NATIONAL GOVERNORS ASSOCIATION

Re-Envisioning State Cyber Response Capabilities: The Role of Volunteers in Strengthening our Systems

Table of Contents

June 2022

Overview

There is a widely recognized shortage of skilled cybersecurity talent, especially across government, and the lasting impacts of the COVID-19 pandemic have introduced new challenges to both the security and workforce landscapes. Despite an increase of 700,000 cyber personnel in the global labor market over the past year, the demand for this talent pool continues to outpace supply.[1] To address this widening gap in the United States, state governments are finding resourceful ways to leverage and balance the incentives that motivate this community of professionals and simultaneously bolster their security posture in a heightened threat environment.

Michigan, Wisconsin and Ohio are among the frontrunners in an effort to build teams of volunteers dedicated to conducting cybersecurity assessments and/or incident response activities on systems and networks within their borders. As these models mature, they are revealing the advantages of such a system for public and private sector entities, the volunteers themselves and the states' residents. Understanding the strengths and weaknesses of these programs can also inform the adoption of similar solutions around the country to better confront the cyber threat.

Introduction

As cyber threat actors get more creative, so too must our defenses. State, local, tribal and territorial (SLTT) governments seeking to enhance their security posture are strained to operate within the bounds of both their personnel and resource limitations. Existing parallel to a highly competitive and lucrative private sector tech industry presents an additional layer of complexity. States understand the value that these companies bring to the workforce and – rather than view them as competitors –see these players as integral partners to the overall wellbeing of the cybersecurity ecosystem. These considerations have led to innovative pathways for engaging a community that has proven eager to contribute to a broader mission of cybersecurity preparedness and response.

Volunteers have long played an integral role in America's emergency response capacity. Most readily called to mind is likely an image of local volunteer firefighters or humanitarian organizations that are deployed across the country in the event of a natural disaster. Still, the notion of cybersecurity volunteers has been around (domestically and abroad) since the early-2000s, with the Homeland Security Act of 2002, which authorized the establishment of a national technology guard comprised of "local teams of volunteers with expertise in relevant areas of science and technology, to assist local communities to respond and recover from attacks on information systems and communications networks."[2] In 2008, after grappling with a three-week-long cyber attack from Russia, Estonia stood up its Cyber Defense Unit, a group largely made up of private sector cybersecurity professionals who volunteered to shore up the country's cyber response capabilities.[3] Most recently, U.S. lawmakers introduced the Civilian Cyber Security Reserve Act, which would enable the U.S. Departments of Homeland Security (DHS) and Defense to each temporarily create a similar team of cyber volunteers at the national level.[4]

Parallel to these initiatives, states across the U.S. have been making strides of their own to augment their existing security framework and incident response efforts, as well as their cybersecurity workforce. With these programs, SLTT governments and eligible under-resourced organizations have gained improved access to highly-skilled cybersecurity incident support, professionals have been provided valuable training and networking opportunities (which in turn benefit their employers) and state residents are more secure. Michigan, Wisconsin and Ohio are regarded as leaders behind these models and present an interesting look into the diverse ways in which programs can be implemented, based on a variety of factors unique to each state's landscape.

Michigan's Cyber Civilian Corps

Program Inception and Context

The State of Michigan pioneered the volunteer cybersecurity unit model in the United States nearly ten years ago in 2013. The group, called the Michigan Cyber Civilian Corps (MiC3), was formed under Governor Rick Snyder's leadership to support the state's capacity to respond quickly and effectively to cyber incidents. The project began as a partnership between the Michigan Department of Technology, Management and Budget (DTMB), the Merit Network, Inc. and the Michigan Department of Health and Human Services' Volunteer Registry.

The vision of the MiC3 was—and continues to be—to incorporate experienced, technical cybersecurity professionals into the state's cybersecurity response framework to fortify the state's networks and systems against attackers. The group is comprised of "trained, civilian technical experts who individually volunteer to…provide mutual aid to all levels of government, education, and business organizations in the State of Michigan in the event of a critical cyber incident."[5] This volunteer force allows the state to augment resource-strapped organizations' cybersecurity infrastructure by outsourcing the services of high-caliber industry professionals to the state at a low cost. Not only are SLTT agencies and small businesses eligible for these free services better off, but residents whose data is housed by these entities are granted an added layer of security that was previously lacking.

Upon its inception in 2013, the Merit Network was largely responsible for the recruitment of MiC3 members across the state, relying on word-of-mouth and informal channels among the information security community. It then administered an online test to gauge cyber knowledge and skills and passed along qualified applicants to the Volunteer Registry before initiating an onboarding process. The goal at the time was to create ten five-person teams, whereby each team would dedicate itself to one of the state's "Prosperity Regions" under the guidance of a Team Lead.[6]

Between 2015 and 2016, however, the decision was made to assign management and oversight (including recruitment and vetting responsibilities) of the MiC3 to the DTMB, supported by a part-time program manager residing within the department's Cyber

Security Division, and to transition the Merit Network to a more advisory role. As part of this restructuring, focus also shifted from preparing specifically for a large, declared cybersecurity event to the creation of a team which could respond more generally. As part of the effort to attract more members, the MiC3 was able to provide training from the SANS Institute, a widely respected organization specializing in cybersecurity upskilling, along with the associated certification exam to the MiC3's members. Notably, all 20 members who opted to participate at the time passed the American National Standards Institute (ANSI)-accredited and U.S. Department of Defense (DoD) Directive 8570-compliant exam, reflecting the quality of cybersecurity practitioners the program had attracted. It was also determined that the geography-based team model did not add any substantive value to MiC3 given the reality of the cyber landscape and members' ability to connect virtually to train or gain access to compromised networks.

In 2017, the MiC3 achieved a major milestone, codifying the program into law via the Cyber Civilian Corps Act (Public Act 132 of 2017).[7] Before the passage, only a cyber incident of very high magnitude could trigger the deployment of the MiC3, which resulted in a pool of volunteers who stood ready for years, waiting for the call to action.[8] The formalization of the MiC3 into law allowed the state to loosen its activation criteria and begin to put the volunteers to use.

Membership

As of May 2022, the MiC3 is enlisting the support of 64 members. To be considered for admission, candidates must:

- Be a Michigan resident.
- Have at least two years of direct involvement with information security, preferably with security operations, incident response or digital or network forensics.
- Possess a basic security certification (with a strong preference for ANSI-accredited and DoD Directive 8570-compliant certifications).
- Pass a series of tests (four out of five) to demonstrate basic knowledge of networking and security concepts, as well as basic incident response and forensics skills. Each test contains 20 questions, takes ten minutes to complete and requires a minimum score of 85%.
- Be able to commit up to ten days per year for training and exercises.
- Provide evidence of employer support.
- Successfully pass a criminal background screening process and sign a confidential disclosure agreement.[9]

In addition to signing a confidentiality agreement with the state, volunteers are provided some additional legal protections, such as "immunity from liability or claims of negligence within the scope of the MiC3 under the Government Liability for Negligence Act," and they are "further covered by a Good Samaritan clause to facilitate their work on behalf of the state."[10] In a similar vein, the state itself is "not liable to a MiC3 volunteer for personal injury or property damage suffered through participation in…MiC3 activities."[11] These parameters

were not initially formalized upon establishing the MiC3, but lawmakers were sure to include them in the provisioning of the Cyber Civilian Corps Act to make the necessary updates noticed as the program matured.

Because MiC3 members are unpaid volunteers, recruitment and retention efforts are continually being reassessed. Beyond the value gleaned from working in a critical mission area and a sense of civic duty, MiC3 offers many non-monetary benefits to its participants, including access to trainings and certifications (which are often expensive to achieve and maintain) and professional networking. Members can also point to their involvement in a unique, first-of-its-kind forum for public-private partnership in the United States. Their experience has served as a model for other state-led volunteer cybersecurity programs and contributed to expanding a culture of cybersecurity that transcends Michigan's borders.

MiC3 participants convene regularly to hone their skills, build community and collaborate. The group meets virtually each month, quarterly in-person and may be invited to attend conferences, meetings or training events on an ad hoc basis.

Operationalization

One of the key strengths of employing a coalition of trained cybersecurity civilian volunteers is flexibility. Typically, if a state has been the target of a serious cyber incident, the state's National Guard or appropriate law enforcement agency is positioned to act; however, this type of response may require the Governor to declare a formal state of emergency to initiate their deployment. As dictated by the Cyber Civilian Corps Act of 2017, the MiC3 is no longer subject to the same requirement.

For the MiC3 to be activated, a "client" organization must first make a request to the Michigan State Police, which will then relay the incident to the MiC3. Organizations in need are instructed to text a central dispatcher operated by the Michigan Cyber Command Center (MC3) and are rapidly directed to the proper channel, based on a description of the incident. This partnership between the state police, MC3 and MiC3 enables a conversation about whether a criminal investigation of the security incident is necessary and which entities need to be involved in the response and recovery process. If MiC3 involvement is agreed upon, and the targeted organization is interested in receiving free incident response services, the program manager will actively identify the appropriate team members, based on availability, location and skills, to assist in the mission.

To date, the MiC3 has been mobilized a handful of times to assist with response and recovery. The longest response effort lasted two weeks and was conducted partially remotely by MiC3 members. The thorough vetting, assessment and training process that members participate in during the recruitment and onboarding lifecycle has proven its ability to staff a team that is positioned to be successful when called upon.

Challenges

In 2016, Michigan's 21st Century Infrastructure Commission recommended that the DTMB grow the MiC3 to accommodate 200 members and invest in their training and professional development.[12] This goal was outlined in support of the modernization and security of the state's digital infrastructure and was assigned a three-to-five-year implementation timeline along with an estimated investment of $3 million in state funding annually for two years. Today, that remains a distant target, as membership sits at 61. At its peak, MiC3 membership stood at 97 total members, but dozens of inactive members were removed from the roster following an audit performed in 2019. This was a deliberate decision made by the MiC3 to build a strong foundation of highly skilled and involved professionals who could then help broaden the team's ability to recruit interested individuals by example. It is now considering opportunities to engage K-12 and collegiate partners to create a pipeline to MiC3 involvement.

The MiC3 also hopes to address the issue of attrition throughout its application process. There have been several candidates who initiate the assessment process but fail to complete all the tests. The MiC3 is currently exploring how to maintain the attention of strong applicants who complete three out of the five required tests, for example, and lower the barrier to entry, while not compromising the quality of its members.

MiC3 leadership has also underscored a need for proper documentation of its standard operating procedures to ensure consistency. Unlike many of its other state counterparts, Michigan's volunteer team is not directly or closely connected to the state's National Guard or law enforcement, which can raise concerns about volunteers interfering with evidence during a response mission, even if unintentional. While the problem has not come up in practice, it is something that the program has been trying to proactively get in front of to prevent any legal issues from arising. The formalization of its processes will—and has—provided necessary guardrails, but it also limits its ability to respond to events where it could participate and accelerate recovery.

Wisconsin's Cyber Response Teams

Program Inception and Context

In 2014, not long after the Michigan Cyber Civilian Corps (MiC3) was introduced, the State of Wisconsin identified the need to establish a cyber volunteer program of its own to defend against the evolving threat environment. Initially, a team led by the State of Wisconsin's Department of Administration (DOA), Division of Enterprise Technology (DET), in collaboration with the Department of Military Affairs (DMA) and the Wisconsin Statewide Intelligence Center, stood up the Cyber Response Team (CRT) program using DHS grant funding. For the past several years, this funding has provided the CRT a sustained average of nearly $600,000 annually to offer training and equipment to its members with the goal of improving the state's cybersecurity workforce skills and scaling up its ability to mitigate significant threats.

In 2021, the state hired a new Chief Information Security Officer whose focus was to continue to strengthen the collaborative efforts the state had in place. DET and DMA created pillars of focus around: Protection, Response, Education, Compliance and the Enablement and Transformation of Security Technologies and Processes. Its governance process remains strong with the Governor's Office, Homeland Security Council and the Homeland Security Council's Cybersecurity Subcommittee. It is because of the increasing number and complexity of cyber attacks that they are improving levels of coordination, information sharing and emergency response between state and federal agencies, local and tribal governments, critical infrastructure owners and operators as well as their out-of-state external stakeholders. Some examples of activities completed include things like supporting multiple tabletop exercises, planning and holding the Governor's Annual Cybersecurity Summit, enhancing application security, maturing cloud brokerage to evaluate risks and continuing to strengthen the state's IT tools and configurations as it looks to manage risk. As part of the expansion of coordination efforts, response responsibilities were shared between several groups. In 2022, management of the CRT operational activities for non-state entities transitioned to Wisconsin Emergency Management (WEM), a division of DMA, while DET, in coordination with state agencies and DMA, maintained overall responsibility for assisting state agencies.

The CRT mission is "to provide support for critical infrastructure in the state of Wisconsin in order to prevent, mitigate, and respond to cyber incidents through assessments, training, and incident response."[13]

At the outset, the CRT was structured to oversee regional teams and enforced quotas on how many people could be on a team per organization. However, like what Michigan had realized, the regional model has its limitations, and the CRT ended up adopting what it refers to as a "hybrid" model: one in which the teams are not sorted based on location, but individuals are often called upon based on their proximity to the incident, if it requires on-site activity.

While there are some significant distinctions between the underlying structures of the CRT and its Michigan analogue in terms of resourcing and organization, two deliberate programmatic differences stand out. First, the Wisconsin team of volunteers explicitly does not provide services to private sector entities unless they fall within the scope of the critical infrastructure sectors. The CRT's constituents are nearly exclusively SLTT government agencies, as well as school districts and public libraries. This helps mitigate any frustration or concerns of private sector companies that offer similar services about unfair competition from a no-cost provider. Second, the CRT actively advertises and provides pre-incident cybersecurity services to its constituent agencies. This often takes the form of disseminating threat intelligence among stakeholders and partners and conducting initial risk assessments so recipients can better understand their posture. While a greater share of personnel and resources have historically been dedicated to incident response activities, the CRT has been ramping up its work to encourage local entities to take advantage of the free assessments it offers, and it is currently on pace to match – or even exceed – time spent performing incident response functions.

Membership

In 2021, the CRT program was restructured to create a program to qualify incident responders and implement four response team leads. The team leads rotate for incident response, ensuring there is a primary facilitator for each mission. The idea is that general members eventually get "promoted" to incident response or assessments after they have participated in some CRT- or CISA-sponsored training and demonstrate their qualifications. Once that status has been earned, they are eligible for activation across the state.

Currently, there are 216 volunteers with the Wisconsin CRT. A substantial share of participants representing county, city and village government as well as the education sector. Sixty-two of these individuals are designated incident responders, while an additional 28 are certified for conducting assessments for constituent organizations.[14]

Members are recruited by word-of-mouth at meetings, events and conferences with partners and industry stakeholders. Notably, the CRT has been able to grow its membership so quickly because once an entity requests assistance, they are invited to participate in the CRT. Because the CRT provides expensive certification courses to its members, which is valuable to both employees and their employers, a successful marketing and recruitment tactic has been implemented. Even in instances where members only choose to participate in a SANS course and receive the accompanying certification, this outcome still moves the needle with respect to Wisconsin's goal of upskilling its workforce.

Because members receive access to the appropriate trainings once they have been admitted to the CRT and cannot be deployed as incident responders until they have attended the required training, there are no prerequisites for experience, education or certifications. Rather, for admission into the CRT as a general member, the program is moving toward requiring applicants to obtain InfraGard membership, which includes a background vetting process and adherence to various privacy and ethics policies. Wisconsin has found success in building a system for involvement that is accessible. A low barrier to entry coupled with a scalable model to progress into more hands-on roles has improved membership diversity in background and skillset, which is proven to enhance outcomes and bears broad cyber workforce implications.[15]

Operationalization

Mobilization of the CRT can take many forms. The emergency management community in Wisconsin is well positioned to assist in the request for assistance and to begin the CRT mobilization process. The request flows through the WEM duty officer system, which subsequently activates the cyber response management group (CRMG) Level 1, which consists of representatives from across the state enterprise and enables the CRT lead to effectively identify the technical needs of the customer and build out the team composition for the initial response. The affected organization and the CRT lead convene to determine a plan of action and subsequently aggregate the appropriate team of incident responders who are available, accessible and best positioned to act. The CRT lead also makes a conscious decision to include at least one incident responder who has not yet participated in a response mission, because they recognize the importance of hands-on experience in gaining confidence and skills development. The CRT has multiple leads and backup leads to provide effective support for concurrent events as various teams can be activated at once in a timely manner. Once employed, the team and its leadership conduct cybersecurity risk assessments and make recommendations to the customer on ways to strengthen its posture, provide security intelligence to industry stakeholders and carry out incident response measures. They can also provide guidance and expertise to ameliorate lower-scale cybersecurity issues that constituents may experience. This process encourages the community to call on the CRT even if the incident is considered low severity.

As is the case with the MiC3, the CRT is not obligated by the same requirements as the state's National Guard. Still, the Wisconsin National Guard frequently supplements the CRT's operational requirements on-scene. While guardsmen can often provide recommendations to aid volunteer responders, they typically are not authorized to perform physical work on a system. The DMA/WEM keeps a small cell of guardsmen as fulltime state employees; this is done by design to maintain state and federal legal authorities, as well as to facilitate effective integration in response scenarios. This affiliation within DMA and WEM provides an extra layer of expertise and protection for CRT efforts, while also contributing to volunteers' professional development. Additionally, a Title 32 or a "traditional" guardsman can be placed on state active duty under the authority of the Governor should the situation warrant the additional resources. Being positioned to leverage rapid response is helpful in the event of a significant or prolonged response

mission, allowing CRT volunteers to operate in shifts and members of the state's law enforcement and military cyber subject-matter experts to be present as enablers for the customer.

In the event that multiple organizations across the State of Wisconsin are impacted by an incident concurrently or the event may lead to physical security concerns, the CRT elevates to CRMG Level 2, which includes additional state leadership to conduct an impact analysis to understand the threat, assess state needs, and gauge the potential magnitude of an unresolved incident or delayed response.

As the CRT has matured and grown its reputation, it has formed a crucial partnership with cybersecurity insurance providers across the state. Often, when entities are hit with a cybersecurity attack, they are told to first contact their cyber insurance company. Because these companies do not necessarily reside locally and insurance requires a great deal of paperwork to be completed before they can address the issue, agencies lose valuable time to contain the damage from the attack. In Wisconsin, if the organization has cyber insurance, they are told to contact *both the insurance company and the CRT* to get the processes started simultaneously. If the incident is severe, the CRT can be mobilized to the site and assist until the digital forensics and/or incident response firm hired by the insurance company is in place.

Challenges

In general, several common complexities that stem from the planning and development of a new government program need to be considered, including the need for careful definition of the roles, responsibilities, logistics and other foundational elements of the team. While not exclusive to the CRT, these requirements must be clearly delineated to establish an effective organizational structure and chain of command, ensure funding is sustainable, establish a baseline for training that is aligned to industry standards and build the legal guardrails needed to work with non-government employees.

Maturing the CRT over time to encompass new mission areas has presented some additional difficulties. As the CRT moves to offer its constituents cybersecurity assessment opportunities, it must develop and implement a flexible recruitment strategy to target individuals who possess the relevant skillsets or may reside outside the CRT's initial network. Supporting proactive assessment capabilities is time-intensive and requires the procurement and funding of new tools and technologies. The state is also refining its messaging campaign to encourage SLTT entities to take advantage of its free assessment services and to explain the importance of understanding their weaknesses before they are exploited.

Finally, while the Wisconsin CRT has found success in its ability to recruit a wide base of members, that success has come with the challenge of finding ways to ensure members are staying engaged with the team. Delivering valuable training and networking opportunities to volunteers through hands-on training can contribute to stronger recruitment and productive retention outcomes. Leveraging these incentives is foundational to many similar programs.

Ohio Cyber Reserve

Program Inception and Context

With the MiC3 and CRT as predecessors, a similar function, the Ohio Cyber Reserve (OhCR), was signed into law by Governor Mike DeWine on October 25, 2019, via Ohio Senate Bill Number 52 (S.B. 52).[16] It was the result of an evaluation of the cybersecurity workforce and the realization that legislators needed to leverage more talent in the state. It was agreed that Ohio's cyber experts were stretched too thin, and its smaller government entities and critical infrastructure firms lacked sufficient resources and expertise to combat cyber threats.[17] Attracting and organizing volunteers to operate in this capacity was a way to address this gap economically and sustainably.[18] The OhCR took effect 90 days after it was signed into law, on January 23, 2020.

The Ohio National Guard, overseen by the Adjutant General, formed the Ohio Cyber Collaboration Committee (OC3) to create an enterprise-wide approach to cybersecurity that prioritizes collaboration between key players across the state.[19] The OhCR is one of the primary initiatives established as part of the OC3, addressing the following three mission areas:

1. Providing outreach, training, education and security assessments to reduce cyber vulnerability and increase resiliency;
2. Assisting K-12 education efforts to support cyber clubs and student mentorship and
3. Responding to cyber incidents at eligible governmental and critical infrastructure entities.[20]

Per its website, "OhCR teams of trained civilians [are] available for the governor to assist eligible municipalities with cybersecurity vulnerabilities and provide recommendations to reduce cyber threats."[21] The intended recipients of these services include agencies representing the state's townships, villages and small cities and counties as well as small utilities and emergency service providers, elections bodies and qualifying nonprofit organizations.[22] OhCR volunteers will "also provide workforce development to train the cyber talent of the future and assist STEM teachers by providing mentors for high school cyber clubs."[23]

The OhCR's placement under the state's National Guard is one of the primary differences from the Michigan and Wisconsin models. This was done purposefully; this governance structure, modeled after the Ohio Military Reserve Ohio Revised Code Chapter 5920, facilitated introduction of the OhCR and its passage into law as it was explained alongside a familiar system.[24] Proponents worked within the existing framework and demilitarized the reserve forces' language, making the concept of a group of civilian cybersecurity responders more palatable and realistic. Establishing the Ohio National Guard as the OhCR's parent organization not only served to build more trust in a new program but also drastically reduced overhead costs and afforded members legal protections by treating them as state active duty members, which confers authority to take temporary leave from their full-time jobs.

Membership

OhCR membership is a competitive process; to be considered, candidates must meet the following criteria:

- Be a U.S. citizen or legal permanent resident (who has not been expelled or dishonorably discharged from the Armed Forces).
- Live in Ohio.
- Pass a background check.
- Be considered a subject matter expert (or nearly a subject matter expert) within a cybersecurity discipline. The OhCR benchmarks cybersecurity expertise at about five years of relevant experience.
- Undergo and documents and certification review attesting their cybersecurity knowledge and skillset.
- Complete and pass an administered SANS test.
- Sign and adhere to relevant legal policies and procedures, including a non-disclosure agreement and code of conduct and ethics.[25]

Unlike the programs in Michigan and Wisconsin, qualified members of the OhCR are divided into ten regional teams across the state, which is meant to expedite deployment when a cyber incident occurs. Each team is comprised of members filling the following roles:

- Team Manager,
- Deputy Team Manager,
- System Administrator,
- Network Administrator,
- Technical Support,
- Forensics Technician,
- Intrusion Detection,
- End Point Analyst and
- Information Analyst.

The program budget supports at least two ten-person teams per region, but the OhCR is actively working to increase the size of its teams to accommodate twenty individuals, adapting to growing needs and interest. This move not only accommodates the state's professional development goals in cybersecurity, but it offers an added layer of security in the event volunteers are unavailable to serve on a mission when requested. As of June 2022, the OhCR is overseeing 80 members in three regional teams, more than 50 of whom are trained to perform at least one of the three missions.[26]

Admitted members are then outfitted with equipment and security credentials on behalf of the state and are expected to conduct their work in Ohio National Guard readiness centers.[27] Similar to the MiC3 and CRT, volunteers are provided access to ongoing training

to develop their cybersecurity skillsets and prepare them for the likelihood of mission response activities.

Ohio has also noticed that its active volunteers are intrinsically motivated to join and participate in the OhCR because they have a shared enthusiasm for volunteer work and particularly enjoy opportunities to work with and mentor young people to instill a culture of cybersecurity. This is a commonly shared experience among the volunteer cyber teams in Michigan, Wisconsin and Ohio, and program leadership often notes that members of the cybersecurity community are tightknit and enjoy collaborating with and learning from their colleagues.

Operationalization

Though the OhCR is considered a volunteer force, members are eligible for monetary compensation, if and when they are mobilized for incident response efforts (reviewing the three mission areas outlined previously, the first two mission activities are unpaid, while the third results in payment in an amount equivalent to the civilian General Schedule pay scale). While in a training status, before they are cleared to participate in an incident response mission, OhCR volunteers: 1) work to obtain the necessary certifications and clearances; 2) provide outreach, assistance and assessments to recipient organizations and entities and 3) support K-12 educational objectives and mentor students.

Distinct from the MiC3 and CRT, incident response services by the OhCR still require the Governor's activation. This limits the number of missions the volunteer team has undertaken, which stands at two today. The first time the OhCR was elevated to state active duty was 16 months after the passage of S.B. 52, in February 2021, to assist an undisclosed government agency by mitigating the consequences of a ransomware attack.[28] In this instance, a single OhCR member was selected (based on his expertise in the affected network equipment) to work alongside the Ohio National Guard and to operate remotely for four days, successfully restoring the network.[29] The OhCR also performed a response mission in early 2022, which lasted several weeks, with six members.

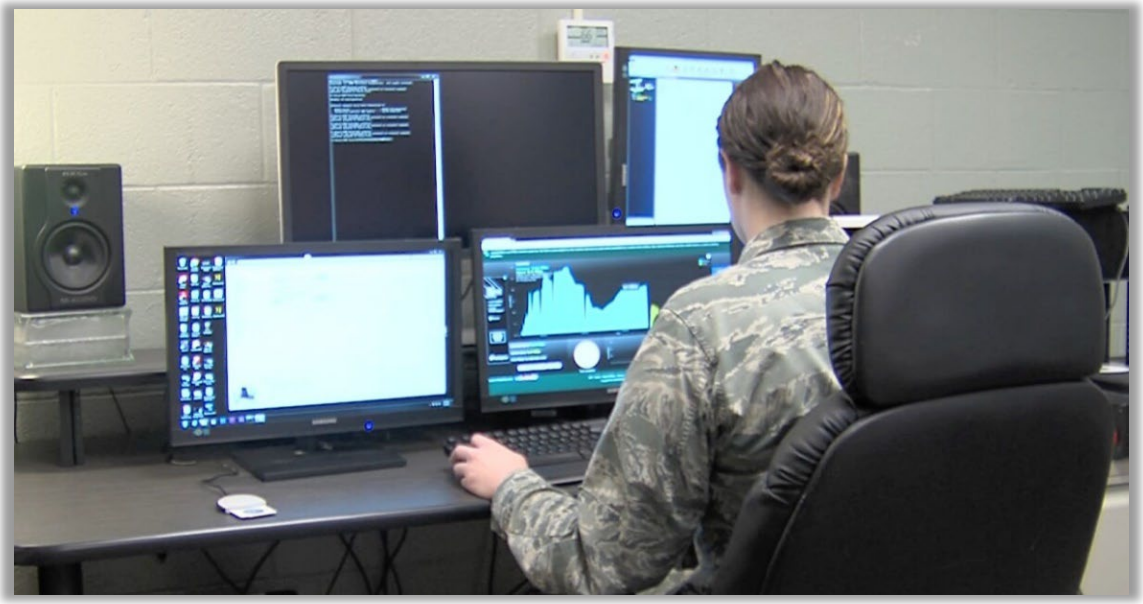
As part of the OC3's larger lines of effort, the OhCR has mentored local high school students, supported the Skills USA Competition held in Columbus, Ohio, helped write the OC3 best practices website and is assisting the Ohio Cyber Range Institute in the development and execution of a pilot red-on-blue cyber exercise in mid-2022. The OhCR has also performed a number of assist missions during which it reviews and assesses local entities' best practices.

Challenges

Because the OhCR is bolstered by the state's National Guard rules and regulations, the greatest setback noted by program leadership has been the administrative burdens associated with completing paperwork ahead of a member's first response mission. Fortunately, this is a one-time challenge (per volunteer) and does not impact the team's ability to help an organization effectively respond and recover from an incident.

As the OhCR approaches its three-year anniversary, it is experiencing tactical challenges concerning expansion into its more proactive mission areas. Its ability to support its outreach and technical assistance work (mission space one) has proven difficult because the organizations it services are less knowledgeable about cybersecurity fundamentals than anticipated. This means that conducting risk assessments and providing recommendations for the remediation of noted vulnerabilities must be preceded by introductory cybersecurity information sessions. To resolve these concerns and cut back on the time commitment asked of volunteers, the OhCR has begun exploring the potential for partnerships with local colleges and universities that are equipped to host "cybersecurity 101" courses aimed at educating SLTT government employees.

The regional model of the OhCR presents an additional recruitment-related challenge as more populous, industry-heavy regions are able to draw more volunteers. This means they also present more opportunities for vulnerabilities to be exploited and organizations to be negatively impacted. Conversely, more rural or resource-constrained regions in Ohio may be easier targets for malicious attackers, because their cybersecurity infrastructure is less robust and access to timely incident response functions may be more difficult to achieve. This dichotomy is not unique to Ohio but it represents a need to balance recruitment and training efforts across the state, which is a factor that is widely discussed when considering cybersecurity workforce gaps across the country.

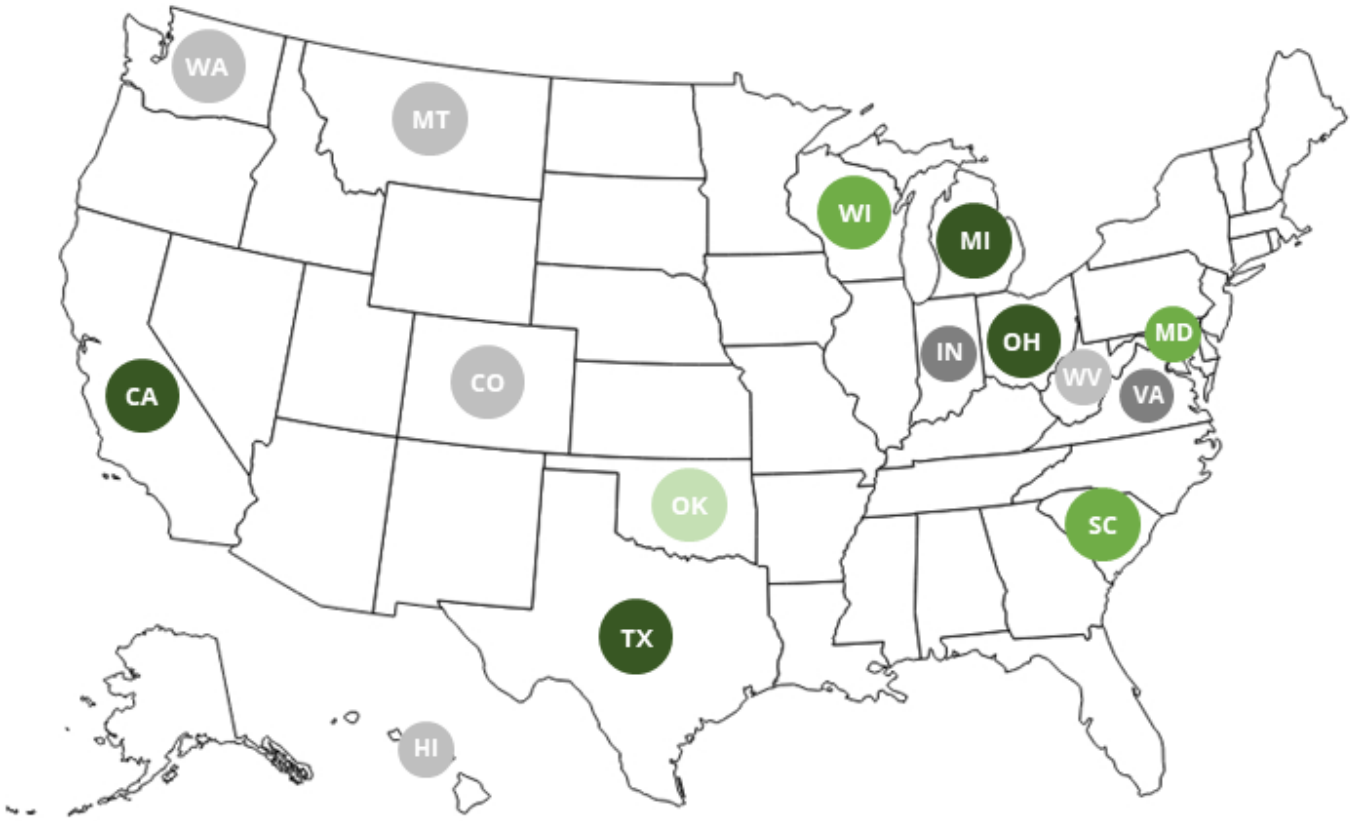


Comparison Matrix

		MiC3	CRT	OhCR
STRUCTURE	Date Established	2013	2014	January 23, 2020
	Umbrella Organization	Department of Technology, Management and Budget	Wisconsin Emergency Management	Adjutant General's Department
	Membership Size	61	216	Currently 100 (target of 200)
	Team(s)	Centralized	Centralized	Regional
	Budget	Estimated $250,000 - $400,000 per year	Around $600,000 per year	$750,000 per year for FY22 and FY23
MEMBERSHIP REQUIREMENTS	Residency	Yes	No specific requirement	Yes
	Background Check	Yes	Yes	Yes
	Years of Relevant Experience	2	No specific requirement	~5
	Cybersecurity Certification(s)	Yes – must possess 1	No	No
	Assessment Process	Must pass a series of tests (4 out of 5)	Not required for entry, but must pass to participate in incident response	Yes – SANS test
	Location Considerations	Proximity to regional team	No specific requirement	Proximity to regional team
	Availability	10 days per year for training and exercises	No specific requirement	No specific requirement
MISSION AREAS	Proactive Risk Assessments	No	Yes	Yes
	Threat Intelligence Sharing	No	Yes	Yes
	Education and Training (for Constituent Organizations)	No	Yes	Yes
	Student Mentorship	Yes (not formalized)	No	Yes
	Incident Response and Recovery	Yes	Yes	Yes

Emerging State Cyber Volunteer Programs

Several states find themselves in various stages of implementation of their own team of civilian cyber volunteer responders. In addition to the MiC3, CRT and OhCR, states that have taken more substantial action to progress their cybersecurity positioning and develop their cyber workforce are indicated on the map below.



Lessons from the Field and Recommendations

An analysis of the Michigan, Wisconsin and Ohio civilian cybersecurity response programs has revealed some overarching themes. With these in mind, the following recommendations can provide some baseline guidance for establishing a statewide volunteer cybersecurity team. Each state has a distinct makeup, and it should be noted that these suggestions are not one-size-fits-all. Rather, they should be applied within the broader framework of the state's governance structure, geographical constraints, budgetary limitations and regional market and workforce trends.

1. **Begin by assessing the state's cybersecurity posture** to identify gaps in capability. This should encompass the state's ability to prevent, respond to and recover from a cyber incident with varying impacts quickly and effectively. This initial step will often involve reviewing the existing statewide cybersecurity strategic plan and evaluating where progress has been made and where it has been lacking. Taking inventory of tools and equipment, studying SLTT government agencies' cyber and IT team resources and understanding SLTT government employees' knowledge of cybersecurity best practices is key to supporting a case for allocating resources to a team of volunteer cyber responders.

2. **To ease administrative, financial and legislative burdens**, house the volunteer cybersecurity team under a governing agency that is already dedicated to the state's cybersecurity response capacity. This will reduce overhead costs associated with establishing a new organization, provide flexibility needed to scope the program's capacity throughout the early stages of launch, improve access to the tools and technology the cyber volunteers will need to use for training and response purposes and facilitate buy-in from government decisionmakers.

3. **Create a plan for how this volunteer group will function** within the state's cybersecurity and emergency response ecosystems. Envision what activation of this force will look like in various circumstances (to account for different types of cyberattacks, their magnitude, diverse locations around the state, etc.), and use this to inform where this group fits into the chain of command and information-sharing procedures. Tabletop exercises with key players are critical to gaining familiarity with the response plan and making the necessary adjustments for success. It is also recommended to consider merging Incident Command System principles and terminology with the state's cybersecurity tactical operations to mitigate confusion and facilitate response and recovery efforts.

4. **Establish a task force** composed of public, private, nonprofit and academic stakeholders to inform policy considerations that account for key players' interests, concerns and independent assessments. A comprehensive task force will include the perspectives of the state's critical infrastructure sectors as well as the likely recipients of the volunteer response services and the industry and academic partners from which volunteers are most likely to be sourced.

5. **Consider the entirety of the cybersecurity lifecycle** (encompassing prevention, protection, mitigation, response and recovery activities) when offering services to constituents. Develop a plan for gradually augmenting capabilities over time that are aligned with growth projections and resourcing limitations (i.e., what can be supplied at the lowest cost while also delivering the greatest benefit?).

6. **Form partnerships** with training providers, cyber ranges, academic institutions and nonprofits to engage the local community and ease the responsibilities of civilian cyber volunteers. Opportunities for collaboration can help deliver results to organizations more quickly and efficiently before, during or after a cyber incident occurs and also eliminate the need for volunteers to spend time educating system users from ground zero. It can also yield significant returns in terms of education and workforce development objectives.

7. **Develop and execute a strategy** for recruitment and retention that focuses on addressing gaps in the cyber workforce. Expand outreach to underrepresented communities and leverage diverse networks across the state to build meaningful partnerships and encourage their involvement with the volunteer cyber response team. Reflect on what has typically barred these individuals from participating in such groups and consider how incentives for membership can be realigned. For instance, college students may be highly motivated to participate on a volunteer cyber team to earn course credit or certifications that will prove invaluable to their entrance into the labor market.

8. **It is a best practice to document** standard operating procedures and the policies and regulations associated with working with various groups during incident recovery. It is also important to create guidance for leadership and volunteers, where possible. This documentation will help to ensure consistency in response efforts and service delivery among members, create guardrails to limit liability concerns and support succession planning within the organization.

9. **Collect both qualitative and quantitative data** to evaluate continually the impacts of the civilian cyber volunteer team's work and optimize processes moving forward. This can help identify trends in workforce development, government-wide and industry-specific cybersecurity challenges and security advancements to support adjustments like reallocating resources over time, reorganizing the team and its leadership and advocating for increased funding. These metrics can also provide insights to improve recruitment, retention and communications strategies as needed.

Conclusion

The United States has a long history of volunteer support in emergency management. States, however, are paving the way for a resourceful approach to incident response that embraces the increasing importance of cybersecurity. Michigan's MiC3, Wisconsin's CRT and Ohio's Cyber Reserve have found unique ways to leverage the skills and knowledge of cybersecurity practitioners to improve outcomes across SLTT organizations, the cybersecurity workforce and the general public. Their experiences can provide "lessons learned," as well as a benchmark for similar programs that are being planned or launched across the country.

The National Governors Association would like to thank the state officials and experts from Michigan, Wisconsin and Ohio for their guidance and involvement in developing this publication.

If your state is interested in standing up a similar function or would like to explore what such a program might look like, please contact Casey Dolen, Senior Cybersecurity Policy Analyst, at cdolen@nga.org, or email cyber@nga.org. Our team at the National Governors Association is eager to provide you with the resources and assistance you need.

Bibliography

Beougher, Stephanie. "Ohio Cyber Reserve member deployed in cybersecurity response." *The Ohio Adjutant General's Department*, February 18, 2021. https://ong.ohio.gov/stories/2021/feb/20210218-ocr-deployment.html.

Beougher, Stephanie. "Ohio Cyber Reserve members train to assist with cybersecurity issues." *The Ohio Adjutant General's Department*, November 29, 2021. https://ong.ohio.gov/stories/2021/nov/20211129-ohcr-training.html.

DHS.gov. House of Representatives. 107th Congress (2001-2003). Public Law 107-296 – *Homeland Security Act of 2022*. Enacted on November 25, 2022. https://www.dhs.gov/sites/default/files/publications/hr_5005_enr.pdf.

General Assembly of the State of Ohio. Senate. *S.B. No. 52*. 133rd General Assembly, Regular Session 2019-2020. https://search-prod.lis.state.oh.us/solarapi/v1/general_assembly_133/bills/sb52/IN/00?format=pdf.

GIS Open Data. "Michigan Prosperity Regions." https://gis-michigan.opendata.arcgis.com/datasets/ae387365c550430ebbdc2c54b839030d/explore?location=44.618175%2C-86.313400%2C6.00.

Herras, Ray, Jack Janson, Takayuki Miyazaki, Marie Natsvlishvili, Shenhav Ruttner, and Yushan Xu. "Helping Cities Respond When A Cyber-Attack Strikes: Leveraging Cyber and Technology Professionals as Volunteers During a Response." *Columbia School of International and Public Affairs* (May 2020). https://www.sipa.columbia.edu/academics/capstone-projects/helping-cities-respond-when-cyber-attack-strikes.

(ISC)² 2021 Cybersecurity Workforce Study, 2021. "A Resilient Cybersecurity Profession Charts the Path Forward." https://www.isc2.org//-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx.

Lachow, Irving. "Equity and Diversity in the Nation's Cyber Workforce: Policy Recommendations for Addressing Data Gaps. *Center for Strategic & International Studies* (April 2022). https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/220405_Lachow_Cyber_Equity.pdf?0bZKVinRnTdtukT4P0uVKNDAbuGoQvPc.

Michigan Department of Technology, Management & Budget. "Michigan Cyber Civilian Corps (MiC3)." https://www.michigan.gov/dtmb/services/cybersecurity/michigan-cyber-civilian-corps-mic3.

Michigan Legislature. Senate. *Cyber Civilian Corps Act*. Act 132 of 2017. Effective January 24, 2018. https://www.legislature.mi.gov/documents/mcl/pdf/mcl-Act-132-of-2017.pdf.

Ohio Adjutant General's Department. "Ohio Gov. Mike DeWine signs cyber reserve legislation. News release," October 25, 2019. https://ong.ohio.gov/press-releases/2019/20191025-log29.pdf.

The Ohio Adjutant General's Department. "Ohio Cyber Reserve (OhCR)." https://www.ong.ohio.gov/special-units/cyber/ohcr/index.html.

"Ohio Cyber Collaboration Committee (OC3)." 2019. https://homelandsecurity.ohio.gov/op3_files/2019/oc3.pdf.

"The Ohio Cyber Reserve: Bringing Cyber Talent to the Fight." Slideshow Presentation. May 5, 2022.

Pattison-Gordon, Jule. "What Makes a State Volunteer Cybersecurity Program Work?" *Government Technology*, June 14, 2021. https://www.govtech.com/security/what-makes-a-state-volunteer-cybersecurity-program-work.

Ruiz, Monica M. "Is Estonia's Approach to Cyber Defense Feasible in the United States?" *War on the Rocks*, January 9, 2018. https://warontherocks.com/2018/01/estonias-approach-cyber-defense-feasible-united-states/.

State of Wisconsin Division of Enterprise Technology. "Cyber Response Team Program (CRT)." https://det.wi.gov/Pages/Cyber-Response-Teams.aspx.

Wisconsin Department of Administration. "WISCONSIN CRT CYBER RESPONSE TEAM PROGRAM." Slideshow Presentation. April 18, 2022.

21st Century Infrastructure Commission. "21st Century Infrastructure Commission Report." November 30, 2016. https://www.michigan.gov/documents/snyder/21st_Century_Infrastructure_Commission_Report_555079_7.pdf.

Congress.gov. Senate – Homeland Security and Governmental Affairs. 117th Congress (2021-2023). *S.1324 – Civilian Cybersecurity Reserve Act*. Introduced in Senate April 22, 2021. https://www.congress.gov/bill/117th-congress/senate-bill/1324.

Endnotes

[1] (ISC)² 2021 Cybersecurity Workforce Study, 2021, "A Resilient Cybersecurity Profession Charts the Path Forward," https://www.isc2.org//-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx.
[2] DHS.gov, House of Representatives, 107th Congress (2001-2003), Public Law 107-296 – *Homeland Security Act of 2022*, Enacted on November 25, 2022, https://www.dhs.gov/sites/default/files/publications/hr_5005_enr.pdf.
[3] Ruiz, Monica M., "Is Estonia's Approach to Cyber Defense Feasible in the United States?" *War on the Rocks*, January 9, 2018, https://warontherocks.com/2018/01/estonias-approach-cyber-defense-feasible-united-states/.
[4] Congress.gov, Senate – Homeland Security and Governmental Affairs, 117th Congress (2021-2023), *S.1324 – Civilian Cybersecurity Reserve Act*, Introduced in Senate April 22, 2021, https://www.congress.gov/bill/117th-congress/senate-bill/1324.
[5] Michigan Department of Technology, Management & Budget, "Michigan Cyber Civilian Corps (MiC3)," https://www.michigan.gov/dtmb/services/cybersecurity/michigan-cyber-civilian-corps-mic3.
[6] GIS Open Data, "Michigan Prosperity Regions," https://gis-michigan.opendata.arcgis.com/datasets/ae387365c550430ebbdc2c54b839030d/explore?location=44.618175%2C-86.313400%2C6.00.
[7] Michigan Legislature, Senate, *Cyber Civilian Corps Act*, Act 132 of 2017, Effective January 24, 2018, https://www.legislature.mi.gov/documents/mcl/pdf/mcl-Act-132-of-2017.pdf.
[8] Pattison-Gordon, Jule, "What Makes a State Volunteer Cybersecurity Program Work?" *Government Technology*, June 14, 2021, https://www.govtech.com/security/what-makes-a-state-volunteer-cybersecurity-program-work.
[9] Michigan Department of Technology, Management & Budget, "Michigan Cyber Civilian Corps (MiC3)."
[10] Herras, Ray, Jack Janson, Takayuki Miyazaki, Marie Natsvlishvili, Shenhav Ruttner, and Yushan Xu, "Helping Cities Respond When A Cyber-Attack Strikes: Leveraging Cyber and Technology Professionals as Volunteers During a Response," *Columbia School of International and Public Affairs* (May 2020), https://www.sipa.columbia.edu/academics/capstone-projects/helping-cities-respond-when-cyber-attack-strikes.
[11] Ibid.
[12] 21st Century Infrastructure Commission, "21st Century Infrastructure Commission Report," November 30, 2016, https://www.michigan.gov/documents/snyder/21st_Century_Infrastructure_Commission_Report_555079_7.pdf.
[13] State of Wisconsin Division of Enterprise Technology, "Cyber Response Team Program (CRT)," https://det.wi.gov/Pages/Cyber-Response-Teams.aspx.
[14] Wisconsin Department of Administration, "WISCONSIN CRT CYBER RESPONSE TEAM PROGRAM," Slideshow Presentation, April 18, 2022.
[15] Lachow, Irving, "Equity and Diversity in the Nation's Cyber Workforce: Policy Recommendations for Addressing Data Gaps, *Center for Strategic & International Studies* (April 2022), https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/220405_Lachow_Cyber_Equity.pdf?0bZKVinRnTdtukT4P0uVKNDAbuGoQvPc.

[16] General Assembly of the State of Ohio, Senate. *S.B. No. 52*, 133rd General Assembly, Regular Session 2019-2020, https://search-prod.lis.state.oh.us/solarapi/v1/general_assembly_133/bills/sb52/IN/00?format=pdf.
[17] "Ohio Cyber Collaboration Committee (OC3)," 2019, https://homelandsecurity.ohio.gov/op3_files/2019/oc3.pdf.
[18] "The Ohio Cyber Reserve: Bringing Cyber Talent to the Fight," Slideshow Presentation, May 5, 2022.
[19] "Ohio Cyber Collaboration Committee (OC3)."
[20] "The Ohio Cyber Reserve: Bringing Cyber Talent to the Fight."
[21] The Ohio Adjutant General's Department, "Ohio Cyber Reserve (OhCR)," https://www.ong.ohio.gov/special-units/cyber/ohcr/index.html.
[22] "The Ohio Cyber Reserve: Bringing Cyber Talent to the Fight."
[23] The Ohio Adjutant General's Department, "Ohio Cyber Reserve (OhCR)."
[24] "The Ohio Cyber Reserve: Bringing Cyber Talent to the Fight."
[25] General Assembly of the State of Ohio. Senate. *S.B. No. 52*.
[26] Beougher, Stephanie, "Ohio Cyber Reserve members train to assist with cybersecurity issues," *The Ohio Adjutant General's Department*, November 29, 2021, https://ong.ohio.gov/stories/2021/nov/20211129-ohcr-training.html.
[27] Ohio Adjutant General's Department, "Ohio Gov. Mike DeWine signs cyber reserve legislation, News release," October 25, 2019, https://ong.ohio.gov/press-releases/2019/20191025-log29.pdf.
[28] Beougher, Stephanie, "Ohio Cyber Reserve member deployed in cybersecurity response," *The Ohio Adjutant General's Department*, February 18, 2021, https://ong.ohio.gov/stories/2021/feb/20210218-ocr-deployment.html.
[29] Ibid.