



# Cybersecurity Practices for K- 12





# Introductions

Merri Lynn Colligan, Washtenaw ISD

David Larson, Livingston ESA

Matt McMahon, Gratiot-Isabella RESD

Joel Phillips, Newaygo County RESA



# How are ya now?

As a rank, how important has cybersecurity become to you?

To your superintendent?

How prepared are you if “that call” comes right now?

What’s holding you back?

If you could only fix one thing, what would it be?





# The Problem

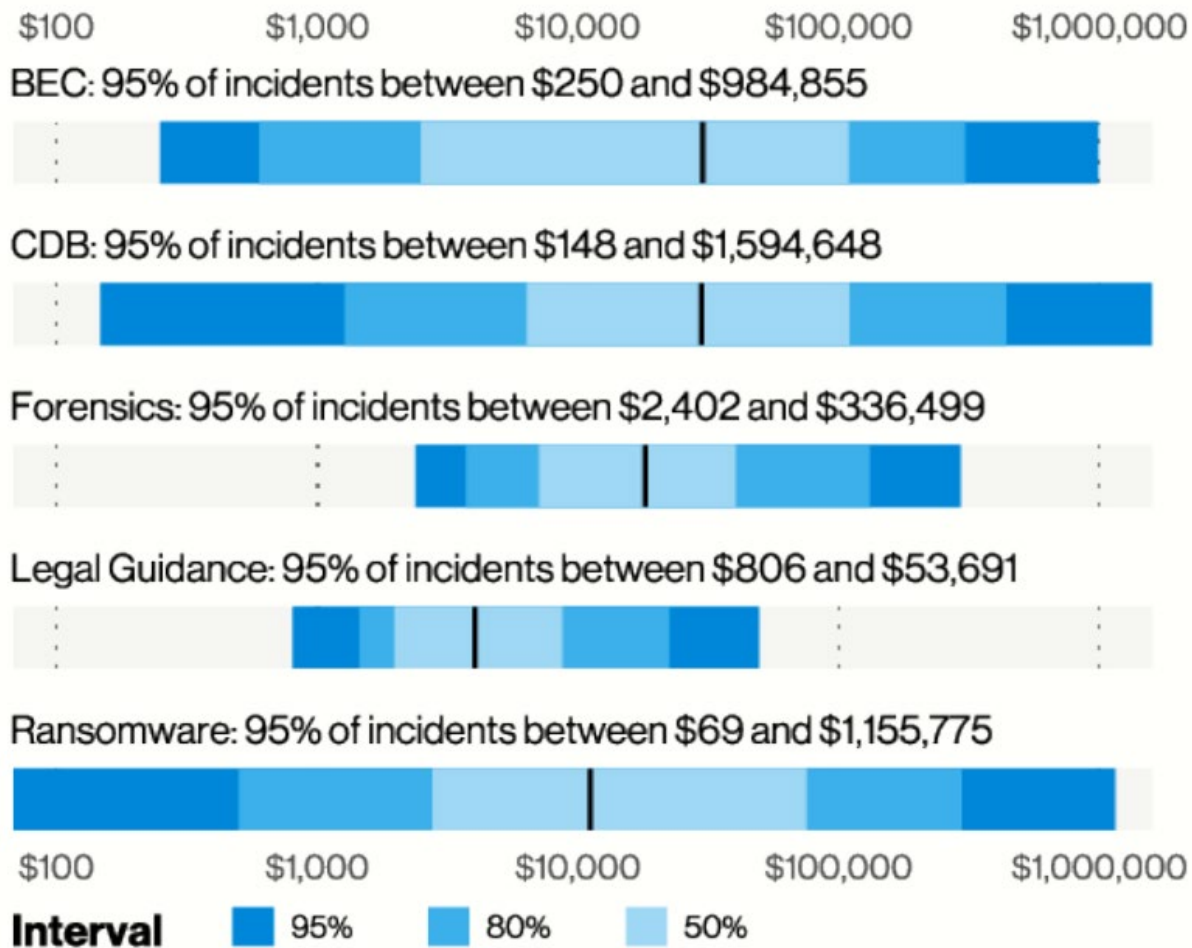
[Cyberattacks on Schools Soared During the Pandemic](#) *(EdWeek, March 10, 2021)*

- ◇ Cyberattacks on school districts surged by a whopping **18%** in calendar year 2020, likely due to the greater reliance on classroom technology during the pandemic, according to a report released March 10 by the K12 Security Information Exchange and the K-12 Cybersecurity Resource Center.
- ◇ 408 **publicly disclosed** [cyber-attacks](#) last calendar year, compared with 348 in 2019, the report found

[Cybersecurity training still lacking in schools, some IT leaders say](#) *(District Administrator, December 7, 2020)*

- ◇ Disruptions in systems, such as Email, SIS, Finance, Payrolls, Learning Management Systems, files and cloud storage, and more.
- ◇ It could take **weeks** after an incident to get closer to back to normal operations and it could be **months** before systems are fully restored.
- ◇ Cybersecurity threats are getting very common in schools, healthcare, and businesses.





Source: [Verizon 2021 Data Breach Investigations Report](#)



*What are you struggling with the most right now?*

# The Guide



# Essential Cybersecurity Practices for K12

Free download: <http://misecure.org/>

Distributed to every CEO/CFO/CTO

**Why?** Common language/framework

**Who?** Created by MI K12 for MI K12



## Basic

- 1 Inventory and Control of Hardware Assets
- 2 Inventory and Control of Software Assets
- 3 Continuous Vulnerability Management
- 4 Controlled Use of Administrative Privileges
- 5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
- 6 Maintenance, Monitoring and Analysis of Audit Logs

## Foundational

- 7 Email and Web Browser Protections
- 8 Malware Defenses
- 9 Limitation and Control of Network Ports, Protocols, and Services
- 10 Data Recovery Capabilities
- 11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
- 12 Boundary Defense
- 13 Data Protection
- 14 Controlled Access Based on the Need to Know
- 15 Wireless Access Control
- 16 Account Monitoring and Control

## Organizational

- 17 Implement a Security Awareness and Training Program
- 18 Application Software Security
- 19 Incident Response and Management
- 20 Penetration Tests and Red Team Exercises





# The Audit & Self Assessment





# MI Secure Quick Self - Audit

Based on *Essential Cybersecurity Practices for K12*

Single page, 21 questions in 5 categories

By MI K12 for MI K12

Encourage conversations: low bar, no right/wrong, easy entry, **informal**

Can be done in minutes, not days

Get it: <https://misecure.org/selfaudit/>



# 1. People

- A. Regular, scheduled conversations
- A. Add to existing meeting
- A. Start in your tech dept
  
- B. Free MConnect training available
- B. Better: KnowBe4, Proofpoint
- B. Phishing campaign, tracking
  
- C. How much damage can you do?
- C. Where are the keys kept?
  
- D. Talk to your HR: policies for on boarding & off boarding?
  
- E. Recurring calendar event (email, VPNs, AD, what else?)



## 1. People

- a. When was your most recent internal conversation about cybersecurity? Who was involved in that conversation? (Control 17 and 19)
- b. Does your district provide cybersecurity training? For who (admin, staff, students)? (Control 17)
- c. Who has the keys to your kingdom? Do they use different accounts for daily activities and system administration work? (Control 4)
- d. Do you have a procedure for assigning appropriate access when staff are hired and for removing access when staff leave or change roles? (Control 14, 16)
- e. Do you perform regular audits of user accounts to make sure that people have access to what they need, but no more? (Control 14, 16)

# 2. Things

- A. AngryIP Scan, LANSweeper
- A. HVAC, Contractor VPNs, IoT,
- A. Are you alerted of new devices?
- A. Given an IP address, could you locate that device?
  
- B. LANSweeper, Windows Defender ATP, ideas? SCCM, InTune?
  
- C. What is “sensitive data”?
- C. Shared drives, Cloud storage - who has access?
- C. DLP



## 2. Things

- a. Do you know what hardware is connected to your network? (*Control 1*)
- b. Do you know what software is in use on all systems? (*Control 2*)
- c. Do you know which systems contain sensitive data and who has access? (*Control 13*)

# 3. Design



## 3. Design

- a. Do you intentionally deploy and maintain systems with security in mind? (*Controls 5,9*)
- b. Are you requiring MFA ('multi-factor authentication') for any logins? Which ones (staff, admin, everyone)? (*Control 16*)
- c. Does your district segment your internal network to control the access of data between those networks? Does segmentation include separation of guest network, and HVAC (or other controls) networks from business networks? (*Controls 12 and 15*)
- d. Do you provide remote access to your systems? How do you ensure that access is safe and secure? (*Control 12*)

A. Are images specifically audited for security?

A. Updated?

A. Turning off unneeded services?

A. Who vets this and how?

B. Can user's turn this on?

B. Required for admins?

B. Not talking your Netflix account

C. How much could a guest user infect?

C. Have you recently tested this?

C. Are vendors fenced off?

D. How do people get in? VPNs, LogMeIn

# 4. Process

A. How do you know when something is out of date?

A. Windows updates automated?

A. other software is harder?

A. Quickly roll out updates?

B. Do you get notified of end-user incidents?


C. Have you used a network scanner?

C. Have you set up regular reports?

C. Are you doing *internal* scanning?

D. Are you using just a password? How well known is that password?

D. How do you manage guests?



## 4. Process

- a. Do you keep your systems up-to-date? How frequently do you apply updates? (*Control 3*)
- b. Do you keep phishing & malware protection enabled and up-to-date everywhere? (workstations, email systems, servers) (*Control 7 and 8*)
- c. Do you scan your network for security vulnerabilities? (*Control 11*)
- d. Do you control who has access to your wireless network? (*Control 15*)

# 5. Response

A. Incident Response Plan

B. Are you regularly testing backups?

B. Are they off net?

C. Are logs time synced?

D. Where is this recorded?

D. Test it out - is your activity recorded someplace?

E. This one should scare you.

E. Are devices encrypted?

E. Is it a Windows machine?



## 5. Response

- a. Do you know what you would do in the event of a cyber incident? Do you know who would be involved from the district? Do you know who you would call for help? (Control 19)
- b. Are you doing regular backups? Are you testing and keeping a copy of your backups offline? (Control 10)
- c. Are you keeping logs so that someone could go back and find out how, when and why something bad happened? (Control 6)
- d. Can you identify [who, where, how, when] administrative access or system changes have occurred? (Control 4)
- e. If a district laptop or phone is lost or stolen, is that data still secured? (Control 13)



How do I get  
started?





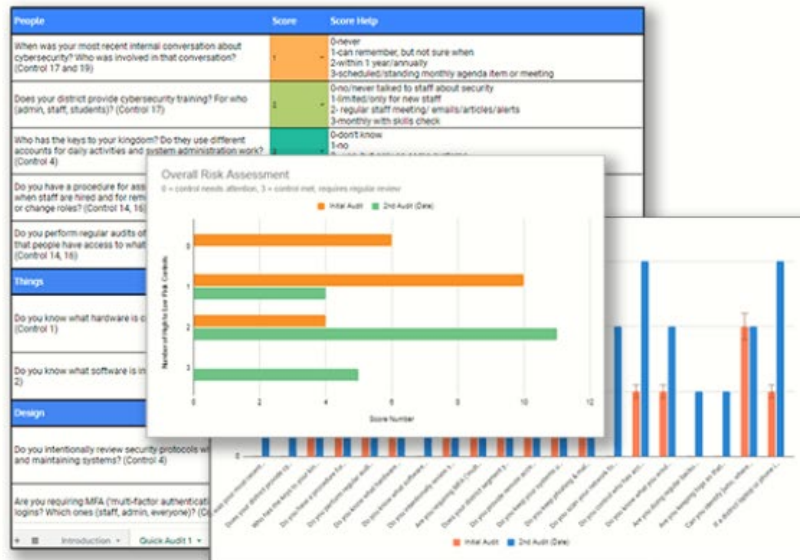
<https://misecure.org/selfauditdct/>

## MISecure Quick Self-Audit Data Collection Tool

Store results from the MISecure Quick  
Self-Audit and track growth.

Open the Google Sheet

*You will be prompted to sign-in and make a copy of the Google Sheet.*





# Self Audit Data Collection Tool

- ◇ [Make your own copy](#)
- ◇ Choose from a list of responses
- ◇ Not a replacement for CSAT
- ◇ No aggregate score (on purpose)

Copy of MISecure Quick Self-Audit Data Collection Tool

File Edit View Insert Format Data Tools Extensions Help Last edit was seconds ago

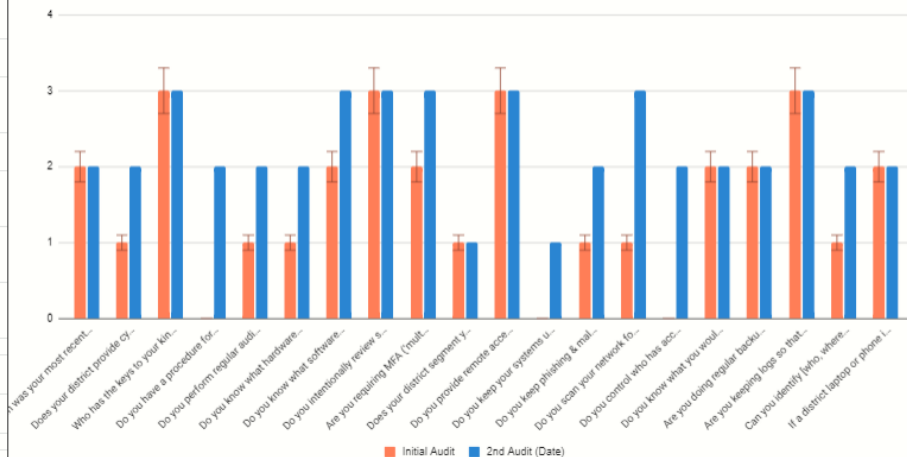
100% \$ % .0 .00 123 Roboto 14 B I S A

	A	B	C
3	People	Score	Score Help
4	When was your most recent internal conversation about cybersecurity? Who was involved in that conversation? (Control 17 and 19)	2	0-never 1-can remember, but not sure when 2-within 1 year/annually 3-scheduled/standing monthly agenda item or meeting
5	Does your district provide cybersecurity training? For who (admin, staff, students)? (Control 17)	1	0-no/never talked to staff about security 1-limited/only for new staff 2- regular staff meeting/ emails/articles/alerts 3-monthly with skills check
6	Who has the keys to your kingdom? Do they use different accounts for daily activities and system administration work? (Control 4)	3	0-don't know 1-no 2- yes, but only on some systems 3-yes, on all systems
7	Do you have a procedure for assigning appropriate access when staff are hired and for removing access when staff leave or change roles? (Control 14, 16)	0	0-don't know 1-ad hoc, some systems have procedures 2-informal procedure 3-documented procedure with reporting
8	Do you perform regular audits of user accounts to make sure that people have access to what they need, but no more? (Control 14, 16)	1	0-don't know 1-never 2-when people change roles 3-regularly scheduled (at least annually), process involves data owner review
9	Things	0	Score Help
		1	
		2	0-don't know 1-written list of equipment (or spreadsheet) 2-documented list of equipment updated regularly 3-automated network discovery tool with alerts for newly attached equipment
		3	
10	Do you know what hardware is connected to your network? (Control 1)		
11	Do you know what software is in use on all systems? (Control 2)	0	0-don't know 1-documented list of supported software (or spreadsheet) 2-documented list of software updated regularly

## MISecure Quick Self-Audit Data Collection Tool

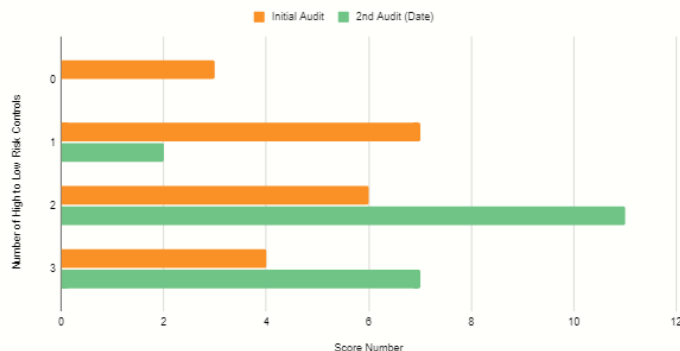
	Initial Audit	Quick Audit (Date)
When was your most recent internal conversation about cybersecurity? Who was involved in that conversation? (Control 17 and 19)	2	2
Does your district provide cybersecurity training? For who (admin, staff, students)? (Control 17)	1	2
Who has the keys to your kingdom? Do they use different accounts for daily activities and system administration work? (Control 4)	3	3
Do you have a procedure for assigning appropriate access when staff are hired and for removing access when staff leave or change roles? (Control 14, 16)	0	2
Do you perform regular audits of user accounts to make sure that people have access to what they need, but no more? (Control 14, 16)	1	2
Do you know what hardware is connected to your network? (Control 1)	1	2
Do you know what software is in use on all systems? (Control 2)	2	3
Do you intentionally review security protocols when deploying and maintaining systems? (Control 4)	3	3
Are you requiring MFA ('multi-factor authentication') for any logins? Which ones (staff, admin, everyone)? (Control 6)	2	3
Does your district segment your internal network to control the access of data between those networks? Does segmentation include separation of guest network, and HVAC (or other controls) networks from business networks? (Controls 3 and 13)	1	1
Do you provide remote access to your systems? How do you ensure that access is safe and secure? (Controls 6, 12 and 13)	3	3
Do you keep your systems up-to-date? How frequently do you apply updates? (Control 7)	0	1
Do you keep phishing & malware protection enabled and up-to-date everywhere? (workstations, email systems, servers) (Control 9 and 10)	1	2
Do you scan your network for security vulnerabilities? (Control 7)	1	3
Do you control who has access to your wireless network? (Control 15)	0	2
Do you know what you would do in the event of a cyber incident? Do you know who would be involved from the district? Do you know who you would call for help? (Control 17)	2	2

Quick Self-Audit Comparison



Overall Risk Assessment

0 = control needs attention, 3 = control met, requires regular review





# MICIP

Michigan Integrated  
Continuous  
Improvement Process  
(MICIP)

## Including Technology in MICIP

- ◇ Technology Planning
- ◇ Supporting CI process
  - Templates
  - Data driven
  - Strategies
- ◇ Examples, Lessons, Resources
- ◇ Cybersecurity data sets






# Steps You Can Take - Tomorrow

- ◇ Talk about cybersecurity
- ◇ It's not an IT-only problem
- ◇ Work with your ISD & neighboring districts
  - Share the wisdom
  - What tools are in your neighbor's shed?
- ◇ Have a plan (**Incident Response Plan**)
- ◇ Share this Information
- ◇ Cyber Liability Carriers are prioritizing these controls
  - MFA (multi-factor authentication)
  - Employee information security training
  - Ensure you have a Offline / Off Net Backups of critical data



# Steps You Can Take - Planning

- ◇ Develop a **team** that meets regularly to improve your cybersecurity profile (including Tech Dir, Superintendent, CFO)
- ◇ Establish Emergency Operations Procedures, Cyber Incident Planning, Business Continuity
- ◇ Include Protection Strategies in MICIP - School Improvement Processes and Budget for:
  - CyberSecurity **Training**
  - Cyber Security **Enhancements**: Firewall, AntiMalware Protection
  - Systems Audit and mitigation
- ◇ Hold a **Tabletop Exercise** to practice



# Future (?) Requirements to Get Cyber Insurance

- ◇ Multi-factor Authentication (MFA) - for all remote access
- ◇ **Backups** – cadence, segregation, testing, redundancy
- ◇ **Incident response plan** – tested
- ◇ Employee cybersecurity **training**
- ◇ Patch management
- ◇ Endpoint protection (EDR)
- ◇ Web traffic filtering
- ◇ Email filtering/sandboxing
- ◇ **Phishing simulations** & staff training
- ◇ Account configuration assessment – **least privilege**
- ◇ Penetration testing
- ◇ Internal & external **vulnerability scanning**





# Questions/Discussion

What are your 2 biggest challenges

What do you need from the task force?

Ideas, suggestions?

What are some things that could be done  
at a state level to help?

