Cybersecurity Governance in the State of Michigan

A CASE STUDY

December 2017

Homeland Security

NASCIO
Representing Chief Information Officers of the States

Michigan State Fast Facts[1,2,3]

ELECTED OFFICIALS:

- Governor Rick Snyder
- Michigan House of Representatives: 110 Representatives
- Michigan State Senate: 38 Senators

STATE CYBERSECURITY EXECUTIVES:

- Chief Information Officer (CIO) David DeVries
- Chief Security Officer (CSO) Rajiv Das
- Chief Technology Officer (CTO) Rod Davenport

STATE DEMOGRAPHICS:

- Population: 9,886,095
- Workforce in "computers and math" occupations: 2.1%

EDUCATION:

- Public with a high school diploma: 54.4%
- Public with an advanced degree: 34.5%

COLLEGES AND UNIVERSITIES:

- 33 community colleges[4]
- 15 public universities[5]
- 54 private colleges[6]

KEY INDUSTRIES:[7]

- Manufacturing
- Agri-business
- Cybersecurity
- Defense
- Information Technology

Executive Summary

The Overall Challenge:

How to address a range of cybersecurity challenges that cut across multiple government, public, and private sector organizations?

Overall Lessons Learned from Michigan's Governance Approach:

- **Leadership Matters**. Leaders across multiple government, public, and private organizations make cybersecurity, and cybersecurity governance, a priority.
- **Leadership Is Not Everything**. Laws, policies, structures, and processes instantiate and align cybersecurity governance with cybersecurity priorities so that focus does not change as personalities change.
- **Governance Crosses Organizational Boundaries.** The distributed nature of cybersecurity requires a range of governance mechanisms that connect across multiple organizations and sectors.

This case study describes how Michigan has used laws, policies, structures, and processes to help govern cybersecurity as an enterprise-wide, strategic issue across state government and other public and private sector stakeholders. It explores cross-enterprise governance mechanisms used by Michigan across a range of common cybersecurity areas—strategy and planning, budget and acquisition, risk identification and mitigation, incident response, information sharing, and workforce and education.[*]

This case study is part of a pilot project intended to demonstrate how states have used governance mechanisms to help prioritize, plan, and make cross-enterprise decisions about cybersecurity. It offers concepts and approaches to other states and organizations that face similar challenges. As the case covers a broad range of areas, each related section provides an overview of Michigan's governance approach, rather than a detailed exploration. Individual states and organizations seeking greater detail would likely need to engage directly with Michigan to better understand how to tailor solutions to their specific circumstances.

Since the early 2000s, the state of Michigan executive and legislative branches have taken a series of deliberate steps to enable cybersecurity to be governed as an enterprise-wide strategic issue both across state government and across a diverse set of public and private sector stakeholders. As former Michigan Department of Technology Management and Budget (DTMB) Director and Chief Information Officer (CIO) David Behen

[*] For purposes of this case study, governance refers to the laws, policies, structures, and processes that enable people within and across organizations to address challenges in a coordinated manner through activities such as prioritization, planning, and decision making.

said, "The focus is state of Michigan cybersecurity, not [just] the state of Michigan government's cybersecurity."[8]

The state of Michigan government governs information technology (IT) through a centralized structure, which enables a unified and coordinated approach to cybersecurity across the executive branch. Under Michigan law, the DTMB has authority for IT, including cybersecurity, management, and budget operations, for all state departments and agencies. (In this case study, "agency" refers to executive branch agencies.) The DTMB is led by a Director who is also the CIO.[9] Under the direction of this single Director and CIO, Chief Technology Officer (CTO), Chief Security Officer (CSO), and Agency Service Information Technology leads, the DTMB is responsible for coordinating and executing a unified executive branch strategic IT plan, which includes cybersecurity and aligns with overall statewide management and budget priorities.

Michigan also utilizes a range of governance structures and processes to address a variety of cybersecurity challenges that require collaboration and coordination across public and private stakeholders. For example, Michigan has established a cross-ecosystem governance approach to managing cyber incident response. Working collaboratively with federal, state, local, and private sector organizations, leaders from the Cyber Security Infrastructure Protection Division of the DTMB and the Emergency Management and Homeland Security Division of the Michigan State Police developed the Cyber Disruption Response Plan (CDRP). The CDRP provides a framework for emergency management and IT agencies to identify cyber threats and coordinate cyber response and recovery operations. The plan uses a threat matrix that considers cyber events along a five-level escalation/de-escalation path and articulates which organization is responsible for the cyber response management at each level. Stakeholders across the ecosystem rely on consistent, informal communications, in combination with formal communication lines, to stay prepared for cyber disruptions.[10]

Information sharing has also played a critical role in connecting a cybersecurity ecosystem of public and private sector stakeholders. This started as a grassroots effort by the Governor's and CIO's offices to reach out across stakeholders and ask for input. The initiative has evolved into an intentional set of formal and informal communication governance mechanisms to solve problems at strategic, operational, and tactical levels. "Over time, relationships and trust were built with partners across government, private, academia, etc., to a point where communication and partnership are part of the fabric of how [the state of Michigan approaches cybersecurity]," Ashley Gelisse, the Chief of Staff to the CIO, said.[11]

To strengthen the cyber workforce, Michigan called on a governance approach developed by Michigan's education community. Specifically, it utilized Merit Network[12] (Merit), a consortium of 300+ members, including Michigan's public universities, K-12 schools, libraries, local government agencies, and not-for-profits. Merit led the effort to build the Michigan Cyber Range (MCR), an unclassified virtual private training cloud that can be used for hands-on adaptive training and certification in cybersecurity and IT as well as product development and testing. The MCR also provides a controlled environment to perform a variety of simulations and testing, including running attack scenarios, applying responses, and analyzing the effect on a network without putting an organization or network at risk. The MCR services can be accessed through a virtual connection or at a physical extension of the MCR called a hub.

Cybersecurity is a challenge that cuts across many issues and many interdependent stakeholders. Therefore, Michigan uses a range of governance mechanisms to work across different public, private, academic and nonprofit organizations. The approaches described in this

case study were the result of many years of intentional effort by many leaders and individuals who made cybersecurity and cybersecurity governance a priority across the state. Governor Rick Snyder made cybersecurity a top priority. He and others in the executive branch agencies, state legislature, and private organizations addressed cybersecurity as important from both a threat mitigation and economic development perspective. However, leadership was not everything. Protecting data and critical infrastructure across the state, not just in state-run systems, required engagement and partnership across the entire cybersecurity ecosystem. In Michigan, tangible laws, policies, structures, and processes instantiated and aligned cybersecurity governance with broader cybersecurity priorities

Table of Contents

Background & Methodology

This case study was developed as part of a pilot project to identify how states have used laws, policies, structures, and processes to help better govern cybersecurity as an enterprise-wide, strategic issue across state government and other public and private sector stakeholders. This project emerged as a result of the *Department of Homeland Security (DHS) Advisory Council Final Report of the Cybersecurity Subcommittee, Part II – State, Local, Tribal & Territorial (SLTT*), which recognized the importance of governance in addressing a range of cybersecurity technology and operational challenges.[13]

The case study explores cross-enterprise governance mechanisms used by Michigan across a range of common cybersecurity areas—strategy and planning, budget and acquisition, risk identification and mitigation, incident response, information sharing, and workforce and education. It is not intended to serve as a formal evaluation. Instead, the case offers concepts and approaches that may be useful to other states and organizations that face similar challenges. As this case covers a broad range of areas, each related section provides an overview of Michigan's governance approach, rather than a detailed exploration. Individual states and organizations seeking greater detail would likely need to engage directly with Michigan to better understand how to tailor solutions to their specific circumstances.

DHS' Office of Cybersecurity and Communications (CS&C) initiated and leads the project in partnership with the National Association of State Chief Information Officers (NASCIO). NASCIO is a nonprofit association "representing state chief information officers and information technology executives and managers from the states, territories, and the District of Columbia."[14] The Homeland Security Systems Engineering and Development Institute (HSSEDI), a DHS owned Federally Funded Research and Development Center (FFRDC), developed the case studies.

Candidate states were identified to participate in the pilot project based on:

- analysis of third party sources,
- diversity of geographic region, and
- recommendations from DHS and NASCIO with awareness of SLTT cybersecurity practices.

Candidate states that agreed to participate in the DHS-led pilot project did so on a voluntary basis. Researchers used open source material and conducted a series of interviews to gather the necessary information to develop each state case study.

I. Strategy & Planning

The Challenge:

How to set direction and prioritize cybersecurity initiatives across multiple organizations?

Features of Michigan's Governance Approach:

- The Governor developed an overarching strategy to focus and frame how the state would address cyber risks.
- The Department of Technology Management and Budget (DTMB) Director/Chief Information Officer (CIO) develops a statewide strategic information technology (IT) plan that sets direction for how the state government will use and secure technology.
- The state has established a formal governance structure to execute its strategic IT plan.

In 2011, Governor Snyder developed the *2011 Michigan Cyber Initiative*, the state's plan to defend against cyber attacks and position the state to benefit economically from the cybersecurity industry. This Cyber Initiative was an action plan that emphasized Michigan's commitment to cybersecurity and identified actions the state would take to protect Michigan's citizens, infrastructure, and economy. These actions included creating a State Police-run cyber emergency command center, launching a Cyber Defense Response Team, building partnerships with the private sector, and focusing on expanding online and classroom training to target students from preschool through age 20.[15, 16]

Building on this effort, four years later Governor Snyder announced the *2015 Michigan Cyber Initiative*, which articulated Michigan's cybersecurity approach as "…a holistic and continuously evolving concept" that is about more than just technology.[17] This initiative highlighted successes since 2011 (e.g., brought physical security and cybersecurity under one Chief Security Officer [CSO], launched the Michigan Cyber Range, hosted and participated in number of cyber response and recovery exercises). It also laid out a series of next steps to advance cybersecurity over the next four years across areas such as education, workforce development, and incident response. Examples include continuing to evolve the state's approach to cyber incident response by advancing its cyber disruption plan and "transition[ing] from a compliance-centric approach to cybersecurity to a risk-based approach."[18]

Both initiatives served as guiding documents with sets of specific actions emphasizing that cyber work should be approached as a whole-of-state challenge that requires engagement both across state government and across a larger ecosystem of public and private organizations.

Across state government, setting cybersecurity priorities falls to the Department of Technology Management and Budget (DTMB). The DTMB is

responsible for coordinating a "unified executive branch strategic information technology plan" and managing cybersecurity risks to state technology systems.[19] Figure 1 provides an organizational chart for the DTMB.

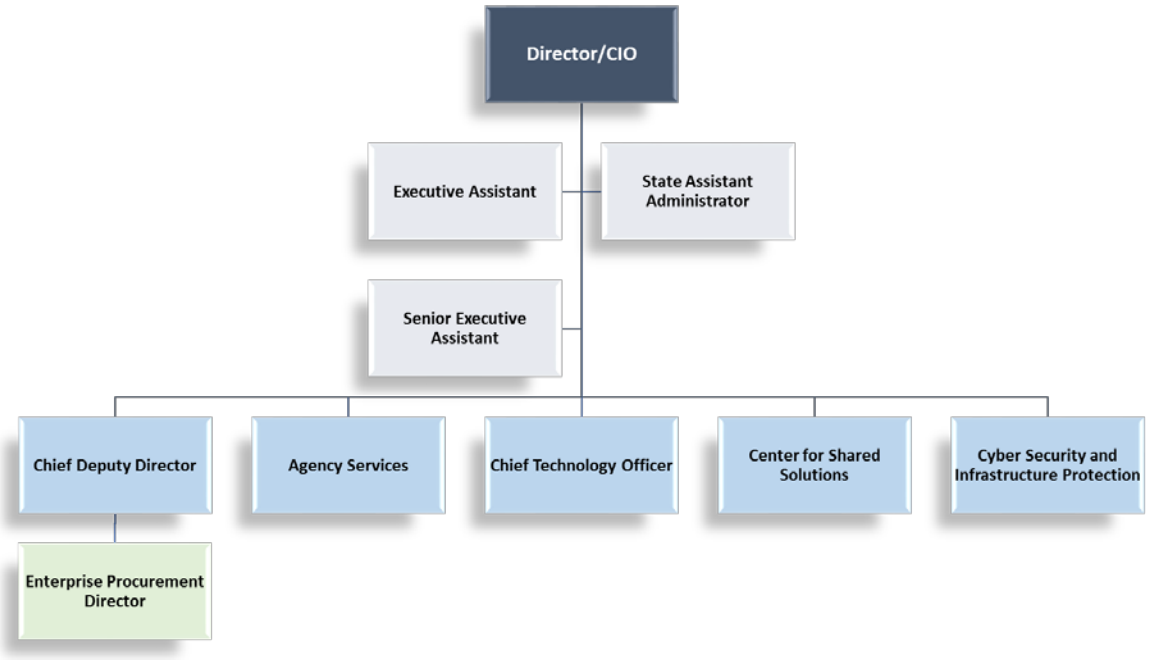

Figure 1. DTMB Organizational Chart

The DTMB utilizes a variety of cross-organizational governance bodies to execute the strategic direction. During 2017, the DTMB rolled out an information technology (IT) governance model informed by industry practices. Figure 2 shows a portion of this model; the remaining elements are shown in Figure 3 in the Risk Identification and Mitigation section.

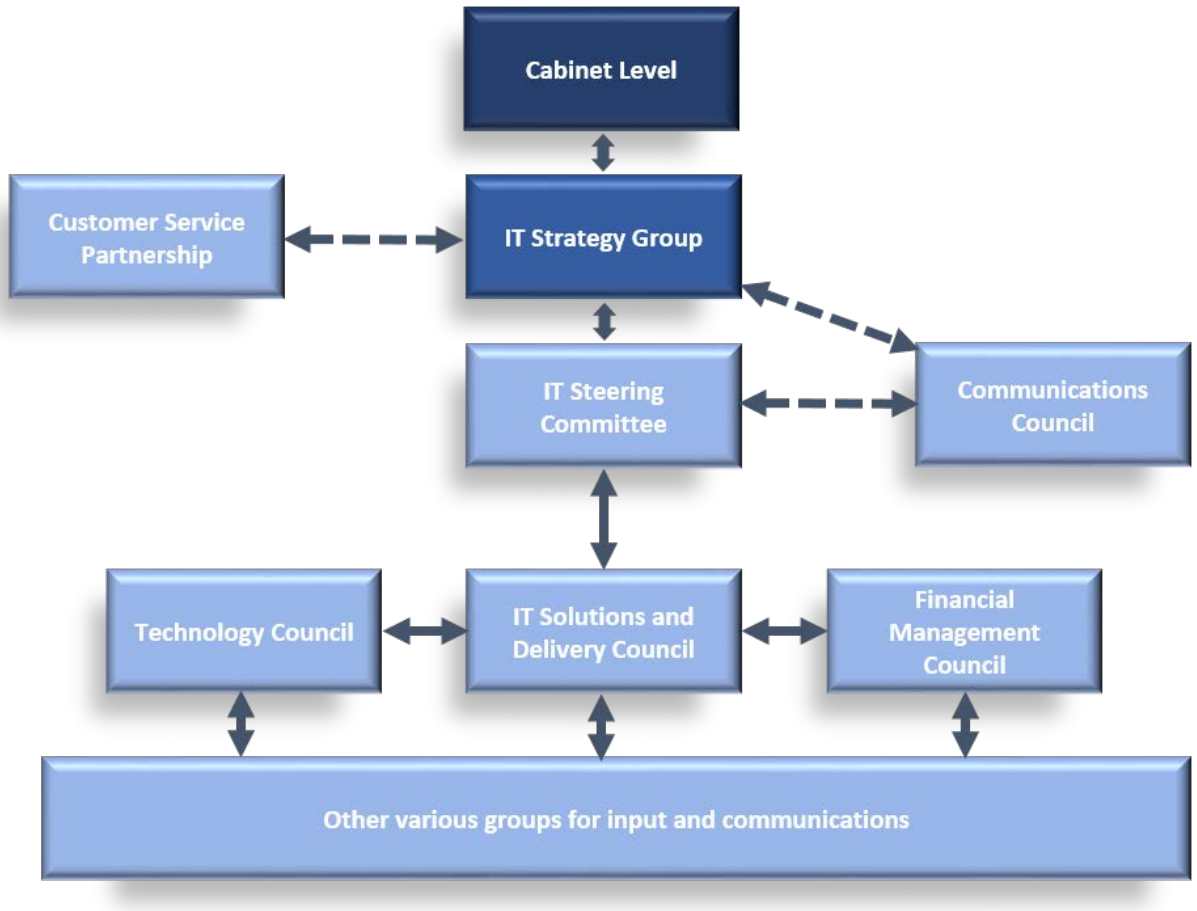

Figure 2. Portion of DTMB Governance Model

(See Figure 3 in the Risk Identification and Mitigation section for the complete DTMB Governance Model. The Customer Service Partnership is not discussed in this case.)

At the top of this model sits the *Cabinet Level* body, which is composed of various cabinet members, members from the Governor's Office, DTMB Director, and Deputy Director. It sets business strategy and vision and ensures that internal decisions are aligned with the direction it sets. These types of enterprise-level governance bodies allow the state to take a systematic view of IT decisions and risks across the state network, better define processes, and create consistent lines of decision making.

Below this body is the *IT Strategy Group*. This group consists of the DTMB leadership (i.e., CIO, CTO, CSO, Director of Agency Services, Chief of Staff, Legislative Liaison and Policy Advisor, Director of the Center for Shared Solutions, and Enterprise Procurement Director). It meets weekly to "oversee and deliver all investment decisions, including the overall strategic direction of the enterprise,"[20] align specific strategies (e.g., cybersecurity, cloud, and mobile) with timelines and metrics, and "[ensure] that technology services deliver business value."[21]

Below the IT Strategy Group are five specialized councils with participation from groups across the DTMB which conduct analysis, provide recommendations, and make decisions for their areas of responsibility. One of these councils, the IT Steering Committee,[22] performs/delegates analysis for the IT Strategy Group, makes policy decisions, approves/decides IT standards, collaborates to develop an annual project plan, and works with

leadership to establish metrics for the enterprise-wide IT budget, among other responsibilities.[23] The other four specialized councils share information up to and receive direction and information from the IT Steering Committee:

- The *Technology Council*[24] reviews new technology requests from the DTMB and the agencies by assessing total cost of operation and associated risks, including cybersecurity risks, from an enterprise perspective.[25]
- The *IT Solutions and Delivery Council*[26] makes recommendations to the IT Steering Committee based on group feedback, receives directives from the IT Steering Committee, serves as an entry point for operational governance, reviews hardware/software life cycle management, maintenance, and updates,[27] and has authority to decide how agencies implement IT solutions.
- The *Financial Management Council*[28] "work[s] with the IT Steering Committee to ensure effective and efficient use of [Michigan] financial resources and that submitted proposals are consistent with enterprise financial and technological strategy."[29]
- The *Communications Council*[30] keeps governance functioning within Michigan by providing administration guidance across the governance bodies to ensure operational consistency and gives advice and the tools necessary to effectively communicate information among the bodies.[31] It meets weekly.

II. Budget & Acquisition

The Challenge:

How to manage investments in strategic cybersecurity priorities as part of budget and acquisition processes across multiple organizations?

Features of Michigan's Governance Approach:

- The CIO and State Budget Office evaluate IT and cyber-related spending requests across state agencies and make recommendations to the legislature for approval.
- The CSO is responsible for the IT acquisition approach used to evaluate and manage risks associated with proposed IT acquisitions across state agencies.

State law creates a centralized budget process through which IT budget requests for the executive branch are submitted annually to the DTMB and State Budget Office (SBO). This process serves as one way the state operationalizes cybersecurity priorities across state agencies.[32] The DTMB CIO and SBO jointly evaluate all IT and cyber-related spending requests from state agencies to ensure proposals put forth for funding consideration "… fit into the overall strategic information technology management plan of the state and that provide a reasonable return on investment."[33] An agency's annual budget includes money to put toward a shared service model in which the CIO's office provides IT services, including cybersecurity, to the agencies, and those agencies pay for the services with funds allocated to them from the annual IT budget or a discretionary budget line available for IT and non-IT related expenses. The DTMB and SBO consolidate requests and submit an overall IT budget package to the legislature for ultimate funding approval.

Consistent with its role in the centralized budget process, the DTMB is also responsible for all IT acquisition activities. Michigan's IT acquisition is managed through an integrated acquisition and delivery framework focused on minimizing cybersecurity risks and keeping the overall system as secure as possible. The acquisition process is supported by policy stating that the "DTMB will adopt, acquire, develop and/or implement all [State of Michigan] IT products. The DTMB will also be responsible for managing all IT activities of agency projects that involve IT Resources."[34]

Led by the CSO's office, the state manages IT acquisition and implementation through an integrated approach designed to assess and manage cybersecurity risks. To assist with this, one of the three directors within the CSO's office is focused on risk assessments, compliance, and security awareness. For acquisitions, after determining that a need exists, Central Procurement conducts a market scan to identify qualified vendors. After a vendor is selected, the CSO's office begins running a series of checkpoints throughout the process to confirm

that the vendor is meeting security requirements. For more information on risk management during design and development of new systems, see the Risk Identification & Mitigation section below.

III. Risk Identification & Mitigation

The Challenge:

How to identify and mitigate cybersecurity risks across multiple organizations?

Features of Michigan's Governance Approach:

- The state merged its cyber and physical security teams under a single role, the CSO.
- The CSO sets policies and standards to govern information security that apply to all state government systems and conducts security assessments.
- The CSO's office actively works with state agencies to assess and manage cybersecurity risks in system development, from acquisition through implementation.
- The state is using a shared service model to provide CISO services to local municipalities that cannot fully fund their own.

The Management and Budget Act grants responsibility to the DTMB for the development, acquisition, and implementation of standardized risk management policies, practices, and programs across state agencies.[35] This responsibility is executed by a single CSO who manages Michigan's cyber and physical security teams. As the state saw cyber and physical risks converging, it created the CSO role in 2012 to manage all cyber and physical risks to the state government network. The CSO's office uses National Institute of Standards and Technology (NIST) guidance to inform its policy development for cyber risk management, provides risk assessment and management services across the DTMB and state agencies, and ensures that the DTMB and agencies comply with the policies.

Regardless of whether a new IT application is purchased or in-house development work is being completed, the CSO's office identifies risks that need to be mitigated throughout the system development life cycle.[36] As Rajiv Das, CSO and Deputy Director, said, "We want to deliver applications where we know the vulnerabilities are low. This approach also allows us to move to a risk-based model rather than a compliance-based model. The risk assessments point us to gaps and then we address the gaps through initiatives."[37] Using information from an application's initial risk assessment, the CSO's office conducts reviews to identify risks at design, coding, and testing checkpoints. Agency Services, a division within the DTMB, works with the agencies to remediate any identified risks. The CSO validates that the risks were properly mitigated before an application is deployed.

After the system integration work is done, the CSO's office regularly conducts application and network scans to detect vulnerabilities and corrects them if found. The CSO also helps remove communication gaps by maintaining at least one monthly meeting with each agency's Security and Privacy Officer to discuss upcoming DTMB projects, agency needs, etc.[38] Other offices within the DTMB have responsibilities associated with assessing and managing the risk of new applications. For example, within the software development life cycle, the CTO's Enterprise Solution Design Services division works to ensure that cyber risk is addressed during high-level design.[39]

To help govern this risk management approach, the DTMB also uses its overall DTMB Governance Model. In addition to the governance bodies introduced in the Strategy and Planning section (see Figure 2), Figure 3 introduces two other governance bodies that play important roles in decision making and risk resolution for the enterprise.

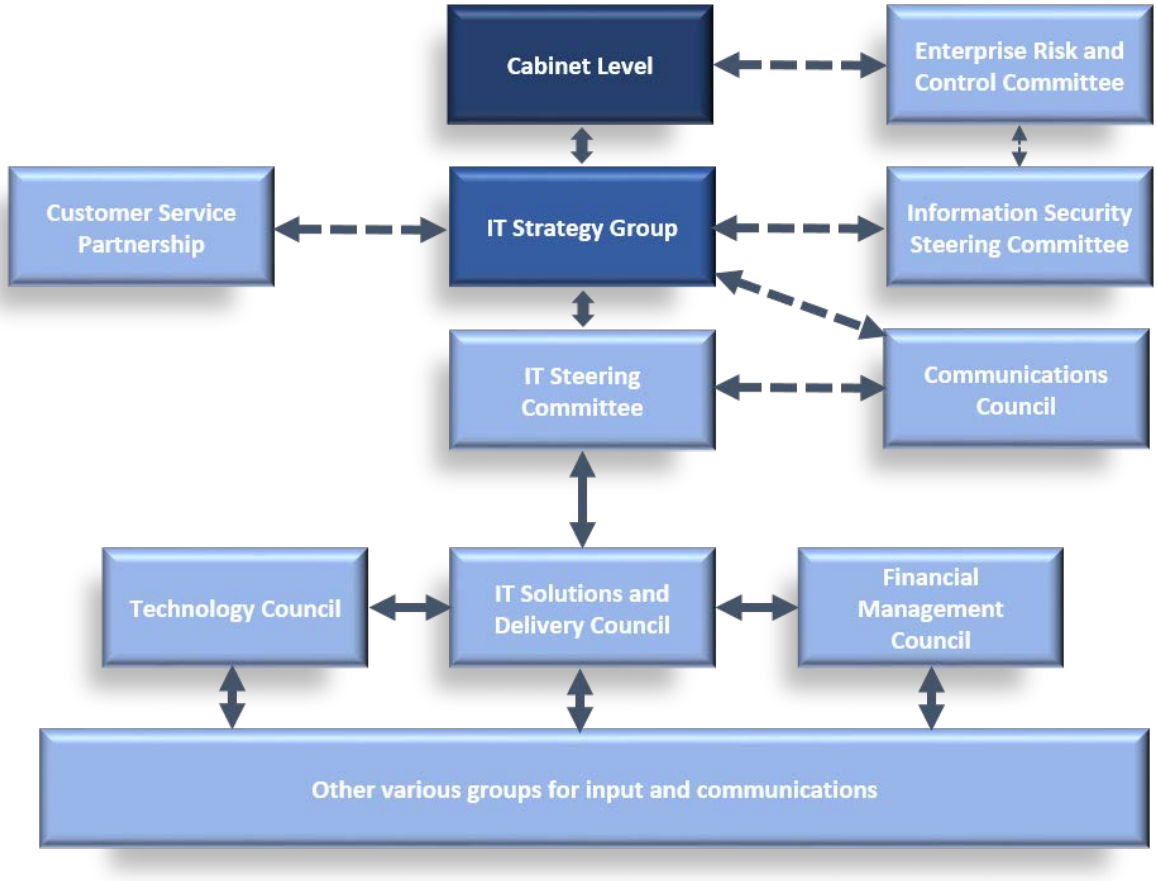

Figure 3. Complete DTMB Governance Model

(Detail on the bodies not discussed in this section was provided in the Strategy and Planning section. The Customer Service Partnership is not discussed in this case.)

The Information Security Steering Committee reports to the CSO, with representatives from Agency Services and two state agencies who rotate on an annual basis. It meets monthly to discuss variations from cyber risk policies or processes (i.e., exception requests) and propose solutions to resolve the issues from an enterprise perspective.[40] If needed, this group escalates unresolved risks to the Enterprise Risk and Control Committee (ERCC). The ERCC, which

reports to the Governor's office, has representatives from the Governor's office, the DTMB, and agencies outside the DTMB. It meets quarterly and is focused on examining and resolving macro-level risks and making enterprise-wide decisions.

In addition to managing risk in its own network, the state is addressing risk for local government entities through a new capability called "CISO as a service."[41] Under this model, local governments can opt via a memorandum of understanding to pay for a portion of a Chief Information Security Officer's (CISO) time. This initiative allows local governments, which may not be able to pay for a full-time CISO, to take advantage of an affordable shared service and apply cybersecurity risk management expertise across the state.[42]

Michigan also has formal governance structures and approaches to manage risks associated with preparation for and response to cyber incidents that cut across the government and private organizations. These are discussed in the Incident Response section below.

IV. Incident Response

The Challenge:

How to prepare for and respond to cyber incidents that require coordinated action across multiple organizations?

Features of Michigan's Governance Approach:

- The state worked with federal and state government, private industry, and others to create a Cyber Disruption Response Plan (CDRP) that guides preparation for and response to cyber incidents across public and private organizations.
- The state tailors existing emergency management response and recovery approaches and structures to cyber incidents.
- The CDRP uses a five-level threat matrix to move cyber incidents through escalation and de-escalation of the incident across the DTMB and the Emergency Management and Homeland Security Division.

Michigan has worked across multiple public and private organizations to develop and articulate its approach for managing cyber incident responses, from minor incidents to severe attacks. Michigan's approach to incident response has evolved through a series of efforts, beginning with Governor Snyder's 2011 and 2015 Cyber Initiatives (described in the Strategy & Planning section), which included incident response-related actions.

As part of this overall priority, in 2013 the state developed a Michigan Cyber Disruption Response Strategy that outlined "a framework for the prevention of, protection from, response to, and recovery from a significant cyber incident."[43] This strategy provided the foundation for the Cyber Disruption Response Plan (CDRP), a cross-ecosystem approach to addressing cyber incidents.[44] To develop the CDRP, leaders from the DTMB and emergency response agencies brought together members of the cyber ecosystem from state government, federal government, private industry, and others to understand requirements, collaborate, and come to consensus on a plan that would work for all stakeholders.[45]

The CDRP "provides a common framework for identifying and responding to technological threats with corresponding responses to address threats of increasing scope and severity."[46] The plan uses the Federal Emergency Management Agency's National Incident Management System structure for its cyber response, and outlines roles and responsibilities, communication procedures, training and exercises, and a risk assessment process by providing "guidelines to partner organizations to best protect Michigan's critical cyber infrastructure."[47]

The state's overall approach was intended to tailor emergency management response and recovery concepts to cyber incidents, not reinvent emergency response. As Captain Chris Kelenske, Commander of the Emergency

Management and Homeland Security Division, Michigan State Police, said, "Cyber incident response in Michigan is not a different emergency management process; the process just starts differently."[48]

To this point, the CDRP uses a threat matrix to move cyber incidents along a five-level cyber escalation/de-escalation path. At levels 1 and 2, the CIO's office and the security operations center manage day-to-day cyber events, including the Michigan State Police's Michigan Intelligence Operations Center (MIOC), or fusion center, as needed. At level 3, the CDRP begins to trigger emergency management processes and the involvement of other organizations, such as the Governor's office, Michigan Cyber Command Center, State Emergency Operations Center (SEOC), National Guard, and Cyber Civilian Corps. Depending on the incident's size, impact, and level of severity, other organizations, including non-government entities, are brought into the SEOC.

For level 3 through 5 cyber incidents, Michigan uses an Incident Command System (ICS), through which a Cyber Disruption Response Team (CDRT) helps staff the ICS and provides domain and cyber expertise from across the ecosystem (see Figure 4). The CDRT is a group of subject matter experts from public and private emergency management and IT fields whose role is to support federal, state, local, and private organizations in the preparation for, response to, and recovery from cyber events.[49] It is led by the CSO as the Chairman and the Deputy State Director of Emergency Management and Homeland Security as the Vice Chairman when the SEOC is not activated. Once the SEOC is activated, the Chair and Co-Chairs appoint a CDRT lead to act as the incident commander.[50] Figure 4 illustrates the ICS structure when a SEOC is activated.

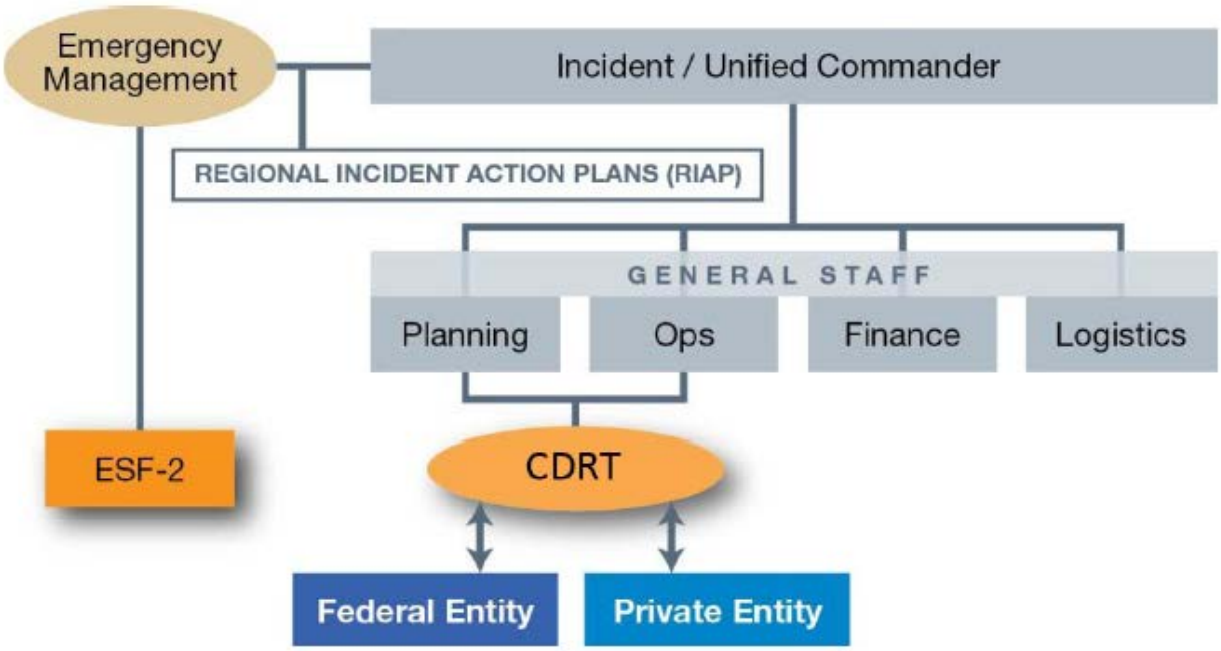

Figure 4. Incident Command System Organization Chart[51]
(This organization chart is from Michigan's CDRP.)

The CDRP and its supporting documentation (workbook and job aids) provided to responders outline how events are managed along the escalation path. To prepare for cyber incidents and update the CDRP, the state conducts discussion-based (e.g., tabletop exercises) and

operations-based (e.g., drills) exercises throughout the year, using post-exercise feedback loops and after-action reports.[52]

Members of the CDRT also regularly use informal communication channels to notify their peers and partners about cyber events before those peers are formally involved.[53] Consistent formal and informal communications help keep the CDRT prepared for cyber events and are key underpinnings of the CDRP's and Michigan's approach to cybersecurity incident response.

V. Information Sharing

The Challenge:

How to engage across multiple organizations to share cybersecurity-related information?

Features of Michigan's Governance Approach:

- The state is intentional in its formal and informal information sharing mechanisms at strategic, operational, and tactical levels.
- The state participates in cross-state information sharing bodies (e.g., the Multi-State Information Sharing and Analysis Center [MS-ISAC] and NASCIO).

One of Michigan's most defining features of cybersecurity governance is its interconnected ecosystem, which reaches across state, federal, private, academic, and not-for-profit organizations. According to David Behen, former DTMB Director and CIO, "The focus is state of Michigan cybersecurity, not [just] the state of Michigan government's cybersecurity."[54] To accomplish this, the state uses a combination of formal and informal information sharing mechanisms to help solve problems at the strategic, operational, and tactical levels.

From a strategic perspective, Governor Snyder has promoted information sharing by engaging with individuals and organizations across the ecosystem to provide input into the 2011 and 2015 Cyber Initiatives. The governor stays connected with private sector organizations on cyber-related topics through the quarterly Cyber Advisory Council, which provides an opportunity for sectors (e.g., critical infrastructure, finance, education, and health) to share with the Governor what they are seeing and how the ecosystem is responding.[55] These connections help the Governor's Office set priorities for the state.

The DTMB uses a variety of groups, councils, and committees to share strategic and operational cyber information across the ecosystem. For example, the CIO chairs and the CSO leads the Cyber Executive Team, which brings together public sector members of the ecosystem, such as National Guard, Michigan State Police, academia, and Michigan Economic Development Corporation, on a quarterly basis and helps the DTMB focus on topics such as the budgeting process and regional training.[56]

The DTMB has also created structures to share information with the private sector. When David Behen became Michigan's DTMB Director and CIO, one of his first initiatives was to develop the CIO Kitchen Cabinet. This forum brings together nearly two dozen Michigan-based CIOs from across industries and different-sized organizations on a regular basis. The group is formally chartered, meets monthly, and provides an opportunity for CIOs to discuss cybersecurity topics. Even though direct economic competitors are represented in the cabinet, the group has found ways to actively engage on a range of common challenges, including sharing strategies for mitigating risks

and addressing workforce concerns. Behen used the cabinet as a sounding board on topics such as the state's cybersecurity strategy and budgeting exercises.[57]

Inspired by success of this Kitchen Cabinet, the CSO Kitchen Cabinet and two industry-specific sub-councils focused on the healthcare and finance industries were created.[58] The CSO Kitchen Cabinet and councils operate similarly to CIO Kitchen Cabinet. The Michigan Healthcare Cybersecurity Council, which includes 20 major and minor healthcare providers, is pursuing 501c3 status to secure grant funding and sustained support to accomplish common needs, such as emergency response training. The council is also creating a standardized approach for all Michigan healthcare organizations to work with vendors on cybersecurity issues. This will help provide a consistent approach for healthcare organizations and vendors, which will ultimately help to better secure healthcare data.[59]

From operational and tactical perspectives, both the DTMB and the Michigan State Police require ongoing coordination to execute their important roles in cybersecurity response. They use the formal platform of the MIOC, which provides 24-hours-a-day statewide information sharing among local, state, and federal organizations and private sector partners. Outside of this formal communication channel, the entities err on the side of overinforming each other through informal networks.[60] In addition, the state participates in the MS-ISAC to gather information on cyber threats across the nation and the state. The MS-ISAC provides the state with two-way information sharing channels and incident response training and awareness.[61] The DTMB and Michigan cybersecurity ecosystem also routinely collaborate and share information with federal government partners.

While there are now many formal channels for information sharing, according to CTO Rod Davenport, informal information sharing is still very important. When informal, ad hoc information sharing between groups is motivated by personal interest and passion, it frequently becomes the "most sustaining because it's the most authentic," Davenport said.[62]

VI. Workforce & Education

The Challenge:

How does Michigan work across multiple organizations to shape responses to cybersecurity workforce shortages and education needs?

Features of Michigan's Governance Approach:

- The state uses Merit Network (Merit), a nonprofit organization, to help address the cyber workforce gaps across state government, private industry, and other partners.
- The Michigan Cyber Range (MCR), operated by Merit, provides an unclassified physical range for education, training, and product development for organizations across multiple sectors.
- Merit works across and serves diverse institutions, industries, and age groups to offer several other programs to develop cybersecurity skills for a broad range of geographic and demographic populations.

Workforce development and education are areas of critical need for Michigan, because the state government and its private and public sector partners face a common cyber workforce gap. The state government recognized that the cybersecurity workforce gap cuts across multiple organizations and sectors and that creating a sustainable model to help grow the workforce would benefit the entire state. The state is addressing this gap through Merit, a "…non-profit, Member-owned organization governed by Michigan's public universities,"[63] with many links across the education and research fields.

One of the ways that Merit prepares the cybersecurity workforce to address real-world cyber events is through the creation of the first unclassified network-accessible range in the United States. The Michigan Cyber Range (MCR) provides a space for cybersecurity education, training, and product development and testing to its clients across the United States and the world. Training courses, available online or in a classroom, focus on certifying students so that they have professional credentials and certifications necessary to work in the cybersecurity field.[64]

Governor Snyder first proposed the MCR in his Cyber Security Vision Statement in 2011, and it was initially made possible through grants and sponsorship. Now a self-sustaining organization through contracts with its various users, the MCR is operated by Merit. The MCR's resources are available to public and private entities; users include city, county, and state emergency managers, the National Guard, other states,

international organizations, academic institutions, and private organizations and businesses. Its Executive Director works with an Advisory Council to ensure that the MCR's training is aligned with skill demand and the five-year strategic plan is developed to keep it self-sufficient. As a nonprofit, the MCR is well positioned to act quickly and flexibly to meet changing demands.[65]

The MCR has 10 hubs, or physical extensions, that offer more than 40 industry-recognized certifications designed to qualify individuals for cybersecurity positions.[66] With the understanding that developing a strong cyber workforce should begin prior to college, the MCR partnered with the Pinckney Community High School in southeast Michigan in 2016 to serve as one of these hubs. It will expand IT and cybersecurity education and training for its students and surrounding communities in areas such as computer forensics and network security. This hub, or cyber training institute, is the first effort of its kind in the United States, providing "educational and certification opportunities for high school and college students, as well as tech professionals."[67] Through this program, "students can earn college credits and gain access to internship opportunities."[68] Over time, the institute is looking to expand services, including hands-on training, and to "grow the program through partnerships and higher educational institutions."[69]

Merit and the state have developed two other mechanisms to "address the widening gap between the supply of skilled cybersecurity professionals and the demand for those skills."[70] As a part of the MCR, the Regional Cybersecurity Education Collaboration (RCEC) was developed as a self-funded "collaborative between the higher education community[71] and key private sector partners to [grow the cybersecurity workforce and prepare key industries for evolving cybersecurity challenges]."[72] The collaboration encompasses a collection of university curriculums that is accessed through an ecosystem of participating institutions via distance learning over Merit's network. The RCEC leverages Merit's technical infrastructure and bandwidth[73] and the MCR's courses to provide training to individuals who do not have access to a physical hub.[74]

The Governor's second annual High School Cyber Challenge is another Merit-run initiative intended to grow the cybersecurity workforce by developing interest and talent in cybersecurity prior to postsecondary education. Merit works with high schools to conduct a multi-round online competition for small teams of high school students to use their knowledge of IT and cybersecurity, culminating in a head-to-head competition at the North American International Cyber Summit in Detroit.-[75] There is no cost to participate, and the trip to Detroit is all expenses paid, which allows the initiative to reach unserved and underserved areas and eliminate economic and geographic constraints.[76]

Faced with a cybersecurity workforce challenge that stretches across the ecosystem, Michigan developed a governance mechanism, using Merit, to address it from a cross-ecosystem perspective. Through mechanisms like the Governor's High School Cyber Challenge, the MCR and its hubs, and the RCEC, Merit builds the cyber workforce from early education through employment while also filling the pipeline by retraining and educating Veterans. By marketing some of its services (e.g., the MCR) to the private sector and entities outside the state, Merit has diversified its funding streams, making it a self-sustaining organization.

VII. Deep Dive: Michigan Cyber Range

Introduction

The purpose of the "Deep Dive" is to provide a more in-depth look at how Michigan applied a cross-sector solution to address a specific cyber governance challenge.

The Challenge

The demand for a trained, diverse cybersecurity workforce outstrips supply in public and private sectors. Traditional models (e.g., recruit graduates from select undergraduate and graduate schools) have not kept up with the demand. Workforce development must start prior to postsecondary education and continue throughout an individual's professional development.

The Solution

Create a virtual environment for cybersecurity education, training, and testing through a not-for-profit organization—Merit—to address the cybersecurity workforce challenge that affects institutions and industries across the state. The education opportunities, including certification courses, are available to high school and college students and working professionals as individuals and groups. Businesses and other organizations may use the secure environment for product development and testing.

Background

In his 2011 Cyber Security Vision Statement, Governor Rick Snyder noted the need for an environment to help build a cybersecurity workforce to both address cyber threats and attract businesses to Michigan. From this, the MCR was created in 2012 and is operated by Merit, a nonprofit, member-owned[77] organization serving research, education, and public sector communities. The MCR "prepares cybersecurity professionals to detect, prevent and mitigate cyber-attacks" through a variety of services:[78]

- Access to an unclassified private cloud.
- A secure environment in which to test attack and defense strategies on small or large networks without introducing actual risk to an organization's network.
- Training courses (for certification)[79] and exercises using a virtual training environment called Alphaville to test cybersecurity skills. Alphaville provides real-world situations that show how information systems across communities are connected, therefore increasing risk and vulnerabilities. This environment includes "virtual machines that act as web servers, mail servers, and other types of machines."[80]
- Research in areas such as new internet protocols, network security, and the development of tools to monitor and secure networks.[81]

Founded in 1966, Merit owns and operates the longest running regional research and education network in the United States and is governed by Michigan's public universities. Its membership includes 300+ members, including Michigan's public universities, K-12 schools, libraries, local government agencies, and not-for-profits. The MCR leverages Merit's experience and resources.

The MCR was funded by grants from NIST, the Michigan State Police, and DHS. Initial sponsorship was also provided by three private sector companies.[82] Since the MCR is operated by Merit, it leverages Merit's 4,000 miles of fiber-optic infrastructure throughout Michigan and neighboring states and use a "national high-speed backbone network" that makes the MCR available nationwide.[83]

The MCR provides training under contract to U.S. and worldwide organizations, such as the National Guard; city, county, and state emergency managers; other state governments; various private sector organizations; and academia. These training courses and other services allow the MCR to be financially self-sufficient; its independence from government allows it to be flexible. Dr. Joe Adams, Vice President for Research and Cyber Security and Executive Director of the MCR, meets with a Board of Advisors every quarter to discuss direction and financial solvency. He also meets with an Advisory Council that is focused on aligning the MCR's training with the demand for certain skills and helps create a strategic five-year plan to guide training programs.[84]

In addition to its eight existing physical hubs,[85] in 2016 the MCR announced two new Cyber Range Hubs at Wayne State University and Pinckney Community High School to expand training and certification offerings. The new facilities will provide trainees with access to computing infrastructure testing labs, cybersecurity training exercises, and product testing and offer certification courses in over 20 cybersecurity disciplines.[86] Both hubs offer courses to college students and cybersecurity professionals, and the Pinckney Community High School hub will be the only program in the state to offer cybersecurity courses to high school students.

Adding to the MCR's physical hubs, in 2017 Merit launched the RCEC as a virtual hub, or extension, of the MCR to reach high schools, colleges, Veterans, and others who cannot reach a physical hub. The RCEC is another mechanism for growing the cybersecurity workforce through seminars, classes, and exercises by leveraging capabilities such as Merit's fiber-optic network and the MCR's intellectual property, including Alphaville. The RCEC is structured as a partnership with three higher education institutions[87] and key private sector partners to become a lasting, financially self-sufficient organization. The RCEC incentivizes participation by students and industry through the solicitation of scholarships for students from private sector organizations.[88] Scholarships will range from $3,000 to $5,000, depending on the course and certification, with the goal of complete coverage for the student.[89] In the initial offerings through the RCEC, the MCR is seeing demand from students and organizations like the Michigan Municipal Services Agency that want to get involved early. As it grows, the RCEC will provide "a platform for instructors to share curriculum throughout the state," and will help it to add more two- and four-year colleges to the collaborative.[90]

Faced with a cybersecurity workforce challenge that stretches across the ecosystem, Michigan developed a governance mechanism, using Merit, to address it from a cross-ecosystem perspective. Through mechanisms like the Governor's High School Cyber Challenge, the MCR and its hubs, and the RCEC, Merit builds the cyber workforce from early education through employment while also filling the pipeline by retraining and educating Veterans. By marketing some of its services (e.g., the MCR) to the private sector and entities outside the state, Merit has diversified its funding streams, making it a self-sustaining organization.

VIII. Acronyms

Acronym	Definition
CDRP	Cyber Disruption Response Plan
CDRT	Cyber Disruption Response Team
CFO	Chief Financial Officer
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CS&C	Office of Cybersecurity and Communications
CSO	Chief Security Officer
CTO	Chief Technology Officer
DHS	Department of Homeland Security
DTMB	Department of Technology Management and Budget
ERCC	Enterprise Risk and Control Committee
FFRDC	Federally Funded Research and Development Center
HSSEDI	Homeland Security Systems Engineering
ICS	Incident Command System
IT	Information Technology
MCR	Michigan Cyber Range
MIOC	Michigan Intelligence Operations Center
MS-ISAC	Multi-State Information Sharing and Analysis Center
NASCIO	National Association of State Chief Information Officers
NIST	National Institute of Standards and Technology
RCEC	Regional Cybersecurity Education Collaboration
SBO	State Budget Office
SEOC	State Emergency Operations Center
SLTT	State, Local, Tribal & Territorial

[1] Michigan.gov, “Branches of Government.” Available: http://www.michigan.gov/som/0,4669,7-192-29701---,00.html.
[2] Statistical Atlas, “Overview of Michigan.” Data based on US Census Bureau 2010 census. Available: http://statisticalatlas.com/state/Michigan/Overview.
[3] Information regarding elected officials and state cybersecurity executives was validated in November 2017. "Fast Fact" details were collected in August 2017.
[4] Collegestats.org, “Michigan Colleges.” Available: https://collegestats.org/colleges/michigan/.
[5] Michigan Economic Development Corporation, “Michigan’s Public Universities.” Available: http://www.michiganbusiness.org/universities-and-colleges-partners/.
[6] CollgeCalc, “Private Colleges in Michigan.” Available: http://www.collegecalc.org/colleges/michigan/private/.
[7] Michigan Economic Development Corporation, “Core Industries.” Available: http://www.michiganbusiness.org/core/industries/.
[8] Interview with David Behen, former Chief Information Officer, DTMB. (2017, March 2).
[9] MCL Chapter 18 Section 18.41. Available: http://www.legislature.mi.gov/(S(1kzimy1qiufegyrvb4usw53n))/mileg.aspx?page=getObject&objectName=mcl-18-41.
[10] Interview with Captain David Kelly, Commander of the Intelligence Operations Division, Michigan State Police; Captain Chris Kelenske, Commander of the Emergency Management and Homeland Security Division, Michigan State Police; and Chris Christensen, Director of Infrastructure Protection, DTMB. (2017, April 14).
[11] Interview with Ashley Gelisse, Chief of Staff, DTMB. (2017, March 2).
[12] Read more about Merit Network in the Workforce & Education section.
[13] Department of Homeland Security Advisory Council, “Final Report of the Cybersecurity Subcommittee, Part II – State, Local, Tribal & Territorial (SLTT).” (2016, June). Available: https://www.dhs.gov/sites/default/files/publications/HSAC_Cybersecurity_SLTT_FINAL_Report.pdf.
[14] About NASCIO. Available: https://www.nascio.org/AboutNASCIO.
[15] Michigan.gov, “Michigan Announces Cyber Initiative.” Available: http://www.michigan.gov/snyder/0,4668,7-277-57577_57657-263758--,00.html.
[16] More about the P-20 initiative. Available: http://greatstartforkids.org/content/so-what-p-20-anyway.
[17] Michigan Cyber Initiative 2015. (2015). Available: http://www.michigan.gov/documents/cybersecurity/Mich_Cyber_Initiative_11.13_2PM_web_474127_7.pdf.
[18] Ibid.
[19] MCL Chapter 18 Section 18.41. Available: http://www.legislature.mi.gov/(S(hn2qlonq5mn1lktnuf5rheug))/mileg.aspx?page=getObject&objectName=mcl-18-41.
[20] “IT Strategy Group Charter.” Made available by DTMB. (2017, June 23).
[21] Ibid.
[22] The IT Steering Committee is composed of at least two Agency Services representatives, Infrastructure & Operations General Manager, Agency Services Director, IT Procurement representative, IT Finance Director, Deputy CSO, and others. It meets every other week.
[23] “DTMB IT Governance.” Made available by DTMB (2017, June 23).
[24] The Technology Council is composed of the Deputy CSO, Enterprise Architecture Director, and others. It meets every other week.
[25] Interview with Rajiv Das, Chief Security Officer, DTMB. (2017, June 23).
[26] The IT Solutions and Delivery Council is composed of the Chief Financial Officer (CFO), Business Relationship Managers, Center for Shared Solutions representatives (product owners), General Manager from IT Steering Committee, and others. It meets every other week.
[27] “DTMB IT Governance.” Made available by DTMB (2017, June 23).
[28] The Financial Management Council is composed of the CFO, IT Finance Director, DTMB Internal Audit representative, and others. It meets monthly.
[29] “Financial Management Charter.” Made available by DTMB. (2017, June 23).
[30] The Communications Council is composed of the Director’s Office Assistant Administrator, Communications Specialist, Office of Organizational Performance Management Representative, and others. It meets weekly.
[31] “Communications Council Charter.” Made available by DTMB. (2017, June 23).
[32] MCL Chapter 18 Section 18.41. Available: http://www.legislature.mi.gov/(S(oaeofmiadbhoherqkwo4pqv1))/mileg.aspx?page=getObject&objectName=mcl-18-41.
[33] Executive Order No.2001 – 3. Available: http://www.michigan.gov/formergovernors/0,4584,7-212-31303_31305-3054--,00.html.
[34] Policy 1365.00 Information Technology (IT) Standard Adoption, Acquisition, Development and Implementation. Available: http://www.michigan.gov/documents/dmb/1365.00_281431_7.pdf.
[35] The Management and Budget Act 431 of 1984. Available: https://www.legislature.mi.gov/(S(ywkpivhjgisruy5qu4oyxeao))/mileg.aspx?page=GetMCLDocument&objectname=mcl-18-1204.
[36] Interview with Rajiv Das, Chief Security Officer, DTMB. (2017, April 12).
[37] Ibid.
[38] Ibid.
[39] Interview with Rod Davenport, CTO. (2017, May 4).
[40] Interview with Rajiv Das, Chief Security Officer, DTMB. (2017, April 12).

[41] The "CISO as a service" capability was developed in response to findings identified by the 21st Century Infrastructure Commission, which was created by Executive Order 2016-5 in March 2016 and was "responsible for identifying strategic best practices to modernize the state's transportation, water and sewer, energy and communications infrastructure." It was composed of state and independent industry experts. Available: http://www.michigan.gov/snyder/0,4668,7-277-57738_57679_57726-381081--,00.html.
[42] Interview with Dr. Joe Adams, Vice President for Research and Cyber Security, Merit Network, Inc., and Executive Director, Michigan Cyber Range. (2017, April 10). Interview with Rajiv Das, Chief Security Officer, DTMB. (2017, April 12).
[43] Michigan Cyber Disruption Response Strategy. (2013, September 16). Available: https://www.michigan.gov/documents/cybersecurity/Michigan_Cyber_Disruption_Response_Strategy_1.0_438703_7.pdf.
[44] Interview with Captain David Kelly, Commander of the Intelligence Operations Division, Michigan State Police; Captain Chris Kelenske, Commander of the Emergency Management and Homeland Security Division, Michigan State Police; and Chris Christensen, Director of Infrastructure Protection, DTMB. (2017, April 14).
[45] Ibid.
[46] State of Michigan Cyber Disruption Response Plan, p. 1. (2015, October). Available: https://www.michigan.gov/documents/cybersecurity/120815_Michigan_Cyber_Disruption_Response_Plan_Online_VersionA_507848_7.pdf.
[47] State of Michigan Cyber Disruption Response Plan, introduction letter. (2015, October). Available: https://www.michigan.gov/documents/cybersecurity/120815_Michigan_Cyber_Disruption_Response_Plan_Online_VersionA_507848_7.pdf.
[48] Interview with Captain Chris Kelenske, Commander of the Emergency Management and Homeland Security Division, Michigan State Police. (2017, April 14).
[49] Complete list of CDRT organizations in section 6 of the CDRP. Available: https://www.michigan.gov/documents/cybersecurity/120815_Michigan_Cyber_Disruption_Response_Plan_Online_VersionA_507848_7.pdf.
[50] Ibid.
[51] Ibid.
[52] Interview with Captain David Kelly, Commander of the Intelligence Operations Division Michigan State Police; Captain Chris Kelenske, Commander of the Emergency Management and Homeland Security Division, Michigan State Police; and Chris Christensen, Director of Infrastructure Protection, DTMB. (2017, April 14).
[53] Ibid.
[54] Interview with David Behen, former Director and CIO, DTMB. (2017, March 2).
[55] Interview with Rajiv Das, CSO, DTMB. (2017, June 23).
[56] Interview with Ashley Gelisse, Chief of Staff, DTMB, and Chad Laidlaw, Senior Policy Analyst, DTMB. (2017, June 8).
[57] Interview with David Behen, former Director and CIO, DTMB. (2017, March 2).
[58] A third Kitchen Cabinet sub-council is being formed for Utilities and Resources. Source: Interview with Rajiv Das, CSO, DTMB. (2017, June 23).
[59] Interview with Meredith Grant, Chief Information Privacy & Security Officer, Henry Ford Health System, and Chair, Michigan Healthcare Cybersecurity Sub-Council. (2017, May 2).
[60] Interview with Captain David Kelly, Commander of the Intelligence Operations Division Michigan State Police; Captain Chris Kelenske, Commander of the Emergency Management and Homeland Security Division, Michigan State Police; and Chris Christensen, Director of Infrastructure Protection, DTMB. (2017, April 14).
[61] Interview with Ashley Gelisse, Chief of Staff, DTMB, and Chad Laidlaw, Senior Policy Analyst, DTMB. (2017, June 8).
[62] Interview with Rod Davenport, CTO. (2017, May 4).
[63] Merit Network, Inc., "About Us." Available: www.merit.edu/about-us.
[64] Training courses meet the Department of Defense's 8570 Information Assurance Workforce Improvement Program requirements and meet other needs such as incident response handling.
[65] Interview with Dr. Joe Adams, Vice President for Research and Cyber Security, Merit Network, Inc., and Executive Director, Michigan Cyber Range. (2017, April 10).
[66] Merit Network, Inc., "Get Trained at a Cyber Range Hub Today." Available: www.merit.edu/cyber-range-hubs.
[67] A. Alusheff, "Pinckney schools first in nation with cybersecurity program," Detroit Free Press. (2016, December 12). Available: http://www.freep.com/story/news/local/michigan/2016/12/12/pinckney-schools-cyber-security/95325834/.
[68] Ibid.
[69] Ibid.
[70] Merit Network, Inc., "Regional Cybersecurity Education Collaboration." Available: https://www.merit.edu/cybered/.
[71] The three initial higher education partners are Central Michigan University, Northern Michigan University, and Wayne State University.
[72] Merit Network, Inc., "Regional Cybersecurity Education Collaboration." Available: https://www.merit.edu/cybered/.
[73] In addition to leveraging its existing technology, technical donors like Cisco Systems provided video distribution equipment. Source: Interview with Joseph Sawasky, President and Chief Executive Officer, Merit Network, Inc.; Dr. Joe Adams, Vice President for Research and Cyber Security, Merit Network, Inc., and Executive Director, Michigan Cyber Range; and Pierrette Templeton, Director of Communications and Marketing, Merit Network, Inc. (2017, June 23).
[74] Ibid.
[75] K. Johnson, "Governor Snyder is Seeking High School Students for a Unique Cybersecurity Competition." (2016, August 16). Available:

https://www.merit.edu/governor-snyder-is-seeking-high-school-students-for-a-unique-cybersecurity-competition/.
[76] Interview with Joseph Sawasky, President and Chief Executive Officer, Merit Network, Inc.; Dr. Joe Adams, Vice President for Research and Cyber Security, Merit Network, Inc., and Executive Director, Michigan Cyber Range; and Pierrette Templeton, Director of Communications and Marketing, Merit Network, Inc. (2017, June 23).
[77] Members include higher education, K-12, government, healthcare, libraries, research institutions, and other Michigan nonprofits. Available: www.merit.edu/services.
[78] Merit Network, Inc., "Michigan Cyber Range." Available: https://www.merit.edu/cyberrange/.
[79] Training courses meet the Department of Defense's 8570 Information Assurance Workforce Improvement Program requirements and meet other needs such as incident response handling.
[80] Ibid.
[81] Merit Network, Inc., "Research and Development." Available: www.merit.edu/research.
[82] Merit Network, Inc., "Michigan Cyber Range." Available: https://www.merit.edu/cyberrange/.
[83] Ibid.
[84] Interview with Dr. Joe Adams, Vice President for Research and Cyber Security, Merit Network, Inc., and Executive Director, Michigan Cyber Range. (2017, April 10).
[85] "A Cyber Range Hub is a facility that provides certification courses, cybersecurity training exercises and product hardening/testing through a direct connection to the Michigan Cyber Range. A hub is a place where community can learn about cybersecurity, helping individuals to prepare for a career in cybersecurity and providing economic development." Available: www.merit.edu/become-a-cyber-range-hub.
[86] C. Halcom, "Wayne State to host new Michigan Cyber Range hub," Crain's Detroit Business. (2017, June 17). Available: http://www.crainsdetroit.com/article/20160621/NEWS/160629922/wayne-state-to-host-new-michigan-cyber-range-hub.
[87] The three initial higher education partners are Central Michigan University, Northern Michigan University, and Wayne State University.
[88] Interview with Joseph Sawasky, President and Chief Executive Officer, Merit Network, Inc.; Dr. Joe Adams, Vice President for Research and Cyber Security, Merit Network, Inc., and Executive Director, Michigan Cyber Range; and Pierrette Templeton, Director of Communications and Marketing, Merit Network, Inc. (2017, June 23).
[89] Regional Cybersecurity Education Collaboration. Available: https://www.merit.edu/wp-content/uploads/2016/10/RCEC_overview10_12.pdf.
[90] Interview with Joseph Sawasky, President and Chief Executive Officer, Merit Network, Inc.; Dr. Joe Adams, Vice President for Research and Cyber Security, Merit Network, Inc., and Executive Director, Michigan Cyber Range; and Pierrette Templeton, Director of Communications and Marketing, Merit Network, Inc. (2017, June 23).