



# IT for the New Business Manager



# Introductions



Furney Brown

Title

Plante Moran

Email@plantemoran.com



Matt McMahon

MiSecure Director

MAISA

MMcMahon@gomaisa.org



Nick Morse

Cyber Security Consultant

Kent ISD

NickMorse@kentisd.org









# Turn & Talk



- ◇ What could be going on?
- ◇ What's your role right now?
- ◇ How are you feeling?
- ◇ Next steps?















# BAD RABBIT

If you access this page your computer has been encrypted. Enter the appered personal key in the filed below. If susseed, you'll be provided with a bitcoin account to transfer payment. The current price is on the right.

Once we receive your payment you'll get a password to decrypt your data. To verify your payment and check the given passwords enter your assigned bitcoin address or your personal key.

Time left before the  
price goes up

41:18:14

Price for decryption:



- 0.05

Enter your personal key or your bitcoin address





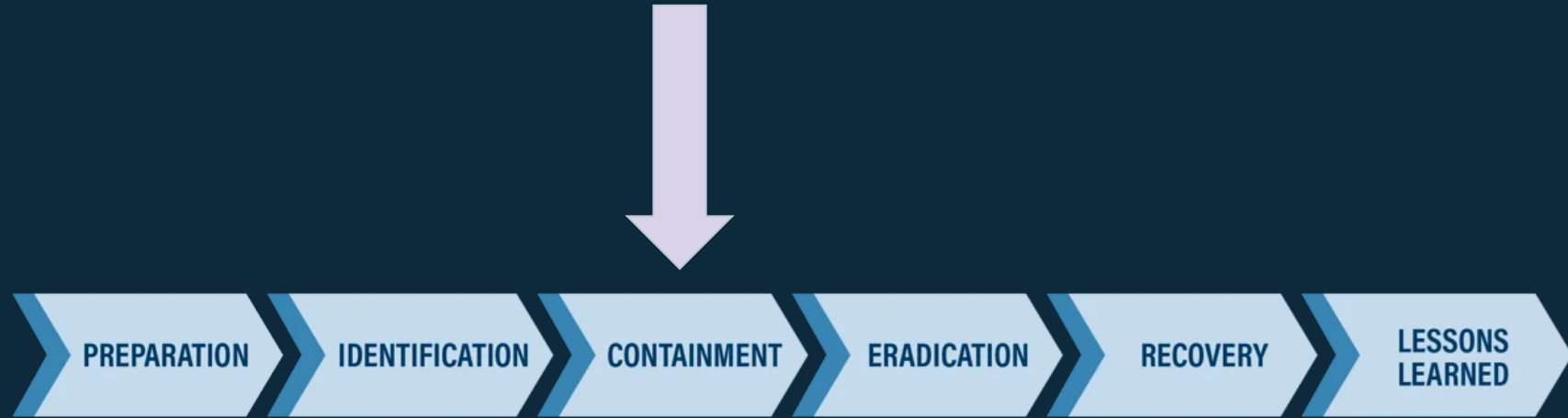
# Turn & Talk



- ◇ What happens if the Internet goes down?
  - What systems are impacted?
- ◇ Do you need to communicate with anyone?
- ◇ Can you hold school tomorrow?









The Reveal...





Two months ago...

- Coach received **fake email requesting info** for a tournament that had been posted to the website
- Entered **credentials** but errored out
- Never thought about it again
- Hacker used credentials to **VPN** into network (no MFA)
- Sat inside for **2 months** gathering info
- Finally leveraged a **vulnerability** on VMWare and ransomed the server infrastructure.

PREPARATION

IDENTIFICATION

CONTAINMENT

ERADICATION

RECOVERY

LESSONS  
LEARNED



# Be prepared for questions

- ◇ How will you inform your staff? The public?
- ◇ Can we hold school tomorrow?
- ◇ Prepare a statement for the media
- ◇ What do you tell your board?
- ◇ How will you run payroll?





How prepared are  
you?



# Michigan Headlines



**Lansing Community College** @LCCStars · 20h

In response to an ongoing cybersecurity incident, LCC will suspend all college classes, events, practices and activities beginning immediately and continuing through Thursday, March 16, and Friday, March 17.



**Lansing Community College**

@LCCStars

LCC is back online! See [lcc.edu/alert](https://lcc.edu/alert) for details. Technical support begins at 8 a.m.

Michigan Radio  
Here and Now

91.7 Ann Arbor/Detroit 104.1 Grand Rapids  
91.3 Port Huron 89.7 Lansing 91.1 Flint

## Ransomware attack closes all Kellogg Community College campuses "until further notice"

Michigan Radio | By Lauren Talley  
Published May 2, 2022 at 10:49 AM EDT

[f](#) [t](#) [in](#) [e](#)

RECORD EAGLE

NEXT UP  
Business Memoranda: 04/24/2024

**ALERT**

## TCAPS: Hackers claim they caused computer disruption

By Jordan Travis [jtravis@record-eagle.com](mailto:jtravis@record-eagle.com) and Travis Snyder [tsnyder@record-eagle.com](mailto:tsnyder@record-eagle.com) Apr 17, 2024

1 of 2

NEWS 10

News First Alert Weather Livestream Closings Sports Submit Photos and Videos Watch Preview

## CYBER ATTACKS

**PARENTS REACT TO CYBER ATTACKS**  
JACKSON AND HILLSDALE COUNTIES

NEWS 10

# What is METL?

A “leadership network” within MAISA  
ISD IT Technology Directors, meeting monthly



## Vision for the Future

The Michigan Education Technology Leaders will be a proactive, key decision-making group that fosters collaboration and efficiencies on projects, issues and policy regarding technology in education.

## Mission

METL's mission is to provide leadership and direction focused on technology in education among Michigan's ISDs/RESAs.



# <http://MiSecure.org/>

- ◇ November 2018: Essential Cybersecurity Controls for K12
- ◇ November 2019: Published & delivered
  - 18 CISA Controls
  - By MI K12 for MI K12
- ◇ 2019: MiSecure website
- ◇ 2020: Cybersecurity talking points
- ◇ 2020: Cybersecurity training
- ◇ 2021: MiSecure Quick Self-Audit
- ◇ 2023: MiSecure SOC & MDR
- ◇ 2024: Incident Response Planning tools



# Essential Cybersecurity Practices for K12



K12 Operations Center



Incident Response  
Planning Tools



Essential Cybersecurity  
Practices for K12



Quick Self-Audit



Professional Learning



Terms

End of Life

EDR

SOC

IRP

Patch Management

Backup

MFA

DRP

SIEM

Cyber Assessments

Phishing

XDR

MDR

Remote Access

BCP



# Cyber Term: Phishing

## Explanation

- the fraudulent practice of sending emails or other messages purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers.

## Example of abuse:

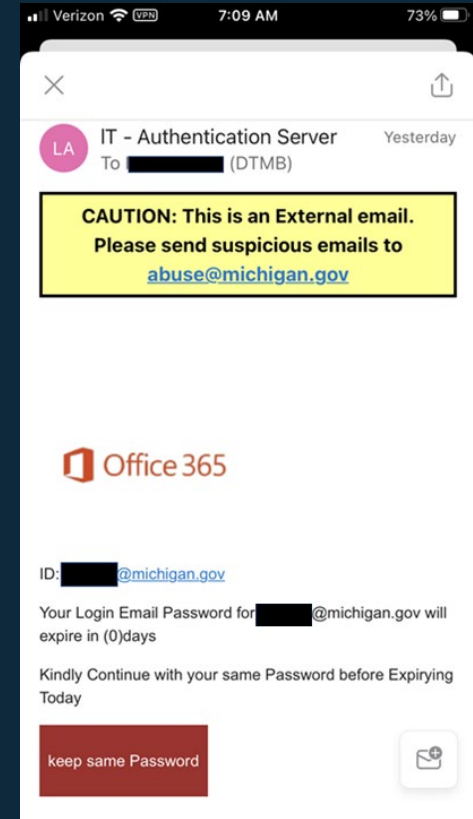
- Case Study: K-12 District Enrollment 5000k
  - Threat Actor Pretended to be superintendent
  - Wire transferred \$154,000 and \$169,000 to fraudulent vendor

## Solution:

- Security training, fake phishing campaigns
- KnowBe4 (\$17/year/FTE), Wizer, SecureHalo

COST:

Subscription



# Cyber Term: MFA

## Explanation

- Multi-Factor Authentication / 2FA
- Phone, email, text, app (e.g. Authy)

## The “why”

- MFA protects you
- All critical systems, email, remote access
- Push back
  - Some systems require MFA \*every\* time
  - Use of personal devices → yubi keys ~\$25 ea.

## Solution:

- Google/Microsoft - included
- PowerSchool example SSO
- Duo for systems that don't support it
- \$36/account/year for RDP



Subscription

# Multi Factor Authentication

◇ Something you Know:

- Password

◇ Something You Have:

- Phone, Code, Token

◇ “Included” in Most Apps:

- GSuite
- Microsoft 365
- Munis via Azure

◇ Cost/Benefit

- Slight Problem 4U
- Major Problem 4 bad guy

*Pro Tip:*

Enable MFA wherever you  
can (personally):  
Email, Bank Account, etc.

Users email compromised



Michigan GMIS List <MI-GMIS@LISTSERV.GMIS.OF  
To • MI-GMIS@LISTSERV.GMIS.ORG

Reply

Reply All

Forward



Thu 11/17/2022 9:10 AM

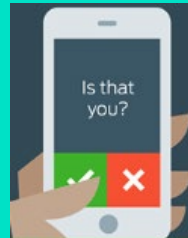
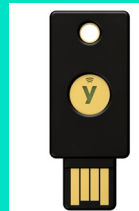
Hi Everyone,

Just wanted to follow up after we had one user's Office 365 account compromised earlier this week.

Her account was used to send hundreds of phishing emails to her contacts in a matter of minutes. Since she works in the mayor's office, it was a wide variety of Municipal and State contacts. We quickly discovered this and changed all of her passwords.

## MFA is...

- Your User ID and Password
- + Second “Factor”



27

One-time password code

979 757



# Cyber Term: Patch Management / End of Life

## Explanation

- An attempt to mitigate software vulnerabilities by actively checking for updates or replacing hardware where the vendor is no longer actively closing software vulnerabilities.

## Example of abuse:

- End of life (EOL) issues (unpatchable)
- Rogue/non-supported devices
- IoT

## Solution:

- Microsoft Intune; PDQ Deploy & Inventory; PatchMyPC

COST: Typically by device or FTE.

Subscription



# Cyber Term: Backup

## Explanation

- What is it?

## Example of abuse:

- Cloud too
- Target for ransomware
- Offsite, off network, air-gap, encryption, immutable

## Solution:

- Veeam
- Synology

Hardware





# Cyber Term: Incident Response Plan (IRP)

## Explanation

- The documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of a malicious cyber attacks against an organization's information systems(s).

## Example of abuse:

- Panic

## Solution:

- MiSecure IRP
- Michigan Cyber Partner IRP template
- Consultant

## COST:

People Time

# MiSecure IRP tools “CRAWL”



## MiSecure Incident Response Quick Reference

Last updated: [Date Here]

Where are the printed copies of the Incident Response documents? *[enter locations here]*

### Key Information

Command Center Location	
Alternative Communications	
Location of Passwords	
Network Diagram	
List of IP Addresses, VLANs & Routing Tables	
How to Disconnect from The Internet	

### Incident Response Team Members

Role	Name	Email	Phone	Cell
Cyber Inc. Res. Management				
Cyber/Inc. Res. Coordinator				
Lead Tech Engineer				
Admin Support / Inc Recorder				
Cyber Security Analyst				

### Response Contacts

Role	Name	Email	Phone	Other
Cyber Insurance				
Legal Representative				
Board President				
ISD Support				

### External Resources

Role	Name	Email	Phone	Other
Michigan Cyber Command Center (MC3)	Michigan State Police	mc3@michigan.gov	1-877-642-6237 1-877-MI-CYBER	
MS-ISAC Cyber Incident Response Team (CIRT)		soc@oisecurity.org	1-800-787-4722	
Internet Service Provider				

### Support Systems

Role	Name	Email	Phone	Other
EDR / MDR / XDR				
Mass Notification				
Firewall / Network Support				



# MiSecure IRP tools “WALK”



**MiSecure**

## Incident Response Worksheet v2.0

Last updated: [Date Here]

### Where does this document live?

**Digital location:** [Enter the on-line location]

**Physical location:** [Enter the location of a printout of this document, often in the Emergency Operations Plan]

### Key Information

The resources listed below will almost certainly be critical during a cybersecurity incident. You should list where both physical and digital versions of this information exist. You should develop a process to keep an off-network version up-to-date.

Resource	Purpose / Note
<b>Command Center Location</b> [Enter Here]	This is the physical location in the building, away from technical operations, where the incident response team can eat, meet & retreat. This should not be in the IT operational area.
<b>Out-of-band (OOB) Communication Method</b> [Enter Here]	Define how you will communicate during the event. Members of the team will need access to devices that are secured, probably not attached to the local domain. All members will need access to a site such as Slack, ... Where messages can be securely exchanged and files shared. Make sure your team does not use work email accounts on systems such as Slack. This should be tested regularly.
<b>Location of Passwords</b> [Enter Here]	Where are your passwords for key systems stored and/or backed up? This may be a backup of a Bitwarden or KeePass system or a simple printout of each team member's passwords.
<b>Network Diagrams</b> [Enter Here]	Where is the most recent print out of your network diagram. Network diagrams should include important IP and VLAN information as well as the physical location of MDF and IDF locations.
<b>IP Addresses, VLANs &amp; Routing Tables</b> [Enter Here]	This should be a print of a digital backup of your IP address database. Your core routing table should also be included.
<b>How To Disconnect From The Internet</b> [Enter Here]	This should list the physical location of the router / switch port(s) that need to be physically disconnected in order to disconnect from the Internet.

### 1. Incident Response Team Members

Enter the name of the person that will be primarily responsible for each role. You may consider adding a secondary person if feasible. One person may fill multiple roles. Individuals from other partner organizations may also fill roles. Make sure each member is notified and reminded regularly of their role and understand their responsibilities. Enter the name here and the contact information in the Appendix.

Role	Contact(s)	What They Do
<b>Cyber Incident Response Management</b>  <i>Usually the superintendent, associate superintendent or principal. They need to have the authority to make major operational decisions for the district.</i>	<b>Name</b> Email Phone	<ul style="list-style-type: none"> <li>Decide whether to cancel school</li> <li>Provides authorization for major steps such as whether to contact legal or insurance</li> <li>Works very closely with the Coordinator to make these decisions</li> <li>Support the ongoing effort to recover from an event</li> <li>Coordinate the effort of the entire team</li> </ul>
<b>Cyber Incident Response Coordinator</b>  <i>Usually the IT Director. For smaller districts or bigger crises, this may be the ISD IT Director</i>	<b>Name</b> Email Phone	<ul style="list-style-type: none"> <li>Provide overall support to the entire team.</li> <li>Make sure the right people are doing the right things.</li> <li>Communicate to Administration.</li> </ul>
<b>[Lead] Technical Engineer(s)</b>  <i>Whoever manages the servers, backups, networks and firewalls.</i>	<b>Name</b> Email Phone	<ul style="list-style-type: none"> <li>Review extent of compromise</li> <li>Able to change passwords and policies</li> <li>Review EDR reports / alerts</li> <li>Access user activity logs</li> </ul>

Role	Contact(s)	What They Do
<b>Technical Support Team</b>  <i>Multiple names may go in here. Google Workspace admins, field technicians. This team will change depending on the specifics of the event</i>	<b>Name</b> Email Phone	<ul style="list-style-type: none"> <li>Review user email activity</li> <li>Access server logs</li> <li>Manage firewalls and review logs</li> <li>Check various servers and systems for compromise and manage those servers</li> </ul>
<b>Administrative Support / Incident Recorder</b>  <i>Usually an administrative assistant familiar with the technology department</i>	<b>Name</b> Email Phone	<ul style="list-style-type: none"> <li>Maintains the incident logs</li> <li>Provide lunches</li> <li>Run errands</li> </ul>
<b>Communications / Media Team</b>  <i>The PR or HR Director if there is one or someone from the Business Office. Could also be a principal or other administrator</i>	<b>Name</b> Email Phone	<ul style="list-style-type: none"> <li>Manage public communications</li> <li>Manage staff communications</li> <li>Manage parent/student communications</li> <li>Maintain backup communication methods for parents</li> <li>Set up a call center</li> <li>Talk to press or prepare talking points for other leaders</li> <li>Develop a call tree for front-line communications</li> <li>Update social media</li> </ul>
<b>Data Governance</b>  <i>Usually principals or guidance counselors. Whoever manages student data imports and exports</i>	<b>Name</b> Email Phone	<ul style="list-style-type: none"> <li>Determine severity of data leaks</li> <li>Identify most likely data sources that may have been breached</li> <li>Contact appropriate reporting authorities</li> </ul>
<b>Business / Finance</b>  <i>The Business Manager and possibly other staff from the business department</i>	<b>Name</b> Email Phone	<ul style="list-style-type: none"> <li>Review financial systems</li> <li>Contact Cyber Insurance</li> <li>Authorize emergency spending</li> <li>Place holds on accounts</li> </ul>

### 2. Response Contacts

These are individuals/organizations that you will likely need to notify and/or work with, but not part of the IRT.

Role	Contact(s)	What They Do
<b>Cyber Insurance</b>  <i>If you have cyber liability insurance, they can provide legal representation, forensics, mitigation and recovery resources.</i>	<b>Name</b> Email Phone	<p>Immediately. They should be contacted as soon as you determine you have a serious cyber incident.</p> <p>The business office will be able to identify whether you have cyber liability insurance and the proper contact procedures.</p>
<b>Legal Representative</b>  <i>All communication with staff and the public needs to be reviewed by your district's legal. This may be provided by your cyber insurer.</i>	<b>Name</b> Email Phone	You can get this from your business manager and/or superintendent
<b>Board President</b>  <i>Typically contacted by the Superintendent or the Cyber Incident Response Manager.</i>	<b>Name</b> Email Phone	As soon as an incident is confirmed
<b>ISD Technology Director</b>  <i>If you are a local district and utilize the ISD for technology services (networking, firewalls, internet, etc), they will play a critical role at all stages in the event and need to be contacted in order to protect other networked entities.</i>	<b>Name</b> Email Phone	As soon as an incident is confirmed

### 3. Extended Resources

You may not need all of these resources.

# MiSecure IRP tools Download

<https://misecure.org/incident-response-planning-tools/>





# Cyber Term: Disaster Recovery (DR) Plan

## Explanation

- A written plan for processing critical applications in the event of a major hardware or software failure or destruction of facilities.

## Example of abuse:

- My systems are ransomware. What do I do?

## Solution:

- Find a template or work with your ISD

## COST:

People Time



# Cyber Term: Business Continuity Planning (BCP) or Continuity of Operations

## Explanation

- The documentation of a predetermined set of instructions or procedures that describe how an organization's mission/business processes will be sustained during and after a significant disruption.

## Example of abuse:

- How do I continue to operate if my systems are down?

## Solution:

- Find a template or work with your ISD
- METL is **currently** working on a guide

## COST:

People Time





# Cyber Term: Assessments / Pen Test

Explanation

- What is it?

Example of abuse:

Solution:

- MiSecure Quick Self-Audit
- TetraDefense
- CISA Cyber Hygiene
- MIDEAL Assessments
- Arctic Wolf
- Cyber insurance audits
- Financial audits

People Time



# 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/>



bitly



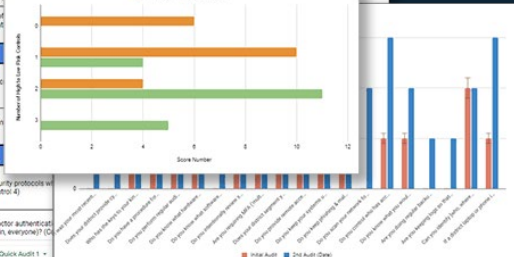
# MI Secure Quick Self - Audit


People	Score	Score Help
When was your most recent internal conversation about cybersecurity? Who was involved in that conversation? (Control 17 and 19)	1	0=never 1=don't remember, but not sure when 2=within 1 year/annually 3=bracketed/standing monthly agenda item or meeting
Does your district provide cybersecurity training? For who (admins, staff, students)? (Control 17)	2	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
Who has the keys to your kingdom? Do they use different accounts for daily activities and problem administration work? (Control 4)	3	0=don't know 1=not 2=not 3=not

## Overall Risk Assessment

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

Initial Audit 2nd Audit (Date)



This is MISECURE Quick Self Audit Version 2.2 Final				
 MISECURE.org		MISECURE Quick Self-Audit Data Collection Tool		Date of Audit 1
These 20 questions will help you to think about cybersecurity practices in your organization and focus your improvement efforts. This Quick Self Audit references cybersecurity best practices and "controls" that are outlined in more detail in the Essential Cybersecurity Practices for K12, which can be found at <a href="http://www.misecure.org">www.misecure.org</a> .			Document thoughts and ideas as well as goals for the improving your organization's security profile.	
To Continue: 1) Score your organization on each of the 20 questions; 2) Go back to the lowest scored items and plan your improvements. Remember: you don't have to fix everything at once!				
Essential Questions	Score	Score Help	Ideas/Notes	Where would you expect to be 6 months from now
Do you provide cybersecurity training? (Control 17)	3	1-Nothing formal or regular 2-Limited only for new staff 3-Regular staff training and/or updates in meetings, emails, articles, and/or alerts 4-Regularly scheduled skills training and phishing simulations		
Do you require MFA (multi-factor authentication) for logins? (Control 6)	2	1-Don't know / not required 2-On some systems, but not all 3-On all internet-facing and/or remote access systems (e.g. VPN) 4-On all internet-facing and critical internal systems		
Do you require long and complex passwords and do you monitor failed password login attempts? (Control 5)	4	1-no password policy 2-password policy that requires long passwords 12 characters and complexity requirement 3-automatically enforced strong password policy that prevents password reuse and requires password change at least annually 4-password policy as defined at previous level, plus logging failed login attempts and locking account after a number of failed attempts		
Do you change default passwords on all systems you install and all user and system accounts that you create? (Control 4)	1	1-No or don't know 2-We change defaults on most systems, but some systems have default passwords despite our efforts 3-Consistent practice in place to change default passwords 4-Procedures in place, including checking for vendor default passwords		
Do you keep your systems up-to-date? How frequently do you apply updates? (Control 7)	3	1-No updates are applied or don't know 2-Updates performed manually on some systems 3-Updates performed both manually and automated on all systems that can be updated. Systems that cannot be patched are identified and isolated appropriately 4-Updates applied on all systems and critical vulnerabilities are patched in under two weeks		

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



# Cyber Term: EDR/xDR/MDR



## EXPLANATION

- Detect Security Incident, Contain the Incident, Investigate and Remediate

## EXAMPLE:

- Our example (detection)

## SOLUTION/VENDOR:

- Microsoft Defender, Sophos intercept X, CrowdStrike Falcon

## COST:

Subscription

The screenshot displays the Microsoft 365 Defender interface. The left sidebar contains navigation options: Home, Incidents & alerts, Hunting, Actions & submissions, Threat intelligence, Secure score, Learning hub, Trials, Partner catalog, Assets, Devices, Identities, Endpoints, Vulnerability management, Partners and APIs, Evaluation & tutorials, Configuration management, Email & collaboration, and Investigations. The main content area shows an incident titled 'Execution incident on one endpoint' with a status of 'Active'. Below the title, a message states: 'This incident is read-only because it contains alerts from service sources that you do not have permission to view or manage. Contact a global admin for access.' The incident details panel on the right shows the incident is assigned to 'Unassigned', has an incident ID of '6974', and is classified as 'Not set'. It also shows the first activity on 'Apr 24, 2023 9:51:58 PM' and the last activity on 'Apr 24, 2023 9:52:14 PM'. The central area displays a list of alerts, including 'Suspicious PowerShell command line' and 'Suspicious process executed PowerShell command', both dated 'Apr 24, 2023 9:51 PM' and 'Apr 24, 2023 9:52 PM' respectively. An incident graph shows a communication between a device named 'tardis' and a process named 'powershell.exe - ExecutionPolicy bypass'.





# Cyber Term: EDR/xDR/MDR

## EXPLANATION

- Detect Security Incident, Contain the Incident, Investigate and Remediate

## EXAMPLE:

- Our example (detection)

## SOLUTION/VENDOR:

- Microsoft Defender, Sophos intercept X, CrowdStrike Falcon

## COST:

Subscription

EDR: Endpoint Detection Response

XDR: Extended Detection and Response

NDR: Network Detection and Response

MDR: Managed Detection and Response




# Section 97g funding

## Background

- Section 97g of 23-24 SoM budget
- K12 funding for \$9M for at least 3 years
- Began Oct 1, 2023
- Purchasing Apr 29, 2024

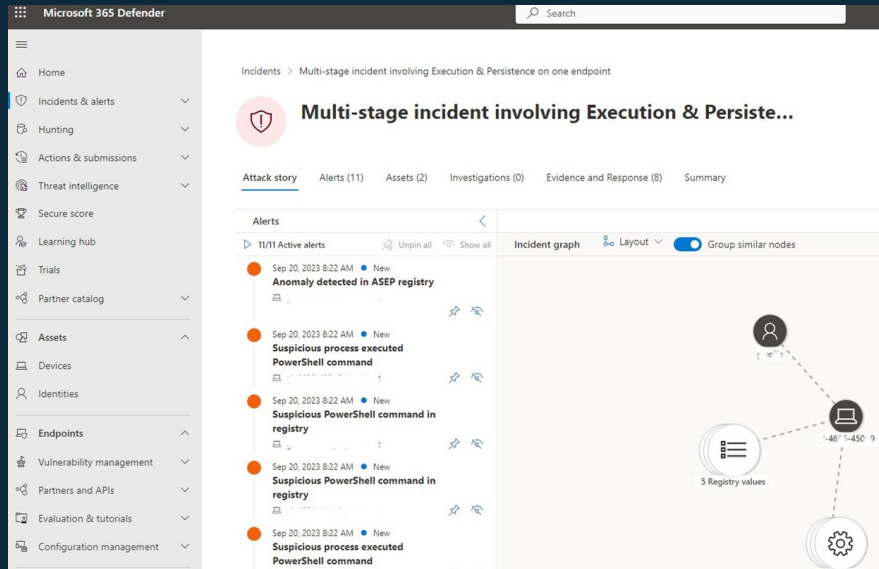
## Key language

- Form a *Statewide Security Operations Center (SOC)*
  - Form an *Advisory Board*
  - Provide *Managed Detection and Response (MDR)*
    - for *Critical Technology Infrastructure*
  - *Train, monitor and track* district progress
  - Prepare a *summary report* to fiscal agencies
- 

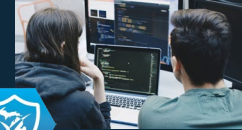
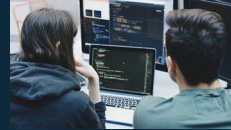


*What is Managed Detection and Response (MDR) software?*

MDR is a software service which combines technology and human expertise in monitoring and responding to digital threats 24x7



# MiSecure K - 12 Operations Center Incident Response Stages







# Cyber Term: SOC/SIEM

## Explanation

- Security Operations Center (SOC); a team of experts that proactively monitor an organization's ability to operate securely.
- Security Information and Event Management (SIEM) tool

## What is it?

- Usually a managed service that monitors your organization

## Solution:

- Achilles Shield, Arctic Wolf, Rehmann, VDA Labs, BitLyft

COST:

Subscription



# Cyber Term: SOC/SIEM

## Explanation

- Security Operations Center (SOC); a team of experts that proactively monitor an organization's ability to operate securely.
- Security Information and Event Management (SIEM) tool

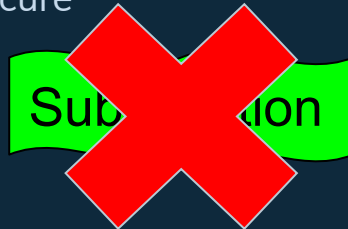
## What is it?

- Usually a managed service that monitors your organization

## Solution:

- Achilles Shield, Arctic Wolf, Rehmann, VDA Labs, BitLyft
- MiSecure

## COST:





# How to Pay for it All

How many of you leverage or rely on bond funding for technology projects?

How many of you have an ISD that provides or could provide some of these services for you?

The main focus: Do what you can as you can - do something!

Bond funding...

- ◆ CapEx items are acceptable (including appliances and operating systems)
- ◆ OpEx items are generally not acceptable (software and subscriptions)



# How to Pay for it All

How does this impact your cloud strategy?

How does this impact your cyber strategy or technology roadmap?

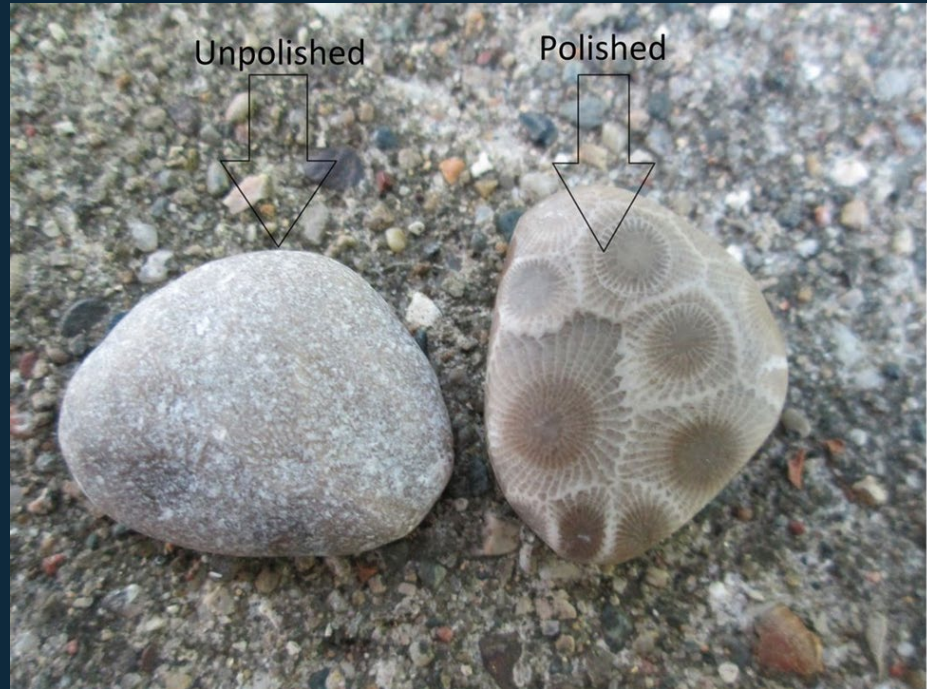
Managed services or subscriptions...

- ◇ Cyber tools and initiatives often rely on both
  - Exceptions: appliances with perpetual licensing
- ◇ XaaS



# Cybersecurity is a process

Keep polishing...



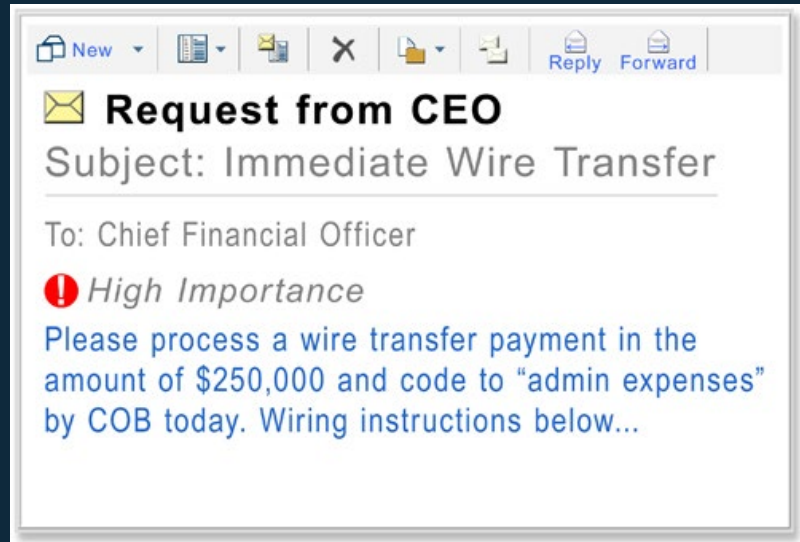


# Less technical threats

◇ Largest Losses = Online Fraud

aka Business Email Compromise

◇ Largest Disruption of Operations = Ransomware



This kind of scam is often referred to as "Business Email Compromise"

# Scams can also take advantage of public information:

Vendor	Great Excavating LLC	C [REDACTED] es, I
General Subtotal Base Bid Price	\$ 354,568.80	\$ 414,52
Phase 1 Subtotal Base Bid Price	\$ 606,973.40	\$ 695,60
Phase 2 Subtotal Base Bid Price	\$ 534,853.00	\$ 645,95
Total Bid Amount	\$ 1,496,395.20	\$ 1,756,07

So much information *has* to be made publicly available and is easily accessible to hackers

## GREAT EXCAVATING INVOICE

DATE: 3/31/2023  
INVOICE # 2292

TO: Center Lake Lincoln Township  
Bellefontaine MI

CUSTOMER ID:  
Calltip

SALESPERSON

JOB PAVING

PAYMENT TERMS

DUE DATE

Oscar Ward

Sales

Due on receipt

1/30/23

QTY	DESCRIPTION	UNIT PRICE	LINE TOTAL
1	Phase 1	Per Contract	606,973.00
SUBTOTAL			\$606,973.00
SALES TAX			20.00
TOTAL			\$606,973.00

Payment via ACH 011401533

Thursday, July 8, [REDACTED]

Prepared by [REDACTED]

# Preventing Email Scams

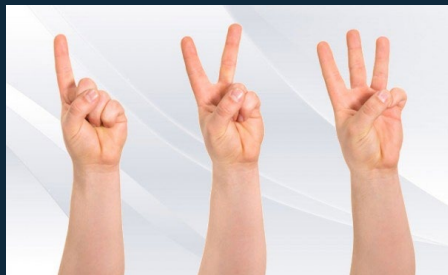
- ◇ Develop good internal processes
  - Talk about it regularly
  - Training
  - MFA
  - Confirmation via secondary channel
  - Require multiple people to process payments
  - Thank people for being cautious

GREAT EXCAVATING INVOICE			
DATE: 3/31/2023 INVOICE # 2292		To: Center Lake Lincoln Township Bellefontaine MI	
CUSTOMER ID: Calltip			
SALESPERSON	JOB PAVING	PAYMENT TERMS	DUE DATE
Oscar Ward	Sales	Due on receipt	1/30/23
QTY	DESCRIPTION	UNIT PRICE	LINE TOTAL
1	Phase 1	Per Contract	606,973.00
		SUBTOTAL	\$606,973.00
		SALES TAX	20.00
Payment via ACH 011401533		TOTAL	\$606,973.00



# Conclusion

- ◇ A lot to digest!
- ◇ *MANY* things that cost money
- ◇ SOME can be done with existing tools, but require effort
- ◇ Every district that has been hit, has then made the investment
- ◇ Drastically reduce your risk with a planful approach
- ◇ Start somewhere... anywhere
- ◇ Little fires will happen, let's keep them contained



1. Use tri-fold to start talking about cybersecurity
2. Schedule a MiSecure Quick Self Assessment today
3. Ask about how to get MDR on your key devices



Terms

End of Life

EDR

SOC

IRP

Patch Management

Backup

MFA

DRP

SIEM

Cyber Assessments

Phishing

XDR

MDR

Remote Access

BCP

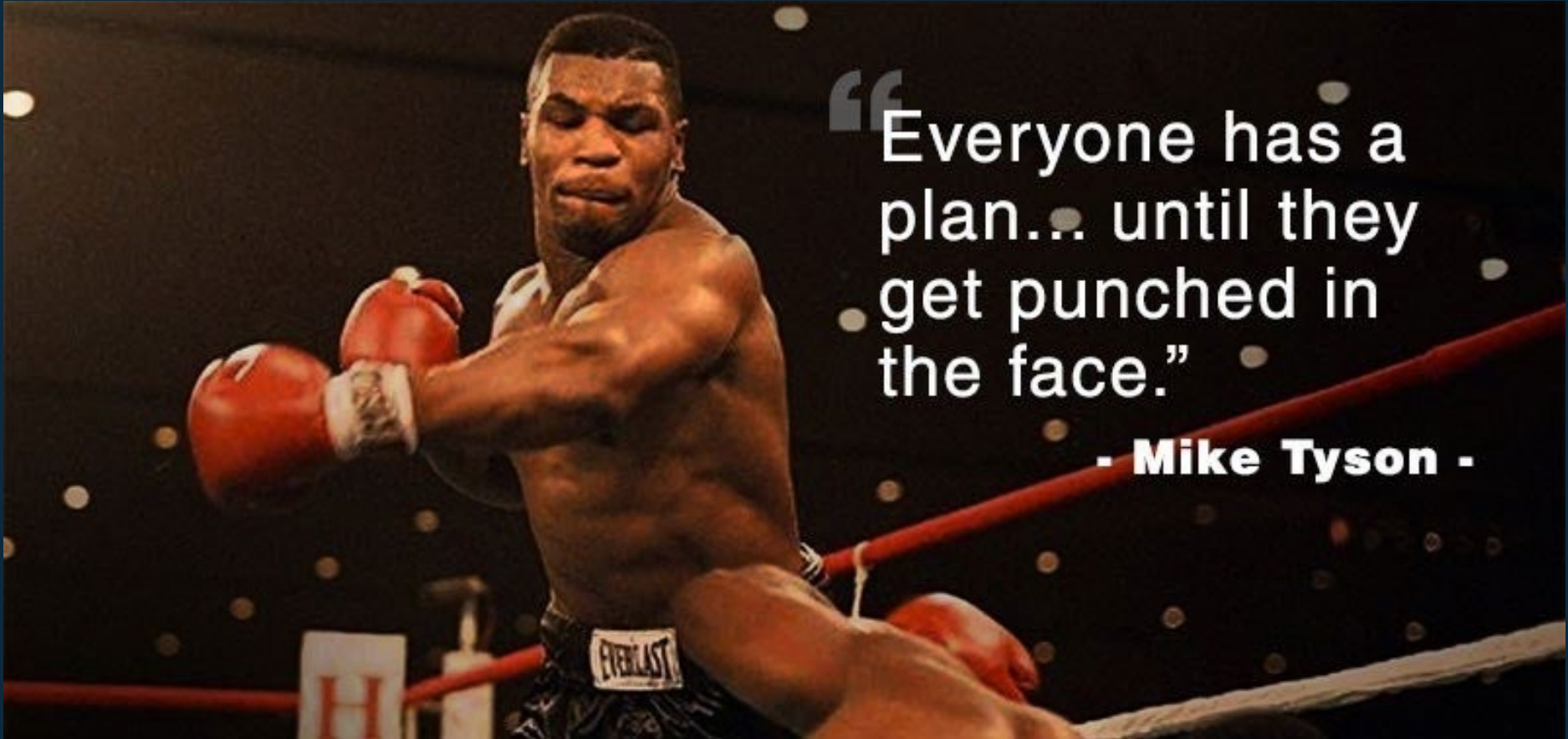




There are only two types of companies: those that have been hacked, and those that will be. Even that is merging into one category: those that have been hacked and will be again.

— *Robert Mueller* —

**AZ** QUOTES

A photograph of Mike Tyson in a boxing ring, shirtless and wearing red boxing gloves and black trunks with "EVERLAST" on the waistband. He is in a defensive stance, looking forward with a serious expression. The background is dark with some blurred lights.

“Everyone has a  
plan... until they  
get punched in  
the face.”

- Mike Tyson -

# Contact Information



Furney Brown

Title

Plante Moran

Email@plantemoran.com



Matt McMahon

MiSecure Director

MAISA

MMcMahon@gomaisa.org



Nick Morse

Cyber Security Consultant

Kent ISD

NickMorse@kentisd.org