



Michigan Cybersecurity Legislative Briefing

Presenters:

Laura Clark, Chief Security Officer for the State, DTMB

Detective First Lieutenant Jim Ellis, Michigan Cyber Command, MSP

Lt. Colonel John Brady, commander of the 272nd Cyber Operations Squadron, Michigan National Guard

June 2021

Agenda

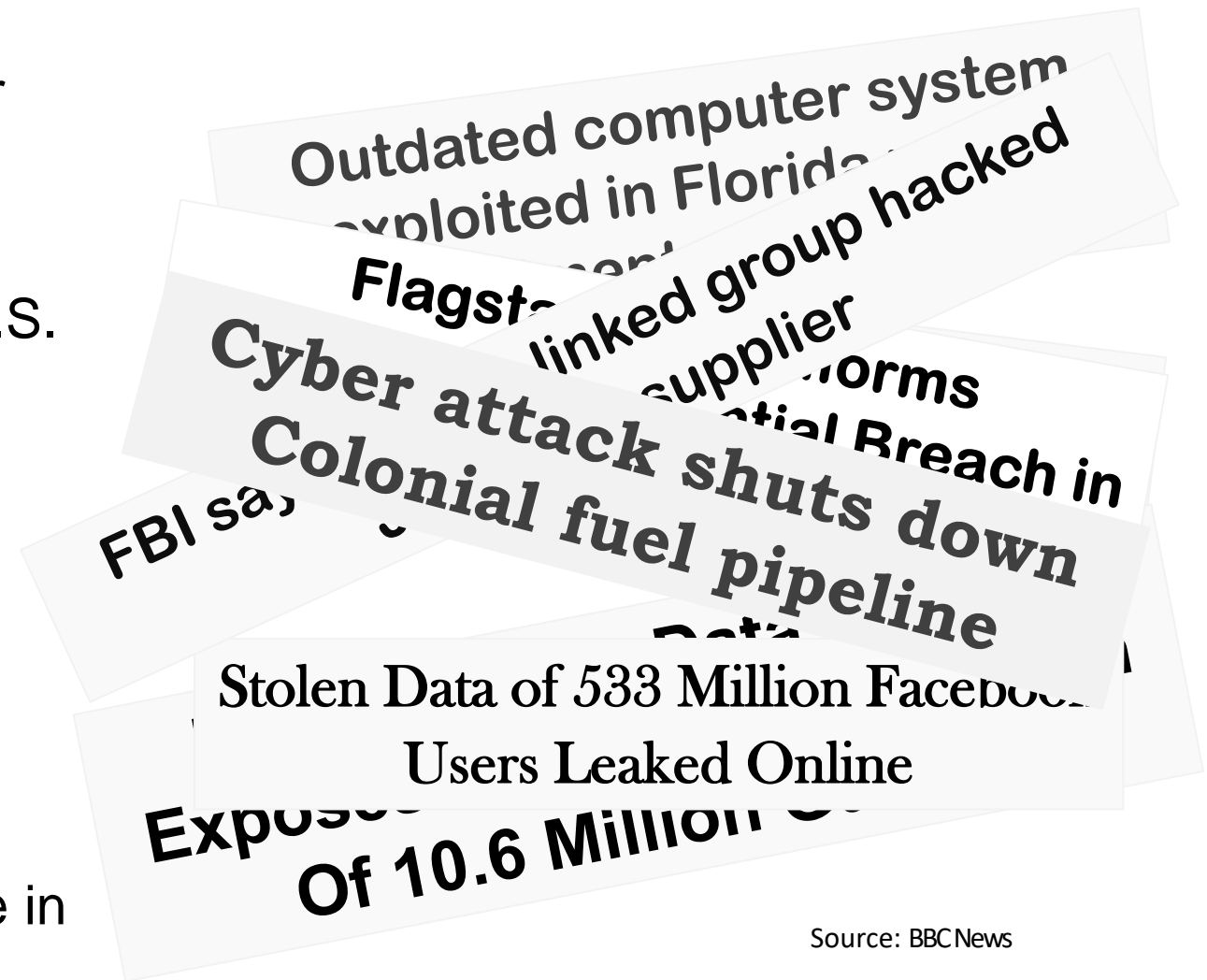
- State of Cybersecurity
- Citizens are Vulnerable Too
- Cybersecurity on the Job
 - State Partners
 - Michigan State Police
 - National Guard
 - Cybersecurity and Infrastructure Protection at DTMB.



State of Cybersecurity

State of Cybersecurity: Attacks and Data Breaches

- U.S. federal government budgeted over \$17 billion for cyber security in 2020.
 - Up 5% over 2019.
- Cost of the average data breach to a U.S. company in 2020: \$8.64 million.
- More than 60 million Americans experienced identity theft.
 - In 2020, the FTC reported 1.4 million reports of identity theft.
 - Doubled from 2019.
- Malicious actors are now targeting government, schools, and infrastructure in addition to individuals and businesses.



Source: BBC News

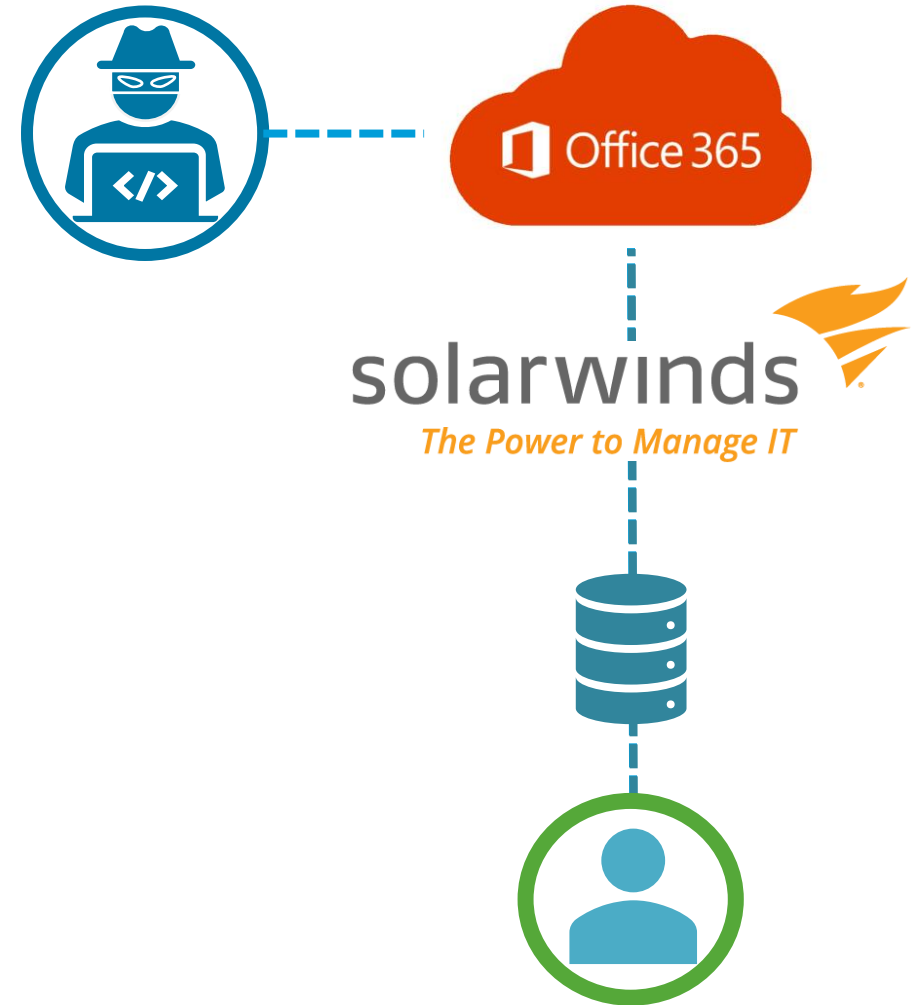
An Attack CAN (and Will) Happen to Anyone

- SolarWinds develops **IT security monitoring and management tools** for SysAdmins and network engineers.
- In March and June 2020, hackers broke into SolarWind's systems and added malicious code into the company's software system called Orion.
- On December 13, 2020, SolarWinds alerted 33,000 that the hack happened.



How Did The Solar Winds Hack Occur?

- SolarWinds uses Microsoft O365 for its email and office productivity tools.
- An attack vector was used to compromise the company's emails; this may have provided access to other data contained in the company's Office 365 productivity tools.
- Solar Winds and Microsoft are still investigating and remediating the incident, but the damage is already done.



“What’s unique... about this particular intrusion is that they used the access they got by compromising SolarWinds itself to insert malware into the build process. This then allowed them to target SolarWinds [and] customers that deployed this back door update.”

-Jacob Williams,
founder of Rendition InfoSec.



solarwinds

The Power to Manage IT

Ransomware on the Rise

7 SAN DIEGO BREAKDOWN CORONAVIRUS L... 65°

HEALTH CARE

147,000+ May Have Had Personal Information Compromised in Cyberattack: Scripps Health

Scripps Health announced they were notifying patients by email that an "unauthorized person" gained access to their network and acquired copies of documents before deploying ransomware that took their systems offline on May 1

Attacks have a virtual impact...

THE WALL STREET JOURNAL.

TECH

NYC's Subway Operator and Martha's Vineyard Ferry Latest to Report Cyberattacks

The New York Times

Today in Business | LIVE Latest Updates Care for Pandemic Pets Tracking the Recovery Global Shortages of Everything

Ransomware Disrupts Meat Plants in Latest Attack on Critical U.S. Business

USA TODAY

News Sports Entertainment Life Money Tech Travel Opinion 78°F ☀️ Subscribe

NATION

Colonial Pipeline paid a \$5M ransom – but will that only invite other malware hacks?: 'If the payments stop, the attacks will stop'

... and more recently, physical impacts.

Mobile Devices Are Affected As Well

Driven by Malicious Actors

- Mobile malware grew 118% from 2020 Q3 to Q4 driven by SMSs. (Source: McAfee)
- 44% of fraud occurs in mobile applications. (Source: RSA Fraud)
- Phishing sites have increased by 6x in 2020. (Source: Zimperium)
 - Common attacks:
 - Leverage the pandemic.
 - Impersonate brands like Facebook, Microsoft, and Amazon.



Driven by User Error

- 14% of Android and iOS apps using cloud storage expose users' personal information, passwords, and even medical information.
- Over 1100 vulnerabilities in Android and iOS in 2020.
- 2/3 of mobile devices run out-of-date and vulnerable operating systems.
- Almost 10% of devices are considered "highly risky" because privacy and security settings impacted or disabled.

Citizens are Vulnerable Too

“At least 34 percent of U.S. consumers experienced a data compromise within 2018...”



From a WFSB-12 broadcast, **“State warns about hackers stealing data from personal phones.”**

<https://www.wsfa.com/2019/07/12/state-warns-about-hackers-stealing-data-personal-phones/>



“We took a hacker to a café and, in **20 minutes**, he knew where everyone else was born, what schools they attended, and the last five things they googled.”

From a Medium.com article titled,
“**Maybe Better If You Don’t Read
This Story on Public WiFi**”
by Maurits Martijn

"Governments have long addressed physical security through public safety services, **like police and fire departments**, as well as public health programs for water purification, sewage treatment and inoculation against infectious diseases. *Similar efforts could – and, in our view, should – help citizens cope with cyberthreats.*"



From *The Conversation*,
“**Swamped by cyberthreats,
citizens need government
protection**” by Karen Renaud and
Merrill Warkentin

Cyber Crime or Fraud on a Computer?

- Just because criminal uses a computer doesn't mean it's cyber crime.

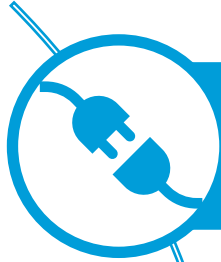


A criminal accessing personal or financial information by sending malware to your computer is a cyber crime.



A criminal communicating to you through a workstation or mobile device to complete a fraud is simple fraud.

Practice Good Cyber Hygiene



Secure your connections and use secure connections.



Use strong passwords and Multi-Factor Authentication on all accounts.



Beware of suspicious outreach through email, phone, or social media.



Protect your home devices with VPN, firewalls, and security apps.

Resources Available for Citizens

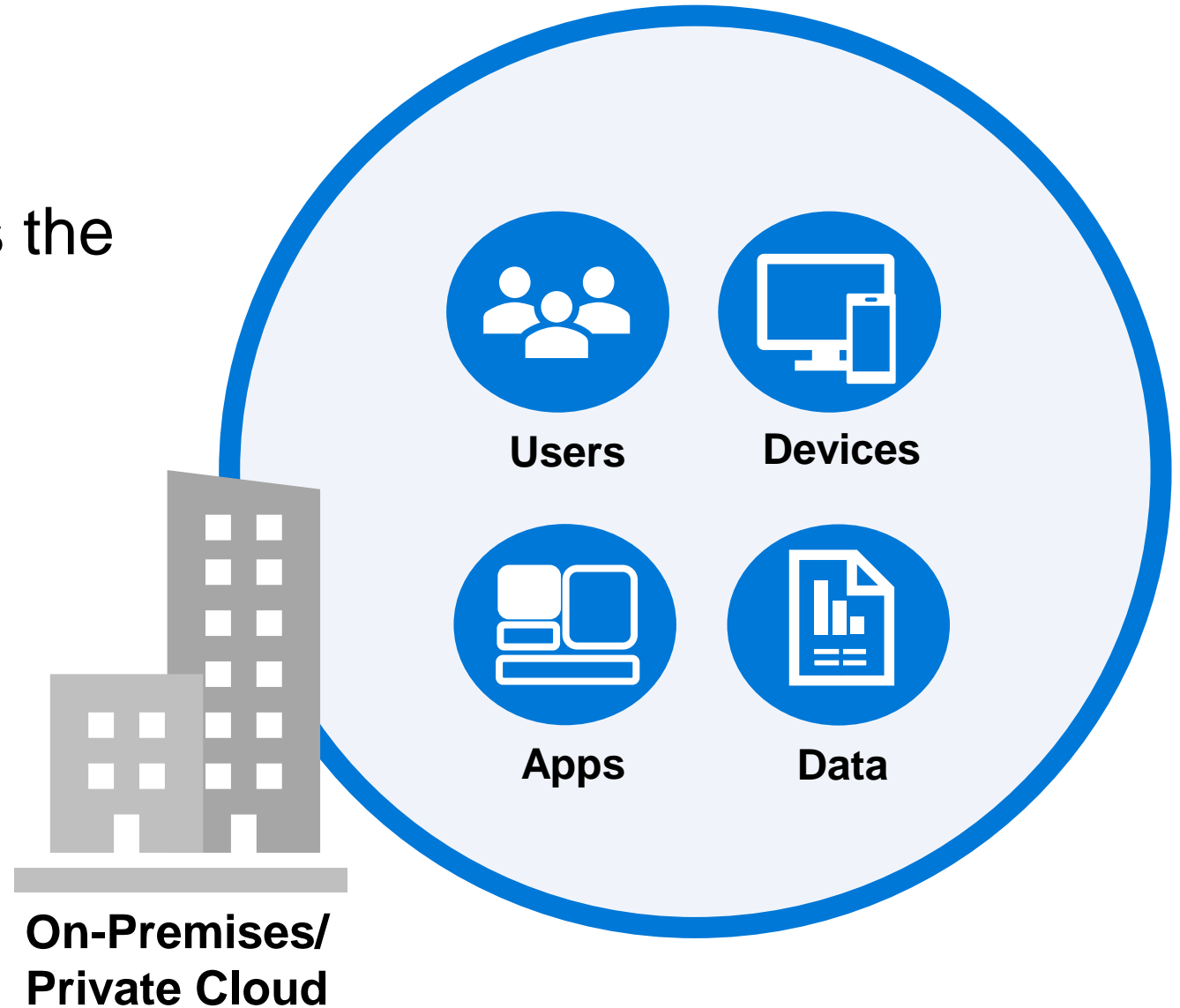


Michigan Secure



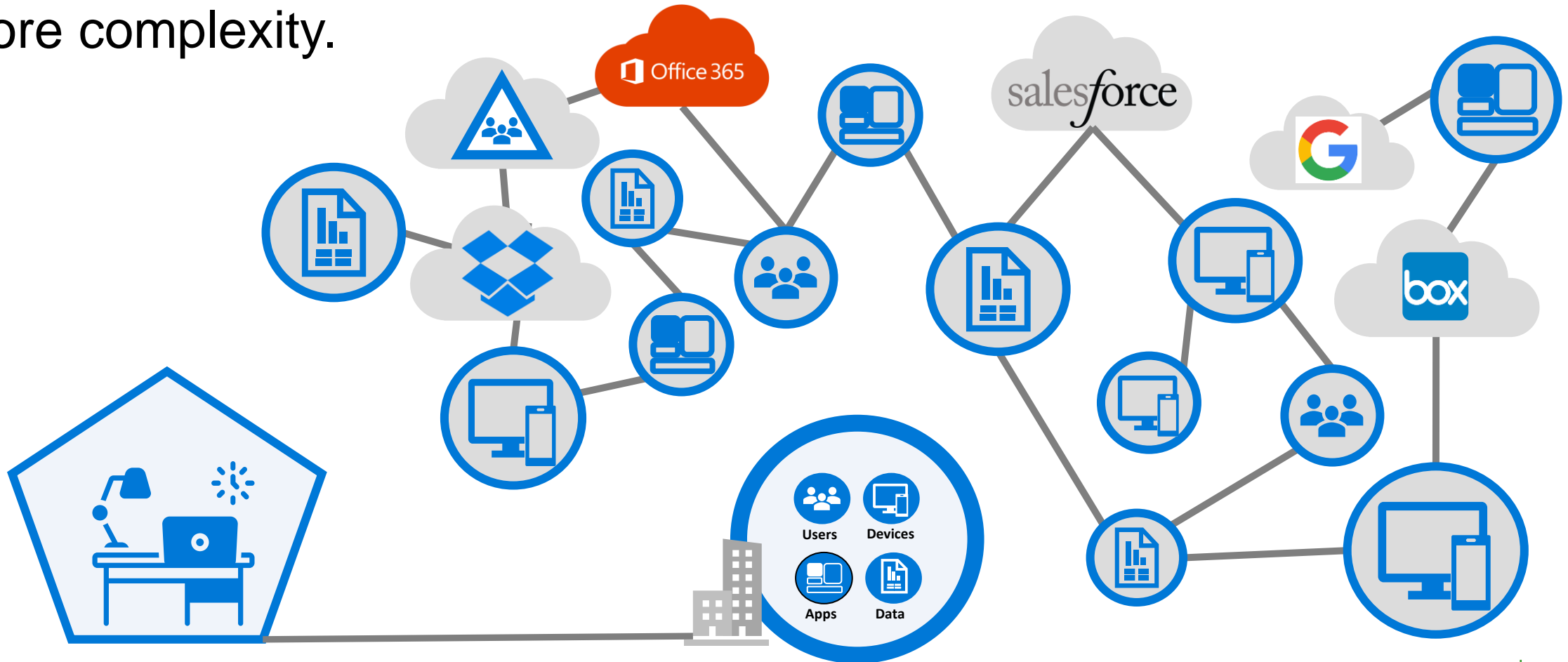
Onsite Work

In the past, the firewall was the **security perimeter**.



Remote Work

With more SOM team members working remotely, the boundary has more complexity.

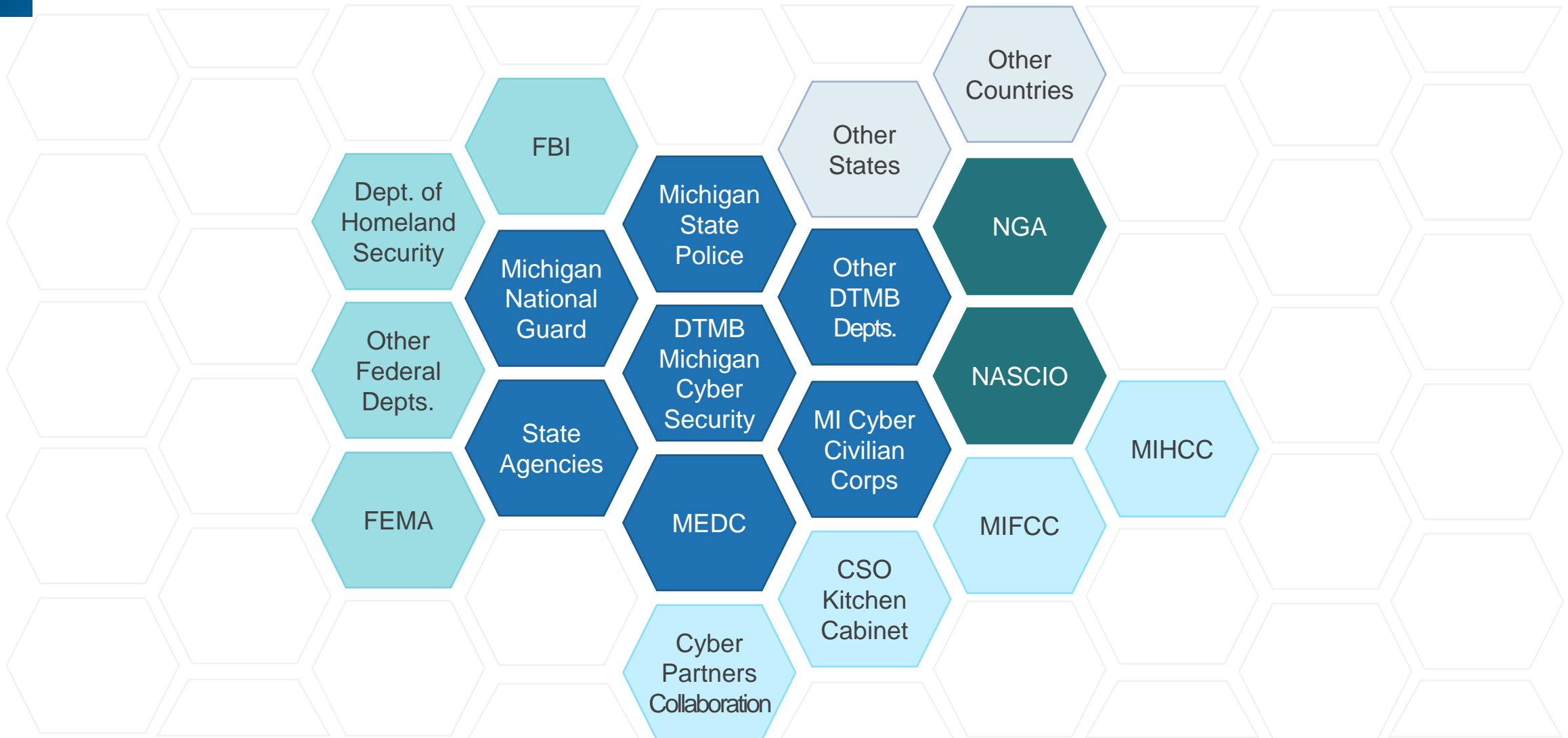


Remote Work Threats

1. Email scams and phishing.
 - Malware is often sent as ZIP or Microsoft Office files labelled “Invoice.”
2. Weakened security controls.
 - “I don’t need my VPN for this work. It’ll go faster.”
3. Attacks on remote-working infrastructure.
 - Threats: Brute force, server-side attacks, DDoS.
 - Why the state uses VPNs
4. Errors and “creative” workarounds.
 - “I don’t like Zoom. Let’s use JoinMe instead.”
5. Physical security.



Cybersecurity Ecosystem



Cybersecurity on the Job

Partnerships with State Agencies

This includes outreach beyond day-to-day handling of network.



MSP Highlights

- **Michigan Cyber Command Center (MC3)**
 - MC3 is the resource for cybersecurity and cybercrime awareness for critical infrastructure; federal, state, and local government entities; other public and private sectors; and citizens of the State of Michigan.
- **Computer Crimes Unit (CCU)**
 - CCU is the statewide leader in responding to and investigating technology digital crimes and in providing forensic data recovery assistance.
- **Internet Crimes Against Children Task Force (ICAC)**
 - In partnership with the CCU, the ICAC is a collection of state, local, and federal partners concentrating on child sexually abusive material trafficking as well as child sexual exploitation investigations.

Cyber Crime Investigation



**Michigan State
Police Contacted**



**Michigan Cyber
Command Center
Investigates**



**Michigan Cyber
Civilian Corp
Deployed**

- Federal partners; FBI, USSS, HSI and others assist with Internet-related investigations.
- Michigan Attorney General assists with cyber crimes against children.
- Cyber crimes from internet services, online shopping, etc., the Federal Trade Commission investigates.

DMVA – National Guard Highlights

- **Army and Air Force Cyber Protection Teams**
 - Responsible to defend military networks.
 - Identify, defend and counter cyber threats.
 - Train, advise, and assist state or local government.
 - Members engaged around the US for past 3 years.
 - Expanding support to include state critical infra-structure inspections, vulnerability assessments, remediation.
 - Partners
 - DoD, USAF, USA, USCC, DHS.
 - Sister States/Nations.
 - Canada, Latvia, Estonia, Lithuania.
 - Industry, Citizen Soldiers/Airmen.
 - Academia, Cyber Patriot.



Day-to-Day Protections: Cybersecurity



Blocks over 90 million potentially malicious intrusions per day at the State of Michigan.



2 BILLION log events per day sent to our security management system, managed by MiSOC.



115,192 pieces of malware detected and blocked.

Incident Response



35K+ Total abuse emails reported.

MiSOC investigates each message and provides a response back to the sender as to whether the email is safe or malicious.



6K+ Total phishing attempts.



380+ Total malicious links found.



75+ Malicious files in phishing emails.

Security Accreditation



174 Authority to Operate (ATO) authorizations.



1079 Mitigated or fully remediated security/compliance gaps.



65 System security classes taught.



Expanded the role-based training series.

Day-to-Day Protections: Infrastructure

Emergency Mgmt. & Central Control


 **12x** Emergency responses coordinated by central control.

 **4** SEOC activations.

 **3** Training exercises completed.

 Capitol Complex prep for inauguration protests.

Security Program Coordination

 **16,256** Visitor processing for COVID.

Security Systems


 **301** Completed work orders.

 **5** New card readers.

 **5030** MICARP requests processed.

 **1133** Items mailed out.

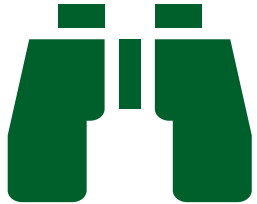
 **348** Accounts deactivated based on reconciliations

 The Access Control team completed large upgrade/renovation project in Jackson.

 RDP PC setup for database work.

External Engagement Functions

These coordinate advisory boards and committees with local businesses, organizations, and other industries to enhance the cybersecurity posture across the state.



Michigan Cyber Civilian Corps (MiC3)

Collaborates with individuals interested in cyber security to share knowledge about incident identification, remedy, and prevention.



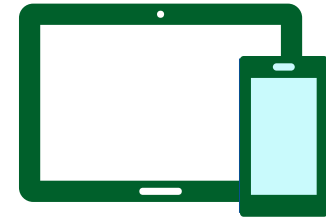
Cyber Partners

Helps prevent cyber attacks on local entities through promotion of best practices and engagement with state and federal resources.



Michigan Cyber Summit

Provides a forum for leaders, professionals, and others to share cyber security knowledge and best practices.



Michigan Secure

A mobile app offered to Michigan residents for free that alerts you if your mobile device, encounters threats, such as a potentially unsecure Wi-Fi network.

Developing the Cyber Education Workforce Framework



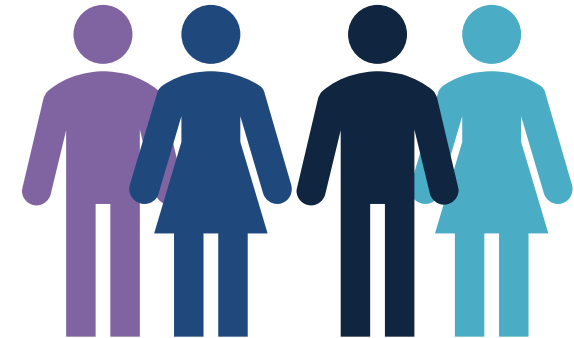
Secure the School

Applying cybersecurity principles to better secure the school's systems and information.



Establish Cybersecurity Curriculum

Integrating cybersecurity into the curriculum.



Build Future Cybersecurity Leaders

Establishing a culture of cybersecurity awareness and exposing students to the field.

Importance of DTMB's Continued Cyber Investment

Continued Investment Needs:

- Reduce vulnerabilities by scanning and patching software/hardware.
- Ensure custom applications and commercial systems are secure.
- Invest in security tools to detect threats and defend the State of Michigan network.
- Train DTMB resources in security and recruit security talent.
- Deploy tools to discover sensitive data and address vulnerabilities.
- Implement tools to better manage access to systems and data.





THANK YOU

Laura Clark, Chief Security Officer for the State, DTMB

Email: Clarkl17@Michigan.gov

Detective First Lieutenant Jim Ellis, Michigan Cyber Command, MSP

Email: EllisJ3@michigan.gov

Lt. Colonel John Brady, Commander, 272d Cyber Operations Squadron, Michigan National Guard

Email: john.brady.2@us.af.mil