RISK MICHIGAN MUNICIPAL RISK MANAGEMENT AUTHORITY

THE RISK JOURNAL

A PUBLICATION FOR MMRMA MEMBERS FEBRUARY 2022

New MMRMA Grant Aims to Protect Against Cyber Threats

by Daniel Bourdeau, Cybersecurity Practice Leader

"An ounce of prevention is worth a pound of cure." — Ben Franklin

These wise words from 1736 still apply 286 years later. If dollars were ounces, RECTify would offer MMRMA members a cumulative one million ounces of prevention against cyber threats.

MMRMA IS EXCITED TO introduce a new component of our Risk Avoidance Program (RAP): the RECTify (Remediate Emerging Cybersecurity Threats) Cybersecurity Vulnerabilities Grant. The Membership Services team developed the new grant, which commits up to $1 million in surplus RAP funds to help members identify and remediate the most recent—and potentially most damaging—technology vulnerabilities.

Over the past decade, an average of 9,352 vulnerabilities per year were discovered and assigned a CVE (Common Vulnerabilities and Exposures). In 2020 alone, an eye-popping 18,325 [1] CVEs were documented.

According to research by Barracuda Networks, 44 percent of global ransomware attacks in 2020 targeted municipalities.[2] With this intense focus by threat actors on state, county, and local governments, the cost impact is staggering. A report by KnowB4 estimated that the average data breach costs government units $665,000, while the average ransom demand tops $835,758.[3]

Log4j, Other Serious Threats

CVE-2021-44228, commonly known as Log4j or Log4Shell, was published in early December 2021 and rapidly exploited by remote actors. This vulnerability is broadly used in a variety of consumer and enterprise services, websites, applications, and operational technology products to log security and performance information. The Log4j bug can allow a remote actor to replace a single string of text, which can then load data from another computer on the internet.

A halfway decent hacker can feed the Log4j library a line of code that tells a server to pick up data from another server owned by the hacker. This data could be anything from a script that gathers data on the devices connected to the server to one that even takes control of the server in question. The only limit is the hacker's inventiveness; skill barely comes into play.

According to Microsoft, hackers' activities to date have included crypto mining, data theft, and hijacking servers. It is a zero-day flaw, which means it was discovered and exploited before a patch to fix it was available.

What's more, Log4j is just one of 1,202 vulnerabilities with a CVSS (Common Vulnerability Scoring System) score of high or critical added to the NVD (National Vulnerability Database) in December 2021.

Application, Review Process

Because of the continuous discovery of new technology vulnerabilities like Log4j and their rapid exploitation by threat actors, the RECTify grant application and approval process is different than for other RAP grants.

continued on page 3

1 Number of common vulnerabilities and exposures 2021 | Statista
2 Municipal Cyberattacks: A New Threat Or Persistent Risk? (forbes.com)
3 https://www.knowbe4.com/hubfs/Cyber-Attacks-on-Municipalities-White-Paper.pdf

Risk Trends Facing Public Safety, Corrections Departments

by Tamara Christie, Communications Manager

These essential services require split-second decision making in situations that can turn from routine to dangerous in the blink of an eye.

MANAGING AND MITIGATING risk is often a matter of balancing longstanding exposures with the inevitability of change and the emergence of new areas of concern. That is certainly the case when it comes to risk trends for law enforcement, fire, and corrections—essential service areas for many MMRMA members.

As we take a high-level look at a few categories of risk facing these departments and personnel, it bears mentioning that such risks are complex and constantly evolving.

Technology

Cyber risk has emerged as one of the most rapidly developing and potentially costly exposures facing organizations of all sorts and sizes. In recent years, cyber criminals have focused extensively on disrupting public entities and agencies, and this trend has most certainly affected law enforcement departments.

Data management systems, mobile tools, and other technological innovations pose opportunities for law enforcement to improve their processes and daily work activities. But they also bring additional points of entry for cyber criminals—and more intellectual property for them to potentially hold for ransom.

MMRMA offers grant opportunities and other resources to help members bolster their cybersecurity efforts and fend off ransomware and other cyber risks. (See pages 1 and 3 for grant information, and previous issues of the *Risk Journal* for our ongoing series of articles on cybersecurity.)

Human Resources

News outlets are abuzz with stories about difficulties recruiting and retaining employees across all sectors. The pandemic and other socioeconomic changes underway in the U.S. seem to have only accelerated the trend.

This is hardly a new predicament for public entities, and there are no easy solutions. To help address a shortage of police officer candidates, some cities have experimented with alternative approaches to certain tasks traditionally handled by police, such as the use of civilian patrols for routine traffic enforcement stops.

A commitment to training, supervision, and sound protocols will serve public safety and corrections departments

Public safety and corrections personnel are under constant scrutiny about how they conduct themselves in their work.

well as they attempt to retain and recruit personnel.

MMRMA offers an array of training and more than 150 protocols for law enforcement and corrections, prepared in partnership with the Legal and Liability Risk Management Institute (LLRMI). Registered users can access resources and a training schedule in our member portal.

Public Services

As public safety and corrections agencies grapple with these and many other challenges, they also face a chorus of often conflicting opinions about how they should conduct themselves as they work to keep the public safe.

These essential services entail frequent, complex decision making and activities that can turn from routine to highly dangerous in the blink of an eye. Those who answer 911 calls and provide dispatch services may work in a somewhat more secure environment, but their jobs can still be highly stressful.

Again, well-written protocols and frequent training can be highly beneficial to public safety and corrections teams. MMRMA's training for law enforcement and fire personnel includes reality-based scenarios that help them develop the ability to make sound decisions under rapidly evolving conditions. We also offer a resource on critical incident debriefing in the aftermath of traumatic incidents.

Additional Resources

https://www.govtech.com/security/are-police-departments-ready-for-cyber-threats-2022-will-bring

https://www.smartcitiesdive.com/news/cities-consider-taking-police-out-of-traffic-stops/600912/

https://www.nfpa.org/News-and-Research/Publications-and-media/Press-Room/News-releases/2021/NFPA-releases-its-Fifth-US-Needs-Assessment-report-showing-both-progress-and-continued-gaps

https://www.governing.com/now/why-we-need-to-transform-the-911-system

New RECTify Cybersecurity Grant,

continued from page 1

It's important for MMRMA to receive and review applications, and award qualifying grants, with all due speed and efficiency. For this reason, RECTify applications are not subject to the usual RAP/CAP grant application deadlines.

Members can submit RECTify grant applications at any time, and the Membership Services team will review and approve qualified applications on a continuous basis.

This streamlined process is intended to provide much-needed financial resources to aid our members in rapidly discovering and remediating new vulnerabilities before threat actors can leverage them. Ideally, this will help prevent more costly data loss, reputational damage, and complex and expensive recovery services.

Specific Grant Criteria

The RECTify Cybersecurity Vulnerabilities Grant is purposely narrow in its criteria to ensure grant funds are focused on the newest and potentially most damaging vulnerabilities such as Log4j and the many other high and critical scored vulnerabilities listed in the NVD[4] (National Vulnerability Database) at nvd.nist.gov.

Qualifying applications must specifically identify vulnerabilities that:

> Have an assigned CVE and are listed in the NVD

> Began up to six months before the date of the grant application

> Have a CVSS score greater than 6.9.

Nearly 300 years ago, Ben Franklin issued a call for careful practices to prevent fires. Today MMRMA, along with the wider cybersecurity professional community, provides an almost identical call to carefully find and remediate technology vulnerabilities before they become a cyber fire in your organization.

The new grant application is available to logged-in users in the MMRMA member portal. If you have questions or need assistance, please email cyber@mmrma.org.

4 NVD - Search and Statistics (nist.gov)

Other Standard RAP, CAP Grants for Cybersecurity Training, Assessment

MMRMA offers several other standard Risk Avoidance Program (RAP) and Certification and Accreditation Program (CAP) grants to bolster members' cybersecurity toolkits.

Standard RAP Grants

- **General Cyber Security Training: 50% funding with a maximum aggregate of $25,000 per member.**
- **Two-Factor Authentication: 50% funding with a maximum aggregate of $10,000 per member.**
- **Vulnerability Assessment/Penetration Testing: 50% funding with a maximum aggregate of $10,000 per member.**

Since 2019, MMRMA has paid out $21,449 in these grants; an additional $33,862 is approved and pending payment.

Member Testimonial

Fabian Knizacky, Mason County Administrator, reported on the benefits of these grants. "RAP funding allowed us to roll out mandatory quarterly cybersecurity training for all employees, which keeps network security at the forefront of their minds," he says. "They can better recognize questionable emails and understand different types of malware and ransomware that could infiltrate our network."

The county also tapped RAP grant funding to implement a two-factor authentication protocol prior to the COVID-19 pandemic. According to Knizacky, "This proved vital when several team members started working remotely, helping our network remain as secure as possible."

Knizacky strongly encourages MMRMA members to apply. Public entities are so dependent on computer networks that having them hacked would result in widespread shutdowns of services to residents.

Cyber-Related Certifications

CAP grants provide funding assistance for member personnel who achieve the following certifications:

- **GIAC Certified Intrusion Analyst**
- **GIAC Continuous Monitoring Certification**
- **Certified Information Systems Security Professional**
- **Certified Chief Information Officer**
- **ICMA Cybersecurity Leadership Academy**

Members with login access can download an application and additional information in our portal at mmrma.org/members/rap-grant-application. For more information, contact Cara Ceci at cceci@mmrma.org.

RISK MICHIGAN MUNICIPAL RISK MANAGEMENT AUTHORITY

Mandated Active Violence Training for Law Enforcement

Start your engines—a new permanent exhibit at The Henry Ford in Dearborn celebrates the history of American car racing, fueled by star drivers such as A.J. Foyt and Bobby Unser. The quest for speed began in 1902 when Ford hand-built his "999" race car, so powerful he was afraid to drive it. Its success propelled Ford's next venture: the founding of Ford Motor Company.

Michael Rhyner
Executive Director

Bryan J. Anderson, CPA
Managing Director

Cindy King
Director of Membership Services and Human Resources

Starr M. Kincaid, Esq.
Director of Claims

The *Risk Journal* is edited by Tamara Christie, Communications Manager, and published six times a year for members of Michigan Municipal Risk Management Authority. We welcome your feedback. To comment or suggest story ideas, please contact Tamara at 734 513-0300, 800 243-1324, or tchristie@mmrma.org.

LAW ENFORCEMENT officers in Michigan are subject to standards set by state legislation. Specifically, Public Act 203 of 1965 created the Michigan Commission on Law Enforcement Standards (MCOLES) and outlined the scope and breadth of its responsibilities, along with many other prescribed requirements, procedures, and related actions.

In March 2019, Public Act 552 of 2018 became law. It amended Public Act 203 of 1965 to add a new section that mandates active violence training for all licensed law enforcement officers in the state.

This new mandate went into effect on January 1, 2020. According to new Section 609e, individuals seeking to become licensed under the Act "shall complete active violence response training that emphasizes coordinated tactical response to rapidly developing incidents in which intentional physical injury or death to a specific population occurs through the use of conventional or unconventional weapons and tactics."

The Act further states that MCOLES "shall promulgate rules establishing the minimum standards for the active violence response training required under subsection (1)."

Funding, Implementation

On its website, MCOLES states, "Funding was not initially appropriated to enable the completion of its requirements. However, using its existing staff, the Commission updated the mandated basic police training academy curriculum and standards to meet the requirements of Sec. 9e(1), in May of 2019." [1]

The mandate, which took effect January 1, 2020, requires active violence training for all Michigan law enforcement officers.

MCOLES reports that partial funding was appropriated later in 2019, but the COVID-19 pandemic arose in early 2020, freezing funding for many projects and activities, including this training. Once this funding freeze was lifted, MCOLES resumed implementation of the required rules and training needed for licensing of Michigan's law enforcement officers.

Training Opportunities

The MMRMA team understands and recognizes the significance of this mandate. We encourage member law enforcement agencies to be well-versed on the requirements prescribed in the Act.

"MMRMA has offered reality-based active violence training to its members for over a decade," states Mike Berthā, Senior Risk Control Consultant. "We will continue to provide assistance to help member law enforcement agencies meet this licensure requirement for their officers."

In addition to Rapid Response to Active Shooter training, MMRMA offers several other reality-based courses each year for public safety personnel, including Tactical Encounters for Patrol Officers and Rescue Task Force training.

MMRMA's Membership Service Team is here to support member agencies and personnel as they serve the public. Call 734-513-0300 if you have questions or would like more information about training opportunities or risk control guidance.

1 https://www.michigan.gov/mcoles/0,4607,7-229-41619-575447--,00.html