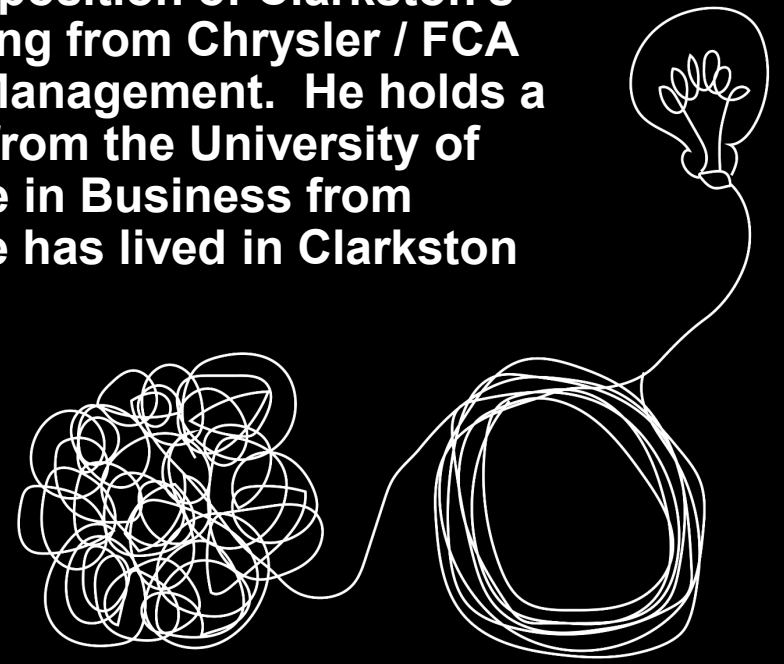
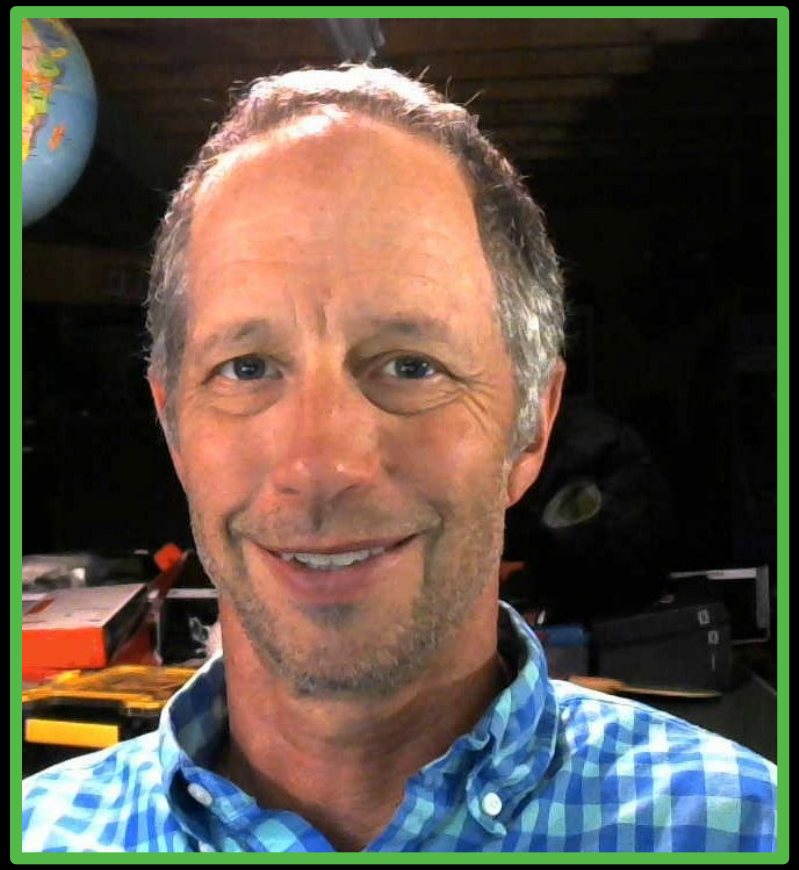
JONATHAN SMITH

City Manager

City of the Village of Clarkston

Jonathan was appointed to the position of Clarkston's City Manager in 2016 after retiring from Chrysler / FCA with 35 years in Supply Chain Management. He holds a Bachelors Degree in Business from the University of Michigan and a Master's Degree in Business from Central Michigan University. He has lived in Clarkston for 40 years.



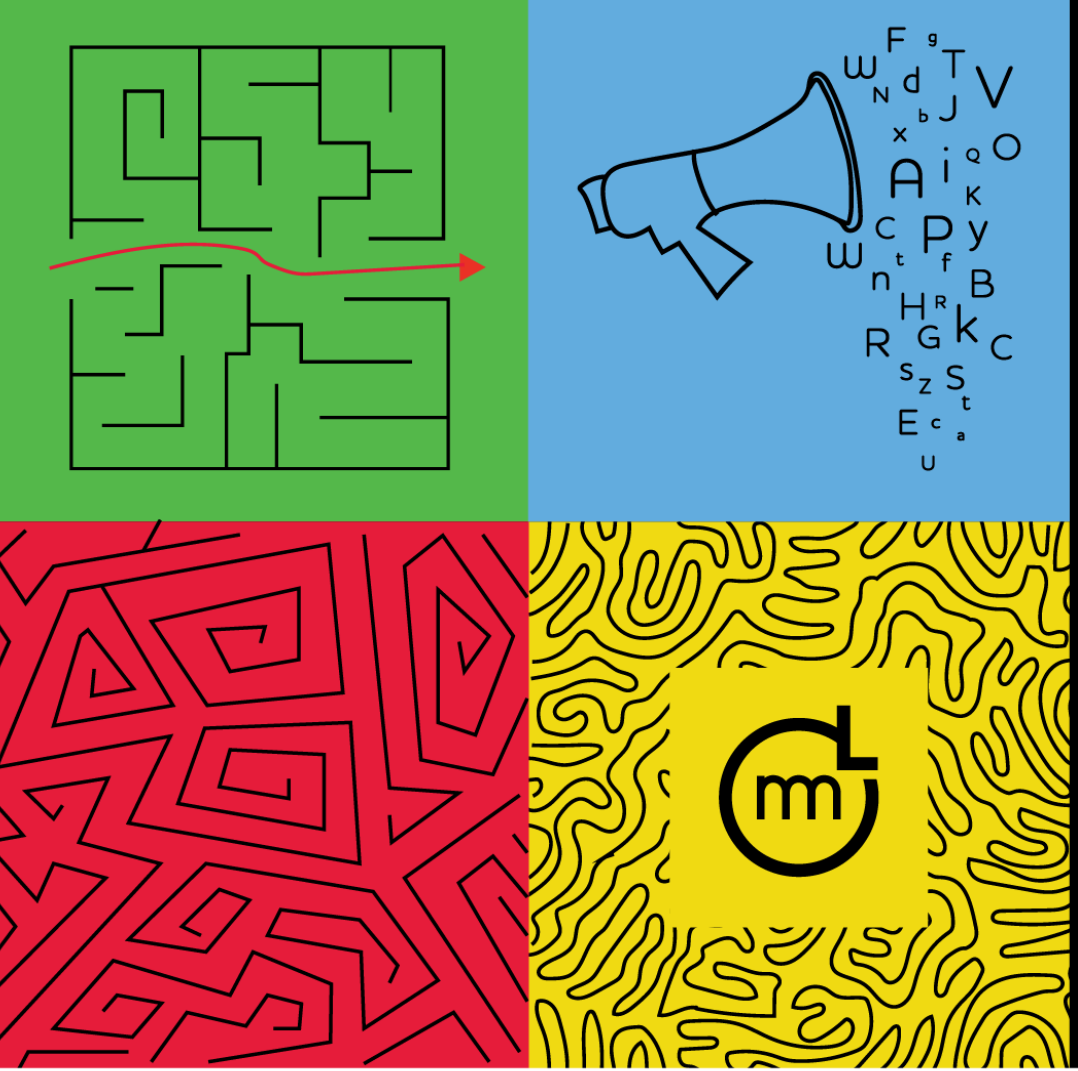


ANDY BRUSH

Program Manager – Michigan Cyber Partners

State of Michigan DTMB

Andy joined the State of Michigan in 2019 to help improve cybersecurity at local public entities across the state. Prior to joining the State of Michigan, Andy served Washtenaw County for 17 years in various roles including Webmaster, Knowledge Manager, Innovations Manager, and spent 7 years as the head of the IT organization. Andy's three formative roles in life: Peace Corps Volunteer, Technical Writer, Teacher, and Dad.



MICHIGAN MUNICIPAL LEAGUE
CONVENTION2022

MUSKEGON, MI

OCT 19-21, 2022

#MMLCONV

Cybersecurity Preparedness

Jonathan Smith, City Manager, City of the Village of Clarkston

The City of Clarkston

- The City of Clarkston is one Michigan's smallest, with only 420 homes
- The Village of Clarkston became a city in 1992 to protect our historic district
- Our annual operational budget is typically less than $900K
- We have just 5 employees, each with their own computer/laptop
- A 6th computer acts as a file server and home for our BS&A application
- For many years the City utilized an independent, one-man contractor for IT support and file backups were a manual process

The Event

- On the morning of 9/11 of 2018, the staff quickly realized that files we had accessed the day before were now “Encrypted” and no longer accessible
- We quickly concluded that that this problem would exceed the abilities of our one-man IT support and called the Oakland County IT Team for assistance
- The County recognized the signs and immediately sent their Team of experts to Clarkston
- The Team identified the fact that Malware known as the Dharma Ransomware was present on our server and quickly spreading
- Both the State of Michigan Police and FBI were notified

“Triage”

- All computers, servers, printers, backup devices, routers – everything- were quickly detached from the network and shutdown in an attempt to stop the spread
- Recognizing that the responsible *Attackers w*ould soon be contacting the City to demand their ransom – *and that the price goes up every hour that passes* – the Team pulled all hard drives and made copies for forensic analysis
- The Michigan State Police and the FBI were provided with copies of the hard drives
- The last full *unencrypted* file backup was determined to be three months old
- Our small City office was suddenly in a total and chaotic lock down

Now What?

- I quickly learned that I will have just two options:
  1. “Slam” the hard drives and restore them using our 3-month-old backup - OR -
  2. Negotiate with the *Attackers* and pay the ransom
- Recreating the last 3 months of file updates, financial transactions, Council minutes, etc. would be a nightmare, but paying the ransom sounded risky too
- Actually, both the State Police and FBI recommended that I pay the ransom
  - Attempting to use the last backup and recreate the lost files could take weeks and any effort to decipher and remove the encryption codes could take months
- All I could think of was, How am I going to explain all of this to my City Council?

Turning Point

- It was late that evening when it occurred to me that in our last MML Insurance renewal that we had accepted a recommendation to add Cyber Security coverage to the policy
- With this revelation, I authorized the IT Team to contact the *Attackers*
- The Attackers responded quickly with the ransom to obtain the decryption key:
  - 1.2 bitcoins ($7,771 in 2018) if paid within 24 hours
  - 2.1 bitcoins ($13,600) if paid between 24 hours and 48 hours
  - After 48 hours, they warned, the offer would be withdrawn
- To confirm we were talking to the right *Attackers*, we asked for decryption proof
- The next morning I received authorization from City Council to facilitate the ransom payment via the MML's Cyber Security partner
- Shortly after making the payment, we received the decryption codes as promised

Forensic Analysis

- An important question still to be answered was, *Were the Attackers strictly profiting from the ransom, or might they have been stealing City data as well?*
- A team from the MML Cyber Security partner, the Michigan State Police and FBI conducted a full analysis of the backed up hard drives:
  - The Attackers accessed our server through a remote user of our BS&A application
  - Their first access was just for 3-4 seconds approximately two weeks before the attack
  - Over the next two weeks, the Attackers accessed the server 42 times, each time for 20 seconds or less
  - The day of the event, when they dropped the “payload” on the server they were logged in for 10 minutes
  - Given the short amount of time logged in and the small number of files accessed, the forensic experts concluded that stealing data was not the Attackers goal, just ransom

Recommendations

- Strong firewalls are crucial; while the City had a firewall, it was not up to current standards
- Manual file backups are unacceptable, they must be automated and daily
- Backups should be stored in a detached device (with “air gap”) or in the Cloud or both
- Continually train the office staff on the latest types of viruses and malware
- Put plans in place on what to do and who to call when a virus or malware is detected
- Reduce your exposure - add Cyber Security coverage to your insurance policy!

Thank you!

Michigan Cyber Command Center - MC3

CYBER SECTION
877-MI-CYBER (877-642-9237)
MC3@MICHIGAN.GOV
Michigan.gov/mc3

Michigan Cyber Command Center (MC3)

Michigan Cyber Command Center - MC3

The Michigan Cyber Command Center (MC3) partners with federal, state, local, and private sector businesses to provide cybersecurity assessments, detection, and criminal investigative resources.

The MC3 provides cyber related information to Michigan residents, groups, businesses, and government agencies regarding current trends relating to cyber incidents to aid in the prevention of cyber anomalies upon Michigan network infrastructures.

Michigan Cyber Partners

Prevent Cyber Attacks on Local Public Entities

* Strategically Promote Best Practices
* Build an Interconnected Community

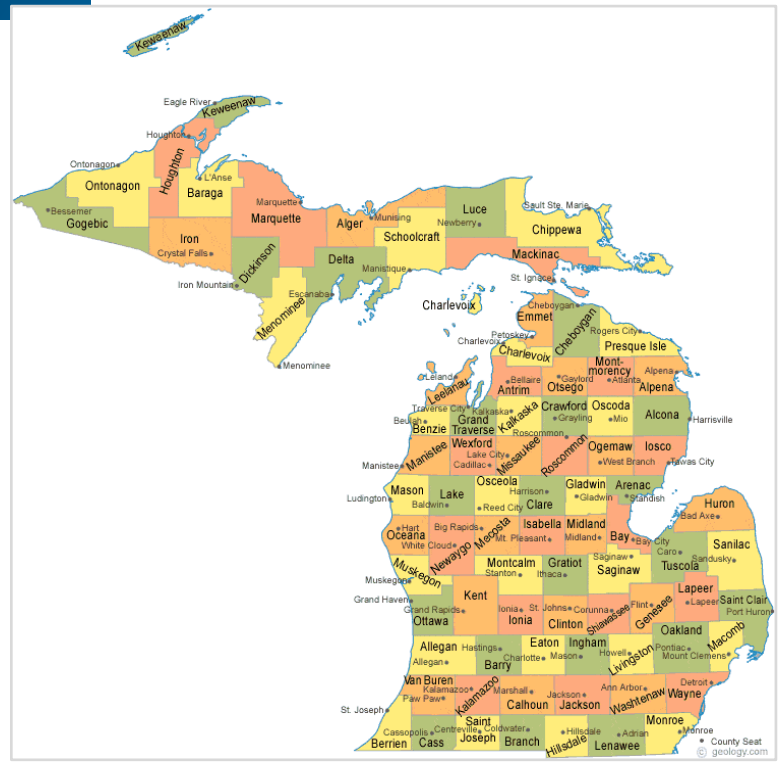
Enhance Response Capabilities

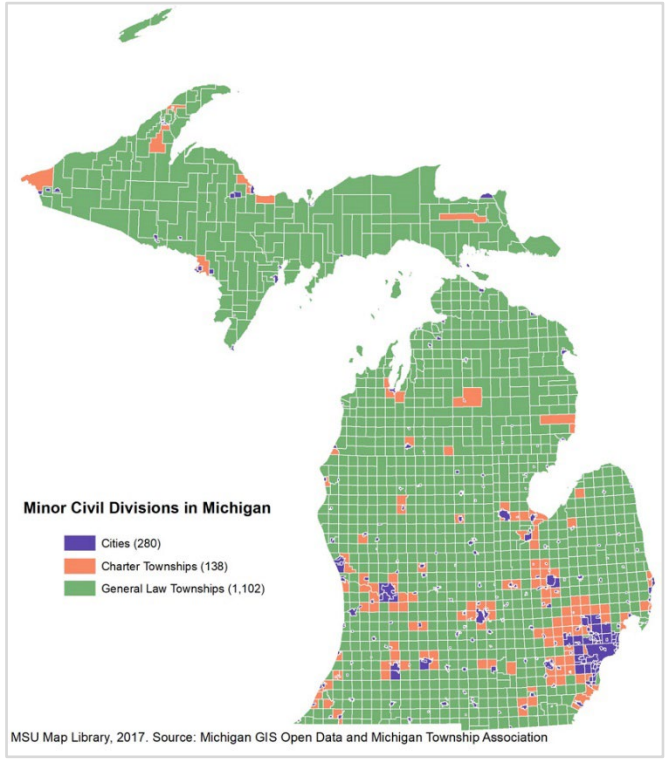
* Support Planning at All Levels
* Conduct Statewide and Local Exercises
* Respond Effectively to Cyber Incidents

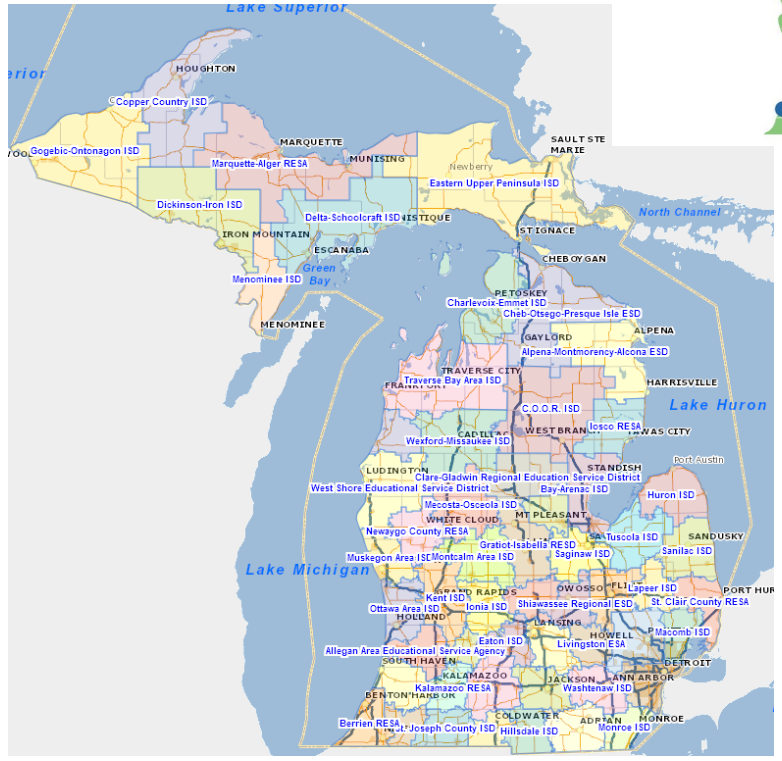
Statewide Reach

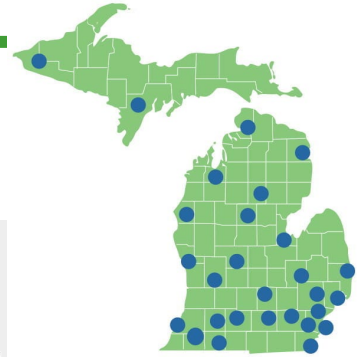
* Increase Reach and Influence
* Build Internal Capabilities
* Use Data to Design Future Activities

Cybersecurity is a Team Sport









STATE OF MICHIGAN SECRETARY OF STATE

MICHIGAN STATE POLICE

MICHIGAN NATIONAL GUARD ALWAYS READY ALWAYS THERE

DTMB

DEPARTMENT OF JUSTICE FEDERAL BUREAU OF INVESTIGATION

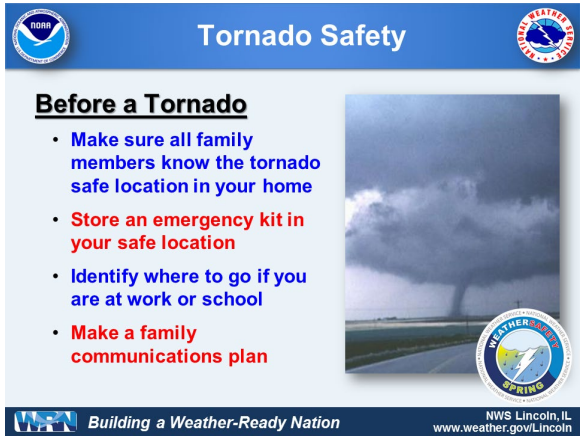
CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY CISA

U.S. DEPARTMENT OF HOMELAND SECURITY

DTMB | Michigan Cyber Security

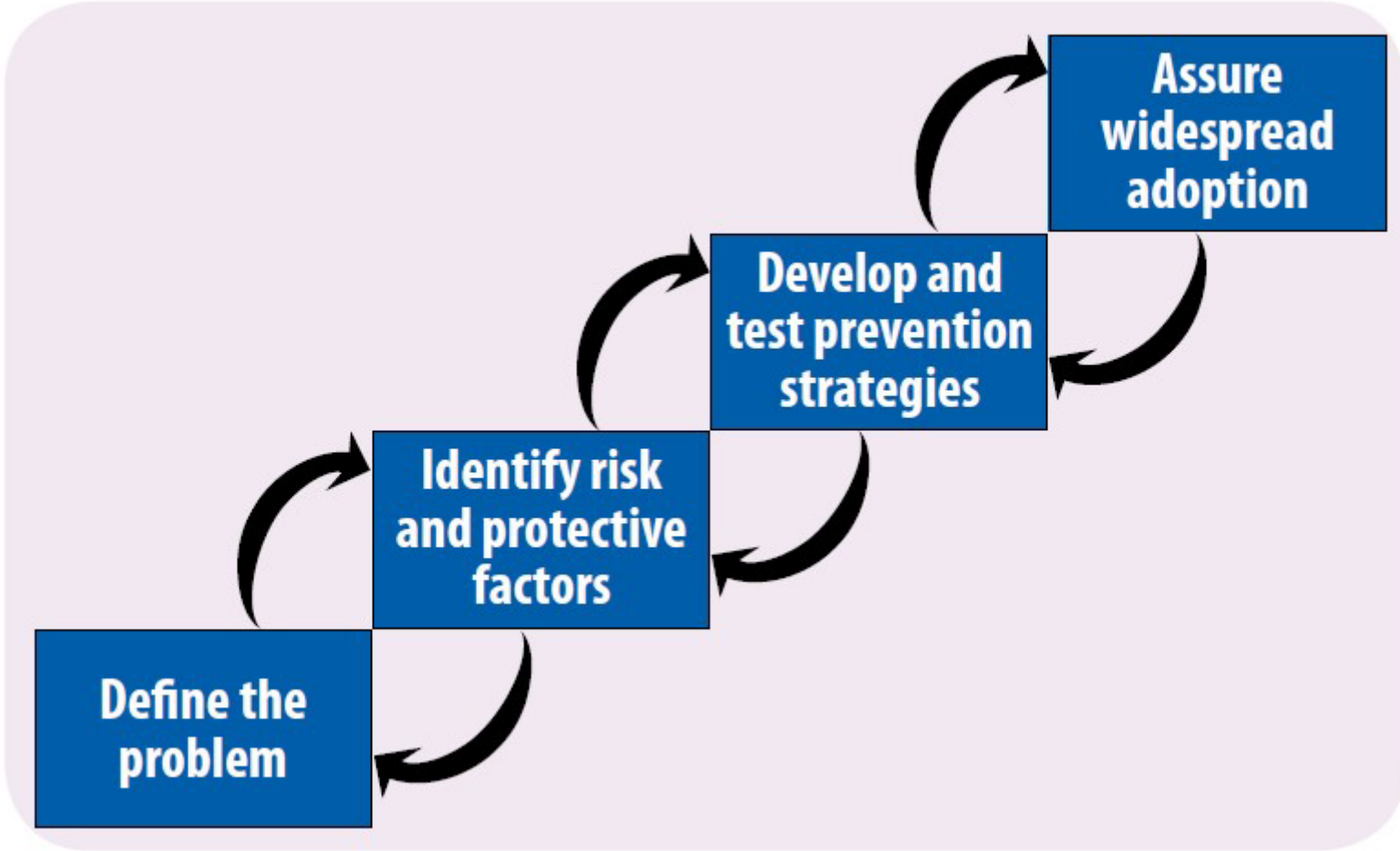
An Emergency Management Model

Prevent | Protect | Mitigate | BOOM! | Respond | Recover



DTMB | Michigan Cyber Security

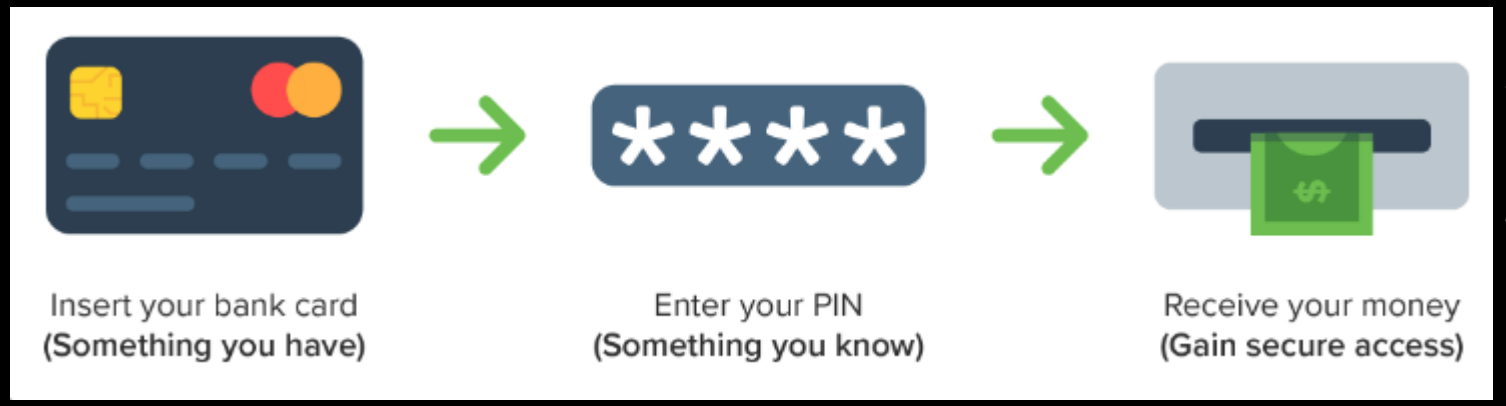
A Public Health Model



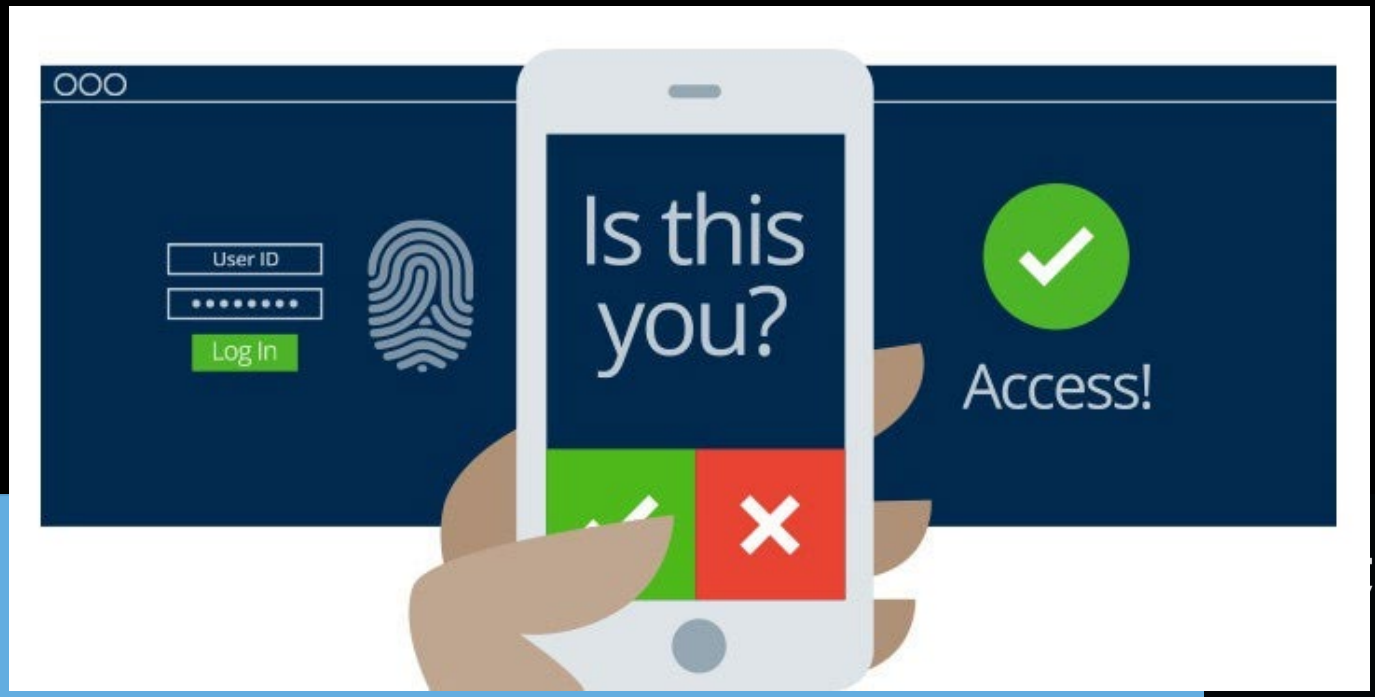
Get Started, Continue the Journey

Reducing the risk of cyber attacks takes effort, but is not impossible.

MFA is...



Duquesne University



Marshall University

Get the Full Picture with a Best Practice Framework

CIS Controls

56 Cyber defense Safeguards

74 Additional cyber defense Safeguards

23 Additional cyber defense Safeguards

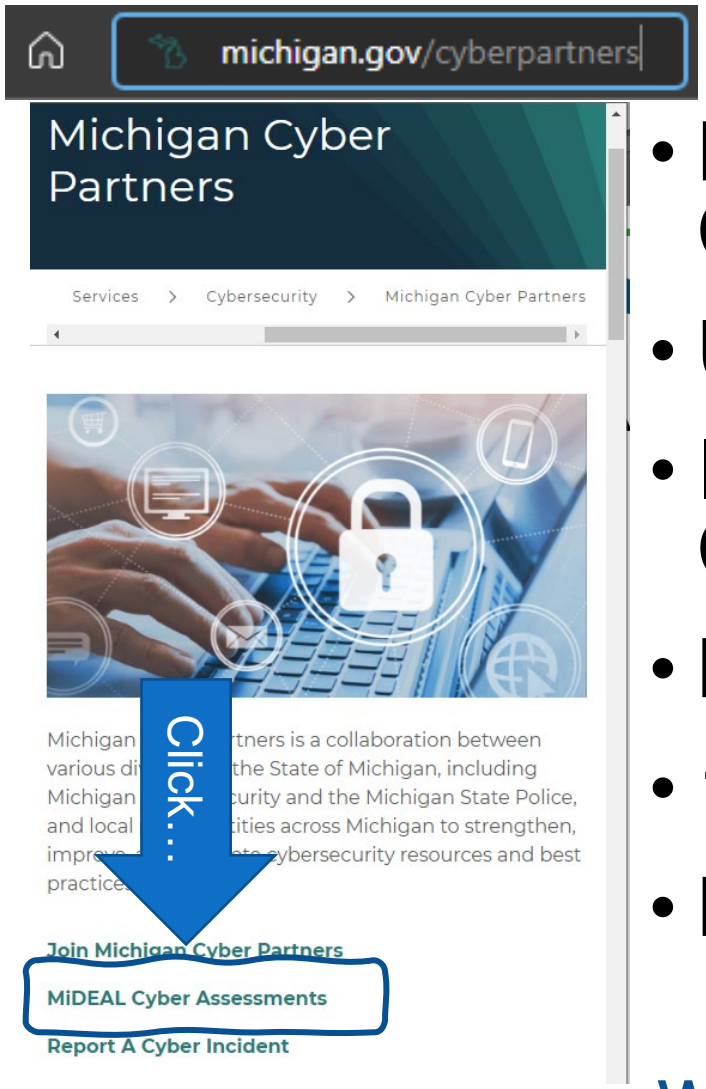
Total Safeguards **153**

Number	Control/Safeguard	IG1	IG2	IG3
01	**Inventory and Control of Enterprise Assets**			
1.1	Establish and Maintain Detailed Enterprise Asset Inventory	●	●	●
1.2	Address Unauthorized Assets	●	●	●
1.3	Utilize an Active Discovery Tool		●	●
1.4	Use Dynamic Host Configuration Protocol (DHCP) Logging to Update Enterprise Asset Inventory		●	●
1.5	Use a Passive Asset Discovery Tool			●
02	**Inventory and Control of Software Assets**			
2.1	Establish and Maintain a Software Inventory	●	●	●
2.2	Ensure Authorized Software is Currently Supported	●	●	●
2.3	Address Unauthorized Software	●	●	●
2.4	Utilize Automated Software Inventory Tools		●	●
2.5	Allowlist Authorized Software		●	●
2.6	Allowlist Authorized Libraries		●	●
2.7	Allowlist Authorized Scripts			●

DTMB | Michigan Cyber Security

If you go full framework, don’t do it alone

Options for Hiring Assessment Help



- Hire a Vendor Using MIDEAL Contracts on Cyber Partners Website
- Uses CIS Controls
- It's a "Friendly" Assessment – Comes With Coaching!
- MIDEAL Prequalified
- 10 Vendor Choices
- Pricing by Organization Size

Vendor	MIDEAL Contract	Vendor Contact	Small Entity <50 Endpoints	Medium Entity 50-500 Endpoints	Large Entity 500-1500 Endpoints	Extra Large Entity 1500 Endpoints
Achilles Shield, Inc Vienna, VA	Contract 210000000299 Contract Expires: 1/24/2026	Kevin Thomas kevin.thomas@a-shield.com 703-501-0094 https://www.a-shield.com/	Not to Exceed $4,950	NTE $4,950	NTE $5,130	NTE $5,490
CyberforceQ, LLC Plymouth, MI	Contract 210000000300 Contract Expires: 1/24/2026	Terrie Mathison Business Operations Coordinator 248-837-1242 tmathison@cyberforceq.com https://www.cyberforceq.com/mideal	Not to Exceed $6,500	NTE $10,000	NTE $10,000-$25,000	NTE $15,000-$35,000
Dewpoint, Inc Lansing, MI	Contract 210000000301 Contract Expires: 1/24/2026	Mike Coyne michael.coyne@dewpoint.com 517-331-0715 https://www.dewpoint.com/cyber-security/	Not to Exceed $11,060	NTE $19,031	NTE $19,030 - $29,896	NTE $29,897 - $39,967
Konica Minolta Ramsey, NJ	Contract 210000000302 Contract Expires: 1/24/2026	Nitzia Payne npayne@kmbs.konicaminolta.us Jack Dixon jack.dixon@kmbs.konicaminolta.us https://kmbs.konicaminolta.us/	Not to Exceed $10,000	NTE $10,000	NTE $10,000	NTE $10,000
Merit Network, Inc Ann Arbor, MI	Contract 210000000303 Contract Expires: 1/24/2026	Kenneth Trumbull kenjt@merit.edu 734-527-0741 https://www.merit.edu/	Not to Exceed $3,800	NTE $7,700	NTE $12,000 - $25,000	NTE $25,000 – TBD
Optech, LLC Troy, MI	Contract 210000000304 Contract Expires: 1/24/2026	Scott Goodwin SGoodwin@optechus.com 313-657-7100 https://www.optechus.com/	Not to Exceed $2,500	NTE $6,000	NTE $6,000 - $18,000	NTE $18,000 - $30,000
Rehman Technology Solutions, LLC Saginaw, MI	Contract 210000000305 Contract Expires: 1/24/2026	Joan Payne joan.payne@rehmann.com Jessica Dore Jessica.Dore@rehmann.com 989-797-8365 https://www.rehmann.com/services/technology-solutions/managed-security	Not to Exceed $6,500	NTE $10,000	NTE $10,000 - $25,000	NTE $15,000 - $35,000
RSI, Inc San Diego, CA	Contract 210000000306 Contract Expires: 1/24/2026	John Shin bids@rsisecurity.com Emily Walsh emilyw@rsisecurity.com 858-621-3155 https://www.rsisecurity.com/	Not to Exceed $13,500	NTE $16,500	NTE $18,000 - $27,000	NTE $28,000 - $52,000
Securely Yours, LLC Bloomfield Hills, MI	Contract 210000000307 Contract Expires: 1/24/2026	Sajay Rai sajayrai@securelyyoursllc.com 248-723-5224 https://www.securelyyoursllc.com/cyber_partners_SOM/	Not to Exceed $5,000	NTE $7,000	NTE $7,000 - $9,000	NTE $9,000 - $15,000
UHY, LLP Farmington Hills, MI	Contract 210000000308 Contract Expires: 1/24/2026	Edward Plawecki EPlawecki@uhy-us.com 248-204-9461 https://uhy-us.com/	Not to Exceed $16,650	NTE $16,650	NTE $16,650-22000	NTE $22,200-$24,050

www.Michigan.gov/cyberpartners

DTMB | Michigan Cyber Security