RISK MICHIGAN MUNICIPAL RISK MANAGEMENT AUTHORITY

THE RISK JOURNAL

A PUBLICATION FOR MMRMA MEMBERS OCTOBER 2023

RISKS IN MEDICAL CARE, PART 8

Managing Infrastructure and Environmental Related Risks

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

THIS ARTICLE CONCLUDES our series on risks in medical care with a focus on infrastructure and environmental risks that may impact the effective delivery of care.

Infrastructure concerns

Inadequate infrastructure may limit the ability of emergency medical responders to reach injured or ill people quickly and safely transport them to the appropriate facility. Many factors can impede timely medical response, including traffic conditions, distance from medical care facilities, or remote locations such as at the bottom of a ravine or underground.

Infrastructure challenges may also include routes with limited access points, slow-moving trains, or roadways that are flooded, blocked by debris, or are otherwise in poor condition. Michigan roads and routes have faced all these challenges over the past several years.

The smoke from wildfires in Canada polluted the air in much of Michigan for many weeks this summer.

Facilities shortage

Availability of facilities and personnel creates other risks. Rural areas often find it challenging to attract healthcare professionals, and many counties and localities lack the resources to build healthcare facilities or invest in the technology for telehealth services.

Mental health challenges

For some time, issues related to mental health and the lack of affordable quality mental healthcare have garnered the attention of the media, public officials, and members of the community.

"People with mental illness… are suffering the tragic consequences of four decades of mental health defunding and privatization," writes Allen Frances in an editorial on Statnews.com. "350,000 people with mental illness are in jails or prisons; 250,000 of them are homeless; and the average life span of those with severe mental illness is 20 years less than that of the general population."

Frances adds: "Law enforcement officers, sheriffs, and judges have become the most vocal critics of the criminalization of mental illness and are now among the strongest advocates for improved community treatment and housing." Sending "untrained police officers to be first responders for people with untreated mental illness puts them in untenable positions… And once in jail, people with mental health issues are difficult to manage." [1]

Environmental factors

Environmental factors compete for agencies' finite resources. Risks include exposure to pollution, lead, or PFAS (to name a few), living or working near nuclear power plants, and the effects of wildfires or other weather-related events. The environment can contribute to chronic diseases, including asthma and cancer.

Healthcare as an industry also creates environmental risks. As the American Medical Association (AMA) notes,

continued on page 2

1 *https://www.statnews.com/2021/07/09/ignoring-mental-health-infrastructure-costly-mistake/*

Infrastructure,

continued from page 1

"The U.S. health care sector is the second-largest industry contributing to landfill waste worldwide." [2]

Weather-related events

Deloitte Insights reports that "In 2021 alone, the United States saw a historic deep freeze in Texas, the hottest summer on record [until 2023], the driest month in California since the state began gathering data, and the third-most named hurricanes in recorded history."

"Each of these events exacted a very real cost on human health. The winter storm and frigid temperatures in Texas overwhelmed hospitals and emergency departments (EDs), seriously disrupted health care operations, and forced the cancellation of elective surgeries. On the other extreme, the heat wave in King County, Washington drove a spike in ED visits for heat-related illness in a single weekend in June 2021." [3]

Climate-related impacts also include air quality and the effects of ground level ozone, the spread of allergens, and mold growth. Disease-carrying insects like the mosquito can spread viruses (West Nile), and deer ticks can spread Lyme disease.

Healthcare facilities are switching to green cleaners, reusable products, and cutting down on use of plastics to reduce their environmental footprint.

Investing in rural healthcare facilities will improve community health and also attract badly needed businesses.

As the American Hospital Association (AHA) notes, "Everything that humans need for their survival and well-being depends, either directly or indirectly, on the natural environment. …Becoming a positive force for environmental health leads to human health and wellbeing." [4]

Mitigating these risks

Jessica Seigel cites the obvious need "to improve telehealth and transportation services to increase availability and delivery of care."

Seigel posits that investments in rural infrastructure will improve overall health in those areas. She suggests that building rural hospitals will attract business, adding that "funding is key to providing educational programs to train rural IT professionals in health care, as well as doctors, nurses, and medical staff how to use technology, including utilization of data and analytic tools to demonstrate and improve quality." [5]

Other mitigation tools include enhanced training for emergency medical care providers in rural areas. Examples include Comprehensive Advanced Life Support (CALS) training and Rural Trauma Team Development Course (RTTDC), which focuses on a team approach to perform initial evaluations and resuscitations on trauma patients.

As to environmental risks, the AMA *Journal of Ethics* states, "A climate lens must be applied to every aspect of healthcare decision making: facility operations, food services, supply chain, employee commutes, waste management, clinical care, and financial investments … [T]he health sector must join other sectors in halving emissions by 2030." [6]

Other recommendations include upgrading equipment and, where practical, switching to reusable products such as washable gowns and blood pressure cuffs. Many medical care facilities have begun using certified green cleaners to reduce exposure to workplace chemicals. Still others are reducing their dependence on plastics. Each such change helps to reduce waste that enters landfills as well as chemicals that contribute to environmental degradation and climate change.

MMRMA counts among its membership many medical care providers. We remain a trusted partner for them and all members through training, policy and procedure brochures, and other resources on www.mmrma.org. The Membership Services team also assists members through risk control guidance, site visits, and much more.

2 https://www.ama-assn.org/delivering-care/public-health/us-health-system-must-come-terms-its-environmental-impact

3 https://www2.deloitte.com/us/en/insights/industry/health-care/climate-change-and-health.html

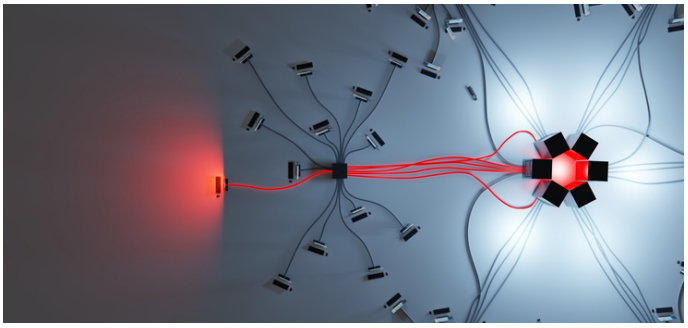
4 https://www.aha.org/sustainability

5 https://www.ruralhealth.us/blogs/ruralhealthvoices/february-2018/rebuild-rural-the-importance-of-health-care-in-in

6 https://journalofethics.ama-assn.org/article/how-should-we-respond-health-care-generating-environmental-harm/2022-10

Security Woes: Be Brilliant at the Basics

by Doug Start
Director of Technology,
City of Grand Rapids
Technology and Cyber-security Risk Control Advisory Committee Member



THE NEWS TODAY HAS no shortage of headlines in the information technology space. Unfortunately, stories on data breaches, network disruptions, and holding data for ransom are just as frequent as those about innovations. Where does network security fit into the IT professional's priorities? With pressures to innovate, enhance communication, help drive products to market, and run a lean but effective operation, today's IT leaders have a lot to handle.

As we all know, adding resources to one priority typically means less for others. Making the business case for enhanced network security can be an uphill battle, and some entities are just not big enough to afford the next-generation tools being touted in the industry.

So, what do you do? Sit and wait for an adverse event to happen? I contend there's a lot that any IT operation can do to shore up the network—and the network edge—to reduce your organization's attack surface. How? By being brilliant at the basics.

Find a framework

Being able to measure and roadmap your activity to a framework gives you a solid base from which to make decisions. Vendors continue to bring the latest must-have security tool to an already crowded market, and there is no shortage of fear mongering too. So where do you start, and how do you justify one path over another?

The answer: a framework. There are two acronyms for widely accepted and comprehensive cyber security frameworks: the National Institute of Standards and Technology Cyber Security Framework (NIST CSF) and the Center for Information Security (CIS) Controls. The difference is that NIST CSF provides security objectives you can work towards, whereas CIS Controls are more prescriptive in nature.

Choosing one framework and evaluating your IT operation against it will give you a path to set priorities and decide where to invest time and money. It costs nothing beyond time to take your team through the process of evaluating where your IT operation stands in relation to each standard. From there it becomes easier to draw a roadmap and communicate to budget decision-makers where investments should be made.

Prioritize patching

We all know how it goes. Looming deadlines, important projects, and a lack of resources often sideline the basics of applying the latest security patches. Yet eighty percent of attacks on network defenses take advantage of vulnerabilities that are three years old or more and have a patch available.

Simply patching the holes in the base layer of security can greatly reduce the attack surface of your environment. You can address any zero-day exploits one at a time as they happen. These are still rare, or at least spread out in a manner that makes individual patching possible.

Test and remediate

Test your network for vulnerabilities to see how susceptible it is to penetration from a threat actor. This is well worth the money spent. Typically, vulnerability and penetration tests will identify a list of prioritized vulnerabilities from "Critical" to "Low" for remediation and include an executive presentation to help with communication efforts. A third-party assessment can go a long way in justifying an increase in budget or capital Investment.

continued on page 4

Members Win IT Awards

Michigan Government Management Information Sciences (Mi-GMIS) presents annual awards to encourage and recognize excellence in the government IT field. Congratulations to the MMRMA members receiving Mi-GMIS awards in 2023:

CALHOUN COUNTY
IT Rookie of the Year
Abbey Labrecque

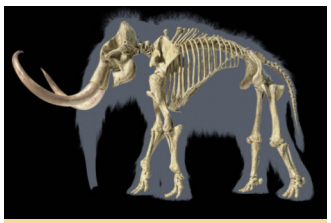
MONROE COUNTY
IT Project of the Year—Organizational Impact
Multi-Factor Rollout

CITY OF WESTLAND
IT Project of the Year—Organizational Impact
Cityworks/ArcGIS Integration

IT Project of the Year—Citizen Impact
Electronic Recycling Day

RISK MICHIGAN MUNICIPAL RISK MANAGEMENT AUTHORITY

Members Highlight Cybersecurity Awareness Month



Michigan's state fossil is the mastodon, so designated in 2002. Fossils of the Ice Age mammal, similar to a wooly mammoth, have been found in more than 250 locations statewide. In 2023, Kent County workers digging a drainage ditch discovered a 13,000-year-old skeleton of a juvenile that was 75–80% complete, an extremely rare find.

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 MEMBERS ARE doing their part to raise awareness of cybersecurity. Recently, the City of Grand Rapids sent out an email (excerpted here) that highlighted Cybersecurity Awareness Month and its efforts to promote security:

October is Cybersecurity Awareness Month, a local, national, and global effort to help everyone stay safe and protected when using technology whenever and how-ever you connect. Now in its 20th year, this [awareness program] continues to build momentum and impact with the goal of providing everyone with the information they need to stay safer and more secure online.

This year's campaign theme "Secure Our World" focuses

SECURE OUR WORLD
CYBERSECURITY AWARENESS MONTH 2023

on a few key behaviors to encourage every employee to take control of their online lives. There are numerous ways to stay safe and secure online, but even just practicing a few cybersecurity basics can make a huge difference.

The Information Technology Department will share weekly emails throughout October to improve individual cybersecurity awareness. The first week will focus on use of Strong Passwords; the second week on Multifactor Authentication; the third week on Recognizing and Reporting Phishing, and the fourth week on keeping software up to date.

The City of Grand Rapids is proud to support this far-reaching online safety awareness and education initiative, which is co-led by the National Cyber Security Alliance and the Cybersecurity and Infrastructure Agency (CISA) of the U.S. Department of Homeland Security.

For more information about ways to keep you and your family safe online, visit:

https://www.cisa.gov/cybersecurity-awareness-month

https://staysafeonline.org/cybersecurity-awareness-month/

Cybersecurity Basics, continued from page 3

Train your staff

A critical area for investment is training staff on security awareness fundamentals, especially in the areas of phishing and social engineering. Ninety percent of successful network breaches are caused by human behavior or error. You can spend all the money you want on the best network threat defenses, but if one of your users hands over their password, it is all for naught.

Running phishing tests quarterly and doing a quick refresher training on security awareness fundamentals each year will reduce your risk of falling victim to a socially engineered attack.

Ninety percent of successful network breaches are caused by human behavior or error.

Incident Response Plans

The worst time to build a plan is in the middle of a crisis. Many templates and formats are available for free on the web. For State, Local, Tribal or Territorial (SLTT) government organizations and educational organizations, most states have templates to use as a starting point. From there, the only cost is in the intentional time to plan. Documenting and reviewing these plans annually can go a long way to speeding you toward remediation during a crisis.

It doesn't require a sky-high budget to have a significant improvement to the security of your network environment. By having a plan, brilliantly and diligently executed around these basics, you can shrink your attack surface, get a roadmap and footholds towards future improvements, and reduce anxiety around the unknown.