DTMB
Technology, Management & Budget

Michigan Cybersecurity Legislative Briefing

Presenters:

Laura Clark, State Chief Information Officer, DTMB

Jayson Cavendish, Acting State Chief Security Officer, DTMB

Detective First Lieutenant Jim Ellis, Michigan Cyber Command, MSP

Lieutenant Colonel John Brady, Commander of the 272d Cyber Operations Squadron, Michigan National Guard

March 2023

Introductions

Laura Clark, State CIO, DTMB

- Chief Information Officer for the State of Michigan.
- Direct the state's technology and security efforts.
- Oversees operations for the department which provides information technology, business, and administrative serves to Michigan's residents, businesses, state agencies, state employees, and retirees.
- Ensures that processes are audited, reviewed, and designed for maximum effectiveness.

Jayson Cavendish, Acting CSO, DTMB

- Acting Chief Security Officer for the State of Michigan.
- Helped formulate and implement policies, strategic plans, directives, and organizational structure.
- Promotes collaboration at all levels to support critical, high-level statewide projects to successful completion.
- Leads several Cybersecurity and Infrastructure Protection committees, as well as programs at the state and local level.

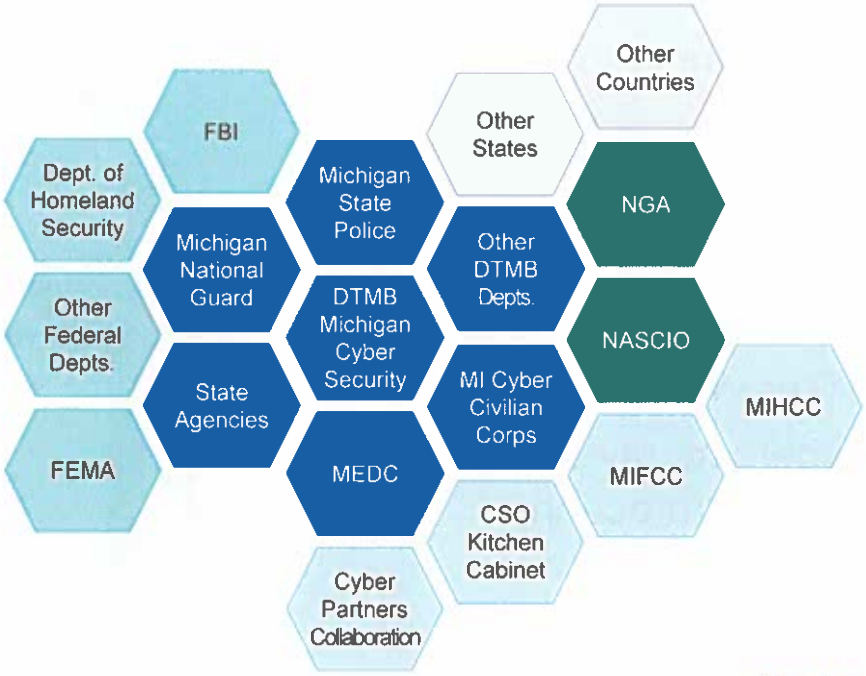
Detective First Lieutenant Jim Ellis, MSP

- Commander of the MSP Cyber Section within the Intelligence and Operations Division.
- Leads a team of over 60 MSP cyber members across MI.
- Oversight of the Michigan Cyber Command Center (MC3). The Computer Crimes Unit (CCU), and the Michigan Internet Crimes Against Children Task Force (ICAC)
- MSP Cyber specializes in high tech criminal investigations, including complex network intrusions and forensic evidential data recovery.

Lieutenant Colonel John Brady, Michigan National Guard

- Commander of the 272d Cyber Operations Squadron, Michigan Air National Guard.
- Leads a team of trained and experienced cyber operators in defense of the DOD Information network as tasked by U.S. Cyber Command and Air Forces Cyber.
- Previously the Director of Operations and the Chief of Operations Training in the 272d Cyber Operations Training and Flight Commander in the 273d Cyber Operations Squadron, Texas Air National Guard.

MI Cybersecurity Ecosystem



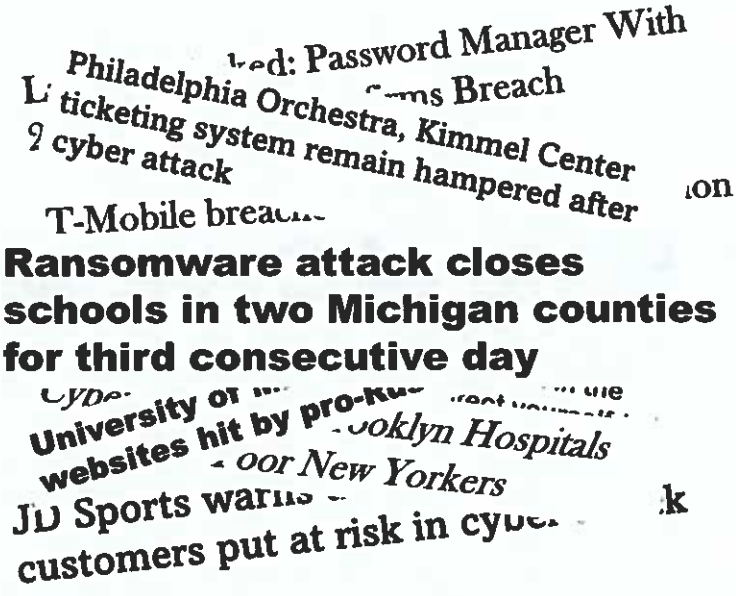
Agenda

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

State of Cybersecurity

State of Cyber: Attacks and Data Breaches

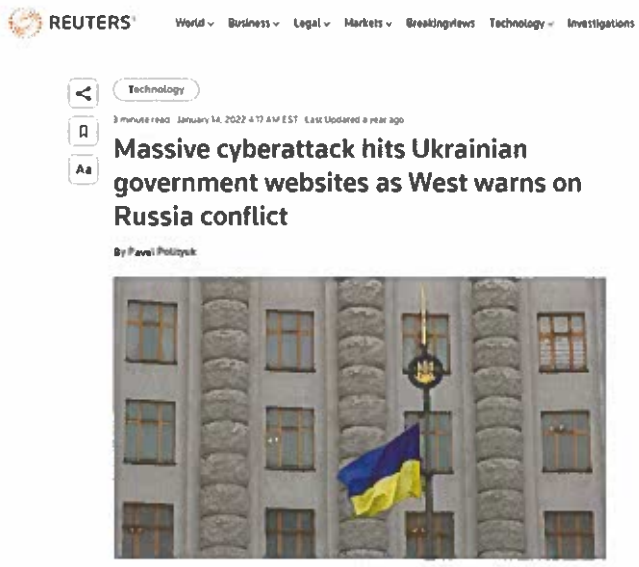
- U.S. federal government proposed $58.4 billion on IT at civilian agencies in FY 2022.
  - $9.8 billion allocated for civilian cybersecurity-related activities.
- Cost of the average data breach to a U.S. company in 2022: $9.44M.
  - $5M more than global average.
- By Q3 2022, the FTC received 555,151 fraud reports.
  - $1k median loss reported.
- 93% of breaches involve financial or espionage motives.



Source: USA Today

Cyber at the Forefront: Geopolitical Tensions

- Geopolitical tensions between Russia and Ukraine have resulted in increased cybersecurity concerns.
- Website compromises, data attacks, and ransomware incidents have occurred between the countries.
- The impact could extend malicious activity beyond the region.


REUTERS World Business Legal Markets Breakingviews Technology Investigations

Technology

Massive cyberattack hits Ukrainian government websites as West warns on Russia conflict

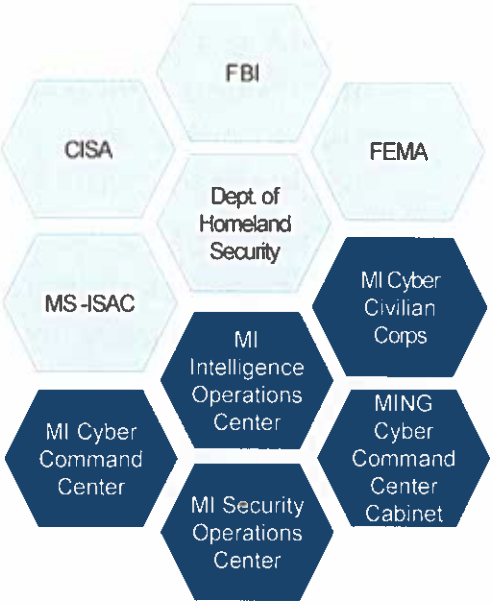
By Pavel Polityuk

Preparing for Cyber Concerns

- In 2015, Michigan published/created the Cyber Disruption Response Plan (CDRP).
  - Details chain of command, responsibilities, and processes for escalation during major incidents.
- Tabletop exercises were completed to prepare for the best course of action in the event of a cyber incident.
  - Tabletop the Vote 2021 and 2022.
  - Local Ransomware Response Escalation.

Addressing Cyber Concerns

- Central Disruption Response Team (CDRT) was activated following heightened tensions between Russia and Ukraine.
- CDRT involves cross-sector support from various groups.
- During the early stages of geopolitical tensions, the CDRT completed:
  - Information sharing and analysis review.
  - Evaluation of the risk to the State of Michigan and local units of government.



Attacks Can (and Will) Happen to Anyone

- Log4J is a popular Java library developed and maintained by the Apache Software Foundation that is widely used in software products as a logging framework for Java.
- In December 2021, Apache announced that Log4J had a serious vulnerability allowed attackers to execute arbitrary Java code to leak sensitive information.
- The vulnerability was given the highest severity rating by Apache as well as other organizations.

Attacks Can Happen to Anyone

Spring4Shell

- Spring Framework provides programming and configuration models for modern Java-based enterprise applications.
- Spring4Shell is a critical remote execution vulnerability that enables threat actors to execute arbitrary code leading to complete compromise of the host or container.

USAHerds

natc
National Agribusiness Technology Center

- USAHerds is a commercial application used by the Dept. of Agriculture for animal health management.
- USAHerds was exploited by a vulnerability, with a hacking group breaching 6 of the 18 states that use the app.

Ransomware is on the Rise

- In 2021, the FBI's Internet Crime Complaint Center received 3,729 ransomware complaints with adjusted losses of more than $49.2 million.
  - 649 complaints were from critical infrastructure sectors.
  - 33.7% increase in victims from 2020.

Hackers accessed data on 270,000 patients from Louisiana hospital system in attempted ransomware attack

By Sean Lyngaas, CNN
Updated 4:16 PM EST, Wed December 28, 2022

KCC systems impacted, campuses closed due to ransomware attack

Posted on May 2, 2022 by Kellogg Community College

Residents are Vulnerable Too

"***More than 422 million people*** were impacted last year due to identity theft, an increase of almost 41.5% from the previous year."

From a NASDAQ article titled "**Data Breaches in 2022 Came Close to an All-Time High**" by Chris Morris

"Criminals or foreign intelligence agencies can set up open Wi-Fi systems that look as if they are from a hotel or a coffee shop, but are actually 'an evil twin, to mimic the nearby expected public Wi-Fi.'"

From The New York Times article titled "**Beware Free Wi-Fi: Government Urges Workers to Avoid Public Networks** " by David E. Sanger and Julian E. Barnes

Resources Available

MiC3

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

Cybersecurity Resource Hub

Contains cybersecurity information, resources, and training to provide residents with knowledge on staying safe in the digital ecosystem.

Cyber Security Partnerships

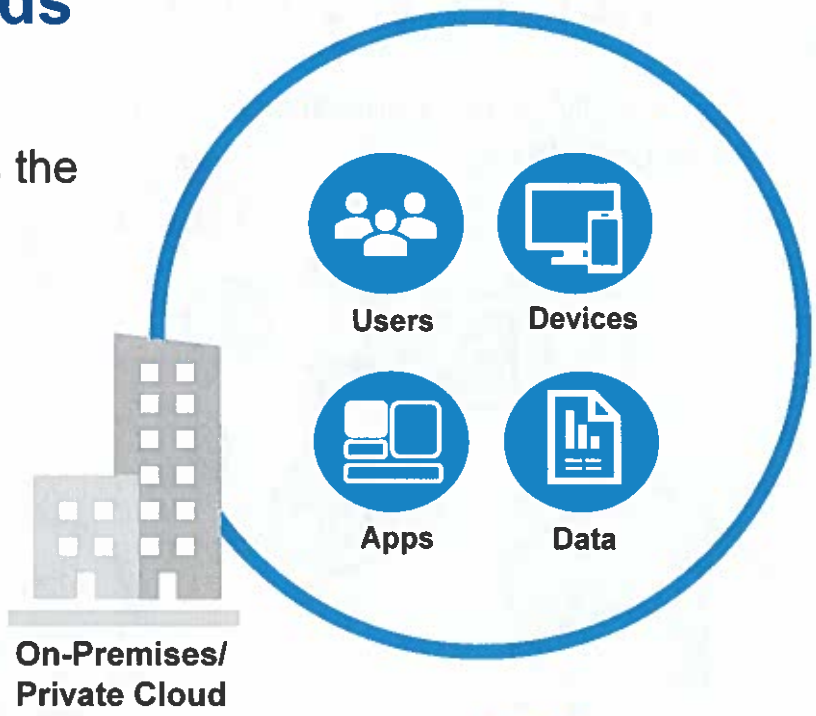
Focuses on building connections between local and municipal governments, schools, and other organizations to improve the state of cybersecurity in Michigan..

Michigan Secure

Free security app for Michigan residents that protects against phishing, unsecure Wi-Fi, unsafe apps, and more.

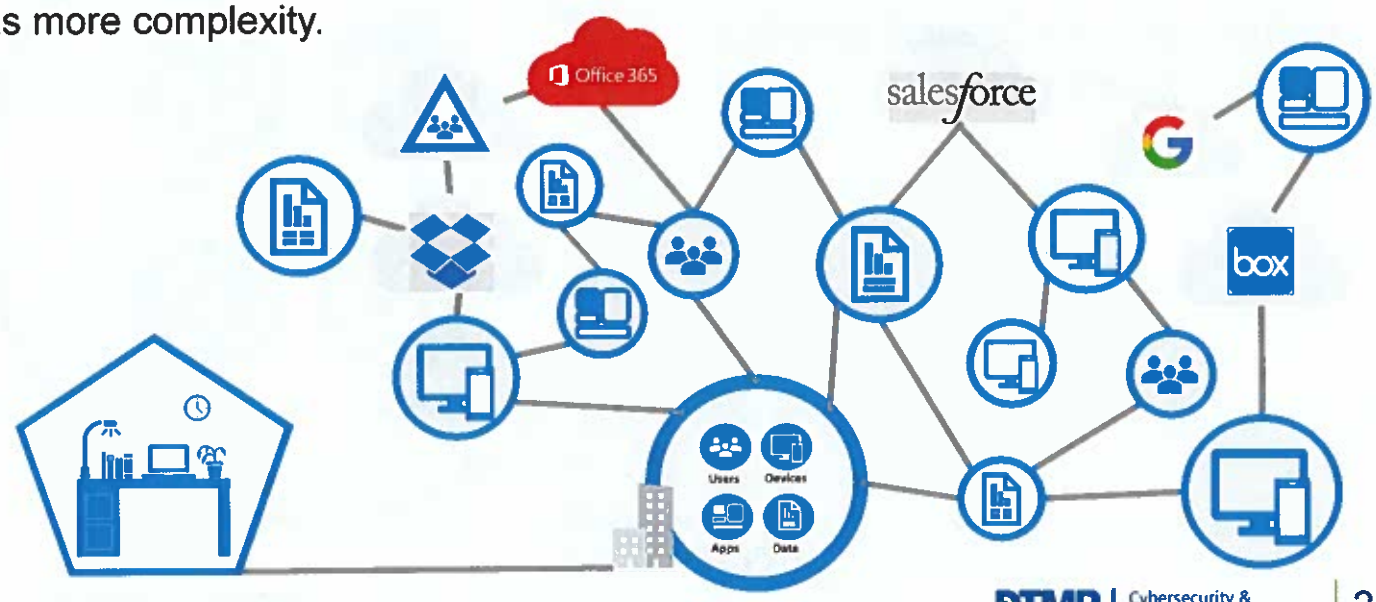
Legacy Workloads

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



Distributed Workloads and Workers

With more SOM team members working in a hybrid environment, the boundary has more complexity.



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.

Cybersecurity on the Job

Partnerships with State Agencies

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

MDOT Michigan Department of Transportation

STATE OF MICHIGAN SECRETARY OF STATE

EGLE MICHIGAN DEPARTMENT OF ENVIRONMENT, GREAT LAKES, AND ENERGY

MDHHS Michigan Department of Health & Human Services

MICHIGAN Department of Education

MICHIGAN NATIONAL GUARD ALWAYS READY · ALWAYS THERE

MICHIGAN ECONOMIC DEVELOPMENT CORPORATION

MiSTEM Network

MICHIGAN STATE POLICE

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.

MSP Cyber 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

MiC3

Contacted

Michigan State Police

Criminal Investigation

Michigan Cyber Command Center (MC3)

Response Resource

Michigan Cyber Civilian Corp

- 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.

MSP Cyber - Proactive Initiatives

- Vehicle Defense Research
- Auto, Truck, Boat Challenge Events
- Host Cybersecurity Investigation Training & Exercises
  - Law Enforcement officers / Industry partners
- High Security Data Project – Cloud storage
- Offensive Forensics
- Cybersecurity Assessments
- Dark Web Scanning
- Cyber Industry related competitions
- Cybersecurity Outreach - Prevention & Awareness

The State of Michigan continues to serve as a leader in cyber Nationally by other states and federal partners

DMVA – National Guard Highlights

- **Army and Air Force Cyber Protection Teams**
  - Responsible for defense of cyber systems/networks
    - Harden and assess cyber terrain
    - Hunt and clear cyber threats
    - Provide advice and assistance to mission partners
  - 70/30% mix of part-time to full-time Guard members
  - Steady-state focus on training for emergency preparedness and federal mobilizations
  - Innovative Readiness Training events support state critical infrastructure assessments
  - Partners
    - DTMB, MSP, MiC3, SOS, DHS-CISA, FBI, TSA
    - Sister States/Nations
      - CA, WA, ID, KS, IA, TX, MD, NJ, PA, VA
      - Latvia

Nationwide

FireEye

DOW

JPMorgan Chase & Co.

DEMATIC

Microsoft

IT Pro

Airman/ Soldier

Citizen

- Technical Expertise
- Business Acumen
- Industry Leadership Skills
- Military Training & Expertise
- Military Leadership
- Dedication, Esprit de Corps
- Patriotism
- Well-rounded and Dynamic
- Technically Savvy
- Seasoned Longevity

NUCOR

VDA LABS

FHLBank INDIANAPOLIS

Synack.

leidos

amazon web services

McAfee

GD

DELTA DENTAL

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, State Chief Information Officer, DTMB

Email: ClarkL17@michigan.gov

Jayson Cavendish, Acting State Chief Security Officer, DTMB

Email: CavendishJ@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