2016 NASCIO Award Nomination
Michigan Cyber Disruption Response Plan

Sponsor: David Behen, DTMB Director and Chief Information Officer

Program Managers: Christian Kopacsi, Chief Security Officer and Deputy Director
Chris Christensen, Director of Infrastructure Protection

Award Category: Cybersecurity

Completion Date: October 25, 2015

Executive Summary

In today's cyber threat environment, it's not a matter of if but when a cyber-attack will occur. Every day, the State of Michigan detects tens of thousands attempts to infiltrate its network. To keep pace with these ever evolving threats, Michigan developed the Cyber Disruption Response Plan (CDRP). This plan protects the health, safety, and economic interests of Michigan's residents and organizations by reducing the impact of disruptive cyber-related events through response, mitigation, planning, awareness, and implementation.

The CDRP provides Michigan's primary emergency management (EM) and information technology (IT) personnel, as well as other potential stakeholders, with a management framework to coordinate preparedness, response, and recovery activities related to a large-scale or long-duration cyber disruption.

This framework helps all participating public and private partner organizations identify and respond to cyber threats by defining five threat levels. Each of these threat levels includes corresponding responses to address threats of increasing scope and severity. The plan also enables closely integrated planning by providing a standard incident response plan template for critical infrastructure entities and their partners. In addition, the CDRP leverages technical training for core team members, well-planned and executed exercises, and risk-based metrics to identify, implement, and track continuous plan improvement initiatives.

Using the CDRP, the State of Michigan seamlessly works with Federal, State and Local agencies and organizations, as well as education institutions and private industry, to respond to, resolve, and address cybersecurity disruptions and events. The plan also largely promotes collaboration and communication across all participating organizations – including the Department of Technology & Budget (DTMB), Michigan State Police (MSP), and Michigan National Guard (MNG) – to ensure better protection against, and quicker response to, cyber-attacks.

The plan allows the State of Michigan to establish a common framework through which all private sector and local government partner organizations can easily and effectively protect their systems.

Michigan's CDRP is widely regarded as a national model. In fact, it was leveraged by the National Association of State Chief Information Officers (NASCIO) to write their Cyber Disruption Response Planning Guide and will be featured in the upcoming National Governors Association (NGA) Cybersecurity Policy Academy. The CDRP has been tested and proven to be an effective tool against any cyber threat. Recently the state has seen increased tension surrounding the Flint water crisis, spurring the international hacktivist group, Anonymous, to threaten to infiltrate the state's network. However, with the CDRP in place, the State of Michigan negated all attempts by the hacktivists to infiltrate the network and was able to effectively and efficiently protect detect and respond to any cyber threat.

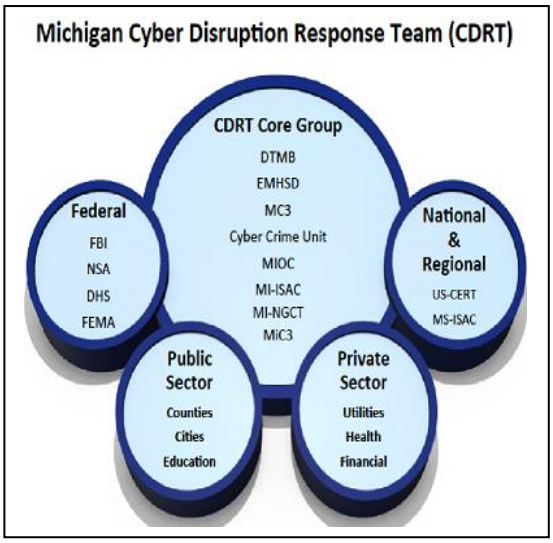
Concept

Prior to the development of the CDRP, the State of Michigan formed a Chief Security Officer (CSO) Kitchen Cabinet to engage cybersecurity executives from the public and private sectors to facilitate a more open dialogue on the plethora of cybersecurity-related concerns and emerging threats. The group meets on a monthly basis and was instrumental in the development of the Michigan Cyber Disruption Response Strategy in 2013, which was designed to combat numerous unauthorized attempts by hackers to probe, scan, access, or disrupt the state's computer networks. However, while the strategy provided an overview for responding to cyber threats, there lacked pertinent details outlining a specific course of action and individual responsibilities, resulting in less effective communication between state officials and the parties affected by cyber incidents.

As outlined in Governor Rick Snyder's 2015 Michigan Cyber Initiative, Michigan vowed to further develop partnerships with the cybersecurity ecosystem to take the cyber disruption efforts to the next level, including establishing the Michigan Cyber Defense Response Team (MCDRT) to support state government and key stakeholders in Michigan during and after a cyber event (detailed below). With this objective in mind, and the continuous partnerships with key stakeholders, the State of Michigan created the CDRP, an official document outlining a specific course of action for organizations dealing with various levels of cyber-attacks. Developed from the ideas of specific initiatives – such as Presidential Policy Directive 21 and the Department of Homeland Security's National Infrastructure Protection Plan – the CDRP offers a framework for any private sector or government organization to define the severity of the incident they are facing and determine whether they must alert state officials.

The plan provides incident action plans, breach classifications, and common terminology to ensure every organization can easily understand the plan and more quickly respond to cyber threats. By establishing the CDRP, the state helps agencies, government organizations, and private sector entities – with or without cyber knowledge – seamlessly communicate to determine the best course of action and ensure all parties are fully informed and engaged throughout the process of responding to the cyber incident.

With the CDRP came the formation of the MCDRT. Led by the DTMB and MSP, the MCDRT is a specialized jurisdictional consultative group composed of subject matter experts primarily from the EM and IT domains. The team aids executives, EM staff, IT staff, as well as other Federal, state, regional, local, and private organizations in preparing for, responding to, and recovering from cyber disruptions. The MCDRT is also responsible for engaging in pre-event planning activities that increase the resilience of critical



cyber assets across Michigan. On top of these responsibilities, the team is also tasked with exercising the CDRP to ensure all state personnel are well-versed in cybersecurity policies, best practices, and evolving cyber-related threats.

The CDRP classifies the aforementioned cyber disruptions into five distinct threat levels – low, medium, high, severe, and emergency – which are impacted by internal and external cybersecurity events. To aid organizations in identifying who to contact in the event of a cyber incident, the CDRP provides an "escalation path," which illustrates level definitions, escalation/de-escalation criterion, and potential impact of an incident, as well as communication procedures for responding to incidents and responsibilities to ensure organizations are responding correctly. Threat levels are based on the risk an event poses and the impact it has on the state government enterprise, which helps organizations determine their next course of action.

To test the CDRP, the State of Michigan met with various organizations for a tabletop exercise designed to examine roles, responsibilities, authorities, and capabilities to enhance the state's readiness posture in the event of a state-level cyber disruption. For the exercise, MSP, Emergency Management and Homeland Security Division (MSP/EMHSD), partnering with the DTMB, MNG, and private-sector partners, brought together 130 people from state, local, and private-sector entities to exercise a state-wide cyber disruption against a scenario that included hacktivist activities causing both cyber and physical incidents.

The exercise proved to be a successful demonstration of Michigan's capabilities and gaps when responding to cyber disruption. Following the exercise, participants came together to identify areas for improvement for the CDRP – such as clarifying conditions surrounding lower threat levels for stakeholders. The exercise allowed the state to update the CDRP to address any gaps and inconsistencies prior to the next exercise. By conducting these exercises, the State of Michigan is able to more effectively respond to and recover from cyber disruptions at any level.

The state collaborated with the DTMB, MSP, and MNG to develop the CDRP. In addition to these organizations, the state called upon Symantec to provide an objective, professional recommendation for how the state should approach drafting and implementing the plan. After working with Symantec numerous times in the past, and utilizing various Symantec products the State of Michigan was confident the company would provide insight into industry standards for cybersecurity plans to ensure the state created the best possible plan to effectively secure its critical infrastructure.
Since its implementation, the CDRP continues to simplify and streamline the process of reporting and responding to various threats for private sector and local government organizations. Previously, the state provided several forms to classify cyber incidents. Now, rather than relying on various forms to determine the severity of the incident, the state offers one plan and one clear course of action, defining who needs to know about the specific incident and how individuals can obtain the information they need.

Significance

The scope of the CDRP was to create a cyber disruption solution to assist key Michigan stakeholders with a quick, efficient, and concise plan for successfully mitigating the impacts of various cyber incidents. But perhaps the most significant factor of the CDRP's creation and implementation is that it is the first cyber response plan of its kind among state government.

When it implemented the CDRP, the State of Michigan was looking to position itself as a leader in the cyber space. The state wanted to not only protect its own networks from cyber incidents, but also provide a cyber response plan other states could easily adopt. The plan's innovative design allows any state to use it simply by making a few updates to the overall document.

Now that the plan is in place, the state is spreading the word across the nation. In 2015, Michigan's governor announced the plan's launch, urging other officials looking for a specific cybersecurity strategy to implement the plan in their own states. The state is also sharing the plan with government chief information security officers (CISOs) nationwide.

The CDRP also significantly improved Michigan's ability to more quickly mitigate cyber threats. Sophisticated cyber criminals are constantly honing their tactics for infecting networks. The use of the CDRP has provided a better means for communicating, the document contains templates of reports, meetings, communications, and action plans. These templates were discussed and agreed upon by all of the parties involved in creating the CDRP. An example of where we have used this process is with the Flint water crisis.

Recently, The Michigan Intelligence Operations Center (MIOC) and the Michigan Cyber Command Center (MC3) received information warning that the State of Michigan, Governor Snyder, the City of Flint, City of Flint Mayor Weaver, and other private individuals and entities faced an increased risk of cyber-attacks. In addition to doxing – the act of gathering and publishing individuals' personal information without permission – threat actors attempted to compromise government servers, workstations, and email accounts.

When a threat is detected, the state publishes and shares a situational report with organizations – such as the DTMB, MC3, and MIOC – to help identify, mitigate, and remediate cyber-attacks threatening state infrastructure. In this case, hackers threatened to reveal the employees involved with the Flint Water crisis. In response, MC3 provided information on how to harden accounts and identify and flag suspicious activity. It also outlined next steps for all parties involved.

Each situational report includes a detailed timeline of all events and incidents, allowing organizations to stay up to date on the state's efforts to mitigate and remediate those incidents. Additionally, the state provides a list of suggested considerations for

participating organizations to help reduce the risk of exposure and targeting by malicious actors in the future.

Prior to the implementation of the CDRP, state organizations would remain in the dark regarding the numerous cyber incidents affecting fellow organizations. Now, with the CDRP's situational reports, participating organizations are constantly aware of the state's efforts to identify, mitigate, and remediate incidents threatening state infrastructure.

Impact

The cyber disruption planning environment in Michigan prior to the CDRP's creation can be characterized as confusing, semi-accurate and lacking pertinent details to successfully mitigate cyber disasters. In the past, communication between the state and organizations during a cyber incident was minimal and disjointed – sometimes taking weeks for organizations to share that an incident occurred. Now, lines of communication are open, providing organizations impacted by cyber incidents with the support they require to combat cyber-attacks and address future threats. With the CDRP, the State of Michigan is able to prevent hackers from infecting critical infrastructure and ensure high-level protection for its most valuable asset: information.

The increasing numbers of cyber-attacks are causing disturbing and stressful situations, especially when they're intended to bring down government functions, our economy and our way of life. Michigan already feels under siege, especially in the wake of the cyber threats surrounding the Flint water crisis. Additionally, every day, there are 2.5 million cyber-attacks on our state government computers. More alarming, that's a million more attacks each day than a year ago. The number is going to continue to increase. Michigan, a state of 10 million citizens and the global hub for automotive design and manufacturing, is a large target for cyber criminals. In Addition, three major research universities are located in Michigan. That's why we've made cybersecurity a top priority.

Even with Michigan's unrelenting dedication to cybersecurity, we understand that this effort requires collaboration across all sectors. Michigan has established CSO and CIO Kitchen Cabinets to partner with cyber experts in the military, government and private sector to establish a model for how government and business can unite for the greater good of our respective customers and citizens. Even Better, it can be used as a template for any city, township, village or county, or for businesses both large and small. The CSO Kitchen cabinet was instrumental in the creation of the CDRP.

An immediate impact of the CDRP is confirmed by a recent organization in Michigan that was hit with a ransomware incident. Luckily, the individual from the organization is a member of the CSO Kitchen Cabinet. When the organization was hit with ransomware they had two essential resources that they did not have before to help in the recovery for the organization. First they had the CDRP in hand and were ready to use the plan because they practiced with the tool before the incident so they were prepared. Second they were able to utilize the relationships created by the CSO Kitchen Cabinet to reach

out to other cybersecurity professionals in the area to provide insight and expert advice on what tools would help mitigate and eventually stop the malicious activity. The impact on the organization displayed firsthand many of the benefits of the CDRP. Incidents like this would have taken months to recover from because of the CDRP the organization was only impacted a few days. The State of Michigan was a vital resource and provided direction in solving the problem and minimized time, money, and resources used in restoring the system.

Because Michigan is the first state to establish an official CDRP, we are routinely asked to work with other state officials and organizations to help them formulate and implement plans of their own. NASCIO recently collaborated with the State of Michigan to establish their Cyber Disruption Response Planning Guide. In addition, NASCIO asked Michigan to discuss their efforts surrounding cyber disruption plans during the Midyear Conference in Baltimore, MD.

Understanding our reputation as the leader in cyber disruption planning, Michigan will continually give back to its fellow states by sharing the plan and urging other CISOs to implement it in their own states to protect, detect, and respond to cyber incidents. In fact, the National Governors Association (NGA) asked Michigan to brief states participating in the upcoming NGA Cybersecurity Policy Academy on best practices related to cyber disruption plans.

The longer term impacts of establishing the CDRP are yet to be seen, but Michigan is very happy with the immediate benefits of the disruption plan. Benjamin Franklin said it best, “If you fail to plan, you are planning to fail!” By creating the CDRP the State of Michigan has created a tool to protect the health, safety, and economic interests of Michigan’s residents and businesses by reducing the impacts of disruptive cyber related events through response and mitigation planning, awareness, and implementation. Cyber disruption events have the ability to severely impact the social, economic and physical welfare of state citizens and businesses through escalated or multiple simultaneously executed attacks on the state’s most critical sectors. The plan provides a framework that enables state emergency management and information technology to work seamlessly with public and private partners to rapidly respond to and minimize the impact of cyber disruption events in Michigan.