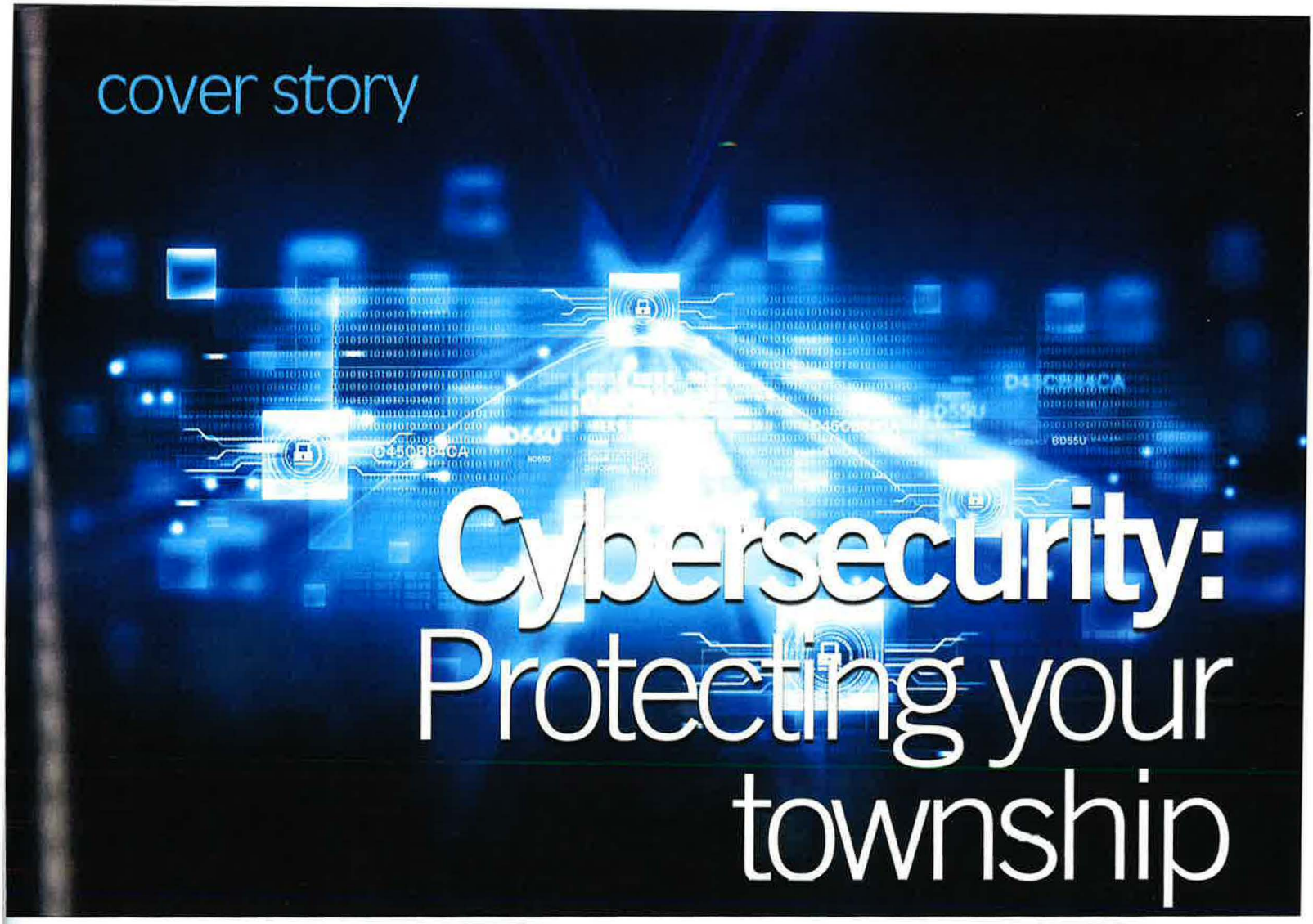


Cybersecurity: Protecting your township

It starts with an innocent-looking email—perhaps from your township's bank, or a computer operating system vendor. Your brow furrows as you read the message. "Your invoice has not been paid," it says. "Please submit payment or your service will be discontinued." You wonder what bill you forgot to pay as you click on the link.

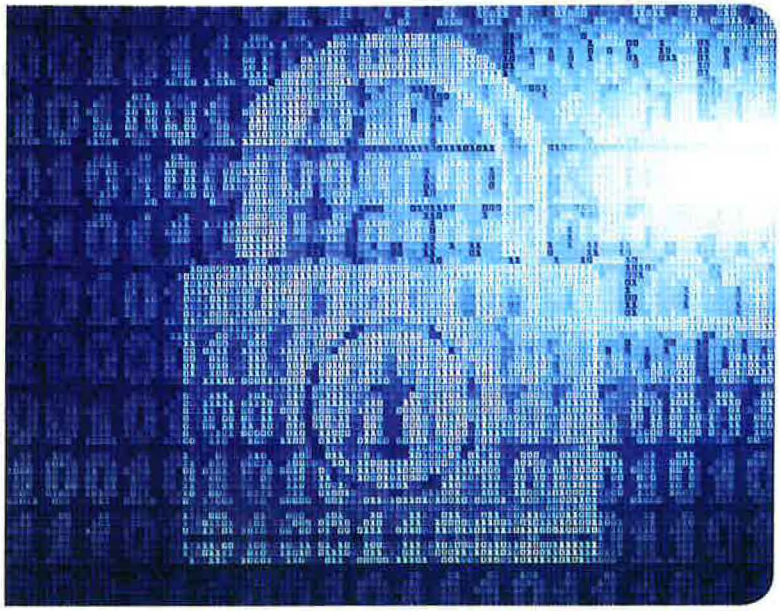
Suddenly, a black box pops up, blocking your computer screen. "All your files are encrypted," it announces in ominous red letters. Your heart beats faster as you read on—if you want your files back, the township will have to pay a hefty fee.

"That would never happen to me," you might say to yourself. "I know better than to click on a fake link. Besides, no one would try to steal our township's information. Our budget isn't that big, and hackers wouldn't pay attention to our little township."

The threat, however, is all too real. In 2018, a hacking group effectively shut down the City of Atlanta, holding its files hostage unless it agreed to pay a $51,000 ransom. Municipal employees couldn't turn on their computers for five days while officials and security experts scrambled to recover the city's networks. Shortly after Atlanta was hacked, Baltimore's 911 system was completely locked by a ransomware attack.

While no blockbuster attacks have been reported in Michigan, it's likely a matter of time. And experts say most local units of government aren't doing enough to prevent it. Sometimes, the reason stems from officials who either aren't aware of the threat's severity or don't believe it could happen to their township. Others might point to their budgets, saying they don't have the money or manpower.

The reality, however, is no township can afford not to take their cybersecurity seriously. Experts agree that at one point or another, your township will experience a cyber breach, if



Your township holds your residents' valuable information that attracts cyber criminals. As elected officials, it's your job to make sure that information is protected.

it hasn't already. It's likely not a question of if—it's when. Your township holds your residents' valuable information that attracts cyber criminals. As elected officials, it's your job to make sure that information is protected.

"If you don't have a secure computer network, it doesn't matter what your budget is because you're going to have problems," said Terrence Weadock, president and CEO of Dominant Systems Corp. "It's sort of like saying we can't afford doors and locks for the township building."

A growing threat

In today's information age, doing business online is a way of life. More and more taxpayers don't want to make a trip to the township hall to pay their sewer bill or write a check for their summer property taxes. They expect their township to provide a way to pay online. Meanwhile, new laws have paved the way for more townships to move to electronic tax rolls rather than printed.

While going digital has made life more convenient, it has also opened the floodgates for cybercriminals. *Governing* magazine reported that each year, Michigan's cybersecurity efforts block 2.5 million web browser attacks, 179.5 million HTTP-based attacks and 5.2 million intrusions.

The Michigan State Police (MSP) had been involved in computer crimes since 1999 but moved to a formal approach in 2013. When former Gov. Rick Snyder called for an initiative to increase Michigan's cybersecurity heft, the Michigan Cyber Command Center was born, dubbed MC3 for short. Operated through the MSP, the center investigates network breaches and hacks while also providing free training to businesses, local governments and other organizations.

Townships with an information technology staff might already be well-positioned to keep cyber criminals at bay. Others without that ability might see cyber protection as a luxury they can't afford.

"They don't have the big bucks that some of these big corporations have to invest in putting together a fancy system and processes," said Jennifer Puplava, attorney at Mika Meyers PLC. "There's a tension there, because the information is really important, and there are ways to protect it, but municipal employees are becoming more aware that something needs to be done. That's a great first step."

What's at risk?

No matter how big or small, every township has something hackers want: information. As more services go online, local governments increasingly store personal information on their taxpayers, such as names, addresses and possibly even Social Security numbers. This data is a major prize for criminals hoping that a person's information is the key to their bank account. Some townships have customer payment information, from residents paying their taxes or utility bills. Even seemingly harmless information, such as a taxpayer's occupation or former address, can be used by a hacker to gain trust from the individual in a future hacking attempt.

While stealing Social Security numbers won't impact your township's day-to-day operations, it's a breach of public trust. Members of the public count on your township to guard their identities and keep them out of the hands of hackers. A data breach can seriously damage the public's faith in your township.

"They need to recognize that citizens are relying on them to do what is needed to protect their information," Puplava said.

The majority of hackers tracked by the MC3 are working in foreign countries, where U.S. laws don't apply to them and Michigan police can't reach them. They aren't the scary men in ski masks you might see in commercials for companies angling to protect your personal information. Unfortunately, a hacker can be anyone connected to the internet who does a little research.

Many times, hackers are interested in personal information about your taxpayers. They could even learn about an upcoming contract and pose as a company to trick the township into sending them money.

Common threats

Phishing emails are one of the most common ways criminals hack into computer networks, MSP Information Technology Specialist Luke Thelen said. Most people have received some sort of scam email posing as someone trustworthy attempting to gain critical information, whether through their personal or business account. Today's threats have evolved past the easy-to-spot emails from a "Nigerian prince" asking for money. Cybercriminals often pose as well-known companies alerting recipients that they need to change their password or provide sensitive information. Some scroll through online employee lists and send emails targeting specific employees, using personal information to convince the employee it's safe to provide information. They might even impersonate someone you know and do business with.

Even if every employee resists the bait of phishing emails, your network can still be compromised by point-of-sale programs or other contracted entities your township counts on to make its daily operations easier.

A common threat is ransomware, a type of malicious software that locks the owner out of a computer network until a ransom is paid. It's the type of attack used in well-known breaches such as Atlanta and Baltimore, but it's even been used to target individual computer users.

> "Think about all the sensitive information we have in the township. What if somebody were to hack people's tax bills and get information about people's identities? It's kind of scary."
>
> **—Paul Pirrone, Supervisor**
> **Bedford Township (Monroe Co.)**

A breach might not mean your entire network is crippled. Hackers also target electronic fund transfers (EFT), duping a user into transferring money to a fraudulent account.

Bedford Township (Monroe Co.) could easily have been the victim of a breach—Supervisor **Paul Pirrone** knows the township's cybersecurity system has stopped several in their tracks.

Bedford Township doesn't take cybersecurity lightly. With the help of an information technology company, the township has prevented several hacks that easily could have allowed criminals to access taxpayer information. Securing township information isn't a one-time fix—Bedford Township makes sure its security system is continually updated to address new threats.

While cybersecurity has always been important to the township, it took on a new weight when Pirrone was approached by a resident interested in forming a cybersecurity hub in the township. He saw the growing threat as an opportunity for young people to receive training and secure jobs fighting hackers and breaches. The more Pirrone learned about cybersecurity while helping to get the hub off the ground, the more he took it seriously.

"You think about all the sensitive information we have in the township," he said. "What if somebody were to hack people's tax bills and get information about people's identities? It's kind of scary."

First steps

Before you can protect your data, you need to know what you have. Do you have only employee data, or do you also have residents' Social Security numbers? Townships should make an inventory of everything they have in place.

Then, analyze your data for its importance to township operations. What would happen if the data was encrypted and could not be accessed? Think through how critical it is that your township access that information.

You'll also need a list of your township's IT assets—in other words, its computers, copiers, phones and any place data is transmitted or stored. Then, take a step back. What are your risks, and what can you do to protect it?

"Unless you're a highly regulated institution, there isn't a law that tells you how to protect things," Puplava said. "You have the flexibility as a local government unit to look at what you have to say, 'What would be a reasonable thing to do, and what can we afford to do to protect all of these assets?' That is often different for every municipality."

Protect yourself

At a minimum, every township, whether it has two computers or 200, needs two layers of protection, Weadock said. First, township networks need up-to-date firewalls to stop cryptoviruses from encrypting your files—often the result of clicking on a bad link from a phishing email. Then, each computer, tablet or cellphone needs antivirus software that searches for and stops viruses in their tracks if they make it past the firewall. They're also designed to attack viruses spread from an infected USB key.

Whatever brand of protection you choose to use, Weadock recommends taking a multi-brand approach. If a hacker knows how to break past one vendor's system, they might not be familiar with the other.

"It's sort of like having two different types of locks," Weadock said. "If somebody can break into one, they might not be able to break into the other."

Once your data is protected, make sure it's backed up so you can access it in case of an emergency. Storing it on another server is an option, as well as the cloud—it just needs to be a place you can get to quickly.

Don't just assume your layers of protection are working. Whether you use a cybersecurity vendor or have an

No matter how big or small, every township has something hackers want: information. As more services go online, local governments increasingly store personal information on their taxpayers, such as names, addresses and possibly even Social Security numbers.

information technology staff, have someone test your defenses each year at a minimum. They can also conduct a phishing test, where they send a fake email to township employees and compile a report on who clicked on the bad link. Then, those employees are sent for further training.

Weadock also recommends running a system recovery test, where your township recreates its network with its backup data. He compares the practice to a fire drill. The last thing you want is to discover you don't have what you need when a crisis strikes.

The human element

The single greatest threat to your township's cybersecurity could be the humans on its network.

A rushed work environment is the perfect breeding ground for even the most conscientious officials and employees to click on links in phishing emails. The need for speed may push an otherwise careful employee to break with the policy to call the other party before transferring money. That split-second decision in the name of efficiency could ultimately result in a data breach.

"We're all expected to move and work so fast, so that we inadvertently become a little more careless with how we do things," Thelen said. "Instead of paying attention to that email, we instantly click the link to see what's there just because we've got to get things done, and we may falter that way."

Experts peg a lack of training as one of the biggest mistakes townships make when it comes to cybersecurity. Every employee, official or anyone with access to the township's network needs to understand the warning signs of a phishing email and what to do if they receive one. All it takes is one person to click on one malicious link for the entire system to be compromised, MSP D/Sgt. Matt McLalin said.

MSP D/Lt. Aric Dowling recommends regular, re-occurring training to keep employees up to date on the latest trends and new developments in the cyber world. MC3 offers free training and other resources, and MTA periodically offers cybersecurity workshops, including at the upcoming MTA Annual Conference. You don't need to wait to get hacked to reach out. MC3 offers cyber assessments and offers advice before anything bad happens.

We were hacked! Now what?

A cybersecurity breach is not the time to take a do-it-yourself approach, Weadock said. First, unplug the infected computer—and if it's a laptop, turn it off. If the virus has already spread to the server, unplug it. Then, call a professional immediately. Now isn't the time to try to handle the situation yourself.

Every township needs a procedure in place in case of a breach. Every employee and official should know what to do with their machine and who to contact. If your township is large enough, each computer or group of computers should have the ability to be cut off from the network so that the malware doesn't spread to everyone. This ensures that your township isn't brought to its knees with one phishing email.

"It is constantly evolving," Dowling said. "These criminals are constantly evolving their tactics. One of our missions is to help Michigan be more secure. Our team is constantly taking phone calls and investigating hacks all over Michigan."

Spotting a phishing email

Even the best filters won't stop every possible attack. Anyone with an email address must stay vigilant and keep an eye out for suspicious emails. Cyber criminals are creative and often design their emails to look official. Emails that look legitimate on the surface might have spelling or grammar errors when read closely. Check the sender's email address—a fake address might have one incorrect letter separating it from a legitimate sender. For example, a hacker posing as a government official might have an address ending with "michigann.gov" instead of "michigan.gov."

Any email asking for a financial transaction should be viewed with suspicion. Don't automatically transfer the money—call the sender instead. Make sure you look up the phone number yourself or use a number you have on record rather than calling the number listed in the email. Hackers have been known to list a fake number and vouch for themselves when called, Dowling said. And whatever you do, don't just hit reply. If you do converse with the sender and

receive an angry response pressuring you to take action, it's typically sign that you're dealing with a hacker.

When you receive an email asking you to change a password or update other personal information, don't click the link. Use your internet browser to visit the website yourself and log in. Then, if the legitimate website prompts you to update the information, you can do so with confidence. Weadock recommends holding your cursor over the link in the email, right clicking to copy the link and pasting it into a word processing document. Chances are, if the link isn't legitimate, you'll see red flags, such as misspelled words or long, complicated URLs.

Some phishing emails can appear to come from a friend or colleague in your email contacts. Criminals are known to hack into email accounts and send links to everyone in that person's address book. If you receive an email that contains nothing but a link, don't click on it—report it.

If you open a phishing email, don't panic. Simply viewing a fraudulent link on an email or on a social networking website doesn't put you at risk, as long as you don't click on it.

"Whether it's social media or a news story that peaks people's interest, that's what will increase the chance of a breach, but it's a moving target," Thelen said. "If you try to block those things on the fly, you're going to be playing whack-a-mole. It's very inefficient."

Phishing emails are the easiest way to break into a network, but they're not the only way, Thelen said. A determined hacker can still break into your server without anyone clicking a link. Thelen has also seen breaches resulting from someone finding a USB flash drive and plugging it into their computer.

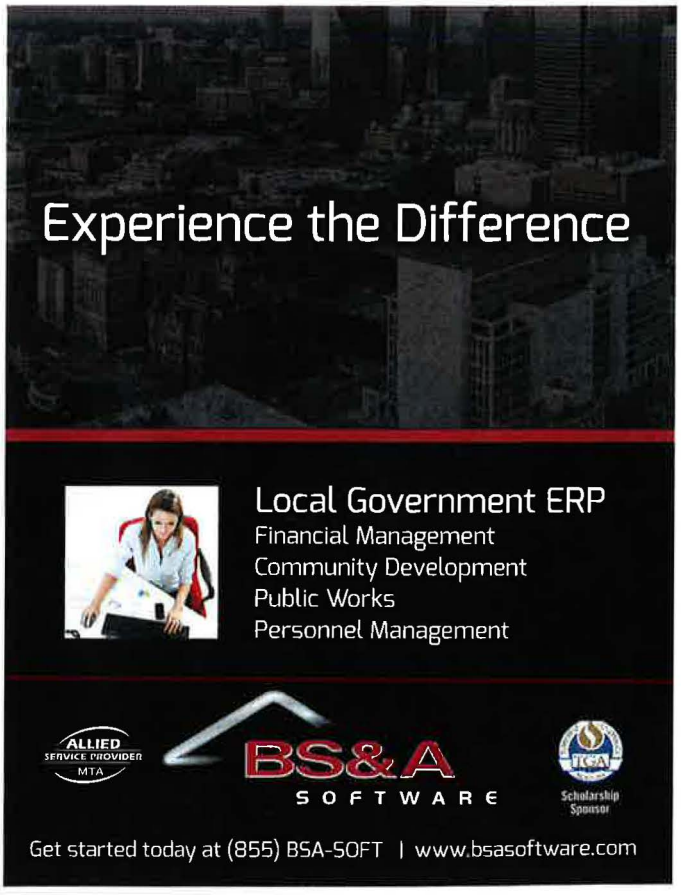
Change your password

Township employees should regularly change their passwords—after all, hackers still break into systems by guessing a user's password. Weadock recommends setting up your township's system to require users to change their password every three months. Don't just keep the same password and change a number or character at the end. That's too easy to guess. Pick a brand-new password.

Passwords as you know them are on their way out—passphrases are the future, Thelen said, and the longer, the better. The traditional eight-character password with an uppercase and lowercase letter isn't secure, and a random jumble of numbers and letters is too difficult to remember. Thelen recommends thinking of a phrase and jamming the words together into one easy-to-remember passphrase that's difficult for criminals to guess.

Then, when it's time to update your password, pick a different phrase to keep your account secure. Dowling discourages the common practice of keeping your password but tacking a number on the end.

Experts also urge taking advantage of two-step authentication, which is available through many email servers, banking websites and other pages. While waiting for a code to be sent to your phone might require a moment or two of waiting, the result will be added protection to your online information.



Not just an IT issue

As townships rethink their cybersecurity, Puplava urges them to stop putting the issue in the IT box. Cybersecurity goes far beyond computers and phones—it should be part of your township's planning. Chances are, your township will experience a breach sooner or later. The time to plan is now, not when you're scrambling to recover your data.

While the best solution likely isn't free, Weadock points to the cost of inaction. If your network is hacked, how much would it cost to recover? The cost of investing today is far less than the benefit of protecting your township.

Bethany Mauger,
MTA Staff Writer

Learn more about cybersecurity and what your township needs to know to protect itself at MTA's 2019 Annual Educational Conference, held April 1-4, at DeVos Place in Grand Rapids. Among the 60-plus educational sessions held during the event will be "Data and Cybersecurity," slated for 2:45 to 4 p.m. on Tuesday, April 2, and taught by Attorney Jennifer Puplava, with Mika Meyers, PLC. Turn to pages 16-20 to learn more about the Conference, or visit www.michigantownships.org for more information or to register online.