SPRING 2024 APRIL/MAY/JUNE VOLUME 68, ISSUE 2

Minnesota Counties

A Quarterly Publication of the Association of Minnesota Counties

Cass County Commissioner

AMC President Neal Gaalswyk during AMC's Board of Directors meeting in April.

Association of Minnesota Counties
125 Charles Avenue
St. Paul, MN 55103-2108

MCIT
Minnesota Counties Intergovernmental Trust
SINCE 1979

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."

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:

- **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.
- **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.
- **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.

- **Determine if backup files are available and viable.** If not, this will affect the member's response options and strategy.
- **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.

- **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.
- **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.
- **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.

Commissioners, administrators, emergency managers, and IT staff from around the state gathered in St. Cloud on April 25 for the first **Cybersecurity for County Decision-Makers conference**, created through a collaboration between AMC and MCIT, and featured local and national speakers addressing important cybersecurity issues at the county level. Attendees learned about current threats to county networks, tools they can use immediately to mitigate these threats, and how to respond to a security breach. AMC and MCIT also provided additional resources for county staff to use in order to better prepare for cyber threats.

- **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.
- **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.
- **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. ●

MCIT, continues on page 22.