RISK Michigan Municipal Risk Management Authority

THE RISK JOURNAL

A PUBLICATION FOR MMRMA MEMBERS AUGUST 2021

CYBER RISK MANAGEMENT, PART 5

# Understanding and Avoiding the Many Risks of Ransomware

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

*Stephen J. Tobler, Senior Risk Control Consultant*


**In a typical ransomware attack, cybercriminals threaten to publicly expose or destroy sensitive information unless a ransom is paid.**

WHAT DO MICROSOFT, Michigan State University, SolarWinds, Broward County School District, Flagstar Bank, and Jones Day law firm have in common? Not to mention Jackson County, Georgia; Riviera Beach, Florida; and LaPorte County, Indiana? All have been victims of ransomware attacks; the three public entities paid ransoms from $130,000 to $600,000.

On July 2, 2021, Miami-based Kaseya Limited experienced a ransomware attack. The developer creates software to help manage information technology infrastructure for businesses in ten countries. The criminals sought $70 million in ransom. Wikipedia reports that a Norwegian supermarket chain, one of over 1,500 businesses impacted, "had to close down its 800 stores for almost a week, some in small villages without any other food shops. They did not pay ransom but rebuilt their systems from scratch after waiting for an update from Kaseya."[1]

## Incidents are on the rise

Ransomware is potentially the most significant and costly type of cybercrime MMRMA members could face. According to Barracuda Networks, "Local government bodies are the most likely target for ransomware attacks." [2]

According to MSN.com, "The number of organizations affected by ransomware has jumped 102 percent compared to the beginning of 2020 and 'shows no sign of slowing down,' according to IT security firm Check Point (May 2021). The average ransom payment in 2020 is up 171 percent to $312,493, compared to $115,123 in 2019." [3]

**Could your organization be targeted next? Are you prepared? Can you afford to pay a sizeable ransom?**

Most organizations don't have an extra $300,000 to spend on a ransom payment. MSN notes: "For many companies, the actual ransom payment isn't even the most expensive part of the attack. Companies have to restore backups, rebuild systems, work with forensic investigators to ensure that the hackers are truly locked out and, in many cases, implement stronger cybersecurity controls to revent future attacks."

Beyond monetary costs are reputational harm and the potential loss of the public's trust in the organization or public entity.

## Cybercrime has many victims

Ransomware attacks victimize not just targeted organizations; they affect all of us. Successful cybercriminals gain access to people's personal, sensitive, and confidential information. What's more, companies could be forced to pass along soaring cybersecurity costs to their customers through price increases for their services or products.

Ransomware has also had a significant impact on the reinsurance market and companies that provide cyber insurance. "The latest report from Marsh, which offers insurance brokering, indicates that U.S. cyber rates were up by 35% in the first quarter of 2021." [3]

A new "triple threat extortion" method could further

*continued on page 4*

# Lightning Strikes and You: Preparing for This Natural Phenomenon

*by Jeffrey Satkowski*
*Executive Director, Lapeer County Central Dispatch*

**Michigan had 1.91 million lightning strikes in 2019, according to the National Lightning Detection Network.**

YOU NEVER KNOW WHEN lightning will strike your business. For most people, this isn't much of a concern because their buildings may not be very tall compared to other structures in the surrounding area.

However, if your building is among the taller ones, you may need to take a more serious look at lightning protection by implementing proper grounding systems.

## Learning from experience

Last month, my office was struck by lightning for the third time in my 20 years of working here. It doesn't help that we have a 238-foot "lightning rod" behind the building, also known as a radio communications tower. It's the second tallest structure in our city: The CN railroad communications tower, a mile down the road, is slightly taller than ours.

The first two strikes we took years ago were quite damaging to some of our systems. *Government Technology* published an article about one of the strikes in November 2010.[1] I recall that we lost several servers, a phone system, parts of the radio and microwave system, among others.

**Lapeer County's power supply and generator systems are essentially a backup to a backup.**

The damage wasn't easy to fix and was costly, in the range of tens of thousands of dollars.

In the years since those two strikes, we have upgraded our entire radio system from our legacy system, migrating to the Michigan Public Safety Communications System (MPSCS). In the process, we moved to the latest industry standard in grounding two-way communications systems, the R56 standard developed by Motorola Solutions.

R56 takes into consideration fire codes, electrical codes, lightning protection, tower grounding codes, and construction codes.[2]

In 2020 we also upgraded our uninterruptible power supply (UPS) and generator systems from a tier I to a tier IV system. That means we went from one UPS and one generator to two UPS and two generators. We now have fully automated and redundant rerouting systems, not only for when commercial power goes out, but also to keep our 911 center operational if any other part of the tier IV system fails.

Essentially, this tier IV system is a backup to a backup system. Combined with the R56 grounding standard, our updated system served us well at the end of June 2021.

## Weathering summer storms

When an isolated thunderstorm descended several weeks ago, lightning struck our tower and caused everything to blink out for a millisecond. Thankfully, due to the UPS system's high industry standard of keeping electricity flowing—and flowing consistently—we didn't lose many operational abilities.

Most computer systems can withstand a 6-millisecond interruption of power without failing or powering off, and these UPS systems kept our systems running well.

Despite the upgraded standard in grounding and new UPS equipment, a lightning strike can still overpower systems and cause weird effects. We didn't come away from this latest strike unscathed, but we fared far better than the two previous times.

The extent of the damage, as we know it today, is that we had problems on two dispatch console phones with heavy static on the lines. Our primary generator was knocked offline and our building security camera system was severely damaged and will need to be replaced.

We were able to repair the phone troubles within an hour or two. Meanwhile, our primary generator was offline for about 12 hours until electricians could assess the damage and find a workaround to bring it back online while awaiting repair parts.

## Outages can have a far-reaching impact

Our rationale for installing the tier IV system was based on our experience of not

*continued on page 3*

*1 https://www.govtech.com/public-safety/how-emergency-responders-avoid-downtime-in-a-disaster.html*
*2 https://blog.westcan-acs.com/2016/03/18/the-r56-standard-and-what-it-means-for-you/*
*3 National Oceanic and Atmospheric Administration, https://www.weather.gov/safety/lightning*

# New Participants Provide Opportunities for MMRMA, Membership

*by Michael L. Rhyner*

LIKE ORGANIZATIONS everywhere, MMRMA is experiencing increased turnover in its membership. These changes are attributable to many factors, including retirements, job changes, and elected officials choosing not to file for re-election. In addition, many employees are seeking alternative working arrangements in a post-COVID environment.

## Succession planning is key

One of the Board of Directors' strategic priorities is succession planning, not only for the MMRMA staff, but also for board and committee members and our membership as a whole.

We still have a significant constituency of longstanding MMRMA Member Representatives and other contributors who became active in MMRMA in its formative years. Some now have decades of involvement and are our most steadfast supporters. Nonetheless, the composition of our constituency is constantly shifting. Over the past three years, we have seen 179 changes in Member Representatives, which accounts for 44 percent of our membership.

## Telling newcomers our story

Often, new member representatives have limited institutional history with MMRMA, so it's important that we familiarize them with the history, structure, and unique benefits of MMRMA. We are designing enhancements to further reinforce our story and the many advantages of this successful organization.

In 1980, a small number of Michigan municipalities


**We will recognize 29 first-time attendees at our Annual Meeting and welcome them to the MMRMA family.**

banded together to provide a mechanism to jointly self-insure risks when commercial insurance was either unavailable or prohibitively expensive. This was the genesis of MMRMA. For over 40 years, through shifting reinsurance markets and emerging challenges, we have met the needs of our membership as it has grown to over 400 public entities across Michigan.

## Training and committees provide a connection

As our membership continues to evolve, we always welcome newcomers to MMRMA's education and training programs and invite them to register for a login on mmrma.org to access our plentiful resources.

We also encourage members to seek an appointment to one of MMRMA's valuable committees. This can enhance participants' risk management knowledge as they network and collaborate with peers statewide. The relationships developed by those serving on our committees have helped them throughout their entire working careers.

Training opportunities and committee vacancies are regularly posted on the MMRMA website. Please contact Tamara Christie at tchristie@mmrma.org for more information.

# Lightning Strikes, continued from page 2

having an operable generator during a period of commercial power outages.

Without the backup to a backup, those 12 hours could have been catastrophic for the residents of Lapeer County. Fortunately, we never lost commercial power and didn't need to run on our secondary backup generator. But if we'd still had only one generator and one UPS, residents couldn't have reached 911 for help, and public safety professionals wouldn't have been able to respond to fires, auto accidents, or ambulance calls.

In such a scenario, the 911 center could not perform its core purposes of serving the public and saving lives. It's difficult to fully fathom the potential exposure if anyone had lost life, limbs, or eyesight because they couldn't reach emergency personnel, or if those responders couldn't communicate effectively to respond to the emergency. Beyond any tragic loss, the costs could potentially be in the millions if the 911 center were sued.

## More than dispatch centers

You may not be running a 911 call center where the odds of a lightning strike might be greater. Still, public entity IT administrators should be aware that this could happen at their properties.

Commercial power surges can and do happen for a variety of reasons, and if computer systems are not properly protected, such a surge could wreak as much havoc as a lightning strike.

It is best practice to have appropriate grounding systems for every IT-related piece of equipment a public entity owns, as well as a UPS system for all critical infrastructure. These steps can help protect against surges and conditions related to electricity flowing through equipment and infrastructure.

Last but by no means least, all data on IT systems should have proper backup and recovery plans and practices in place to ensure the continuity of the public entity and protect against data loss.

# Ransomware Risks, continued from page 1

impact organizations and individuals. *Tech Republic* explains: "[C]riminals send ransom demands not only to the attacked organization but to any customers, users or other third parties that would be hurt by the leaked data. ... In one incident from October [2020], 40,000-patient Finnish psychotherapy clinic Vastaamo was hit by a breach that led to the theft of patient data.

"[Cybercriminals] demanded a healthy sum of ransom [and] also emailed the patients directly, demanding smaller sums of money or else they would leak their therapist session notes. Due to the breach and the financial damage, Vastaamo was forced to declare bankruptcy and ultimately shut down its business." [4]

## Take protective action

No entity is immune from attacks on their hardware and software systems. Members are encouraged to have IT professionals on staff or consultants at the ready, to develop a sound cyber incident response plan, and to implement proper cyber hygiene policies for BYOD (Bring Your Own Devices)—or prohibit business use of personal devices entirely.

**Tech Republic shares these tips from Check Point, a cybersecurity firm:**

**Raise your guard on weekends and holidays.** Most ransomware attacks occur on weekends and holidays when people are less likely to be on the lookout.

**Keep patches up to date.** When the infamous WannaCry attack hit in May 2017, a patch was already available for the exploited flaw. Many organizations had failed to install it, leading to a ransomware attack that affected more than 200,000 computers in just a few days. Keep your computers and systems up to date with the latest patches, especially ones considered critical.

**Use anti-ransomware tools.** Some attackers send targeted spear phishing emails to trick employees into revealing account credentials that can open up access to the network. ... Anti-ransomware tools monitor programs for any suspicious behavior [and] stop encryption of sensitive files before any damage is done.

**Educate users.** Many attacks begin with a phishing email that coaxes the recipient to click on a malicious link. Educating employees on these types of emails can stop an attack before it's too late.

**Stop ransomware before it starts.** Many ransomware attacks don't start with ransomware—they start with malware infections. Scan your network for malware such as Trickbot, Emotet and Dridex, which can pave the way for ransomware.[3]

For more information, visit stopransomware.gov, and download a federal Cybersecurity & Infrastructure Security Agency (CISA) ransomware guide at cisa.gov.

The "Members Only" section of mmrma.org offers risk control bulletins and resources to assist in developing a sound cybersecurity program. Contact Membership Services for further guidance.

*1 https://en.wikipedia.org/wiki/Kaseya_VSA_ransomware_attack*
*2 https://www.thinkdigitalpartners.com/news/2020/08/28/local-governments-biggest-target-of-ransomware-attacks-in-2020/*
*3 https://www.msn.com/en-us/money/other/ransomware-rattles-cyber-insurance-market/*
*4 https://www.techrepublic.com/article/ransomware-attackers-are-now-using-triple-extortion-tactics/*

*Railroads were the vital link between Michigan's vast natural resources and industrial centers in the East and Midwest. Massive coal-fired locomotives like this one on the Pere Marquette Line, now retired in Grand Haven, could pull a mile-long train at speeds of up to 50 miles per hour.*

Michael Rhyner
Executive Director
mrhyner@mmrma.org

Bryan J. Anderson, CPA
Managing Director
banderson@mmrma.org

Cindy King
Director of Membership Services and Human Resources
cking@mmrma.org

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.