MCIT BULLETIN

A PUBLICATION OF MINNESOTA COUNTIES INTERGOVERNMENTAL TRUST

MCIT MISSION:

Providing Minnesota counties and associated members cost-effective coverage with comprehensive and quality risk management services.

VOL. 37, No. 3 | May/June 2024

Dos and Don'ts of Ransomware Response

Provided by Matthew Meade, Esq., Eckert Seamans Cherin & Mellott LLC; and Jeff Birnbach, Sylint LLC

Local government entities, big and small, are often the targets of ransomware and other forms of cyber-extortion. These incidents can have a major impact on the entity's operations, personnel and citizens, ranging from disclosure of sensitive and personal information to permanent deletion of vital documents and records.

Although no two incidents are exactly alike, following basic dos and don'ts can help an organization limit damage, recover faster and reduce the consequences of a cyber-extortion incident.

Ransomware Attacks Unfold Quickly

Imagine you and your team came into the office on Monday morning and found most of your computers were not working and the data on your servers could not be accessed. What would your team do?

Consider this hypothetical ransomware attack timeline.

8:10 a.m.: Amy in accounting calls the IT department but does not reach anyone. She leaves a voicemail message, noting that she cannot log onto her machine after logging off the prior Friday.

8:17 a.m.: Tom in IT is working remotely and tries to log in through the VPN but cannot get through.

8:32 a.m.: Steve in IT calls Tom at home to let him know the servers are not working and asks what he should do. Tom says he is coming into the office and should be there within 30 minutes.

8:44 a.m.: Deputy sheriffs are unable to log into the office's network from mobile devices in their vehicles. Sue in the sheriff's IT suspects the county is having some type of large outage and alerts the chief deputy. She also advises the regional 911 center that the office is having issues.

9 a.m.: The majority of employees have arrived for work and most, but not all, are unable to log onto their computers. The county administrator, Mel, has heard from five department heads so far this morning, and two county commissioners are calling him. His assistant hands him a message that Stan, the local news anchor, wants to do a live interview with Mel for tonight's 5 p.m. broadcast.

9:17 a.m.: Steve and Tom in IT find extortion messages on their file server and their domain controllers with information about how to reach the threat actors via a TOR site. Steve suggests they wipe everything and restore from backups.

9:31 a.m.: The FBI reaches out to the sheriff with information about county devices making connection to a coffee shop in Chechnya.

9:43 a.m.: Ned, the tech rep for the company that leases the copiers to the county, calls to say he heard about this from Steve in IT, and that his brother-in-law is a computer wiz and can help "fix things."

continued on page 5

COMING EVENTS

May 10, MCIT BUILDING, ST. PAUL
9 A.M.: Board of Directors Meeting
1 P.M.: Claims Committee Meeting

May 15 or 22, VIRTUAL, 11 A.M.
"Fundamentals of Performance Management and Evaluations" webinar

May 29, VIRTUAL, 11 A.M.
"Best Practices for Disciplining Employees" webinar

June 12, VIRTUAL, 11 A.M.
"What to Do When Substance Use Affects an Employee's Performance" webinar

June 14, MCIT BUILDING, ST. PAUL
9 A.M.: Board of Directors Meeting
1 P.M.: Claims Committee Meeting

MISSED 'HIRING TOOLKIT' WEBINARS?

Watch Recordings Any Time

This series of webinars offers hiring process risk management best practices for those involved in hiring, such as human resources staff, department heads, managers, etc.

Recordings of the four "Hiring Toolkit" webinars presented in January and February are posted to *MCIT.org/resources*. Use the filters to find them quickly: Enter "hiring toolkit" in the Keyword filter and choose "webinar" from the Resource Type filter.

"Hiring Toolkit" webinars include:

- Hiring Toolkit: Job Applications, Advertising and Job Descriptions
- Hiring Toolkit: Veterans Preference Act and Candidate Screening
- Hiring Toolkit: Interviewing
- Hiring Toolkit: Reference Checks, Background Checks and Pre-employment Testing

Risk Management Consultants: Jim Karels, Joe Cieminski and Richard Miehe

3 Risk Management Consultants Join MCIT Field Services Team

The MCIT field services team filled all open positions earlier this spring when three risk management consultants were hired.

As part of MCIT's commitment to supporting members, the field services team expanded its expertise in data compromise exposures with the hiring of Richard Miehe. He started Feb. 20 and has a background in general liability claims adjusting, risk management and loss prevention in the transportation and manufacturing industry, as well as experience in the technology sector, where he was an account executive for a software management and security company.

Jim Karels joined the team March 18. He has more than 24 years of experience in the public sector and has familiarity with both risk management and loss control. He worked for the Minnesota Department of Corrections and the Metropolitan Airports Commission (Minneapolis-St. Paul International Airport). Karels has a master's degree in risk management from the University of Wisconsin Stout.

Joe Cieminski moved from the property/casualty claims team to take on a risk management consultant role with MCIT April 1. He joined MCIT claims in 2018 and has more than 30 years of experience handling property/casualty claims. He has a bachelor's degree in business administration.

Director of Field Services Kevin Balfanz says, "These hires reinforce MCIT's dedication to proactive risk management, ensuring that members receive top-notch support and guidance in avoiding loss."

Members can contact consultants at **1.866.547.6516**.

RISK MANAGEMENT CONSULTANT DUTIES

MCIT risk management consultants work with members to identify risk exposures of their operations and assist in planning how to mitigate them. Specifically, consultants respond to members' questions about coverage, liability and other risk concerns and can:

- Offer advice about how members can best manage risks
- Provide coverage explanations and analysis
- Review contracts from a risk management perspective
- Train staff about specific topics
- Conduct orientation to the MCIT program for new primary contacts at member organizations

Webinar Series Provides Tips to Improve Employee Performance Management

The four-part "Employee Performance Management" webinar series highlights best practices for managing employee performance, identifies common traps that snare managers and offers strategies to sidestep them. The series kicks off May 15 with webinars every two weeks through June 26.

The sessions are ideal for those who have authority over other employees and are responsible for managing their job performance. Registration is open for all sessions at *MCIT.org/events.*

Each of the below topics is a standalone webinar, but sessions are developed to be attended in series. The webinars run about an hour and offer a Q&A session with presenters at the end of each.

Fundamentals of Performance Management and Evaluations

ATTEND ONE OF TWO LIVE SESSIONS: MAY 15 AT 11 A.M. OR MAY 22 AT 11 A.M.

Presented by Arlene Vernon, consultant with HRx

Vernon reviews the foundations of good employee performance management while discussing areas that often trip up managers. In particular, the session discusses the importance of:

- Coaching throughout the year
- Documentation of employee performance deficiencies and corrective action taken
- Formal annual performance evaluations

Best Practices for Disciplining Employees

MAY 29 AT 11 A.M.

Presented by Ann Goering, attorney and stakeholder with Ratwik, Roszak and Maloney

Goering explores strategies to discipline employees without running afoul of the law. In particular:

- When and how to establish and manage performance improvement plans
- How to make a defensible decision to terminate an employee when necessary

What to Do When Substance Use Affects an Employee's Job Performance

JUNE 12 AT 11 A.M.

Presented by Christina Eberly, clinician and account manager with Sand Creek

Eberly covers signs of substance use and the threshold for reasonable suspicion of substance use by employees. She also addresses:

- Strategies managers can use to respond when an employees' substance use or addiction affects his or her job performance
- Ways to manage an employee's performance while going through treatment
- A review of services available to managers and employees through the Employee Assistance Program to help in these situations

Tips for Effective Difficult Conversations with Employees

JUNE 26 AT 11 A.M.

Presented by Christina Eberly, clinician and account manager with Sand Creek

Eberly provides strategies for having effective conversations with employees about difficult topics, such as poor job performance. Methods discussed include:

- Preparing for the conversation
- Managing emotions during the conversation
- Establishing outcomes

Questions?

Members who have questions about these webinars or their registration status should contact MCIT Communications Manager Heather Larson-Blakestad at *hblakestad@mcit.org* or **1.866.547.6516, ext. 6430.**

HOW TO REGISTER FOR MCIT WEBINARS

Visit *MCIT.org/events* for more information about the performance management webinars and to register for them.

- A person must register separately for each webinar in the series.
- Individuals may register for a webinar any time until the session ends.
- No fee is charged to attend a webinar.

To register for a webinar offered through MCIT:

- Visit *MCIT.org/events* and click the event you want to attend.
- On the event page, click the "Register Now" button to open the registration form.
- Enter information in all required fields and click button to submit the form.

Tip: Be sure to check that the email you enter on the registration form is correct before submitting the form. This is the address to which all communication, including the confirmation email with the link to join, will be sent. If the address is entered incorrectly, you will not receive the link to join.

More tips are provided on the events pages at *MCIT.org/events.*

Avoid the Lure of Phishing Scams

Ransomware attacks get a great deal of press these days, but misdirected payment fraud continues to be a bread and butter scam for thieves. Often the fraud is perpetrated through phishing emails.

The emails typically mimic known vendors, making it easy to fall victim. However a few safeguards and keeping a vigilant eye for fraud can help prevent loss.

Local governments are easy targets for misdirected payment fraud, as publicly available board meeting agendas, summaries and minutes contain listings of vendors, items being purchased or bid and payment amounts.

Spotting and Avoiding a Scam

Although MCIT provides misdirected payment fraud coverage, its limit can easily be exceeded. These best practices can help members spot fraudulent requests before releasing funds:

- **Train all staff** in techniques to identify phishing scams and how to report them.
- Require that staff **verify payment changes** before authorizing a change. Best practice would be to call the vendor or payee using a known, previously verified phone number. Another option is personally to visit the payee.
- **Verification using email is not advised**, but if used, start a new message to the vendor or payee and, again, use a known, previously verified email address for the vendor or payee. This should prevent the message from delivering to the perpetrators of the theft attempt.
- Request that the **member's bank** call a specific contact at the member to **verify a transfer of funds outside of the United States** before processing the release of funds. Most local governments do not send money internationally, but misdirected payment fraud is often perpetrated by those outside of the U.S.
- **Red flag Green Dot Bank in email systems.** This online bank is frequently used in misdirected payment fraud scams.
- **Require the vendor or payee to complete and sign a new direct deposit or ACH form** to provide documentation if an issue arises.
- **Limit** the number of **individuals who can make changes to a vendor or payee's direct deposit or ACH** information and train them on policies and procedures.
- **Investigate unusual requests**, ask questions and verify the authenticity of the request.

MCIT risk management consultant Richard Miehe can assist members with their cyber-security risk management efforts. He has a special focus in this area. Reach Miehe at **1.866.547.6516** or *rmiehe@mcit.org*.

Report Known or Suspected Incidents Immediately

Members should report a misdirected payment incident to MCIT upon discovery. The sooner MCIT can begin investigating the situation, the more likely funds can be recovered. Members should submit claims through the online member portal at *MCIT.org*.

Questions regarding submitting a claim can be directed to Director of Claims Zahir Siddiqui at **1.866.547.6516** or *zsiddiqui@mcit.org*.

SIMPLE STRATEGIES SHORE UP DATA, NETWORK SECURITY

Before taking extraordinary and sometimes expensive steps to implement the latest technical options for cyber-security, an organization should ensure that it has mastered the basics.

4 Best Practices

The Cybersecurity Infrastructure Security Agency of the Department of Homeland Security recommends four key steps to prevent or significantly reduce the risk of data compromises, including ransomware.

1. **Have a strong password policy** that mandates complex and unique passwords. Password management systems can help with the challenges of people forgetting the complicated passwords needed for improved security. Uppercase, lowercase, numbers and symbols are all recommended to be used.
2. **Implement multifactor authentication.** Multifactor authentication requires users to have multiple means to access data, such as first entering a password, then providing a time-limited code that is sent to a mobile phone or a fob.
   - Require employees to double check the authenticity of a payment change request (either amount or where payment should be sent). Staff should check using methods that are currently on record with the member, such as the phone number, not the one included in the request for the change. See "Avoid the Lure of Phishing Scams" above for more.
3. **Repeatedly train employees on how to identify phishing or fraudulent messages.** Most malware comes from phishing. Malware, including ransomware, allows threat actors to gain access to an organization's network and data. Ongoing training about how to spot potential fraud and what to do about it is key to limiting malware and misdirected payments. Certain vendors offer

Dos and Don'ts of Ransomware Response ... continued from page 1

10 a.m.: Mel, the county administrator, calls an emergency meeting for 10:30 a.m. and invites only the IT team and the county auditor.

Although this may seem like a highly condensed and accelerated scenario, it is not. In many cases the situation evolves just this quickly, and in some cases, even faster.

First Steps to Respond

Let's look first at what an MCIT member organization should initially do:

1. **Contact MCIT, the entity's coverage provider.** MCIT can rapidly bring resources including legal counsel experienced in maneuvering through this type of an event, as well as incident response, digital data forensics and investigation experts to help the member limit damage, assess the situation and start working toward recovery.
2. Pull together appropriate department heads for **regular briefings and start planning for work activities** that will likely be restricted for days or even weeks, depending on the severity of the incident.
3. **Use the member's incident response plan** to guide the organization through the process. If the member does not have a response plan, it should start compiling a list of all computers and data repositories. This will be critical to help identify what devices have been affected and what data may not be available.
4. **Determine if backup files are in fact available and viable.** If not, this will affect the member's response options and strategy.
5. **Designate a spokesperson** as the only person authorized to speak on behalf of the organization. Remind all staff and elected officials not to speak with media or discuss the event outside of a "need-to-know" group of key member personnel, legal counsel and forensic investigators. Threat actors often monitor news related to their targeted victims and may use this information to inflict additional damage or leverage against the county in any negotiations.

Common Response Missteps

Now, let's consider what a member should *not* do.

1. **Do not delete any files and start to restore from backups.** Doing this will likely obfuscate or destroy valuable evidence that is crucial to determining what happened and what, if any, data has been accessed or exfiltrated that may trigger notification requirements under state or federal law.
2. **Do not contact threat actors.** Any communications with them should be handled by the incident response experts, as they will have experience in crafting specific communications designed to yield potentially valuable intelligence from the threat actors to help determine data that may have been affected.
3. **Do not issue media statements or give interviews.** Do not share any information the organization may have received from the FBI or other agencies. If absolutely necessary to address an inquiry, the only released information should be limited to "the organization is experiencing a network event and has engaged outside experts to assist in determining the scope and extent of the situation." Once more details are available, accurate and appropriate communications can be developed for public release.
4. **Do not tell departments they will be back up in a day.** Regardless of how solid and complete the organization's backups may be, containment, assessment, preservation and eradication can take days or weeks. The member should let departments know leadership will share accurate information as it becomes available, but the extent of the incident is still being determined.
5. **Do not let outside parties have access to the organization's computers or network**, regardless of how experienced or well-intentioned they are. The incident should be considered a crime scene and treated as any other crime scene would be. This includes limiting information and access only to those who are authorized to engage in the incident response effort.
6. **Do not attempt to "hack back"** or access IP addresses that the member thinks may be related to the attack or the exfiltration of data. Not only is this illegal, but it can also result in damaging important evidentiary information or in some cases, the ability to decrypt.

simulated phishing attacks and training that help keep staff aware of and on guard for attacks.

4. **Require software updates.** Often malware targets vulnerabilities in software that is only fixed via updates. Many updates are made by IT without the end user's knowledge, though with many employees working from home or using mobile devices for work, this becomes even more crucial. The endpoints, which are the specific computers, laptops, tablets or other mobile devices, in addition to the main network servers both need to be updated to maintain security. Staff should not be permitted to delay updates indefinitely.

MCIT Recommendations

Based on actual member cyber claims, MCIT encourages members to implement these additional data compromise risk management strategies:

- **Adhere to the data retention and destruction schedule:** The less data that can be compromised limits the magnitude of an incident.
- **Clean out email:** Email is highly vulnerable to hacking and should not be used as a storage system. Employees should limit how many emails they keep in the email system, particularly those that contain private and personal data. Remind staff that they can save files for future reference in a more secure area on the organization's network.
- **Create a culture of open communication** that makes employees comfortable reporting mistakes and suspected attacks. The quicker the member knows of a potential problem, the faster it can be investigated and addressed, minimizing the fallout.
- **Support cybersecurity infrastructure** such as segmented networks and segregated backups. These two structures allow for better containment of an attack's effects and to return to operations after an incident, so budget for these necessities.

Connect with Staff About Well-being During Mental Health Awareness Month

The Employee Assistance Program offers many resources for members to observe Mental Health Awareness Month in May. The materials make it easy to promote mental well-being across the organization and remind everyone of the support available through the EAP.

Mental Health Awareness Month Resources

AllOne Health is the parent company of the EAP administrator Sand Creek. AllOne Health offers a number of resources specific to Mental Health Awareness Month.

Through the **Mental Health Mondays campaign**, AllOne Health posts shareable graphics and messaging on its LinkedIn page each Monday. Messages focus on themes of mental health matters, self-care, asking for help is a sign of strength and finding help/helping others.

The May **Insights e-newsletter** from AllOne Health covers a range of topics and themes:

- Access to mental health care
- Resilience building and coping strategies
- Psychological safety training

Members can access the current and past newsletters at *AllOneHealth.com/insights*. Members may want to forward the newsletter to staff.

The **webinar** "Mental Health: Support for Others in Distress" is presented by AllOne Health May 23 at no cost. The session explores ways to reduce stigma around mental health issues, provides guidance for initial support to people in distress and identifies resources and how to use the EAP as a next step. Individuals can register for the webinar at *AllOneHealth.com/webinars*.

Mental Health Awareness Month resources from past years are still available at *AllOneHealth.com/blog*.

- Mental Health Awareness Month **Digital Toolkit**
- Mental Health Awareness **Video**
- Mental Health Awareness by the Numbers **factsheet**

General EAP Promotional Items

Remember, MCIT offers items to help members promote the EAP to their employees. Materials emphasize that use of the program is voluntary, confidential and effective.

- Brochures and fliers for employees, supervisors, law enforcement and elected officials
- Wallet card
- Posters and digital images, including law enforcement-specific messages
- Mini discussion scripts to remind staff about the program's services and how to access the EAP
- Series of short videos including ones specifically for supervisors and for law enforcement
- Sample message from sheriff to staff about the EAP, which can be modified as desired

Members can download materials at *MCIT.org/resources*. Choose "Employee Assistance Program" from the Topics filter to find them quickly.

PUBLIC SAFETY WELLNESS INITIATIVE

The Minnesota Public Safety Wellness Initiative is a multi-agency partnership dedicated to supporting the mental health of public safety professionals in Minnesota. MCIT is proud to be a partner.

The initiative is developing public-safety specific information, tools and resources. Currently sheriffs can use these videos with their staff to build a culture of openness about and support for mental health among their teams:

- "Behind the Badge: Mental Wellness in Law Enforcement"
- "Accept, Prevent, Treat"
- "PTSD: It's Treatable"
- "Make Peer Support Part of Your Culture"

Sheriffs can view the videos on the Minnesota Public Safety Wellness Initiative Facebook page. It is also a great place to keep pace with the partnership.

6 Ways to Promote Mental Health Awareness

1. Send a weekly Mental Health Monday email to staff, sharing different resources each week.
2. Post resources on the organization's blog, intranet or social media.
3. Invite staff to attend an AllOne Health webinar.
4. Include brochures, fliers and videos in employee onboarding and training.
5. During a staff meeting, mention the importance of mental health awareness. Remind staff that the EAP is available to support them at no cost and provide the appropriate brochure.
6. Send a personal message to staff about the importance of mental health awareness and summarize EAP services that are available to them.

WHAT IS THE EAP?

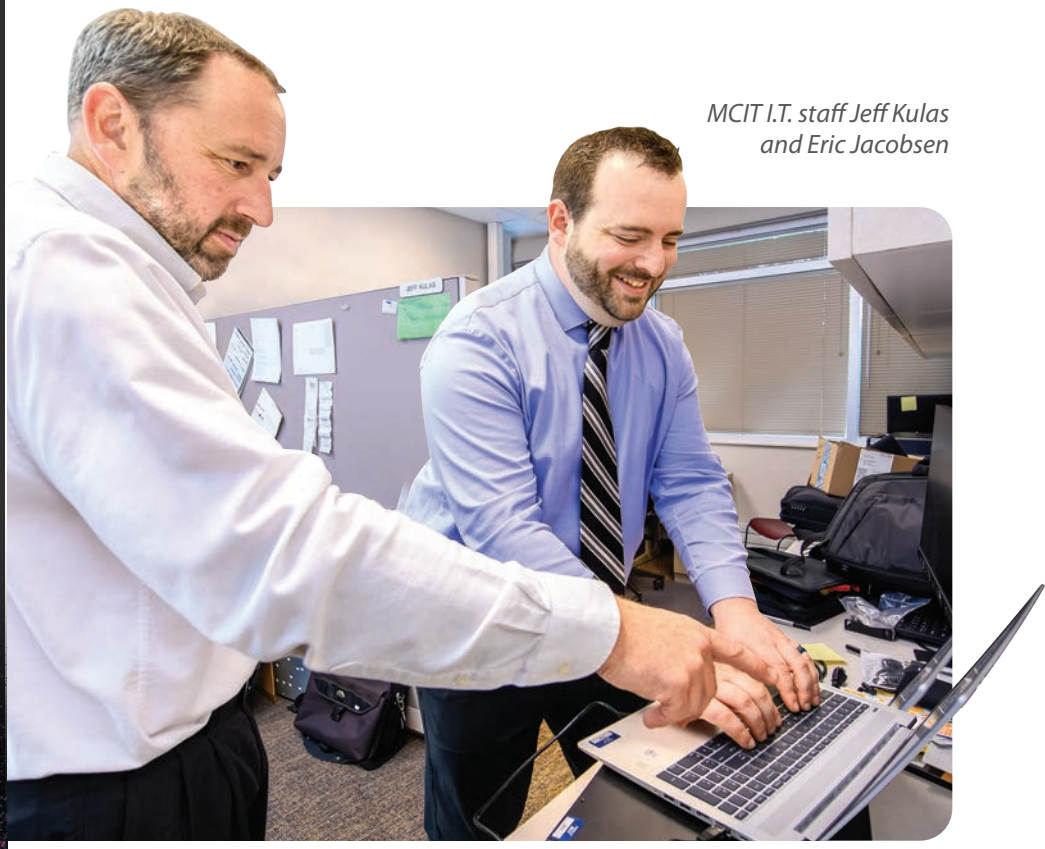
The MCIT Employee Assistance Program helps employees and officials of MCIT member employers identify and resolve challenges that may affect their mental or emotional well-being, personal life or performance at work.

The EAP is a voluntary program that can assist employees, their spouse and dependents through access to six no-cost sessions for each identified issue with a master's level counselor.

Employees should call **1.800.550.6248** or visit *SandCreekEAP.com* (the website of the EAP administrator) to connect with an Employee Assistance Program counselor. Services are available in person, virtually or by phone throughout Minnesota.

For additional information about the Employee Assistance Program, visit *MCIT.org/services-programs*.

MCIT contracts with Sand Creek, an AllOne Health company, for EAP services.



MCIT I.T. staff Jeff Kulas and Eric Jacobsen

Spotlight on MCIT I.T. Department

The MCIT information technology department is tasked with big responsibilities, namely ensuring that the organization's computer systems and applications operate effectively and that those systems remain secure.

The team includes I.T. Manager Jeff Kulas and information technology specialist Eric Jacobsen.

Keeping Systems Running

It takes several servers, systems, applications and backups for MCIT to operate effectively. The I.T. staff continually evaluates them to identify areas of improvement and facilitate upgrades when necessary. The team also troubleshoots issues as they arise to maintain operations.

In particular, Kulas and Jacobsen ensure that the claims and underwriting systems operate effectively, and they work with the system vendor to manage updates and to develop enhancements.

In addition, the team configures the phone system, and monitors and provides communications into MCIT, such as fiber lines for high-speed Internet.

Maintaining Systems Security

The I.T. staff takes the security of the MCIT computer network seriously and continually researches and implements best practices in this area.

The department keeps software and hardware up to date and installs timely patches. The team installs and monitors backups and data protection systems regularly, including antivirus, anti-malware and other cyber-security threat monitoring tools.

The team also manages the multifactor authentication system for users of the MCIT network, a key measure in its security.

Technology Support for Meetings

The MCIT building offers space for members and tenants to host events. Several of these rooms include enhanced presentation technology, such as virtual connections. The MCIT I.T. staff offers support for these capabilities to meeting organizers.