2015 Michigan NASCIO Award Nomination

Cyber Security Initiatives: *Michigan Cyber Disruption Response Strategy*

"It takes a network to protect a network."

Sponsor:

David Behen, DTMB Director and Chief Information Officer

Program Manager:

Rod Davenport, Chief Technology Officer & Acting Chief Security Officer

Completion Date:

December 1, 2014

Executive Summary

The State of Michigan (SOM) faced a big challenge: every day, Michigan government detects tens of thousands unauthorized attempts to probe, scan, and access or disrupt its computer networks. These same computer networks safeguard important information about Michigan's residents, control critical state agency operating systems, and provide our customers with convenient access to state services. Although a majority of these cyber anomalies are successfully blocked by defensive systems, evolving threats represent a significant risk to the continuity of state government. Similar challenges are faced by Michigan's private sector and local government partners, all of whom are also working diligently to safeguard their systems.

With the understanding that it takes a network to protect a network, Governor Rick Snyder introduced the Michigan Cyber Initiative to start various statewide efforts to ensure maximum security involving our critical networks. In response to this initiative, a team of state and local government representatives and private sector critical infrastructure owners and operators have developed the *Michigan Cyber Disruption Response Strategy* (MCDRS). The MCDRS provides an outline to assist critical infrastructure owners and operators in the development of a collaborative, public/private sector team to improve situational awareness and conduct training exercises.

In order to maximize the momentum gained by this ongoing partnership, an aggressive plan was proposed after the MCDRS was implemented in 2013 to increase cyber security exercises. The SOM has achieved these goals by implementing and participating in community wide cyber security exercises. Between 2013 and 2014, DTMB, along with their partners, have been involved in the Cyber Shield Exercise, the Alphaville Cyber Exercise, and 2013 Executive Level Tabletop Exercise. In addition, DTMB, along with Governor Snyder, hosted the 2013 Michigan Cyber Summit involving over 700 participants.

These exercises and summit allowed the SOM to improve their cyber security posture by increasing awareness among critical government and private sector personnel in safe guarding Michigan's most vulnerable data assets.

Business Problem and Solution Description

The SOM faced a complex problem: In 2012, the SOM's governmental computer networks detected an average of 187,000 cyber anomalies per day. Critical state government systems are thus vulnerable to phishing emails, denial of service attacks, attempts at unauthorized access, malware, proves and reconnaissance scans and other forms of malicious intrusions. The same issues are affecting critical infrastructure owners throughout Michigan and the entire nation.

The solution, *The Michigan Cyber Disruption Response Strategy*, provides a framework to assist critical infrastructure owners and operators in the development of a collaborative, public/private sector team to improve situational awareness and conduct training exercises. To achieve this, maximum participation across government and private sectors is needed; as such, the SOM Chief Security Officer and DTMB are responsible for the overall administration and maintenance of this plan and is monitoring and reporting its progress.

Given the evolving nature of cyber threats, the MCDRS is designed to serve as an ongoing agenda for collaborative response to significant cyber events. In addition, the MCDRS provides local governments and critical infrastructure owners and operators a better understanding of their respective vulnerabilities in order to reduce risk to their systems and operations. A key component of any prevention strategy is the deployment of expert personnel who are prepared with the tools necessary to maintain a high level of threat awareness, quickly detect and mitigate vulnerabilities, and minimize the consequences of cyber disruptions. Like any tool, the effectiveness of cyber security tools is enhanced when they are wielded by experts. So, critical infrastructure owners and operators must train staff in cyber security skills, and exercise their teams regularly to protect their systems and respond to cyber disruptions that overcome existing defenses. The achieved purpose of the MCDRS was to develop a plan for training and exercising cyber security professionals charged with the defense of Michigan's critical infrastructure.

The SOM realized a one-size-fits-all training program would not effectively serve the diverse membership of the MCDRS. Michigan's partnership uniquely includes public and private organizations of all sizes and vastly different priorities and resources. As such, the designed training plans represent a set of recommended capabilities, each associated with a domain of cyber security that is essential to the protection of critical

systems. The development of these exercises with partner organizations was a goal for 2013 and 2014. The following represents the core training domains of cyber security for the purposes outlined in the MCDRS:

1. Application Level
    - Known Software/Database Vulnerabilities (Java, SQL)
    - Web Application Security
    - Application Based Attacks (Buffer Overflow, SQL Injection)

2. Hardware and Device Level Security
    - Vulnerabilities of Routers, Switches, Services
    - Cryptography
    - Firewalls

3. Network Level Security
    - OSI Model and Protocols
    - Network Architecture (LAN, Wireless)
    - Network Based Attacks (Wireless intercept, IP spoofing)

4. Disaster Recovery and Business Continuity
    - Business Impact Analysis
    - Business Continuity Planning
    - Interdependency

5. Computer Forensics
    - Seizure Concepts
    - Incident Investigation
    - Digital Evidence and Electronic Discovery

6. Physical Security
    - Risks, Threats and Countermeasures
    - Physical Intrusion Protection
    - Access Control

7. Incident Management
    - Incident Command System
    - Roles and Responsibilities
    - Incident Reporting

Significance

By establishing cyber security exercises outlined within the MCDRS, the SOM improved their overall cyber security posture by increasing awareness among critical government and private sector personnel in safe guarding Michigan's most vulnerable data assets and systems. One of the MCDRS goals was to train key staff beginning in 2013 with the overall goal of launching a full scale cyber exercise within 5 years.

The MCDRS's goal for cyber exercises is innovative because it facilitated the formation of a diverse network comprised of federal, state and local government, as well as private industry to effectively address the evolving nature of cyber threats. In addition, this approach aligned with DTMB's overall vision to make the SOM one of the most innovative, efficient, and responsive governments in the world.

Besides creating cyber exercises, the SOM held a 2013 Cyber summit with over 700 participants, including Michigan students and residents, along with foreign government officials who specialize in cyber security. This provided the audience with exposure to a set of experts with a multitude of backgrounds and experiences. The event was so successful and the demand is so high that Michigan is hosting another Cyber Summit in 2015.

The MCDRS has improved the SOM's ability in creating a diverse network of cyber security professionals who are dedicated to reducing the risks posed by cyber threats. The continued dedication for creating cyber exercises and hosting cyber summits is a validation to the MCDRS's overall objective.

Benefits

The MCDRS document, published in September 2013, provides an agenda for the protection against cyber threats and a unified response approach in the event of a significant cyber disruption incident. Developed with private sector partners, this document focuses on Michigan's key infrastructure (utilities, banking, healthcare, state and local governments) and provides guidelines for communication protocols, response planning, training and exercises, and risk assessments. So far, the SOM has created, conducted, and participated in several cyber security exercises. This allowed for organizations and partners to collaborate in response to simulated cyber threats and improve their overall ability to compact such threats. Between 2013 and 2014, DTMB, along with their partners, have been involved in the Cyber Shield Exercise, the Alphaville Cyber Exercise, and 2013 Executive Level Tabletop Exercise. In addition, DTMB, along with Governor Snyder, hosted the 2013 Michigan Cyber Summit involving over 700 participants.

Cyber Shield Exercise

In 2013, the Michigan National Guard participated in the Cyber Shield Exercise in Fairfax, Virginia, a joined mission assurance team providing Computer Emergency Response Team and Computer Network Defense Service Provider Support. The purpose of this exercise was to build skills related to network defense, recovery of lost data, and restoration of networks. The exercise ran 24 hours a day, over a four day period, and required participants to work both independently and among a group to respond to typical threats in the cyber domain such as stolen data and network control.

The 2013 Executive Cyber Tabletop Exercise

On October 1, 2013, the SOM hosted a Cyber Tabletop Exercise in Lansing, Michigan. The Michigan State Police and DTMB conducted an Executive-level tabletop exercise to examine the roles between federal, state, and private sector partners during a cyber-attack. Participants and observers included company executives, emergency management coordinators, information technology representatives and public information officers from each organization to better prepare for an attack. State agency participants included counterparts in the same categories, creating an excellent opportunity for networking and collaboration between public and private sector partners.

The Alphaville Cyber Exercise

In July 2014, the SOM conducted the “Alpahville Exercise” at Davenport University in Grand Rapids, Michigan. This exercise included attack/defend Red Team/Blue Team scenarios utilizing the Michigan Cyber Range’s virtual city, “Alphaville.” Players included members of DTMB’s Michigan Security Operations Center, the Michigan Cyber Range, the Michigan Cyber Civilian Corps, and the Western Michigan Cybersecurity Consortium.

The 2013 Michigan Cyber Summit

The 2013 Michigan Cyber Summit, a follow-up to the previously sold out Cyber Summit of 2011, was held in Novi with more than 700 in attendance. Attendees and participants included representatives from the White House, Department of Homeland Security, the National Governors Association, the Government of Israel, academia, and private industry. This summit brought together subject matter experts to discuss ways to defend business, education, law enforcement and individuals against cyber-attacks and take

advantage of opportunities in the cyber security industry. These summits have been extremely successful bringing together public and private entities in a collaborative environment to help combat the cyber threats and promote a strong cyber ecosystem. As the demand in attending this event continues to grow, Michigan directs interested citizens and guest speakers to Michigan Cyber Summit for enrollment.

Moving forward to 2015, the MCDRS will routinely be updated to include additional detail and planning milestones. In the continuing effort to maintain a strong cyber security ecosystem, the SOM will remain in partnerships with private sector critical infrastructure entities, manufacturing, local units of government, law enforcement, military, and academia. In addition, the SOM's relationships with federal partners such as the Department of Homeland Security and the Federal Bureau of Investigation have served to strengthen our environment and enable greater information sharing and training cyber exercises. Michigan will continue to use the MCDRS to build upon the accomplishments of the 2013 and 2014 cyber exercises. Finally, Michigan is currently organizing the 3rd International Cyber Summit, which will be held in October 2015 in Detroit.