

THE RISK JOURNAL

A PUBLICATION FOR MMRMA MEMBERS

OCTOBER 2026

Navigating Public Incivility to Mitigate Associated Risks

by Cindy C. King, Director
of Membership Services
and Human Resources

INCIVILITY HAS BECOME increasingly common in public spaces, including in workplaces. Unfortunately, this trend has not spared MMRMA member entities. The negative behavior of individuals and groups can pose serious consequences for members, including poor employee morale and potential liability.

Insults and confrontations
Most member employees can cite instances of uncivil behavior by members of the public, such as insulting or threatening elected leaders and employees. These behaviors may occur in municipal offices, public spaces, during governing body meetings, and in many other situations.

Public employees in the field—including police, firefighters, emergency medical responders, code enforcement officials, and animal control personnel—are too often on the receiving end of someone who is angry or dissatisfied with the work these essential workers perform on behalf of the community.



Incivility is unpleasant, time-consuming, and holds the potential for numerous risks.

Incivility also takes place in public indoor spaces and may be directed at cashiers accepting tax or utility payments, employees in recreation centers and public libraries, and election workers at polls, to name just a few examples.

The potential for risk

Not only is incivility unpleasant and time-consuming, it can also lead to risks for entities. Employees could file claims of harassment or a hostile work environment. Individuals who exhibit incivility may make claims of Open Meetings Act violations or First Amendment infringements if they believe they have been prevented from speaking or otherwise mistreated. Other potential problems include a loss of

public trust, fewer people who are willing to serve in elected or appointed positions, and/or the inability for entities to operate effectively.

An article in the April 2022 *Risk Journal* has guidance on minimizing and de-escalating tense situations and behaviors, and the tips and information are still applicable. Members can access it at mmrma.org/members/newsroom/.

Members are encouraged to have internal awareness and ensure that the conduct of elected officials and municipal employees is professional, courteous, and respectful. If any individuals are identified who sometimes act disrespectfully, the people they serve may respond similarly.

When public entities are short-staffed and find it hard

A well-crafted policy for participation in public meetings supports the rights of the public and preserves the democratic process.

to attract talent, it behooves the entity to actively recognize the difficulties employees are facing and take action to reduce incivility and unacceptable conduct toward them.

Conflict in public meetings

Those who preside over meetings are responsible for moderating the conduct of participants and attendees, including that of officials, employees, and the public.

Effective public meetings balance the need for a productive meeting with constituents' desire and right to voice their displeasure, frustration, or anger. With many differing opinions, conflicts are unavoidable. Give residents the opportunity to express their concerns. Try to avoid being defensive or blaming others,

continued on page 2

Navigating Public Incivility, continued from page 1

and to see both sides of the matter. Try not to address concerns with generalizations or stonewalling, which could foster or exacerbate incivility.

A thoughtful, well-crafted policy that sets forth rules for participating in public meetings—and the benefits of positive, professional, and respectful conduct—will support the rights of the public and preserve the democratic process while prohibiting personal attacks, obscenities, and other threatening language. Setting time limits, usually 3–5 minutes, helps reduce the duration of incivil behavior.

During public meetings, speakers should address the governing body and not others in the audience. It is the meeting moderator's responsibility to consistently apply the rules for public speaking without regard for who is speaking. This can minimize uncivil exchanges.

Employees in the field

Public employees who enforce laws, municipal ordinances, or otherwise regulate activities in the community may experience rude behavior regularly. Yelling and threats can lead to employees feeling stressed or frustrated. They may report feeling unsafe or unable to perform their position responsibilities. This can impact the greater organization if employees experience



low morale or burnout. Left unchecked, uncivil behavior could cause good employees to seek employment elsewhere, create a strain on resources, and compromise service quality.

When acknowledging employee complaints about incivility, it is helpful not to immediately assume the staff person did something wrong. Give employees time to share their experiences with unruly individuals and help them depersonalize negative behavior. Often, a person's rude conduct is a reflection on them and not on the work of the member entity or its employees. However, wise leaders will evaluate and take steps where needed to minimize uncivil conduct, including correcting internal deficiencies.

Remind employees their roles are important. Compliment and thank them for the good work they do despite the challenges they face from rude people, and pay attention to signs of anxiety or

depression, which could arise if uncivil treatment is frequent.

Training and techniques

De-escalation training can provide employees and decisionmakers with tools for dealing with rude or threatening conduct. De-escalation techniques involve staying calm, practicing active listening, and showing respect (even when not being granted it). For example, it can help to lower your voice and speak slowly. If possible, show concern (not necessarily agreement) through your responses and be prepared to react.

John Leo Riley, a conflict de-escalation training facilitator who has presented during an MMRMA Risk Management Workshop, points out how nonverbal or body language can unwittingly escalate a situation. Facial expressions such as eye rolling can undermine the credibility of the person who is upset. A scowl or staring may provoke an angry person. A crossed-arm posture is often viewed as

De-escalation techniques involve staying calm, practicing active listening, and showing respect.

defensive, whereas putting hands on hips may appear to be a hostile action.

Conversely, a simple smile is a form of nonverbal communication that can help defuse conflict. Tilting the head to one side may suggest listening or concentrating on what the other person is saying. Eye contact, provided it doesn't appear to be a stare or threatening, can convey trust or understanding.¹

Members can log into the MMRMA portal and access resources in managing these risks, including *Workplace Harassment Complaints, Prevention and Response Best Practices*, as well as model law enforcement protocols on *Bias Influenced Policing Prohibited, Community Engagement, Crowd Control, Workplace Harassment, De-Escalation, Filming Officers, Persons with Mental Disorders*, and many more. Contact Membership Services for additional assistance.

¹ <https://www.betterhelp.com/advice/body-language/22-body-language-examples-and-what-they-show/>

CYBER RISK MANAGEMENT, PART 3

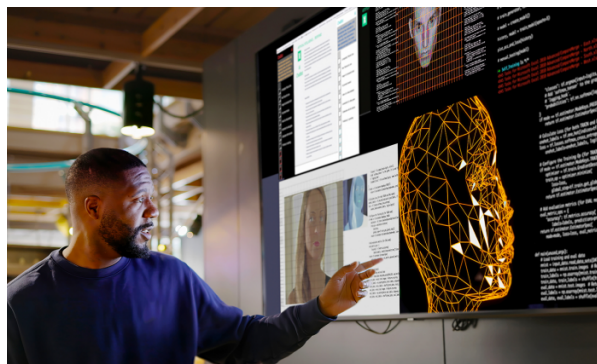
Mitigating, Addressing Increasingly Sophisticated Cyber Incidents

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

CYBERSECURITY THREATS continue to evolve, creating significant challenges for MMRMA members. As local governments increasingly rely on technology to deliver essential services, protecting sensitive information and maintaining operations have become critical risk management priorities.

Cyber incidents can disrupt public services, compromise confidential information, create financial losses, and damage public trust. Recent incidents involving Michigan municipalities demonstrate that no entity is immune, regardless of size or available resources.

The question is no longer simply how to prevent cyber-



AI-generated fraudulent communications are increasingly convincing.

Warning signs include unexpected payment requests, suspicious attachments, and high-pressure tactics.

attacks, but how to prepare for, respond to, and recover from them.

More sophisticated threats

Phishing, ransomware, and social engineering remain significant threats. Social engineering involves manipulating individuals into disclosing sensitive information, transferring funds, or granting unauthorized access to systems.

Cybercriminals frequently impersonate trusted individuals or organizations, using fraudulent emails, telephone calls, and other deceptive techniques. Artificial Intelligence (AI) adds another dimension, making fraudulent communications increasingly convincing through AI-generated phishing messages, voice cloning, and deepfake technology.

Train employees to recognize warning signs, including unexpected payment requests, suspicious email addresses, unusual attachments, and

messages creating a false sense of urgency.

Independent verification is a critical safeguard. Before transferring funds, sharing credentials, or providing sensitive information, employees should confirm unusual requests through trusted communication channels.

Preparation key to response

Cybersecurity requires more than technology. Policies, employee awareness, leadership involvement, and

continued on page 4

Cyber Incident Readiness Checklist

Is your organization prepared to respond to a cybersecurity incident? Take these steps:

- > **Review your incident response plan.** Ensure responsibilities, notification procedures, and recovery protocols are clearly documented and regularly updated.
- > **Train employees to recognize threats.** Reinforce awareness of phishing, social engineering, fraudulent payment requests, and emerging AI-enabled threats.
- > **Establish verification procedures.** Require independent confirmation of unusual requests involving financial transactions, credentials, or sensitive information.

> **Protect sensitive information.** Review access controls, data protection practices, and policies governing employee use of AI tools.

> **Know your coverage and reporting requirements.** Review applicable cybersecurity coverage provisions and notify MMRMA by phone at the first sign that your agency is or was targeted. You needn't wait until you've confirmed active or recent malicious activity. Call 734-513-0300. After hours, prompts will connect you with a knowledgeable member of our team or allow you to leave a message that will be delivered to our team immediately.

> **Identify your response team.** Maintain up-to-date contact information for MMRMA, leadership, IT personnel, legal counsel, communications staff, and other essential resources.

Cybersecurity Incidents, continued from page 3



Michigan boasts several herds of elk, and fall is the best time to view them. The City of Gaylord maintains a herd of 60, grown from just three elk since the 1980s. Your chances of spotting one are good, even in town, from a viewing platform. To see elk in the wild, go to Pigeon River State Forest, which has a dozen designated viewing areas.

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.

© MMRMA 2026

incident response planning are equally important.

Members are encouraged to develop and maintain a documented incident response plan identifying responsibilities, notification procedures, and appropriate internal and external resources.

Key elements for response include immediate containment, evidence preservation, communication protocols, and recovery procedures. Identify key contacts, including IT personnel, leadership, legal counsel, and cybersecurity coverage representatives.

Regular training and periodic reviews will help ensure that employees understand their responsibilities and are able to respond effectively if an incident occurs.

Respond quickly but deliberately

When a cyber incident is suspected, immediate action can help limit damage and support recovery.

Isolate affected systems, notify appropriate personnel, and secure relevant passwords.

Preserving digital evidence is essential. Employees should avoid deleting information or powering down affected equipment without expert direction.

When an incident is suspected, members must notify MMRMA first—and as early as possible—while following applicable coverage requirements.



Preserving the digital evidence of a cyber incident is essential to a coordinated response.

Early notification helps facilitate access to appropriate resources, including cybersecurity specialists, forensic investigators, legal counsel, and other professionals.

A coordinated response may involve determining how an attacker gained access, whether sensitive information was exposed, and what steps are necessary to restore operations safely.

Communication is essential

Cyber incidents can create uncertainty among employees, residents, and other stakeholders. Clear, consistent communication helps maintain confidence while an investigation proceeds.

Designate a spokesperson or communication office in advance and consult with claims staff or counsel before releasing messaging. Initial communications should acknowledge the situation without speculating about its cause, scope, or consequences.

Avoid characterizing an incident as a confirmed data breach before the facts and applicable legal requirements have been evaluated. Notification requirements may extend to affected individuals, regulatory agencies, and business partners. Legal counsel should help determine these requirements and deadlines.

Make it an ongoing focus

Cybersecurity is not a one-time project. We encourage members to continually assess vulnerabilities, update policies, educate employees, and evaluate incident response capabilities.

The goal is not to eliminate every cyber risk, but to strengthen organizational resilience. Through preparation, vigilance, and a coordinated response, members can better protect sensitive information, minimize operational disruptions, and maintain public trust.

Find additional cybersecurity resources in our member portal; login or request an account at mmrma.org/members/login.