RISK MICHIGAN MUNICIPAL RISK MANAGEMENT AUTHORITY

THE RISK JOURNAL

A PUBLICATION FOR MMRMA MEMBERS OCTOBER 2021

CYBER RISK MANAGEMENT, PART 6

Types of Cyberattacks and Guidance for Risk Avoidance

by Cindy C. King, Director of Membership Services and Human Resources and Stephen Tobler, Senior Risk Control Consultant

Ransomware generates the most media attention, but cybercriminals have many other tools in their toolbox.

CYBERATTACKS TAKE MANY forms, and all can create problems and disrupt operations. Some attacks, like ransomware, are typically more serious and costly. The worldwide WannaCry ransomware attack in May 2017 targeted computers using Microsoft Windows operating systems.

According to Wikipedia, the attack was thought to have affected more than 200,000 computers across 150 countries with total estimated damages ranging from hundreds of millions to billions of dollars.

Variety of attack types

Ransomware attacks may generate more media attention, but criminals use many other methods, including:

Email phishing. Emails contain a malicious file, link, or malware that enables the cybercriminal to use a victim's email to spread infection throughout an organization or to the victim's contacts.

Denial of service. Cybercriminals intentionally degrade or block computer or network resources.

Drive-by download. Takes advantage of an outdated browser, app, or operating system with security flaws to lead users to unknowingly download a virus or other malicious software.

Rogue software. Users are tricked into believing their system has a virus and manipulated into paying money to remove the supposed virus, which then downloads actual malware onto the system.

Allowlisting identifies known files, applications and processes and allows only them to run, blocking all others.

Remote Desktop Protocol (RDP) vulnerabilities. By controlling resources and data over the internet, a cybercriminal could deploy malware to attack systems.

Social engineering. This involves psychologically manipulating people, often over the phone, into violating normal security procedures—such as divulging confidential information—to gain access to buildings, systems, or data.

Ransomware. Malware encrypts data on a computer or system, making it unusable. The cybercriminal holds the data hostage until a ransom is paid.

Cyberattacks often occur long before they are detected. By then, cybercriminals have already infiltrated systems and are monitoring activity, reviewing data, and determining when to launch their attack. Organizations may not be aware of an attack until a ransomware demand is made.

Measures to avert attacks

MMRMA members are encouraged to take the following actions to protect their networks and data:

> Back up critical information, offline storage, and test all backup methods for reliability.

> Risk analysis to identify vulnerabilities (see the December 2020 *Risk Journal).*

> Employee training to understand and implement cybersecurity best practices.

> Vulnerability patching of known deficiencies.

continued on page 2

Types of Cyberattacks, continued from page 1

> Allowlisting, which allows only approved programs to be run on the network.

> Implementing incident response plans and regularly conducting tests of such plans.

> Assessment and testing of business continuity to ensure that operations can continue without access to networks.

> Penetration testing of the member's own systems to confirm their security.

Three steps for members

Today, it is not a question of "if" but "when" an organization will become the victim of an attack. Ongoing, routine 24/7 monitoring of a member's network, systems, and data is critical to guard against cyberattacks.

At a minimum, members are encouraged to take three essential steps when it comes to cyber risk:

1. Recognize that all organizations, no matter how large or small, how complex or simple, how vigilant or unprepared, can become the victim of a cyberattack.

2. If your entity has become the victim of a cyberattack or you believe you might be under attack, immediately contact MMRMA's Claims and Legal Services department so we can partner with you and take steps to protect your networks, systems, and data.

Digital forensics examines system data, user activity, and other evidence to identify the extent and source of the attack.

3. If your organization is the victim of a ransomware attack, notify law enforcement, particularly the FBI or Secret Service field offices.

Immediate action is crucial

The U.S. Justice Department recommends the following actions, especially if your organization is infected with ransomware:

> Isolate the infected computer(s) immediately.

> Isolate or power off affected devices that have not yet been completely corrupted.

> Immediately secure backup data or systems by taking them offline.

> Contact law enforcement immediately.

> Collect and secure any parts of the ransomed data that might exist.

> If possible, change all online account passwords and network passwords after removing the system from the network.

> Delete registry values and files to stop the malware from loading.

https://www.justice.gov/criminal-ccips/file/872766/download

Mitigating an attack

Notifying MMRMA's claims and legal staff as soon as an attack is discovered is critical. That way, our team can provide ongoing guidance and may also direct you to other resources to assist with necessary post-attack efforts.

Mitigation might include taking the above actions as well as seeking assistance from a company specializing in Digital Forensics and Incident Response (DFIR).

According to Crowdstrike.com, DFIR has two components:

Digital Forensics: A subset of forensic science that examines system data, user activity, and other pieces of digital evidence to determine if an attack is in progress and who may be behind it.

Incident Response: The overarching process that an organization follows to prepare for, detect, contain, and recover from a data breach.

https://www.crowdstrike.com/cybersecurity-101/digital-forensics-and-incident-response-dfir/

RAP and CAP grants help offset cybersecurity costs

The need for effective cybersecurity has never been more acute. To that end, MMRMA offers Risk Avoidance Program (RAP) grant funding to help offset costs for:

> General cybersecurity training for employees

> Two-factor authentication

> Vulnerability assessment/penetration testing

We also offer CAP grants to assist with the costs of obtaining these cybersecurity certifications:

> GIAC Certified Intrusion Analyst

> GIAC Continuous Monitoring Certification

> Certified Information Systems Security Professional

> Certified Chief Information Officer

> ICMA Cybersecurity Leadership Academy

See the Members Only section of mmrma.org for risk control bulletins and model policies to aid in developing a sound cybersecurity program.

MMRMA Recognizes Milestone Member Achievements

WHILE EACH YEAR PRESENTS its own challenges, the past two years have seemed particularly demanding. That can make success stories especially gratifying, and these MMRMA members achieved some big wins in 2021.

Monroe County

In August, the Monroe County Sheriff's Office became the first in Michigan to be certified for making medication and treatment available to incarcerated individuals with opioid use disorder (OUD).

The Center for Behavioral Health and Justice (CBHJ) at the Wayne State University School of Social Work grants the certification to counties that successfully implement all elements of the In-Jail Medication Assisted Treatment model, including:

- Screening for OUD at booking
- Availability of all three Food and Drug Administration (FDA) approved medications for opioid use disorder (MOUD)
- Providing concurrent psychosocial services for detainees receiving MOUD
- Comprehensive planning for inmates' release.

Starting in April 2020, leaders in Monroe County's jail and healthcare systems partnered to prioritize this

Fewer than 1% of jails and prisons nationwide provide medications for opioid use disorder.

evidence-based standard of care—cited by CBHJ as the gold standard—for detainees seeking recovery.

As the CBHJ's press release states, the Monroe County Sheriff's Office "...demonstrated that it is possible to respond to multiple health crises—the COVID-19 pandemic and the overdose epidemic—concurrently." Ninety-six individuals were enrolled during the program's first year.

"It's the right thing to do," said Sheriff Troy Goodnough. "We find that a portion of individuals who suffer from drug addiction suffer from co-occurring mental health disorders. We need to give them the opportunity to be productive members of society."

https://behaviorhealthjustice.wayne.edu/news/monroe-county-jail-achieves-gold-standard-of-medical-care-for-opioid-addiction-44977

Northville Township

This summer, all nine department heads in Northville Township successfully passed the Fundamentals of Emergency Management course through Federal Emergency Management Agency (FEMA).

The goal: to prepare them for incident management and support activities for any natural, technical, or human-related hazard or emergency. The team is equipped to coordinate resources for an efficient, effective response. They also have a clearer view of how FEMA operates and how it fits in with assisting township residents.

"We want to be prepared because it's our mission to deliver excellent public service and Northville Township has some areas of risk, including the railroad tracks that go through our community," said Todd Mutchler, Township Manager and Public Safety Director.

According to Mutchler and his team, the directors will participate in tabletop simulator training this fall, with the assistance of the Canton Township Emergency Manager, to further develop their skills.

https://www.twp.northville.mi.us/get_connected/news/press_releases/township_leaders_complete_f_e_m_a_emergency_management_training

GRAND RAPIDS: Plaster Creek Park

The City of Grand Rapids' Plaster Creek Family Park received a Park Design award from the Michigan Recreation & Park Association (mParks) in recognition of the park's innovation, aesthetic quality, and functionality.

Plaster Creek is part of the city's partnership with Grand Rapids Public Schools to create green schoolyards in park-deficient areas. It features an outdoor nature classroom, a stump forest, log jam, and other features made from fallen trees harvested by the city's Forestry Division. The park also includes a rain garden, native meadow planting, and picnic area.

Congratulations to Parks Director David Marquardt and the city's entire Parks and Recreation team!

RISK MICHIGAN MUNICIPAL RISK MANAGEMENT AUTHORITY

Celebrating 40 Plus One Years at Annual Meeting

Now in its 21st year, the Apple Fest in Charlevoix each October showcases dozens of Northern Michigan orchards, with samples of more than 30 varieties of the sweet fruit. The Paula Red, available only in October, was discovered in Sparta, Michigan.

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

by Tamara Christie
Communications Manager

THE AUGUST ANNUAL MEETING was a welcome chance for members to reunite with MMRMA, business partners, and one another. Themed "40 Plus One Years of Innovative Leadership," the event acknowledged that we weren't able to celebrate our 40th anniversary in person last year. This year's record registrations amidst an ongoing pandemic demonstrated the importance of face-to-face interactions as a hallmark of our organization.

Honoring our history

Reflecting the leadership theme, MMRMA honored the three surviving past chairmen of the Board of Directors: Jim Kelly, Kurt Humphrey, and Jim Kohmescher. With words of gratitude, current Board Chairman Michael Bosanac and Executive Director Michael Rhyner recognized these contributors to MMRMA's four-plus decades of membership service. Their commitment to the organization and fellow members was integral to our success.

Bosanac and Rhyner also recognized past Board member Tracey Schultz Kobylarz, whose service ended in November 2020 upon her retirement from Redford Township. She described her time with MMRMA as one of the best experiences of her professional career.

Meagan Johnson discussed generational differences in the workplace.

Educational highlights

Certified risk management and project management professional Joseph Mayo gave his perspective on effective risk management at the opening session. He outlined four ways to treat risk—accept, avoid, transfer, or mitigate—and noted that "accepting" risk does not mean ignoring it. On Friday morning, Mayo delved further into the development of risk policies. He stressed the importance of communicating to stakeholders the rationale for managing risk and of identifying roles and responsibilities for risk management governance.

Cyber remains a hot topic

Cyber security expert Jon Engstrom shared his experiences as both an investigator and a "recon specialist," a role in which he joins hacker groups to "see behind the curtain" and understand how to protect against cybercrime tactics. Engstrom demonstrated how easily criminals can infiltrate systems and con people. He also shared a resource with practicable ways to prevent cyberattacks, and how to respond when they occur.

People skills also important

Rounding out Friday's training, journalist Tim Skubick hosted what another speaker described as "the best Zoom presentation" they'd ever seen. Through a rotating camera in the room, Skubick could see his audience. He called upon several members as he taught tips to deal with the media, including connecting with reporters on your beat, getting back to them when you say you will, recording interviews, and never walking out on one.

At Saturday's Annual Business Meeting, the Board and guests heard reports from staff, service providers, and standing committee chairpersons, followed by a vibrant and informative presentation from speaker Meagan Johnson. She shared what she calls "signposts" of the different generations found in today's workplace. Signposts explain how "people born during a given timeframe … experience similar situations." According to Johnson, these groups' differences are largely due to how their environments—including events, technologies and the economy—have shaped them.

Resources from Mayo, Engstrom, and Johnson are available to logged-in users at MMRMA.org. Contact Tamara Christie at tchristie@mmrma.org if you need assistance.