RISK Michigan Municipal Risk Management Authority

THE RISK JOURNAL

A PUBLICATION FOR MMRMA MEMBERS APRIL 2022

Tips and Techniques for De-Escalating Tense Public Situations

by Cindy King, Director of Membership Services and Human Resources

What should we do when confronted by upset people or groups, especially if we're the target of threatening actions?

MONTHLY MEETINGS OF a county health agency are disrupted by a crowd of protesters. A board of supervisors approves a policy change to curtail hate speech and inappropriate conduct at its meetings. Disgruntled citizens follow school board members to their cars to confront them after the meeting adjourns.

Some MMRMA members have experienced such uncomfortable situations firsthand. While many recent incidents stem from actions associated with the COVID-19 pandemic, any number of other issues have galvanized people to show up and express their opposition. For some public officials, it feels like the frequency of these protests and the level of anger involved is on the rise.

Incidents create risk

In recent years, many public meetings have been packed with angry people threatening decision-makers. One Michigan county health official reported an incident of

Meetings of city councils, school boards, health agencies, and other public entities are routinely disrupted.

road rage in which someone upset with a decision he made tried to run him off the road.

In other cases, citizens have entered workplaces and used smartphones to take videos of employees going about their jobs—or have shown up to protest on the front lawns of public employees' private homes.

Understanding anger

We all can relate to an experience dealing with an angry individual or group. We may wonder what causes people to become so angry they act out in ways that are at minimum rude or disruptive—and that all too often cross the line into being hostile or threatening.

Douglas Noll's article titled "3 Powerful New De-Escalation Techniques That Work" identifies common reasons people may become angry in public situations:

> Power struggle

> Overreaction to threats, posturing, or emotional displays

> Not feeling heard or listened to

> Feeling disrespected or threatened

https://dougnoll.com/de-escalate/de-escalation-techniques/

Noll's related article suggests that angry people have needs they want met, including:

> Vengeance

> Vindication

> Validation

> The need to create meaning

> The need for safety

https://dougnoll.com/de-escalate/control-anger-in-relationships/

Interacting with purpose

Understanding the motivation of an angry person is one thing; knowing what do when we come face-to-face with upset individuals or groups—especially if we're on the receiving end of threatening actions or being accused of wrongdoing—is quite another.

The Crisis Intervention Team (gocit.org), a non-profit that provides programs to avoid and minimize crisis, suggests several de-escalation techniques to defuse tense situations.

continued on page 3

CYBER RISK MANAGEMENT, PART 9

Addressing Cyber Risk Requires a Broad, Systematic Approach

by Daniel Bourdeau, Cybersecurity Practice Leader

MMRMA members can use both low– and high–tech tools to help employees on the cybersecurity front lines.

TECHNOLOGY HAS revolutionized our ability to communicate, transact, collaborate, and most recently, to survive a disruptive and debilitating pandemic.

Technology has also made us and our data extraordinarily vulnerable to ransom, theft, and exploitation. Scarcely a day goes by without a news story trumpeting another high-profile data breach affecting tens of thousands, or millions, of stolen records set to be monetized on the dark web.

Beyond firewalls

Technological fortification—the practice of adding more and more layers of security apparatus and services—is no match for today's sophisticated cybersecurity threats, which now directly target an organization's employees.

Of course, organizations must still invest in state-of-the-art firewalls and endpoint protection (antivirus tools). These investments must encompass machine learning and artificial intelligence, because threat actors use those same technologies against us. If you haven't upgraded these systems in the last three to four years, you may not have what you need to effectively detect, respond, and recover from such attacks.

No rest from hackers

As organizations incorporate increasingly advanced cybersecurity technologies, cybercriminals respond with even more costly and complex hacking schemes. This evolution has, in turn, accelerated use of automated attack platforms that scour millions of connected devices for unpatched software vulnerabilities—attacks that require very little time or effort on the part of human beings.

These systems require neither sleep nor food—and without a nanosecond of rest, carefully catalogue vulnerable devices to directly exploit or sell lists to other attackers.

The human factor

As businesses' technology is constantly being tested and scrutinized by bad actors, so are their employees. Phishing and email spoofing continue to be the leading threat vector (point of entry or weakness) into organizations' networks and data.

Phishing and email spoofing continue to be the leading point of entry into networks.

Gone are the days of fake, crudely constructed emails with easy-to-spot grammatical errors, exposed phony email addresses, and other telltale signs. Still, investing in quality employee training on detecting fakes and being wary of every single message, regardless of how polished and routine it may look, is vital to your entity's chances of forestalling a data breach.

Fortunately, MMRMA members can employ both low- and high-tech tools to help employees on the cybersecurity front lines. Most importantly, team members must feel safe in self-reporting honest mistakes. They must also know how to quickly and easily report those incidents, even if they turn out to be false alarms. This open, communicative culture can supercharge your response, investigation, and mitigation efforts.

Processes and tools

Another low-tech, policy-driven security measure requires at least two employees to process electronic requests for changes to sensitive information such as addresses, phone numbers, and banking or payment accounts. In other words, the employee who receives a change request should not be the employee who completes it. This approach doubles the number of eyes, brainpower, and the chances of detecting fake requests.

On the high-tech spectrum of tools is data loss prevention (DLP). Many cloud services such as Microsoft Office 365 and modern firewalls have basic DLP capabilities. DLP searches emails, attachments, and data for identifiable patterns, such as driver's license or social security numbers, and can pause or block

continued on page 4

De-escalating Tense Situations, continued from page 1

De-escalation is defined as:

1. A variety of psychosocial techniques aimed at reducing violent and/or disruptive behavior.

2. Skills to reduce or eliminate the risk of violence during an escalation phase through verbal and non-verbal communication.

3. A less authoritative, less confrontational approach to regain control.

According to *Security* magazine, "The point of de-escalation is to minimize risk—to turn down the heat before a situation can boil over. De-escalation is fundamentally an interpersonal skill. It's all about finding common ground with the person in distress."

Listening and verbalizing

Matthew Doherty, a threat and violence risk management expert, suggests we "listen to the person, find out the reasons why they're so upset, or at least give them some empathy and respect."

Another security expert, Eric Sean Clay, concurs: "When we de-escalate … we're actively listening to what that person is saying. We're watching for verbal cues that may indicate what they're thinking. Sometimes we just allow them to vent. It helps them feel validated, that somebody is actually listening to what they have to say."

https://www.security-magazine.com/articles/95754-top-de-escalation-strategies-and-training-for-security-leaders

Body language speaks volumes; a sincere smile will convey much more empathy than eye rolling or scowling.

Letting people vent helps them feel validated and see that somebody is actually listening to them.

The Michigan State Police, in their presentation *De-Escalation Techniques for Teachers,* makes these suggestions:

> Speak slowly

> Lower your voice

> Don't stare

> Avoid arguing or being confrontational

> Show concern through your responses

> Be prepared to react.

https://www.michigan.gov/msp/-/media/Project/Websites/msp/gcsd/2022-files/PDF/DeEscalation_Techniques_for_Teachers_743471_7.pdf

Body language matters

Conflict de-escalation training facilitator John Leo Riley says our body language can unwittingly make a tense situation even worse. Most people pick up on non-verbal communication very quickly and almost unconsciously.

For example, it's important to be aware of your facial expressions when you meet with people. A scowl isn't likely to calm an angry person. Rolling your eyes can be interpreted as undermining the credibility of a person's views. Standing with one's arms crossed or with hands on hips are seen as defensive, hostile, even aggressive postures.

Non-verbal commmunication

What non-verbal actions can help defuse a situation? Start with a smile. Tilting our head to one side shows that we're listening and concentrating on what the other person is saying. Having your hands open and palms up is seen as being open and honest. Eye contact can convey trust or understanding, as long as it doesn't look like you're glaring.

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

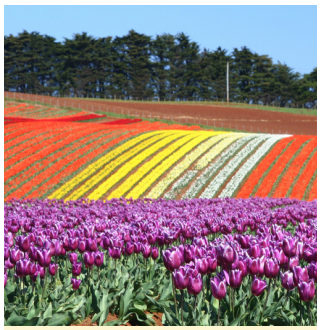
Awareness and practice

At its most basic, de-escalation involves staying calm; practicing active listening; showing respect (even when it's not being shown to you); being aware of non-verbal gestures that might contradict the words you are speaking; and not acting in ways that make matters worse.

While it may not always be possible to give angry individuals the resolution they seek, our willingness to learn and use these techniques could help us convey respect and understanding, thus improving the atmosphere and the chances of constructively resolving difficult issues.

Employing de-escalation techniques takes time and practice. But by honing these skills, we may be able to lower the temperature of difficult situations in the future, reducing risk to ourselves and our organizations.

Workshop Highlights: The Economy, Cyber Risk, and More



Each spring on the west side of Michigan, Holland bursts into bloom, with more than 5 million tulips and six miles of city streets lined with flowers of every color. Since 1929, the annual Tulip Time Festival celebrates the area's Dutch roots. Tour a farm, visit an authentic windmill, or watch dancers clog in their iconic wooden shoes.

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 and Legal Services

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.

MMRMA WAS PLEASED TO host the 2022 Risk Management Workshop in Lansing in late February, a welcome opportunity to gather with members and guests and share the latest in risk control guidance.

Michigan's economy

John Austin, Director of the Michigan Economic Center, explored Michigan's economic history and what today's trends mean for those who want to invest in a successful future. He shared several challenges of the current economic global transformation, including:

> Technology and innovation

> New priorities for workplace talent

> Global supply chain interdependence

These challenges can bring opportunities, as well, for communities that look for innovative ways to capitalize on them to spur growth, rather than becoming stagnant out of reliance on outdated economic forces.

Fostering collaboration is a valuable component in the inclusive leader's skillset.

Cyber assessment, impacts

Jessica Dore of Rehmann discussed exposures, causes, costs, and incident response guidelines for the ever-present threat of cyberattacks.

While the rise of remote work and other global factors have added a new spin to cyber risk, there are measures that organizations and individuals can take to bolster their security efforts.

Dan Bourdeau, MMRMA Cybersecurity Practice Leader, provided his insights on the cyber risk landscape, what members can expect from a cybersecurity assessment, and MMRMA grants and resources.

Inclusive leadership

Bridget G. Hurd presented the benefits, skills, and business and cultural impacts of cultivating inclusive leaders.

As Vice President of Inclusion and Diversity for Blue Cross Blue Shield of Michigan, Hurd shared her perspective on the value of cultural competency, which includes fostering collaboration by empowering team members to contribute and build on one another's ideas.

These four speakers' presentations are available to members. Log into mmrma.org and go to the My Documents section in **Workshop/Training Materials > Risk Management Workshops** folder.

Addressing Cyber Risk, continued from page 2

that data from insecurely leaving your systems.

There are many options for data loss prevention services, with a wide spectrum of cost and efficacy. Carefully evaluating, investing in, and implementing the appropriate DLP service for your entity might well be what prevents you from having to file a data breach claim.

No employee, policy, apparatus, system, service, or training is infallible. That's why it's critical to challenge your technical team and leaders to invest in all of these layers. Such investments will be ongoing, since none of these layers can afford to be treated as one-time purchases.

The tactics and techniques of cybercriminals will continue to evolve and become ever more sophisticated; entities' investments in the best training and systems must do the same.