2017 Michigan NASCIO Award Nomination

Sponsor: David Behen, DTMB Director and Chief Information Officer

Program Managers: Rajiv Das, Chief Security Officer
Paul Groll, Deputy Chief Security Officer
Ray Davidson, Project Manager for MiC3

Project Title: Michigan Cyber Corps Reboot 2016

Category: Disaster Recovery/Business Continuity

Completion Date: December 2016

EXECUTIVE SUMMARY

In today's threat landscape, it's not a matter of if, but when a cyber-attack will occur. The main question is: do you have the resources in place to address the attacks no matter where they occur? Every day, the State of Michigan detects tens of thousands of attempts to infiltrate its network. With the realization small and medium sized businesses and local governments are likely facing the same cyber threats; the State of Michigan created the Michigan Cyber Civilian Corps (MiC3), an all-volunteer force of cyber defenders to supplement its publically available resources such as the Michigan National Guard and Michigan State Police to its citizens. Michigan is unique among the 50 states in having an all-volunteer cyber corps and is routinely sought for guidance from other states.

The original idea came from Governor Rick Snyder and was announced at the 2013 North American International Cyber Summit. The MiC3 started as a partnership among Michigan's Department of Technology, Management & Budget (DTMB), Merit Network of Ann Arbor, MI, and the Volunteer Registry System of the state department now known as the Department of Health and Human Services (DHHS). Members were sought and recruited throughout the state, largely by Merit, and chiefly by word of mouth.

However, in 2016, this initiative underwent a tremendous reboot by having the State of Michigan become the sole owner of the MiC3. The State of Michigan has made aggressive benchmarks for success, including introducing new legislation to create a program under which volunteers can provide services to organizations in Michigan to respond to cybersecurity incidents. In addition, Michigan is actively seeking new ways to increase membership. At its heart, the vision of the MiC3 is to have an experienced, certified group of subject matter experts across a wide range of cyber defense skills, with knowledge of the tools, techniques, and methods used by attackers against networks and systems, and the expertise to defend those systems. Current volunteers come from government, academia, business, financial and healthcare sectors.

Within the next two years, Michigan is committed to increasing MiC3 to 200 members and investing in the continued development and training of MiC3 members. The increase in members will ensure small and medium sized organizations have a low cost cybersecurity response option in case of cyber-attacks or disruptions. The investment in training and certification will ensure the volunteers are current and up to date on their skills. In addition, the MiC3 will continue to serve as a national model while supporting Michigan's cyber ecosystem in case of large-scale attacks to Michigan's critical infrastructure.

CONCEPT

State and local governments have long been tested in their abilities to respond to emergency situations. Whether its fires, floods, tornadoes, or cyber incidents, Michigan is always seeking innovative ways to respond to new and emerging threats. As a result, Michigan's Governor Rick Snyder expressed interest in tapping the state's cyber expertise to strengthen the state's cybersecurity posture. The vision articulated by Gov. Snyder was to have a well-trained, certified group of subject matter experts across a wide range of cyber defense skills, with the knowledge of the tools, techniques, and methods used by attackers against networks and systems. To do this, Michigan created the MiC3, a volunteer IT cybersecurity force that would help the state respond to cyber incidents during a governor-declared state of emergency. This new team of volunteers would work with existing state IT staff and resources to create a broader network of cyber-responders.

The project began by leveraging partnerships amongst the State of Michigan's DTMB, Merit Network, and DHHS. IT security professionals were sought and recruited throughout Michigan – largely by Merit – and chiefly by word of mouth. Word of the organization was spread among the informal information security community through contacts at conferences and annual cybersecurity exercises hosted by the State of Michigan.

Merit administered an online test of cyber knowledge and skills for prospective MiC3 recruits, and passed along qualified applicants to the state's volunteer registry. Once applicants passed the online test and background check, new members were on boarded by the program manager at Merit. The initial goal was to enroll a sufficient number of members to make up ten teams of five, each with a team leader, and assigned to (or living in) one of ten of Michigan's defined "prosperity regions." Information on the prosperity regions can be found here: http://tipstrategies.com/blog/2014/08/tip-engaged-by-east-michigan-cog/. The Michigan team continues to reevaluate the team model, and will likely move from a geographically-based model, as this makes less and less sense as the cyber world, internet of things, and other major changes to the internet landscape lower the value of physical location. In addition, Michigan is examining alternatives for the team model, including teams based on specific industry expertise (finance, healthcare, transportation, government, energy, etc), or teams organized around skill sets targeting a particular type of attack (DDOS, phishing, ransomware, etc.).

Before the MiC3 was created, Governor Snyder initiated another cyber-related project called the Michigan Cyber Range that would serve as a valuable resource for MiC3 members. The Michigan Cyber Range is an unclassified private cloud operated by Merit, and is designed to help cybersecurity professionals prepare for real-world situations, providing a secure environment for cybersecurity education, training, and testing. It also performs research as an advanced platform for industrial control systems

security. In addition, the Michigan Cyber Range is a facile virtual environment set up to challenge attackers and defenders alike, by setting up a red team and a blue team exercise around the concept of a working city, “Alphaville.” By 2013, Merit was offering courses across a variety of skill sets based on various “Alphaville” simulations. Since the MiC3 was created, members were invited to sharpen their skills by leveraging the Michigan Cyber Range. Additional information on the Michigan Cyber Range can be found here: https://www.merit.edu/cyberrange/).

In 2016, DTMB and Merit Network agreed to move the ownership and administration of the MiC3 to the State of Michigan. DTMB hired a subject matter expert and MiC3 member to oversee the transition, and to ensure the continued growth and success of the corps. The Michigan cybersecurity team has engaged with eMichigan, DTMB’s web development shop, to translate the tests from Merit’s website, and bring much more of the vetting and onboarding process under state management. Phase I of the application is now available online.

Current membership in the MiC3 is open to information security professionals who are residents of the State of Michigan. Applicants are encouraged to have at least 2 years of direct involvement with information security, preferably security operations, incident response and/or digital or network forensics. Applicants must also have a basic security certification (ANSI-certified/DOD 8570 compliant certifications such as Security+, C|EH, CISSP, or GIAC certifications are strongly recommended). Applicants are also required to pass a series of tests to demonstrate basic knowledge of networking and security concepts, as well as basic IR and forensic skills. Because of the time commitment (up to 10 days a year for trainings, exercises, and conferences), applicants must provide evidence of employer support before volunteering with the MiC3. Successful applicants are also subject to background screening and are required to sign a confidential disclosure agreement. Interested parties can apply online at: Michigan Cyber Civilian Corps.

SIGNIFICANCE

The MiC3 is innovative because it's a first of its kind in the United States, but perhaps the most significant aspect of the MiC3 is the talent level that exists amongst the volunteers. In 2016, DTMB partnered with the SANS institute to offer their popular course in Incident Handling and Ethical Hacking as an in-person, instructor-led course, to approximately 60 students. These students included DTMB staff, agency partner security officers, MSP staff, and 32 members of MiC3. As part of the course offering, all MiC3 members were granted access to the certification exam. 20 volunteers took the test and all of them passed. This is the noteworthy fact – GCIH is an ANSI-certification exam, and certification satisfies the requirements of Department of Defense Directive 8570, which governs the cybersecurity workforce in the military. As a result, Michigan now has a cadre of civilian s who satisfy military standards for cybersecurity. This is unusual even for state National Guard teams, and a definite first for volunteer civilian teams.

In 2016, Governor Snyder created a 21st Century Critical Infrastructure Commission to address several areas where improvement is needed within the State of Michigan. Cybersecurity was a focus of the commission and they recommended expanding the MiC3 to as many as 200 members. In November and December, the MiC3 processed additional applicants to bring the total to 51 members. As many as 15 members are in the application process now, so Michigan is on pace to reach the 200 member objective within the next year or two.

Since the State of Michigan took over the MiC3 in 2016, several events have been planned to significantly increase participation and membership. For example, MiC3 members met at Consumers Energy to for their first face-to-face meeting and another event is planned at Ferris State University. The Ferris State meeting is especially significant because it will feature a training exercise and current Ferris State infosec students will be invited to participate in all activities as an outreach effort.

The MiC3 has also drawn interest among the various councils created by Governor Snyder. These groups were created to bring both public and private sector IT and security executives across the financial, healthcare, automotive, transportation, education, and government sectors together to discuss cybersecurity and how to make the state better as a whole. Collaboration and cooperation are at the heart of what makes these groups work so well. Some groups meet monthly while others meet quarterly, but the results are the same: a collaborative environment where emerging cyber trends and threats are discussed to make the State of Michigan more secure. During the last Michigan Financial Industry Cybersecurity Council, members committed to send employees through the MiC3 application in an effort to help the State of Michigan reach its goal of 200 active members.

As the MiC3 continues to grow, Michigan has been working with widely acclaimed national experts to develop a bill to establish a framework for volunteers to provide cybersecurity services to organizations within Michigan. This bill will also ensure that the volunteers have the legal protection they need to help in the event of a cyber incident, and this legislation will clarify the roles of the volunteers and responding law enforcement. Finally, the legislation will also provide guidelines for creating a MiC3 advisory board to define its powers and duties.

Now that the MiC3 is under state management, Michigan is spreading the word across the state and nation through various means, such as the National Governors Association (NGA), NASCIO, and existing cybersecurity councils within the state.

MiC3 at the 2016 North American International Cyber Summit with Governor Rick Snyder

IMPACT

The increasing number of cyber-attacks infecting state networks today is forcing governments to accelerate efforts to protect critical data, systems, and citizens, as well as respond to and manage incidents. Because it is the first state to establish an official cybersecurity volunteer corps, the State of Michigan now works with other state officials and organizations to help them formulate and implement volunteer programs of their own. In fact, NGA recently held a Cybersecurity Policy Academy where Michigan and Virginia served as faculty to help select states enhance their current cybersecurity practices and policies. Michigan was routinely asked about how to start a cyber corps and what are some of the best practices in doing so. In addition, our Deputy CSO, Paul Groll, presented on the MiC3 during the National Association of State Technology

Directors Southern Region Seminar – a recap of that speech can be found here: http://statescoop.com/could-a-corps-of-cyber-civilian-volunteers-save-state-networks. As it continues to test and assess the MiC3 effectiveness, Michigan intends to continue giving back to its fellow states by sharing the details of the program and urging other CISOs to implement it in their own states to help small to medium sized businesses and local governments respond to new and emerging cyber incidents. Since Gov. Snyder co-chairs the NGA's Cyber Resource Center, Michigan plans to help NGA write a volunteer cyber corps national guide for other states to consult when they're embarking on similar initiatives. In addition, the MiC3 was awarded the Statescoop 50 IT Innovation of the Year award.

In summary, the MiC3 provides a mutually beneficial relationship for participants and their sponsoring employers. For example, team members benefit in the following ways:

- MiC3 provides members (and their employers) with significant training and certification opportunities.
- Membership in MiC3 enhances professional relationships, through networking and collaboration opportunities with other IT security professionals.
- Members fulfill their sense of civic duty by using their cyber expertise to help the citizens of Michigan.
- As part of this innovative response team that is a first of its kind in the United States, members become leaders in a new form of public-private partnership.
- The MiC3 provides an opportunity for technically oriented professionals to perform a civic duty by aiding the State of Michigan in a time of cyber crisis.
- MiC3 members also have the opportunity to assist in raising the security culture throughout the state.

Employers who allow their employees to participate in the MiC3 benefit in the following ways:

- MiC3 member employees enhance their abilities through unique training and certification enrollment.
- The network of MiC3 members provides an opportunity for informal information sharing, and development of best practices.
- The business becomes an early part of this new form of public-private partnerships which provides mutual aid in times of emergency.
- MiC3 participation provides an employee perk that can attract best cybersecurity employees during time of high competition candidates.
- MiC3 member employees will provide a nexus of information security awareness and training within the business.