

Table of Contents

2	Vision Of Action
2	Collaboration as the Centerpiece
3	Information Security - A Key Part of Business Success
4	Strengthening Operational Security
5	Transforming Information Security

Appendix M | Cyber Security

Cyber Security



Trent Carpenter
Director,
DTMB Office
of Enterprise Security
State of Michigan CISO

OES Mission:
To protect the confidentiality, integrity and availability of State of Michigan information assets and promote a secure cyber Michigan for its citizens.

OES Vision:
Be recognized as a leading authority in the achievement of a secure cyber Michigan

Vision of Action

The 2010-2014 Cyber Security Strategic Plan integrates information security efforts with Michigan's statewide information and communications technology goals. It focuses on collaboration and innovation to provide a secure foundation that leverages technology for improved service.

We can be proud of the end product. It will carry the work of the Michigan Department of Technology, Management & Budget (DTMB) into the future and help us achieve our vision of being a recognized leader in best-practice security solutions that protect the privacy and information of Michigan's citizens.

This document outlines our philosophy for the future, which centers on collaboration, innovation and a commitment to excellence. We proactively protect the systems, networks and data entrusted to us. We accomplish this by deploying technology to our agency clients and developing partnerships with the larger security community, including federal, state and local experts and stakeholders.

Our vision of action ensures we can effectively handle recovery from all types of disasters. An all-hazards approach helps us effectively manage emergencies and keep the business of state government—critical ICT services to Michigan citizens—running smoothly. Finally, we are equipping state employees with training and a solid understanding of their roles and responsibilities in protecting citizen information and maintaining the highest ethical standards.

As we look forward, we realize change will continue. Our security approach enables us to adapt to change in the risk environment.

Guiding Principles

Our vision of being recognized leaders in providing best-practice security solutions is central to everyday operations in the Office of Enterprise Security (OES). Together with our partners, we work to ensure the confidentiality, integrity and availability of State of Michigan information assets.

Our paramount and daily mission is to successfully carry out security operations and oversight in concert with our Michigan Department of Technology, Management & Budget (DTMB) partner divisions and offices to maintain the highest achievable levels of protection of all data resources and reduce the overall threats to critical computer, technology and communications services.

Collaboration as the Centerpiece

Protecting Michigan's critical government information has become an ongoing global challenge. Today's cyber threats against critical infrastructure do not require physical access to targets to inflict great harm. In fact, persons bent on destruction could potentially carry out harmful attacks from the comfort of their homes—anonously and thousands of miles away.

To provide the privacy and security citizens rightfully expect, DTMB has established public and private sector partnerships to help achieve ongoing protections. These local and national partners help us ensure the continued availability of e-government services in a safe, secure manner. Virtually every function of Michigan government depends on our reliable network infrastructure, whether working with local governments in communities across the state or communicating with federal partners.

As we move forward, partnerships will continue to grow and develop added value. Some examples of key partnerships:

- **Multi-State Information Sharing and Analysis Center (MS-ISAC):** DTMB joins counterparts in the other 49 states and Washington, D.C., in this organization that provides real-time information on threats, vulnerabilities and remediation strategies to cyber incidents.
- **Michigan Information Sharing and Analysis Center (MI-ISAC):** The Office of Enterprise Security and the Michigan Chief Information Security Officer (CISO) lead this organization. Rolling out the benefits of the MS-ISAC to Michigan's local governments establishes two-way communication and provides essential coordination for cyber emergencies, virus attacks and other serious cyber situations.

Cyber Security

- Michigan Information Privacy Protection Council: With representation from all state agencies, this group reviews, develops and recommends information security and privacy protection policies and procedures used across the state.
- National Association of State Chief Information Officers (NASCIO) Security and Privacy Committee: This group coordinates public policy and develops research documents in conjunction with states and the federal government.
- Federal Department of Homeland Security (DHS) committees and programs: NASCIO is represented on the Information Technology Government Coordinating Council in Washington, D.C. by the Michigan CISO. Through joint development of documents like the National Infrastructure Protection Plan's IT Sector Plan, a roadmap has been established to protect the nation's critical infrastructure in all sectors – including cyber. This document provides an essential list of future activities, and this relationship continues to lead to new grants, programs and opportunities to protect Michigan families.
- Michigan InfraGard: A close working relationship with the private sector is essential to improving the state's ongoing cyber security efforts. DTMB staff members have participated in many InfraGard programs, conferences and outreach to schools.
- Pandemic Influenza Coordinating Committee: DTMB is actively involved in all aspects of Michigan's Pandemic Influenza Coordinating Committee. Working with public and private sector partners around the state and country, this committee is outlining technology's vital role in planning for affected emergency areas such as transportation, border, human health, animal health, public safety and individual, family and community.



Developing Strong Partnerships

DTMB, in conjunction with the U.S. Department of Homeland Security (DHS), improved the protection of computer systems and networks in state government.

Through the sharing of federally developed technology called Einstein, Michigan government has the ultimate protection when it comes to preventing attacks against government computer systems. Michigan is the first state to utilize the technology from DHS. Einstein puts Michigan in a better position to identify and resolve a greater range of threats to its computer systems and networks.

Information Security - A Key Part of Business Success

Delivering secure, efficient and effective technology services

Information security is an integral part of our client's success. Whether it's the implementation of a new technology or a legacy solution on which our partners depend, understanding the associated cyber threats and exposures is critical to making sound business decisions. As such, it is important that we partner with our clients to ensure they have the cyber security information and understanding they need to make these decisions.

The Office of Enterprise Security is ensuring that its efforts to assist agencies in strategic and tactical security planning are effective and efficient. We work with client agencies to ensure they have the security processes and metrics they need to be successful. Efforts to refine and automate these processes and metrics will provide guidance to our business partners during the development and implementation of new technologies.

This collaboration enables the effective management of cyber risks and ultimately improves the protection of our state's information assets.

Priorities:

- Collaborate with business partners to improve the efficiency and effectiveness of information security planning, including project specific assessments as well as enterprise wide agency security plans. (2010 -ongoing)
- Work with clients to ensure security metrics are effective and appropriately communicate their cyber security posture. (2010)
- Develop new methods to automate and standardize agency security metrics to improve the efficiency of collecting and communicating security information. (2011)
- Assist client agencies with aligning their business continuity plans and DTMB's disaster recovery services to facilitate a coordinated effort to ensure critical business services remain operational. (2011)
- In coordination with agency Information Privacy Protection Officers and the Michigan Information Privacy Protection Council, provide support to agencies in developing strategies to effectively protect the privacy of citizen data. (2011 – ongoing)

Cyber Security

“Whether it’s the overload of spam, the never-ending string of viruses, or malicious attacks against our systems and web pages, we all face these cyber threats together. And it’s that word “together” that is so important. Through collaboration and the sharing of information, we will be better equipped to handle the challenges we all encounter in the security realm.”

Ken Theis
Chief Information Officer
State of Michigan



Strengthening Operational Security

Strengthening operations and security through statewide solutions and universal standards

A recent study by a local consulting firm showed that Michigan citizens fear identity theft more than they fear the loss of a job, home foreclosure, or a terrorist attack. This study emphasizes the importance of cyber security to our citizens. This is one of the many reasons we have made cyber protection our top priority as we move forward with infrastructure security enhancements.

By focusing on a multi-layered security strategy, Michigan currently mitigates most risks associated with offering services over the Internet. These efforts have already provided many positive benefits to both government operations and the public. Through effective mitigation strategies, there has been a reduction in the hardware and software needed to operate e-mail systems, bandwidth available for state operations has been increased, and the numbers of field service calls to remedy malware compromises have been reduced. All of this contributes to reducing costs and more efficiently using staff resources.

We continue our efforts to reduce the likelihood that a cyber attack can affect State of Michigan IT resources. Our goal is to make improvements in our defense-in-depth strategy by layering security protection throughout our network and, whenever possible, focus on proactively reducing cyber threats before they have a chance to impact Michigan.

Priorities:

- Review Michigan's Information Technology Emergency Management Plan to ensure it is up-to-date and accurately reflects current organization and threat environments. (2011)
- Assess current operational security systems to ensure technologies and deployments are effective, efficient and up-to-date (e.g. IPS/IDS, ADS, content filtering, etc...). (2011)
- Work with DTMB partner divisions and offices to develop and enhance processes that reduce risks associated with providing IT services. (2011 and ongoing)
- Improve protection of Michigan's informational assets by strengthening partnerships with federal, state, local and private organizations to minimize the likelihood and impact of information security incidents.
- Enhance operational security activities to better prevent and respond to cyber security issues by: (2011 and ongoing)
 - expanding operational security metrics to improve situational awareness;
 - developing automated processes where feasible;
 - improving the tracking and reporting of cyber security incidents.

Awareness and Outreach

Accelerating partnerships across and beyond state government

Often when thinking of awareness, people associate it with “training.” However, while training is a more formal process to teach and build specific skills for job performance, awareness is the process of providing a broad audience with vital information needed to ensure a general understanding of security and the ability to focus on addressing the issues and situations.

A part of our mission is to facilitate security awareness and to develop an awareness and outreach program that:

- a. encourages employees and trusted partners to have a security-conscious mindset,
- b. cultivates a security-aware culture by facilitating awareness activities that assist our employees and trusted partners in recognizing security concerns and responding appropriately,
- c. compliments the State's policy and technology initiatives and informs employees and trusted partners of safeguards and security responsibilities,
- d. collaborate and partner with local government entities, schools and trusted partners to extend security awareness services beyond conventional limits,

Cyber Security



Secure Transactions for our Citizens

Michigan government continues compliance with the Payment Card Industry's (PCI) strict standards for ensuring that cardholder information is protected and secure. The PCI Data Security Standards (DSS) apply to financial institutions, Internet vendors and retail merchants and detail the security measures and auditing procedures required to protect private cardholder information during payment card transactions. All major card brands require these Data Security Standards to assure the protection of cardholder data gathered during transactions. Michigan is one of the few states to have PCI compliance for all state credit card applications.

Michigan Cyber Security
michigan.gov/cybersecurity

In order to continue educating the public regarding cyber threats, identity theft, and a host of other Internet problems, we have developed an award-winning Web site on cyber security.

The site is constantly updated and improved to provide relevant facts, figures, training and related information to protect all Michigan citizens. Whether individuals, businesses, schools or families go online, we want them to be safe.

By focusing on enhanced communication and user-friendly resources by providing content rich security awareness information components, we will continue to seek out innovative approaches to serve our customers, both internal and external, in the best ways possible.

Priorities:

- Develop and implement a security awareness program that compliments the State's policy and technology initiatives. (2011)
- Include awareness components for both customer agencies and internal DTMB partners. (2011)
- Collaborate with our DTMB partners to better communicate cyber security awareness to our customer agencies. (2011)
- Assist agency Information Privacy Protection Officers and the Michigan Information Privacy Protection Council in the development of communication and awareness strategies regarding implementation of data privacy protection practices. (2011 and ongoing)

Transforming Information Security

Driving innovation and technology to transform Michigan

Michigan's information technology environment is constantly evolving and expanding. Our client partners and citizens continue to increase their use and dependency on technology. At the same time, cyber threats and challenges are also expanding. This constant evolution and expansion is difficult to secure with the limited resources available.

To deal with these challenges, we need to transform how we protect our information assets. We must work smarter and leverage technology to better utilize the resources we have. This means developing solutions that minimize our threat profile, while still enabling our clients to meet their business needs, such as leveraging thin technology to limit exposure of sensitive information at remote hosts.

It also means expanding our use of automated security technologies to improve the effectiveness and efficiency of cyber security resources. This includes expanding the use of intrusion prevention systems (IPS) and data loss prevention (DLP) devices to automatically block security threats, as well as expanding our security incident and event management (SIEM) solution to incorporate more platforms to improve correlation of cyber security events. We will also leverage automated tools to configure, manage and report compliancy with federal, state, and industry requirements.

Priorities:

- Expand use of automated security technologies (e.g. IPS, DLP, Content Filtering, etc.) to improve the effectiveness and efficiency of cyber security protections. (2011)
- Automate the configuration and reporting of compliance with federal, state, and industry requirements. (2011 and 2012)
- Expand security incident and event manage solution to incorporate additional platforms to improve correlation of cyber security events. (2011 and 2012)
- Implement enterprise architecture solutions that minimize security risks and costs to secure (e.g. thin technology to minimize remote client security risks). (2013)

Securely Moving Forward

Provide exceptional secure services to Michigan citizens and businesses anytime, anywhere

The Internet has changed everything, including government opportunities to proactively serve the public in new and innovative ways. Not only have Michigan citizens come to expect secure e-government transactions and ease of use on a 7x24x365 basis, the public is now calling for a new generation of "Web 2.0" transactions with a higher level of collaboration. From MySpace to Google to YouTube to Facebook, Michigan is forging ahead to provide new services and communication techniques that utilize evolving technologies.

Cyber Security

Michigan Information Privacy Protection Council:
Data Privacy Protection in the Forefront

Michigan's newly formed Information Privacy Protection Council leads the way in developing statewide strategies to protect citizen data.

The Michigan Information Privacy Protection Council was formed by Executive Order 2009-18, which established a cross-agency body to address the privacy protection needs of citizen data handled by the state. The council acts in an advisory capacity to the Governor on matters related to coordinating information privacy protection measures across all executive agencies.

Collaboration with Local Governments

DTMB performed cyber security vulnerability assessments of information technology systems used by local government, giving local decision makers the information they needed to protect their systems. The information gathered during the assessments enhanced local preparedness and allowed for the prioritization of resources to execute protective measures. Many local units of government do not have the resources to implement computer security programs on their own.

Two essential keys to success ensure we move forward in a secure manner--one that addresses the serious challenges that accompany these new technologies while addressing traditional and evolving cyber threats posed by the Internet.

Proactively responding to cyber security incidents with partners such as MS-ISAC and the Department of Homeland Security's US-CERT has greatly enhanced our ability to identify and respond to threats. Utilizing a notification network to quickly and effectively disseminate warnings of potential security issues, we continue with our efforts to encourage state, local and university participation in MI-ISAC activities.

The development and provision of timely metrics related to cyber security incidents will assist our partners in identifying risks and making the business decisions necessary to enhance their security posture and continually improve the services they provide, all the while providing the protection required to maintain public confidence.

Priorities:

- Collaborate with our customers and department partners to provide better and more secure services to Michigan's citizens.
- Develop communication strategies to share knowledge and resources necessary to efficiently address security considerations during business development.
- Continue to assist in the development of cyber security solutions (i.e. cloud computing, virtualization, thin client, mobility technology growth) to enable the secure adoption of new technologies in state government.
- Continue to update and refine security policies to adapt to cyber security challenges and evolving technologies.

Cyber Security
