Published in News on by **Martha Keeley, Freelance Writer**

Organizations in every industry are worried about information security. Attacks take place nearly every day, often resulting in the exposure of vital personal records or attackers using data to extort money.

The FBI's Internet Crime Complaint Center reports that cyberattacks have roughly quadrupled since the COVID-19 pandemic began in early 2020. The shift to remote work increased the number of possible failure points and created a large, distracted workforce vulnerable to cyberattacks.

Erich Falke, chief information security officer for ePlace Solutions, a cyber risk management company that works with MIIA members, said building a strong security culture within an organization is essential to protecting against threats and mitigating attacks. An organizational commitment to cybersecurity, he said, must start at the top.

"Cybersecurity is a business issue that city and town leaders must manage," Falke said. "An attack can shut down your municipal website and all online functions. Any data that is stolen or accessed could result in financial and reputation loss.

"While a community could potentially pay the ransom, systems may still be down for days, oftentimes weeks. And even if a city or town doesn't pay the ransom and uses a backup, it can still take weeks for the municipality to restore operations."

A culture of security means that all employees feel accountable and the organization has prudent practices and policies to ensure resilience in the face of cyberthreats, Falke said. Humans are the weakest link in an organization's cybersecurity shield. If an employee is compromised due to social engineering (coercion such as phishing), the entire cyber environment could be exploited by malicious users.

Two key aspects to fostering a strong cyber culture are:

- Building an understanding among employees and ensuring that they recognize their role
- Regular education and training

Employee understanding and relevance

Cybersecurity relies on more than just the IT department doing its job. Everyone in the organization must see themselves as responsible for ensuring data security. Leadership should understand employees' attitudes and behavior toward security protocols and issues. Do they see data security as the sole responsibility of IT and not something under their control? What are their work-from-home habits (such as password reuse or letting family members access work devices)? How often do they hear directly from municipal leaders about the importance of cybersecurity and are provided updated information?

A survey of 3,000 remote workers and IT professionals by CyberArk found that 77% of remote employees use unmanaged, insecure devices to access corporate systems, while 37% save passwords in browsers on their corporate devices.

Falke recommends protecting all remote access with multi-factor authentication. Privileged users such as the administrator and IT staff should have to go through multiple security layers before being able to access critical data.

Regular education and training

Falke said employees must be educated about their responsibilities so they can willingly help build a strong security culture. Organizations should develop the context for employees, and be transparent about the risks, implications and cascading effects of inferior security practices.

Educating employees is not one size fits all. All employees need to understand their specific responsibilities and how their roles and behaviors can help or hinder the city or town's overall security. This includes developing cybersecurity procedures that integrate into daily work routines and procedures.

Ransomware is the biggest cyberthreat, followed by email fraud such as phishing, and wire transfer/invoice fraud. Falke recommends providing social engineering training to help employees understand the techniques used by cyber criminals.

Training should happen all year, with simulated phishing attempts (conducted by IT) taking place during the year to help keep employees alert. Employees also need to know how to respond when something happens.

MIIA offers its members an online e-learning platform called CyberNET, which they can use to train their employees on cybersecurity best practices. Among other resources, the platform includes phishing simulation services, access to expert cyber risk advisors, and online training courses in the form of individually targeted training modules.

IT best practices

Falke recommends three critical practices for IT departments – two that can be used to prevent problems, and a third to use in the event that a criminal gains access.

First, make sure all systems and software are up-to-date. New versions of software are often released daily to fix known vulnerabilities. IT staff should also test updates before deploying them to avoid business interruption.

Second, have "endpoint" protection that identifies potential issues before they start. Endpoints are desktops, laptops, mobile devices, printers, etc., that are connected to the central network. Endpoint protection works by examining files, processes, and system activity for suspicious or malicious indicators.

Third, have trusted backups and make sure at least one backup is isolated to prevent criminals from accessing/destroying that copy.

The long-term view

Over the coming years, government agencies and other experts that track cyber issues say the problem can be expected to continue intensifying and becoming more complex. The evolving "internet of things" landscape will surpass the traditional network in use today, further intensifying privacy and cybersecurity challenges.

Municipal leaders are advised to continue to beat the cybersecurity drum and prioritize collaboration and education for all employees. They should look to implement pragmatic solutions that address cybersecurity throughout their organizations, and be sure to recognize success at every turn.

Resources

There are some great resources available to help.

The MassCyberCenter has developed a range of online online training materials to help local leaders implement cybersecurity best practices, and developed a Minimum Baseline of Cybersecurity for Municipalities.

The U.S. Department of Health and Human Services offers free cybersecurity awareness training.

The U.S. Cybersecurity and Infrastructure Security Agency offers a range of free services to help cities and towns protect against cyberthreats.

The Federal Virtual Training Environment (FedVTE) provides free online cybersecurity training to federal, state, local, tribal and territorial government employees, federal contractors, and U.S. military veterans.

MIIA offers training and grant options to its members, as well as phishing simulation.

Know the Law to Reduce Risk of Pothole Claims

Lin Chabra MIIA's Senior Manager of Risk Management

With the arrival of spring weather conditions, MIIA is seeing a large volume of claims for property damage to vehicles because of potholes and compromised road conditions.

Claims for defects in or on public ways in Massachusetts are governed by Section 15 of Chapter 84, which sets forth conditions necessary to establish liability and establishes a maximum damage cap of $5,000.

Two elements of the law are particularly important from a municipal risk management perspective.

Breach of duty

A breach of duty claim requires two key elements: notice of the condition, and an opportunity to repair the defect. Someone filing a claim must establish that the municipality had either actual or constructive notice of the defect prior to the accident. The claimant must also prove that the municipality had a reasonable opportunity to repair the defect prior to the loss and failed to do so.

Notice of claim

A person intending to file a road defect claim must provide written notice to the municipality within 30 days of the incident. The written notice must contain specific information sufficient to allow a municipality to investigate.

From a risk management perspective, it is essential that a municipality be able to demonstrate when they received notice of the defect and document the time and date of their repair response. What constitutes a reasonable response is fact-specific as to the nature of the defect and proximity to weather conditions.

Maintaining some type of tracking log is a critical best practice. This log can be something as simple as a spreadsheet. (Download MIIA's Pothole Log.) There are also applications available that allow for tracking as well as the ability to upload photographs of repair responses. The key is to be able to establish that you have a system to track and document notice of defects and the time and date of your response following notice.

← Return to View All News

The Massachusetts Interlocal Insurance Association

3 Center Plaza, Suite 610,
Boston, MA 02108

CONTACT

Staff
Address & Phone Numbers
Maps & Directions
Legal & Privacy
Report a Claim

FOLLOW US ON

MIIA is a Membership Service of MMA Massachusetts Municipal Association