State Notes

TOPICS OF LEGISLATIVE INTEREST

Spring 2022

Cybersecurity Through Collaboration

By Elizabeth Raczkowski, Fiscal Analyst

Cyberattacks and threats of electronic extortion, sabotage, and theft against state and local governments have steadily increased in recent years.[1] Previously sporadic assaults have become more organized and systematic, posing a serious threat to public entities rich in sensitive data but low on the funding needed to keep up with the latest cybersecurity measures. To address this challenge, some states have created programs to facilitate collaboration among many groups, including state, local, and federal government entities, private individuals and companies, and nonprofit organizations.

Challenges Facing Governments

Ransomware and other forms of cyberattacks against state and local governments and agencies have increased substantially in the past decade, with hundreds of cases reported since 2019.[2] Ransomware attacks are those in which entities are blocked from using their systems or accessing files until they pay a ransom (thus the name) or perform a demanded action. State and local governments are particularly attractive targets for this type of attack.[3] In addition to their own internal information, they frequently possess large amounts of sensitive data pertaining to their residents, including Social Security numbers and financial details.[4]

Budgetary constraints limit the ability of state, and particularly local, governments to invest in technological upgrades, cybersecurity measures, and employee training.[5] Information technology (IT) staffing itself often is limited because of financial concerns, including competition with the private sector or large institutions that can offer greater financial incentives. A government outage is a significant attraction to hackers because of the large number of people affected. A high level of disruption is likely to create greater public pressure to resolve the issue and expedite payment of the ransom.

State-Local Collaboration

Collaboration between states and local units of government on cybersecurity issues is part of a "unified defense" strategy against these increased threats.[6] According to the National League of Cities, 36 states require that municipalities report cybersecurity data breaches to their state government. Michigan has no such requirement, although local governments must notify affected individuals.[7] In addition to the financial and staffing challenges noted earlier, low inter-communication levels and policy silos can result in missed opportunities to guard against cyberattacks, even within the same county, city, or township.[8] A security deficit might appear in one department's software, for example, but if this information is simply dealt with on the surface but not shared with other offices that rely on the same or similar systems in the network, a government could miss an opportunity to spot an ongoing weakness in its system. Similarly, two departments might be dealing with the same security issue, but if there is no communication, then each may use time and resources trying to resolve the same problem on its own.

To combat these obstacles, governments and groups like the National Governors Association and the National League of Cities have begun to advocate for increased and ongoing collaboration. The Governors Association has an online resource center with memos, guides, and potential assistance for state governments. In 2020, the National League of Cities produced a state-by-state report on state and local cybersecurity partnerships.[9] This report highlighted differences among states and offered some case studies as a guide to officials looking to learn more about how to develop such collaborations.

Michigan's Core Cyber Assistance Programs

Michigan funds two programs specifically aimed at increasing state, local, and private collaboration: Michigan Cyber Partners and the Michigan Civilian Cyber Corps (known as MiC3). Both are housed within the Department of Technology, Management, and Budget (DTMB).

Michigan Cyber Partners

History

The Department of Technology, Management, and Budget developed Michigan Cyber Partners from the former CISO-as-a-Service program (CISO is an acronym for Chief Information Security Officer). The CISO-as-a-Service program began in 2017 as an 18-month-long pilot in which a cybersecurity professional assisted 13 local governments with cybersecurity issues.[10] The program was redesigned and relaunched under its current name in 2019.

Purpose and Current Status

Cyber Partners is meant to connect private cybersecurity experts with local governments. The staff of cities, counties, tribes, and other qualifying groups and organizations may join Cyber Partners at no cost. They then can obtain access to expertise that otherwise would be prohibitively expensive or difficult to obtain. The program allows employees to receive the latest cybersecurity updates via email, attend monthly webinars, draw on private and governmental expertise, and more easily access technology assessments and recommendations.

The program allows a local public entity to contract with independent vendors for a year at a time, during which the vendor conducts assessments and assists the entity with improving its cybersecurity practices. The program hosts monthly online meetings for participants to share news and updates related to cybersecurity.

As of January 2022, 10 vendors have been reviewed and approved by the program through a request-for-proposal process. Each received a MiDEAL contract through January 2026. The MiDEAL program allows local governments, schools, universities, and colleges to buy products

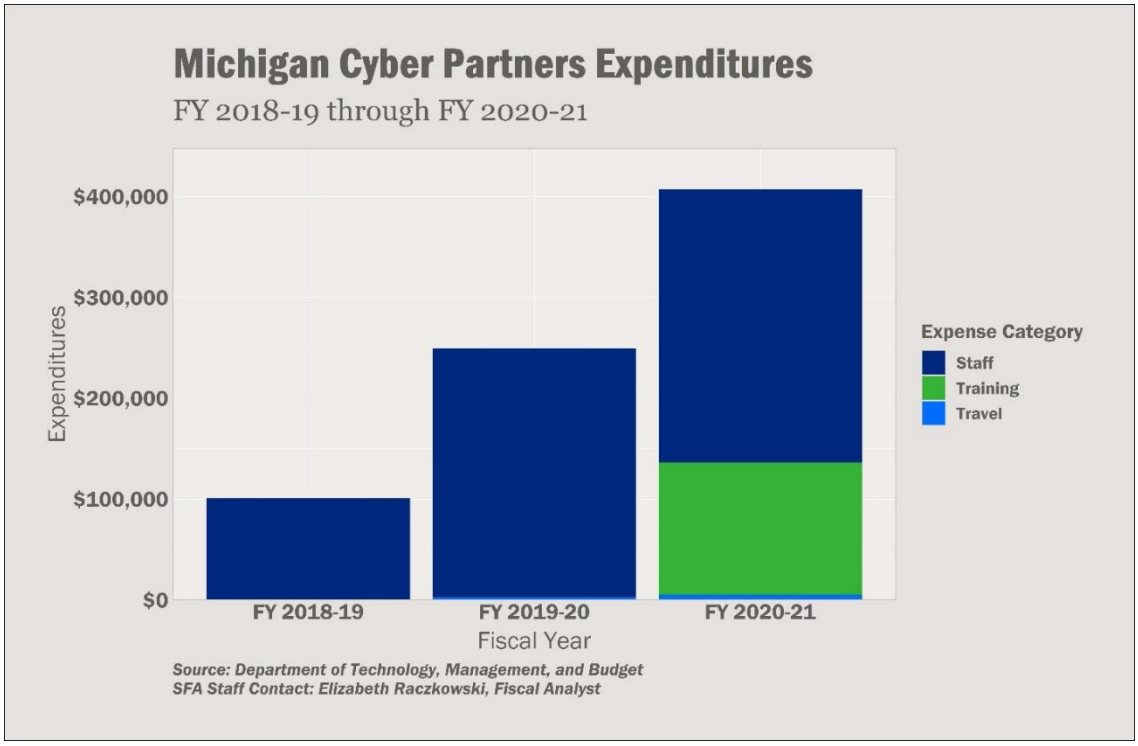
or services through State contracts; Cyber Partners' participation allows locals and schools to more easily contract with vendors. This often allows those entities to save money compared to if they had sought a contract independently. Seven of these vendors are based in Michigan. Core-fixed pricing is based on the size of the entity measured in terms of the number of computers used. This pricing means that the vendor will charge the client (e.g., a county government) a price that will not exceed an amount specified in the vendor contract.

Program staff report that its partnerships are primarily with local governments and schools, and that hundreds of employees have signed up to the program email list. Over 400 information technology staff from local governments and K-12 schools were trained in best practices in 2021 and DTMB officials reported an average attendance of about 100 individuals at monthly meetings.

Funding

Funding for the Michigan Cyber Partners program, exclusive of Federal dollars, is from the State's General Fund/General Purpose (GF/GP) revenue. As seen in Table 1, most funding is spent on program staff. A Federal Department of Homeland Security (DHS) Grant Program provided funding for training in computer information systems totaling $131,000 in fiscal year (FY) 2020-21. Annual funding, excluding the DHS grant, averaged about $209,000 from FY 2018-19 to FY 2020-21.

Table 1



Michigan Cyber Corps (MiC3)

History

According to a National Governor's Association memo, the MiC3 began as a volunteer program associated with the DTMB and the Merit Network, a nonprofit organization founded by Michigan State University, the University of Michigan, and Wayne State University. Governor Rick Snyder's purpose was to encourage qualified volunteers with cybersecurity knowledge to make themselves available for consultation or assistance should the State experience a cybersecurity incident.[11] Full operations by the State began in 2016. The Civilian Cyber Corps was officially established under Public Act (PA) 132 of 2017.

Rather than focusing on connecting local governments and their employees with cybersecurity resources as in the Cyber Partners program, the MiC3 program allows volunteers with expertise in cybersecurity to be called upon when the State or local government entities are facing an emergency. These volunteers must pass an exam, adhere to certain restrictions, and make themselves available for training and other events. In return, they receive training opportunities and the chance to assist governments in times of crisis.

Michigan Cyber Corps is open to experts in cybersecurity and is designed to create a network of "mutual aid to all levels of government, education, and business organizations" in Michigan.[12] While similar to Cyber Partners, MiC3 specifically promotes the involvement of individuals outside of government and focuses on emergency response rather than preparedness. The DTMB also may appoint volunteers if needed.

The Civilian Cyber Corps Act

Public Act 132 of 2017, the Civilian Cyber Corps Act, established the program in statute. It allows the DTMB to contract with individuals who agree to serve as volunteers. The Act also provides immunity from tort liability under certain circumstances and establishes immunity for the State for the actions of volunteers.

In addition to a report on the current condition of the entity's cybersecurity, an assessment may include improvement plans and limited monthly consultations. Another core service is the end-of-the-year assessment update, which the DTMB states, "identifies progress made towards improving priority items identified in initial assessment and items remaining to be addressed", allowing the entity to make plans and considerations for future improvements.

Volunteers may have access to sensitive information and systems as well as secured systems if participating in a cyber incident response. Thus, PA 132 requires that the Department of State Police (MSP) perform a criminal history and records check on all volunteers accepted into the MiC3 program. If an individual's fingerprint matches a criminal arrest fingerprint, the MSP is responsible for informing the DTMB whether the person is cleared or is not eligible to participate.

Contracts with cyber volunteers must contain confidentiality clauses and require these individuals to avoid conflicts of interest related to their activities and to comply with security procedures established by DTMB.

2019 Auditor General Findings and Recent Actions

A 2019 audit report of MiC3 by the Michigan Office of the Auditor General identified two issues related to volunteer accountability.[13] The first finding was that not all volunteers were sufficiently qualified and that the required background checks on volunteers were incomplete for a little over one-third of the participants. Another 2.0% had failed their background checks but were allowed to participate. Other qualification-related deficiencies also were identified. It should be noted that the Merit Network, and not the DTMB, administered this program prior to the enactment of PA 132.

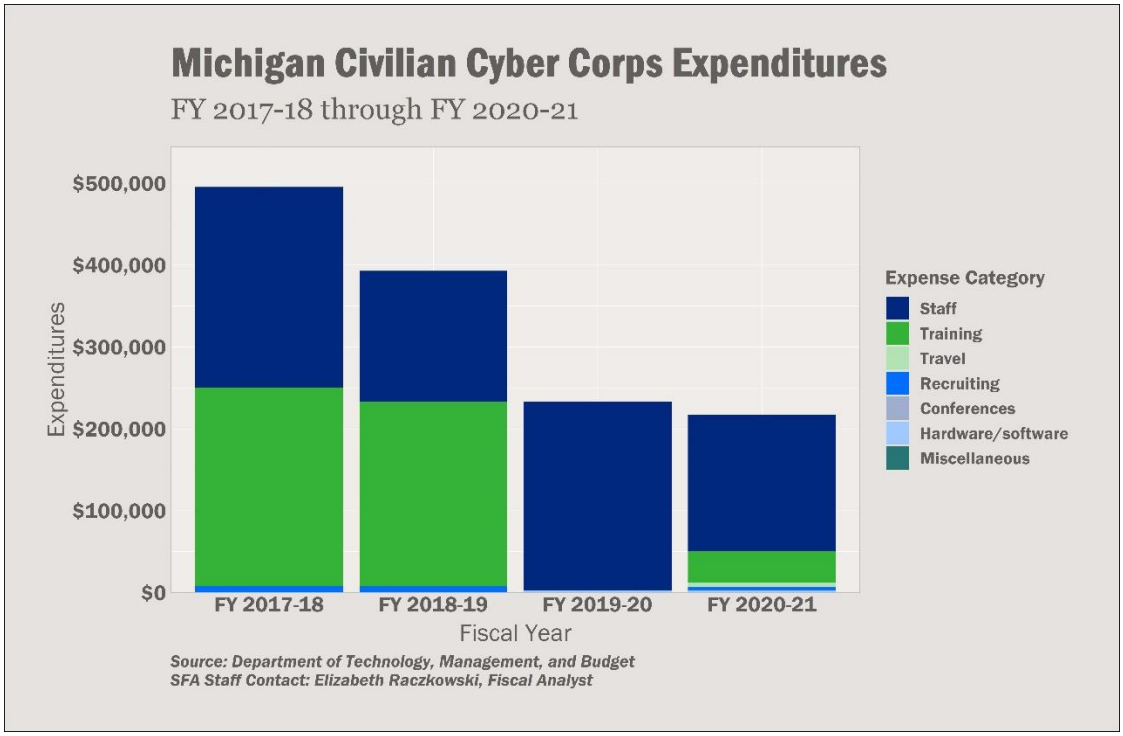
Partly in response to the audit findings, the program now has a multi-step application process to ensure that every volunteer is qualified. The process moves in stages, so that an applicant must complete one step before progressing into the next, thus ensuring that each test or qualifying characteristic is evaluated.

As of January 2022, the Civilian Cyber Corps had over 60 active members, an increase from about two dozen at the time of the transition to DTMB leadership. Membership levels have been somewhat decreased by the COVID-19 pandemic, but the Department expects those levels to increase as in-person operations return.

Funding

When PA 132 was enacted, the Senate and House Fiscal Agencies estimated that the program would have little fiscal impact on the DTMB, as the costs could be absorbed by existing appropriations. For FYs 2017-18 through 2019-20, expenditures averaged about $276,500 per fiscal year. Planned expenditures for FY 2020-21 totaled $297,366. Most of the annual expenditures have been related to staffing costs and training.

Table 2



Cybersecurity Collaboration in Nearby States

Several states geographically close to Michigan have programs similarly aimed at allowing state and local entities to receive assistance or training from cybersecurity experts, but none take the same form as Michigan's programs:

Indiana

Under Indiana law, state agencies and local units of governments are required to report cyberattacks to the Indiana Office of Technology within two business days.[14] The Indiana Executive Council on Cybersecurity was created in 2017 via an executive order to create an interdisciplinary team focused on cybersecurity improvement in the state. State, local, and Federal government representatives are on the Council, as are representatives from the private sector, the military, and academia. There are nearly 200 members as of 2021, but only 25 are official voting members, with the majority serving as advisory members or contributors. The Council submitted a strategic cybersecurity plan in 2018, but it is largely focused on the state rather than local level.

Ohio

As with MiC3, OhCR relies on civilian volunteers with expertise in cybersecurity and who are willing to assist local governments. However, Ohio's program is a reserve of the Ohio National Guard and its volunteers function as civilian members. The law governing the program allows the governor to adopt rules regarding the organization and maintenance of the reserve. In addition to being called upon to assist municipalities with cybersecurity emergencies or maintenance, members may also serve as mentors to high school students.

Wisconsin

The State of Wisconsin has volunteer Cybersecurity Response Teams largely composed of IT professionals employed by local governments who were previously trained by the state. According to a *State Tech* article, Wisconsin developed these teams over three years as part of its state cybersecurity strategy.[15] The overall team has 60 members that meet regularly over online calls, while smaller teams meet to assist other local governments during cybersecurity threats. The state provided grant funding to local governments for those employees to receive training.

State and Local Cybersecurity Improvement Act

The State and Local Cybersecurity Improvement Act (2021 HR 3138) was passed by the US House of Representatives in July 2021. If enacted, the bill would direct the Cybersecurity and Infrastructure Security Agency (CISA) within the DHS to create a program to distribute grants to states and local governments for cybersecurity improvements. The program would be funded at $500.0 million annually. Eligible applicants would submit plans for improving their cybersecurity for review and approval by the Agency.

If passed, the bill would require CISA to create a State and Local Cybersecurity Resiliency Committee to facilitate communication between the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency and state and local entities. Entities include tribal and territorial governments. The Agency also would be tasked with creating reference resources on cybersecurity issues directed at states and locals. The bill is currently in committee in the US Senate.

Conclusion

Protecting government cyber infrastructure demands constant education, training, and funding. The obsolescence of hardware, new software packages, and changing responsibilities make maintaining up-to-date training difficult, but even with the best training, government entities are vulnerable to attacks. Collaboration offers a dynamic means of both preparing for and responding to cyberthreats while conserving resources.

[1] Donald F. Norris, "A Look at Local Government Cybersecurity in 2020," International City/County Management Association, July 14, 2021.
[2] *Id*.
[3] Karina Elwood, "Ransomware poses threat to vulnerable local governments", *The Washington Post*, Aug. 22, 2021.
[4] Lisa N. Thompson, "Cybersecurity Best Practices for Municipalities," New Hampshire Municipal Association. Retrieved Nov. 2, 2021.
[5] "2016 Deloitte-NASCIO Cybersecurity Study - State Governments at Risk: Turning Strategy and Awareness into Progress," Deloitte/National Association of State Chief Information Officers, 2016.
[6] "CISOs make a case for more state-local cybersecurity collaboration", StateScoop Radio [Podcast]. Available at: https://statescoop.com/podcast/cisos-make-a-case-for-more-state-local-cybersecurity-collaboration/.
[7] National League of Cities Center for City Solutions, "State and Local Partnerships for Cybersecurity: A State-by-State Analysis", 2020.
[8] Benjamin Freed, "Ransomware Attacks Map chronicles a growing threat", *StateScoop*, Oct. 22, 2019.
[9] National League of Cities, "State and Local Partnerships for Cybersecurity: A State-by-State Analysis," 2020.
[10] "About Michigan Cyber Partners", State of Michigan. Retrieved Nov. 3, 2021.
[11] Michael Garcia, "Building a Civilian Cyber Corps," NGA Center for Best Practices, June 2017.
[12] "Michigan Cyber Civilian Corps (MiC3)," Michigan Department of Technology, Management, and Budget. Accessed Feb. 14, 2022.
[13] Michigan Auditor General Performance Audit. "Michigan Civilian Cyber Corps," (Sep. 2019)
[14] Benjamin Freed, "Indiana 'very aggressive' on cyber partnerships with cities", *StateScoop*, Apr. 29, 2021.
[15] McCarter, Mickey, "NASCIO 2019: Wisconsin Fosters Volunteer Cybersecurity Response Team," StateTech, Oct. 15, 2019.