Michigan Cyber Security

MISA Conference, September 15-16, 2016
Bellaire, Michigan

DTMB

ENABLING MICHIGAN'S REINVENTION

Cyber Security 2017 Performance Measures

CyberSecurity STRATEGY
Mission to ensure the confidentiality, integrity, and availability of State of Michigan information and IT assets; to handle IT security operations and recovery from all types of disasters; and to effectively manage emergencies and keep the business of state government - critical information, communication, and technology services to Michigan citizens- running smoothly.

STATE OF DTMB STRATEGY IN 2016

Top Metrics Describing Initial State

- ~10% Policies aligned to NIST
- <5% Security Plans completed
- <5% of Assets scanned monthly
- 0% of Data scanned
- 0% of Events correlated
- Cyber/MCS is staffed at ~60

Top Strategy Initiatives

1. Security Framework
2. Governance Risk and Compliance
3. Asset Security
4. Data Loss Prevention
5. Security Incident Event Management
6. Organization Redesign, Training, Staffing

Top Underlying Beliefs and Assumptions

1. Policies not organized and aligned to a framework
2. Policies & Risk Assessments not managed effectively
3. Asset Security is not implemented at enterprise level
4. Sensitive data is leaving the enterprise
5. Event not being correlated or reviewed
6. Understaffed and lack effective security skills

STATE OF DTMB STRATEGY IN (Calendar Year End) 2017

Top Metrics Describing End State

- **100% Policies aligned to NIST (M1)**
- **50% Security Plans Completed (M2)**
- **75% of Assets scanned monthly (M3)**
- **50% of Data is scanned (M4)**
- **50% of Events correlated (M5)**
- **25% Cyber/MCS staff growth (M6)**

State of Michigan – Cyber Security Vision

Ensure the confidentiality, integrity, and availability of State of Michigan information and IT assets; to handle IT security operations and recovery from all types of disasters; and to effectively manage emergencies and keep the business of state government – critical information, communication, and technology services to Michigan citizens – running smoothly.

Michigan Cyber Priorities

Priority Themes

1. Cyber Outreach & Reporting	• Establish a communications strategy and plan • Develop a risk-based cyber framework that aligns to business objectives • Develop meaningful reporting for the business	• Develop/Revise executive dashboards • Align the enterprise security strategy to the technology and business strategies • Manage security governance committee
2. Executive Engagement	• Improve executive understanding of security investment needs and business value • Train senior executives, privileged users, and third parties on security responsibilities	• Enhance security awareness program
3. Application & Asset Protection	• Improve security requirements for application development processes • Improve teaming and partnership with IT, operations, and business leadership	• Identify critical information assets
4. Define the Talent	• Design strategy to attract, retain, and develop talent including outsourcing and succession planning	• Change the tone / culture of the team
5. Cyber Analytics	• Leverage advanced data analytics techniques • Develop capabilities to digest / process cyber threat intelligence data	• Prioritize threat intelligence source and feeds

Michigan Cyber Operations

- Asset Management
- Governance
- Risk Assessment
- Risk Management

- Access Control
- Awareness and Training
- Data Security
- Information Protection Processes and Procedures
- Support
- Protective Technology

- Anomalies and Events
- Security Continuous Monitoring
- Detection Processes

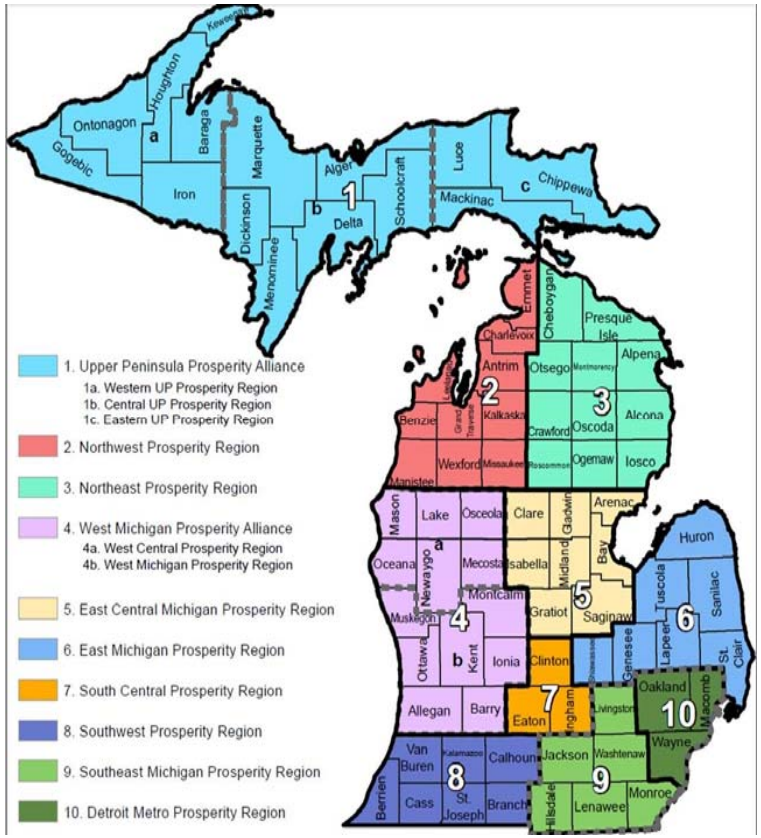
- Remediation and Mitigation
- Root Cause Analysis
- Communications

- Recovery Planning
- Communications
- Continuous Improvements

North American Cyber Summit – 10/17/2016

Michigan Cyber Civilian Corps

- Voluntary program for civilian cyber professionals
- 10 regional teams and 3 specialty teams based on industry verticals
- Managed by DTMB leadership
- Trained by DTMB with latest cyber skills
- Year long calendar with frequent cyber exercises



Cybersecurity Continuous Improvements
COMPLETED Program Details - 2016

Project Name	Scope / Features	Current State / Status
Monitoring Security Service (MSS) • Vendor = Symantec	Intrusion detection monitoring Incident response coverage After hours support	• In place • Operational • 5 year contract
Firewall Management Upgrade • Vendor = Tufin	Firewall Policy Management	• In place • Operational
Digital Incident Response or DIR • Vendor = FireEye	End-point Forensics Malware Detection Device monitoring	• Upgraded in July, August • Major performance improvements
Vulnerability Assessment (VAS) • Vendor = Cyber Defense	Penetration Testing Services	• Contract is now in place • Engagement is operational

Cybersecurity Continuous Improvements ACTIVE Program Details - 2016

Project	Purpose
Cybersecurity Framework (LockPath)	• Policies & standard procedures (PSPs) • Establish initial governance, risk and compliance (GRC) capabilities
Asset Security (Qualys)	• Asset Identification • Expand Scanning Platform • Vulnerability Reports & Dashboards
Data Loss Prevention (Symantec)	• End Point Protection • Network Discovery and Protection • Email Data Protection (MS 365) • Advanced Threat Protection
Security Incident Event Management (QRadar)	• Single Pane of Glass Monitoring • Unified Architecture Integrating Security Information and Event Management

Cybersecurity Continuous Improvements OTHER Program Details - 2017

Projects / Initiatives	History / Scope	Current State / Status
MICWRAP	Large audit remediation program MCS owns IT Security Theme area MCS consults in other Theme areas Scope evolves/expands and objectives shift Does not align to Cyber Improvement Goals	Operational
PCI	Historically a Treasury owned Program Now Co-Sponsored Treasury & MCS	2016 Record of compliance received/ 2017 project is in progress
Network Access Control (NAC)	Began as Agency specific audit remediation Desire for Enterprise platform Listed on MI Cyber Initiatives On Enterprise Architecture Roadmap	POCs with Cisco & Forescout Estimates are gathered/assess
Oracle Database Security Program (ODSP)	Program owned by CSS Phase 1 complete Phase 2 is underway Oracle Vault licenses purchase in 2013-2014 POC stood up / Not an operational platform Desire to transition Run & Maintain to MCS	To be reviewed at IT Strategy

Cybersecurity Continuous Improvements PLANNED Program Details - 2017

Name	Description	Context / Status
Network Security	Refresh and policy cleanup of firewalls and other network devices such as routers, switches, VPN concentrators, etc.	Several device refresh projects being implemented by DTMB's Network & Telecommunication organization.
Enterprise GRC	Implementation of an enterprise-wide GRC program to enable overall security management.	Dependent on the rollout of the Security Framework and security platforms projects.
Server Security	Server remediation of vulnerabilities, weaknesses and exploits. Enhanced patch management processes and file integrity monitoring.	Dependent on the rollout of the Cyber Security Framework and Asset Security Projects.
Data Classification	Enterprise data classification project to identify, classify, diagram data flows and provide control over with particular emphasis on "sensitive data," integrated with the existing EIM project.	Data Classification is dependent on the rollout of the Security Framework and specifically, the Policies around data, as well as initial GRC capabilities to enable compliance.
Security Analytics & Business Intelligence	Development of security dashboards and security reporting processes	Dependent on the implementation of the foundational platforms, specifically the implementation of the SIEM.
Security Awareness & Training	Enterprise wide effort to educate the enterprise on Security Policies and Standards	Dependent on the rollout of the Security Framework.

Contacts:
Rajiv Das, Chief Security Officer
DasR@Michigan.gov
517-896-5972 (Mobile)

Paul Groll, Deputy Chief Security Officer
GrollP@Michigan.gov
517-242-3680 (Mobile)