while improving security posture. For example, by offering an Independent Study course overseen by a computer teacher or IT director, students can learn to direct their curiosity about their school's network in a positive way, searching for and reporting on discovered issues while learning invaluable skills. Students should sign appropriate confidentiality agreements, be given strict limits on the scope of their activities, and obtain approval before attempting attacks outside of their classroom

Case Study

Sunnyside Schools hired Secure Solutions to perform a penetration test. During the pre-engagement meeting, they agreed upon the scope and duration of the testing. After the testing was complete, Secure Solutions provided a report **identifying vulnerabilities** in the school's Wordpress website allowing the testers unauthorized access to modify webpage content. The report also identified weak employee passwords which allowed the testers to gain entry into the school's private network. Sunnyside Schools **remediated** the Wordpress vulnerabilities by including Wordpress in their patch management process and implemented two-factor authentication to better secure employee logins. Sunnyside Schools scheduled Secure Solutions to perform a follow up test to ensure the identified issues were addressed.

Appendix

For all the links listed here and throughout this publishing visit: **misecure.org**

Inventory and Control of Hardware Assets

1. Netdisco
   http://netdisco.org/
2. LanTopoLog
   https://www.lantopolog.com/
3. Locating a device on your network
   http://packetlife.net/blog/2010/apr/19/locating-host-port-ip-address/

Inventory and Control of Software Assets

4. CIS Control 2 Information
   https://www.cisecurity.org/blog/understanding-cis-control-2/
   https://www.cisecurity.org/controls/inventory-and-control-of-software-assets/
5. Michigan Government General Retention Schedule, #800 - Technology Inventory (page 26)
   https://www.michigan.gov/documents/hal_mhc_rms_local_gs2_171482_7.pdf

Controlled Use of Administrative Privileges

6. US CERT Choosing and Protecting Passwords
   https://www.us-cert.gov/ncas/tips/ST04-002
7. CIS Control #4
   https://www.cisecurity.org/controls/controlled-use-of-administrative-privileges/
8. How to enable Multi-factor authentication for various online services
   https://twofactorauth.org
9. Microsoft LAPS
   https://www.microsoft.com/en-us/download/details.aspx?id=46899

Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers

10. CIS Control #5
    https://www.cisecurity.org/controls/secure-configuration-for-hardware-and-software-on-mobile-devices-laptops-workstations-and-servers/
11. CIS Benchmarks
    https://learn.cisecurity.org/benchmarks
12. Security Technical Implementation Guides
    http://iase.disa.mil/stigs/Pages/index.aspx

Maintenance, Monitoring and Analysis of Audit Logs

13. Syslog-ng
    https://www.syslog-ng.com/
14. Graylog
    https://www.graylog.org/
15. CIS
    https://www.cisecurity.org/controls/maintenance-monitoring-and-analysis-of-audit-logs/

Email and Web Browser Protections

16. CIPA
    http://transition.fcc.gov/cgb/consumerfacts/cipa.pdf
17. iBoss
    https://www.iboss.com/
18. Barracuda
    https://www.barracuda.com/

Malware Defenses

19. Emotet virus
    https://www.us-cert.gov/ncas/alerts/TA18-201A
20 & 21. Michigan GOV Cyber Security Resources
    https://www.michigan.gov/documents/cybersecurity/120815_Michigan_Cyber_Disruption_Response_Plan_Online_Version_003_544764_7.pdf
    https://www.michigan.gov/som/0,4669,7-192-78403_78404---,00.html
22 & 23. CIS Control 8 - Malware Defenses
    https://www.cisecurity.org/controls/malware-defenses/
    https://en.wikipedia.org/wiki/CSC_Version_6.0#CSC8
24. Microsoft SCCM EndPoint Protection
    https://www.systemcenterdudes.com/sccm-endpoint-protection-guide/
25. Free AntiVirus Solutions for Non-Profits
    https://www.cnet.com/forums/discussions/free-antivirus-for-non-profit-154232/

Limitation and Control of Network Ports, Protocols and Services

26. Shodan
    https://shodan.io
27. MxToolbox
    https://mxtoolbox.com
28. Nmap
    https://nmap.org
29. Schedule daily Nmap scans with a script
    https://nmap.org/book/ndiff-man-periodic.html
30. Disabling older protocols
    https://blogs.technet.microsoft.com/askpfeplat/2018/02/12/retire-those-old-legacy-protocols.html

Data Recovery Capabilities

31. Data Recovery Capability
    https://www.cisecurity.org/controls/data-recovery-capability/
32. CIS Critical Control 10
    https://blog.rapid7.com/2018/03/12/cis-critical-control-10-data-recovery-capability/
33. Data Backup Options
    https://www.us-cert.gov/sites/default/files/publications/data_backup_options.pdf

Boundary Defense

34. CIS Control #12
    https://www.cisecurity.org/controls/boundary-defense/
35. Rapid 7 Blog
    https://blog.rapid7.com/2018/04/02/cis-critical-control-12-boundary-defense -explained/

Data Protection

36. Sudent Privacy White Paper
    https://cosn.org/sites/default/files/Platform_Student_Privacy_White_Paper.pdf
37. FERPA:
    https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

Controlled Access Based on the Need to Know

38. IP Addressing and VLAN Planning Document
    http://www.secantcorp.com/wp-content/uploads/2017/11/secant_ip_addressing_vlan_numbering.pdf
39. NetIQ eDirectory Permissions
    https://www.netiq.com/documentation/edirectory-91/edir_admin/data/fbachifb.html
40. MicroFocus Open Enterprise Server File System Permissions
    https://www.novell.com/documentation/open-enterprise-server-2018/stor_filesys_lx/data/bs3fjo7.html
41. Microsoft Active Directory Security
    https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/best-practices-for-securing-active-directory
42. Windows Server File System Permissions
    https://blog.netwrix.com/2018/05/03/differences-between-share-and-ntfs-permissions/
43. Google Drive Permissions
    https://support.google.com/a/answer/60781
44. Protect access to data and services in Office 365
    https://docs.microsoft.com/en-us/office365/securitycompliance/protect-access-to-data-and-services
45. Securing Privileged Access
    https://docs.microsoft.com/en-us/windows-server/identity/securing-privileged-access/securing-privileged-access
46. Avenues Of Lateral Movement
    https://attack.mitre.org/tactics/TA0008/
47. MicroFocus ZENworks Full Disk Encryption
    https://www.microfocus.com/products/zenworks/full-disk-encryption
48. Microsoft Bitlocker Disk Encryption
    https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/bitlocker-overview
49. VeraCrypt Disk Encryption
    https://www.veracrypt.fr

Wireless Access Control

50. Microsoft Guide on Network Policy Servers (NPS) and RADIUS authentication:
    https://docs.microsoft.com/en-us/windows-server/networking/technologies/nps/nps-top
51. US-CERT Security Tip: Securing Enterprise Wireless Networks:
    https://www.us-cert.gov/ncas/tips/ST18-247
52. SANS Institute: A Secure Approach to Deploying Wireless Networks:
    https://www.sans.org/reading-room/whitepapers/wireless/secure-approach-deploying-wireless-networks-37342

Account Monitoring and Control

53. Account Monitoring and Control
    https://www.cisecurity.org/controls/account-monitoring-and-control/
54. Rapid7: Account Monitoring and Control
    https://blog.rapid7.com/2018/05/07/critical-control-16-account-monitoring-and-control-aint-nobody-got-time-for-that/

Security Awareness and Training Program

55. Cybersecurity: Everyone's Responsibility (by Cisco):
https://www.cisco.com/c/dam/en_us/solutions/industries/docs/education/C45-626825-00_Cyber_Security_Responsibility_AAG.pdf
56. The Importance of Security Awareness Training (SANS Institute):
https://www.sans.org/reading-room/whitepapers/awareness/importance-security-awareness-training-33013
57. It's Everyone's Job to Ensure Online Safety at Work (CSIAC):
https://www.csiac.org/national-cyber-security-awareness-month-october-2018/its-everyones-job-to-ensure-online-safety-at-work-national-cyber-security-awareness-month-week-3-october-15-19/

Incident Response and Management

58. National Incident Management System
https://www.fema.gov/national-incident-management-system
59. Relevant NEOLA Policy: 8305 - Information Security
https://www.us-cert.gov/ncirp
https://cyberdefenses.com/incident-response-ebook/

Penetration Tests & Red Team Exercises

60. Penetration Tests and Red Team Exercises
https://www.cisecurity.org/controls/penetration-tests-and-red-team-exercises/
61. Penetration Testing Methodologies
https://www.owasp.org/index.php/Penetration_testing_methodologies
62. Penetration Testing Guidence
https://www.pcisecuritystandards.org/documents/Penetration-Testing-Guidance-v1_1.pdf

Credits

This guide was made possible by the efforts of the following organizations:

Michigan Educational Technology Leaders (METL) Group, an MAISA affiliated Organization.

Michigan Statewide Educational Network (MiSEN)

Merit Network, Inc.

The following individuals participated in the creation of the content:

Troy Calgaro, Ottawa Area ISD, Manager/ Network Operations, Author

Ryan Goyette, Washtenaw ISD, Technology Security Specialist, Author

Andrew Hahn, Washtenaw ISD, Supervisor, Technology and Data Services, Author

Alex Hargrove, Clare Gladwin RESD, Senior Systems Engineer, Author

Nicholas A. Hay, Monroe ISD, Director of Information Services, Author

Josh Hayes, REMC 1, Director of the ETA,Author

Kevin Hayes, Merit Network, Chief Information Security Officer, Technical Editor

Bob Hodges, Wayne RESA, Network Engineer, Author, Technical Editor

David Larson, Livingston ESA, Network Engineer, Author

Sam Lutgring, Calhoun ISD, Assistant Superintendent, Author

Matt McMahon, Gratiot-Isabella RESD, Associate Superintendent for Technology, Author, Project Manager

Bill Patterson, Ingham ISD, Network Security Analyst, Author

Joel Phillips, Newaygo County RESA, Director of Technology, Technical Editor

Matt Stark, Misen, SEN Project Manager, Author

Nick Strieter, Merit Network, Inc., Designer

Ken West, Genesee ISD, Solutions and Security Supervisor, Author

Thanks to the following individuals for their support during this effort:

Charlotte Bewersdorff, Merit Network, Inc.

Tim Brown, Muskegon ISD

Jackie Carstens, Shiawassee RESD

Tammy Evans, Oakland Schools

Christopher Hammond, Oakland Schools

Jenny Kirshman, Merit Network, Inc.

Jim Rarus, Wayne RESA

Darren Schiltz, Dickinson-Iron ISD

Daryl Tilley, Ingham ISD

Kevin Tomlinson, Shiawassee RESD

Ryan Velzy, Oakland Schools

Michael Verschaeve, Bay Arenac ISD

Jameka Williams, Merit Network, Inc.