RISK MICHIGAN MUNICIPAL RISK MANAGEMENT AUTHORITY

THE RISK JOURNAL

A PUBLICATION FOR MMRMA MEMBERS JUNE 2026

CYBER RISK MANAGEMENT, PART 1

Addressing Cybersecurity Threats That Target Public Entities

by Dan Bourdeau, Director of IT and Cybersecurity, and Tamara Christie, Communications Manager

The best way to protect payment-related transactions is to call the requester at a known number stored in your directory or master file.

CYBER THREAT ACTORS continue their activities in the public sector and MMRMA members have been—and will remain—in their sights. This new *Risk Journal* series will examine different areas of cyber risk and share insights from our team on how to avoid, mitigate, and, if need be, respond to cyber incidents. The aim is to protect members, the funds they manage, and the entire MMRMA membership.

Public funds are appealing targets

Here we explore ways threat actors exploit social engineering and other methods to access and steal public funds. For this type of attack, the culprits turn their sights on public entity finance and treasury professionals who control the flow of money.

Nearly every successful business email compromise and wire fraud incident in the public sector last year required a finance or treasury employee to either approve a payment, update a vendor banking record, or release a wire or ACH file.

A successful phishing attack lets the perpetrator read your messages, send emails as you, and hide their tracks.

These incidents cost billions of dollars in 2025 alone across all organization types in the U.S. In 2026, 62% of breaches still involve a human element. Once members understand the ways in which these types of incidents are most likely to occur, they can work to train everyone in their agencies to slow down, look for signs of potential phishing and other scams, and verify, verify, verify.

Email compromise = keys to the kingdom

Phishing methods continue to mature, and the proliferation of artificial intelligence (AI) use by cyber threat actors has only increased their effectiveness. Grammar is better than ever and sender addresses use lookalike domains, which make phishing emails harder for busy employees to spot.

A successful phishing attack on an email account lets the perpetrator read your traffic, identify patterns, send emails as you, and hide their tracks. Passwords are widely compromised and often sold on the dark web. It is never a good idea to reuse personal passwords for work accounts. Instead, use a password manager and passkeys whenever possible. Phishing-resistant multi-factor authentication (MFA) is also a great approach (see graphic above for recommended types).

Hybrid work hygiene is often overlooked

Many member employees work at home at least occasionally. Several risks can be mitigated with the proper education and protocols:

- Keep employer email, apps, activities, and credentials off personal devices.

continued on page 2

Addressing Cybersecurity Threats, continued from page 1

- Lock device screens at work and at home. Family members, guests, and service people who are in your space are not authorized to see and access employer data.
- Avoid using public Wi-Fi to access personal or work banking apps or to conduct banking transactions.
- Never paste vendor or member data, invoices, or banking details into public, non-secure AI tools.

WEAK: Don't trust financial transfers to:

✗ **SMS text codes.** The National Institute of Standards and Technology has advised against SMS multi-factor authentication since 2017.

✗ **Push approval (tap to approve).** Attackers spam your phone until you tap by mistake.

✗ **Voice and email codes.** If email is compromised, so is multi-factor authentication.

STRONG: Use for financial transactions:

✔ **FIDO2 hardware keys.** Cryptographically bound to the real site; will not authenticate on a fake page.

✔ **Passkeys.** There is no password to phish. Passkeys are built into iOS, Android, Windows Hello, and macOS.

✔ **Authenticator with number matching.** Users type in a number, don't just tap to approve.

Anatomy of a business email compromise (BEC)

Michigan public entities have been affected by several types of business email compromise, which can all lead to fraud incidents and loss of public funds. Some examples:

Vendor email compromise is the hardest variant to catch and allows attackers to send banking info change requests to public entities from a legitimate vendor email account.

Executive impersonation involves spoofing or compromising an organization or department leader's email address or mobile number and sending an urgent request for fund transfer or payment to a new account. Recipients of such requests often feel compelled to comply and act quickly.

Attorney impersonation can also provoke a recipient's sense of urgency and confidentiality to act without verification.

Hackers try to provoke a sense of urgency to persuade people to act without verification.

Payroll diversion is when an attacker accesses an employee's email and sends updated direct deposit information to accounting, which if successful will route payroll deposits to the wrong account.

Data theft and W2 fraud involves threat actors impersonating senior officials to request sensitive documents and identifying information for an "audit," thereby exposing employees to tax refund fraud and identity theft.

Phone verification and other safeguards

These types of incidents and their potential exposures are the tip of the iceberg when it comes to ways cyber attackers may seek to pilfer public funds. One thing these and other scams have in common is that they can often be thwarted by effective training, sound protocols, and constant vigilance with an eye to **verify.**

- For *any* payment-related instruction, the best way to protect your member agency is for the person receiving the request to pick up the phone and call the requester at a known number already stored in your directory or master file. **Never verify by calling a phone number provided in an email, on the email signature, or on the invoice.**
- Before acting on a request, call and speak to a known person, confirm account numbers digit by digit, and document the contact in writing.
- If the requester asks to call *you* back, it's a red flag.

Implement dual control on wire transfers and ACH payments, with one employee of the member originating the transaction and a second employee reviewing and releasing it. Ensure separate logins and multi-factor authentication to make the most of a dual-control policy.

Segregation of duties is best practice for all areas of financial transactions and activities. Set approval thresholds that scale with risk, so larger transaction amounts require a more senior official or governing body to approve.

Reconcile high-volume accounts daily and all other accounts no less than weekly, and cross-train on policies and procedures to ensure compliance during vacations—which can be fully transparent to attackers if they have accessed an employee's email and calendar.

Members are entrusted with public funds to conduct the business of their residents. Awareness, training, and proper protocols can help every member entity and employee be informed on how to best perform their duties while protecting those funds.

MMRMA has several related and additional cybersecurity resources, including podcasts and model guidelines, available to member employees in our web portal. Request a login at https://mmrma.org/member-sign-up/

For additional assistance, contact our team at cyber@mmrma.org.

Membership Services Announces 2026 Grant Program Updates

by Cara Ceci, Member Resources Manager

MMRMA'S SIGNATURE RISK Avoidance Program (RAP) has been providing grant funding to members since 1997. In 2016, MMRMA added Certification and Accreditation Program (CAP) grants to provide members with funding opportunities for higher educational programs. Since RAP's inception, over $31 million in grant funding has been returned to members to help offset the costs of projects aimed at reducing risk and liability.

Annual Review Process

The Membership Services team, in collaboration with the Membership Committee, conducts a routine annual review of grant program guidelines to ensure that program goals and funding levels are aligned with the overall strategic objectives set forth by MMRMA's Board of Directors each year.

The grant program was developed to encourage members to use funding as part of their entity's comprehensive risk management program. The primary goal is to mitigate members' highest risk exposures. Currently, the top five categories of focus are: property, law enforcement, corrections, cybersecurity, and employment practices.

At its May 6, 2026 meeting, the Membership Committee reviewed and approved several recommended updates to the overall grant program and associated guidelines. General guideline revisions included minor language and formatting revisions.

The top five categories of focus are: property risk, law enforcement, corrections, cybersecurity, and employment practices.

Updates to Standard Grants

Updates were made to Standard Grant Guidelines as outlined below.

Public Safety Equipment

To help better manage the growing practice of purchasing bundled equipment under multi-year payment plans, individual funding categories for TASERS, in-car cameras, and body cameras have been eliminated.

The new Public Safety Equipment Grant will cover ANY combination, bundle, package pricing, individual pricing, or similar practices associated with this specific area of equipment. Funding will be allowed at 50% up to an aggregate maximum of $100,000 per member every 5 years for new contracts only. (Members may apply for funding one time per vendor contract.)

General Cybersecurity Training for Employees. Members will be limited to applying for funding one time per year. However, up to 12 months of invoices may be included with the application for funding consideration.

Corrections Security/ Physical Improvements

Grant language has been updated to restrict funding for security projects

continued on page 4

Reasons RAP Applications May Not Be Funded

The Membership Committee provides rationale when denying a grant application, noting one of the following:

1. Grant does not comply with guidelines or meet the goals of the program. There is no direct correlation to loss reduction.

2. Grant addresses a risk for which MMRMA does not provide coverage to the member.

3. Funding is requested for routine operations.

4. Funding is requested to replace or upgrade outdated and/or obsolete systems and software.

5. Application lacks clear objectives, a timeframe in which to complete the project, and/or a member-approved budget for funding the project.

6. Application is vague or does not present a strong argument that project will mitigate the identified risk.

7. The Membership Committee identified other applications addressing priorities that focus on higher exposure or more pressing risk management needs.

June is National Pollinator Month, a celebration of the Black Swallowtail (Michigan's state butterfly) and other insects responsible for pollinating about 75% of the nation's flowering plants. Pollinators play a significant role in agriculture by enabling plants to reproduce and providing food and shelter for wildlife.

Bryan J. Anderson, CPA
Executive Director

Daniel Bourdeau, Director of IT and Cybersecurity

Cindy King
Director of Membership Services and Human Resources

Starr M. Kincaid, Esq.
Director of Claims and Legal Services

Debra Lichtenberg, CPA
Director of Finance

The *Risk Journal* is edited by Tamara Christie, Communications Manager (tchristie@mmrma.org), and published six times a year for members of Michigan Municipal Risk Management Authority.

Please note that the *Risk Journal* may include AI-assisted content. The authors and editor thoroughly reviewed and vetted all such material.

RAP/CAP Grant Program Updates, continued from page 3

that address risk exposures, evolving safety standards, or conditions not reasonably foreseeable or commonly incorporated into correctional facility design at the time of original construction. Funding is limited to retrofitting existing facilities constructed in 2015 or earlier. Facilities constructed or substantially renovated in or after 2015 are not eligible for funding.

New Grants Added

New funding opportunities were added, including:

Grappler Police Bumper

50% funding up to a maximum of $30,000 per member for first-year costs (including initial training) only. Subsequent yearly subscriptions, continuation fees, etc., are not eligible for funding.

Fire Department HAAS Digital Alerting System

50% up to a maximum of $10,000 for first-year costs only. Subsequent yearly subscriptions, continuation fees, etc., are not eligible.

CDL Licensing for Emergency Responders Assigned to Specialized Response Teams ONLY.

Will be included under General Risk Management and Leadership Training and is eligible for 50% funding.

RAP/CAP GRANT TIMELINES

Submission Window	Quarterly Deadline	Funding Awarded	Funds Expire
Oct. 11–Jan. 10	Jan. 10	Feb./March	Sept. 30
Jan. 11–April 10	April 10	May	Nov .30
April 11–July 10	July 10	August	Feb. 28
July 11–Oct. 10	October 10	November	May 31

Assistance Available

Membership Services staff is available to answer questions. We encourage members to request assistance before submitting a final grant application to discuss compliance with guidelines, risk reduction benefits, and any other aspects of the project highlighted for funding.

Important Timelines

Members are encouraged to submit applications as timely as possible to increase their chances of receiving funding. MMRMA's fiscal year runs from July 1 to June 30. Grant applications are reviewed quarterly, with committee meetings taking place in February or March (in conjunction with the Risk Management Workshop), May, August (at the Annual Meeting), and November.

Contact us at grants@mmrma.org or log into the member portal to access the latest guidelines and application forms at **mmrma.org/members/rap-grant-application.**

Sneak Peek: 2026 MMRMA Annual Meeting

JUNE IN MICHIGAN BRINGS SUNSHINE, summer storms, and construction barrels. It also means MMRMA's Annual Meeting is right around the corner! Registrations are rolling in and we look forward to gathering with members and business partners to connect, learn, and network.

Training highlights

Author and leadership expert Matt Brauning will kick things off at the Thursday night opening session and present again Friday morning, sharing his expertise on unlocking lasting motivation and leveraging generational communication styles for successful teamwork.

Austin Hatch, a two-time plane crash survivor and former University of Michigan basketball player, reminds us that we all face adversity every day, but there's no obstacle we can't overcome if we work together.

Board Meeting

All attendees are invited to the Saturday morning Annual Business Meeting of the Board of Directors for an update on all things MMRMA! Check out the full agenda at **https://mmrma.org/2026-annual-meeting-registration/.**