



Cyber Security and Infrastructure Protection & the Michigan Cyber Disruption Response Plan




We will make the State of Michigan one of the most innovative, efficient and responsive governments in the world.





Strategic Plan/Culture Change

- 1 DTMB
- Conducting agency partnership meetings
- Providing resources to managers and supervisors
- Reviewing DTMB processes
- Hosting service area open houses



Utilizing the Strategic Plan, results from the Employee Engagement and Customer Satisfaction Surveys and DTMB Branding, the Department is creating 1DTMB. A unified approach to assisting our customers, providing requested services and discovering solutions.



Merging Teams



In 2013 DTMB merged the cyber security and physical security teams to create Cybersecurity and Infrastructure Protection (CIP). Creating one organization to investigate, assess, mitigate and resolve security risks was a natural progression to the organization. Ultimately, both groups were trying to mitigate risk by lowering the vulnerability of state employees and facilities to attack.

As a team, CIP helps prevent Phishing attacks targeting State employees, the loss of IT equipment through theft, crimes and violence in the workplace and cyber attacks. Working together to teams have prevented cyber attacks, helped MSP investigate theft of IT assets from state facilities and developed the Michigan Cyber Disruption Response Plan.

Cyber Attacks – By the Numbers

Each Year in Michigan State Government:

- 2.5 million web browser attacks
- 179.5 million HTTP-based attacks
- 79.5 million network scans
- 5.2 million intrusion attempts

**2014 statistics*

1.7 million attempted attacks every day

**** YTD 2015 Statistics**

OIP Overview



Part of DTMB's Cybersecurity and Infrastructure Protection Division, the Office of Infrastructure Protection (OIP) is responsible for security and emergency response efforts at all DTMB-managed and select leased facility properties. Integral services provided include the issuance of state access cards, property access control, and 24-hour monitoring of security, life safety systems and heating, ventilation and air conditioning systems. Staff also monitors surveillance cameras throughout all DTMB-managed facilities. OIP administers the employee parking program; managing parking assignments and initiating payroll deductions for state employees utilizing the system. OIP coordinates all programs and activities associated with Homeland Security and emergency management activities for DTMB offices and State facilities.

OIP is divided into the following major focus areas:



Central Control



Central Control monitors security and building systems in DTMB-managed facilities as well as select leased facilities 24 hours a day, 365 days a year. As the main point of contact for emergencies in DTMB-managed facilities, Central Control coordinates response, including contacting 911, for medical, fire and security-related emergencies. Central Control staff monitor surveillance cameras in 9 cities around the state and respond to panic alarms, intrusion alarms and calls from Code Blue emergency phones. Building systems, including heating, ventilation, air conditioning, and lighting systems are monitored in Central Control and appropriate staff contacted if there are error alarms or other issues that need to be addressed.





Customer Service Center

The Customer Service Center (CSC) provides a range of centralized services to both State employees and the general public. The CSC offers services related to parking, employee ID/facility access cards, facilities support, and telephone directory assistance. Parking services oversees parking options for agencies, employees, contractors, and visitors through the management of assignments in 33 lots and ramps in 7 cities with a total of more than 8,000 parking spaces. ID and access card services are provided for State employees and contract employees to allow access to DTMB-managed facilities. Facilities support services assists the DTMB, Building Operations Division through customer communication, request processing and conference room scheduling. State of Michigan telephone directory assistance is available to State employees and the general public.



State Security Program



The OIP State Security Program is responsible for daily management of 153 security guards throughout the state, management and contract oversight of the State standard electronic card access system as well as oversight of the State-wide security surveillance camera network.

Aside from managing daily operational activity the program offers security awareness training to all State agencies and physical security assessments of State occupied facilities. The program partners with Michigan State Police as well as local and regional law enforcement agencies on criminal and security related matters.



Security Services



Security Services focuses on managing access into and within State facilities to create a safe and secure environment. Physical access management services include lock and key system design, hardware installation and maintenance, key creation and key issuance. Electronic access management services include hardware installation, setup and maintenance, access level creation and programming, and system reporting.





Emergency Management

The Emergency Management program creates procedures for structured response to emergency situations in DTMB-managed facilities, coordinates annual fire and tornado drills and developed the Emergency Monitor Network. The program leads the State's Continuity of Government initiative assisting agencies with continuity plan development. Additional roles include program and activity coordination relating to Homeland Security grant funding and participating in the State Emergency Operations Center to assist in the management of state-wide emergencies; physical or cyber.





Michigan Cyber Disruption Response Plan

The Michigan Cyber Disruption Response Plan is the result of a four-month project to update the 2013 Michigan Cyber Disruption Response Strategy. Based on federal and state best practices, Cyber Security and Infrastructure Protection leveraged the experience of a large security company's incident response personnel and the knowledge of public partners to develop a comprehensive response plan in the event of a state-wide disruption to cyber services.

The Need...

Being Prepared for the Worst



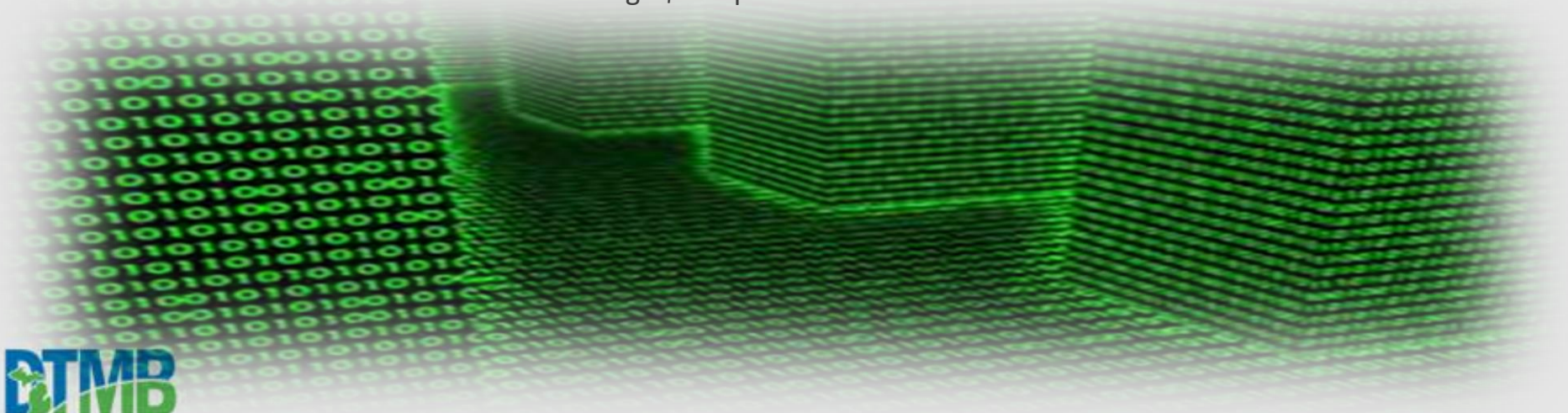
“There are two kinds of big companies in the United States. There are those who have been hacked... and those who don’t know they’ve been hacked.”

-James Comey, FBI Director

According to a report released by IBM and the Ponemon Institute, the per-record cost of a data breach reached \$154 this year, up 12 percent from last year's \$145. In addition, the average total cost of a single data breach rose 23 percent to \$3.79 million.

May 27, 2015

Ponemon: Data breach costs now average \$154 per record...



The Need...




Breach Frequency



In 2014, cybercriminals continued to steal private information on an epic scale, by direct attack on institutions such as banks and retailers' point-of-sale systems.

While there were fewer "mega breaches" in 2014, data breaches are still a significant issue. The number of breaches increased 23 percent and attackers were responsible for the majority of these breaches.

Fewer identities were reported exposed in 2014, in part due to fewer companies reporting this metric when disclosing that a breach took place. This could indicate that many breaches—perhaps the majority—go unreported or undetected.^{91,92}

2014		312 +23%
2013		253 +62%
2012		156
Total Breaches Source: Symantec		

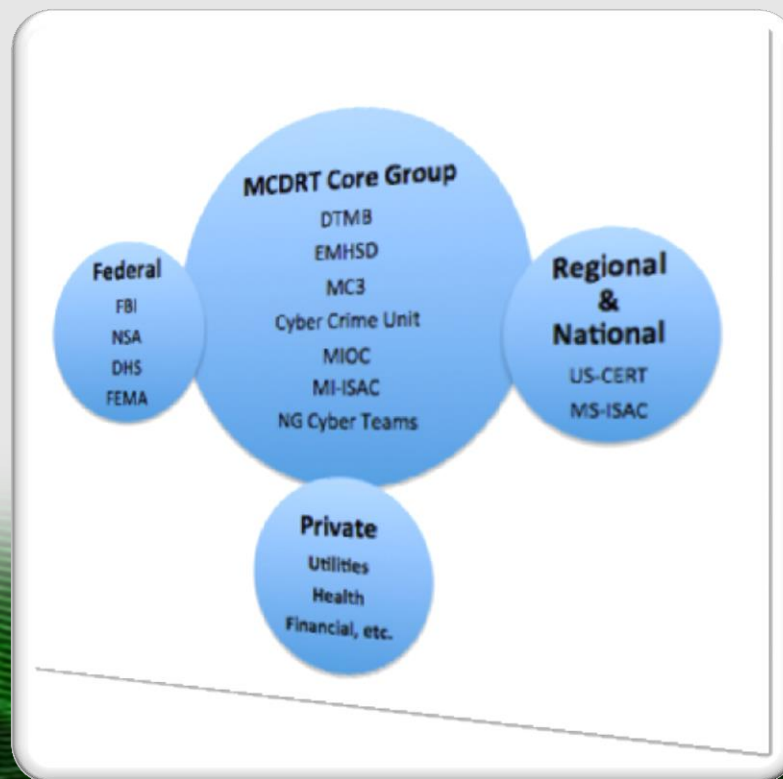
At a Glance

- There were fewer mega breaches (with more than 10 million identities disclosed) in 2014 than 2013.
- The overall number of data breaches increased.
- Attackers are responsible for the majority—49 percent—of breaches.
- Attacks on point-of-sale systems have grown in scale and sophistication.
- According to a survey carried out by Symantec, 57 percent of respondents are worried their data is not safe.

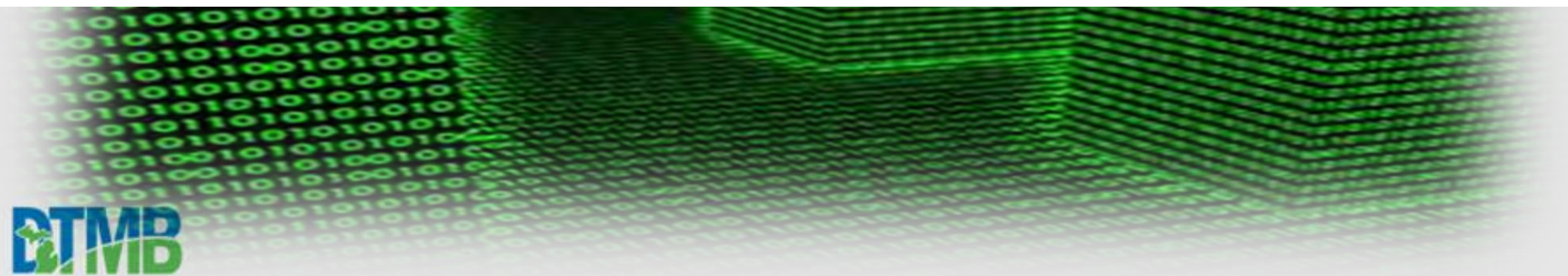
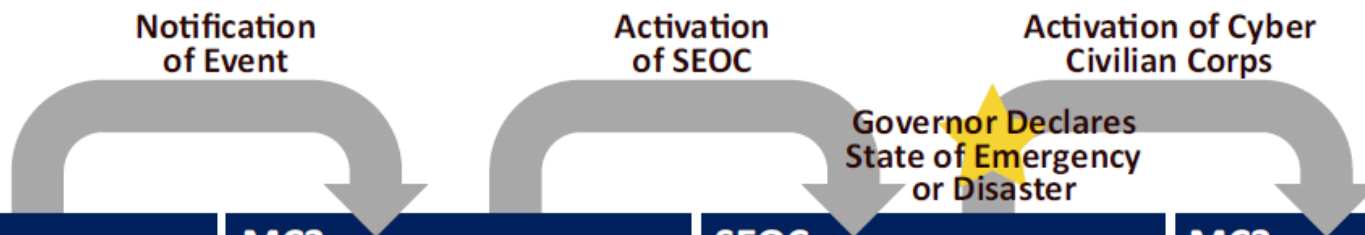


Cyber Disruption Response Team Membership

The CDRT internal structure follows ICS principles, with the Chair and Co-Chairs appointing a CDRT lead to act in the incident commander role. CDRT membership will fill Planning, Operations, Logistics and Finance roles as needed and as appointed by the CDRT Lead.



Early Detection and Rapid Response



Michigan Cyber Disruption Response Plan



Development of the Michigan Cyber Disruption Response Plan has reminded us that it is important to know and understand your cyber security ecosystem. Under-communication and assumptions are your enemies and it is important for all parties to understand the formal (and information) roles of everyone involved in response. Engaging stakeholders in plan creation has aided the State in creating a comprehensible and usable plan. Now the tool has been created, next will be implementation and practice beginning with a tabletop exercise being held in October to train and rehearse for real life scenarios.

