CYBER

SECURITY 101

Townships Can **TAKE STEPS** to **PROTECT DATA,** Prepare for Recovery

BY **BRENDA WILT** / ASSISTANT EDITOR

CYBERATTACKS ON MUNICIPALITIES ARE INCREASING, and the size of the community doesn't matter. Townships collect a lot of data about their residents and need to take steps to secure it. At the same time, they need to craft a recovery plan to respond to a cyber incident because experts say it's not a question of *if* they will be attacked but *when*.

It sounds like a story ripped from the headlines: A website is hacked by cybercriminals from Russia. Rather than a website for a federal agency or a multinational corporation, however, this website belongs to tiny South Creek Township in Bradford County, population 1,128.

The story starts with secretary Linda Leonard, who has been at the township since 1994 and resisted getting a website for some time.

"I'm 75 years old, and I knew that if we got one, I'd have to maintain it," she says.

Nonetheless, the board of supervisors eventually contracted with a company in Elmira, N.Y., to set up the website, which was hosted by a company in the Midwest.

All seemed peachy until one day, Leonard couldn't get into the site to update it. She tried calling the company in New York, but no one answered. Then things took a scary turn.

"I started getting calls from people who tried to go to the website and were redirected to a site in Ukraine," she says. "Plus, I started to get about a hundred emails a day in Russian!"

Would your township know what to do in this situation?

Here's another real story: One recent Monday morning, the staff of East Hempfield Township in Lancaster County was unable to log into its document management server that houses archived real estate records, invoices, payroll records, and even police department documents.

The township IT consultant was also locked out. Finally, the company that manufactures the software gained access through a "back door." Deep in the server's recesses it found a ransom note that said the township would have to pay to receive a key to free the files that the hackers had encrypted.

Would you know what to do if you got locked out of your server?

If you're thinking that this won't happen to your township, think again. Cyber attacks on municipalities are increasing at an alarming rate. There were at least 174 ransomware attacks nationwide on municipalities in 2019, according to antivirus software provider Kaspersky.

Lou Romero, a cybersecurity expert and consultant for 64 South Jersey municipalities, told the *Philadelphia Inquirer* that municipalities are easy prey for hackers.

"The odds of a municipality becoming a cybervictim are one in four," he said, "so it's not a matter of 'if'; it's only a matter of time."

Townships, however, can take steps to minimize the risk and respond to an eventual attack.

Security is a moving target

It is helpful to understand why municipalities offer such a temptation to hackers.

"Municipalities are very attractive targets for cyber criminals," says attorney Devin Chwastyk, chair of the privacy and data security group at McNees Wallace & Nurick. "They have substantial amounts of personally identifiable information, but they don't have resources for IT security defenses."

"If you have data about your residents, that's valuable information to bad actors," says Matthew Meade, an attorney for Eckert Seamans Cherin & Mellott. "The size of the municipality doesn't matter. It's the kind of data you have."

Experts point to the following factors that make municipalities low-hanging fruit for cyber criminals:

- lack of resources, including funding and technological knowledge;
- aging technology, including outdated hardware and software;
- new technology that is implemented without technical resources or adequate training; and
- a lack of understanding that cybersecurity is everyone's responsibility and not simply a function of IT.

"Lack of awareness is a big problem," says Bryan Gembusia, a supervisor for South Middleton Township in Cumberland County and owner of a cybersecurity firm. "Everybody thinks it's not going to happen to them, that they're not going to click on a bad link.

"The problem is, security is not a fixed line; it's a moving target. These problems are going to continue to get worse."

Gembusia says it's particularly problematic for municipalities because they are oriented toward customer service.

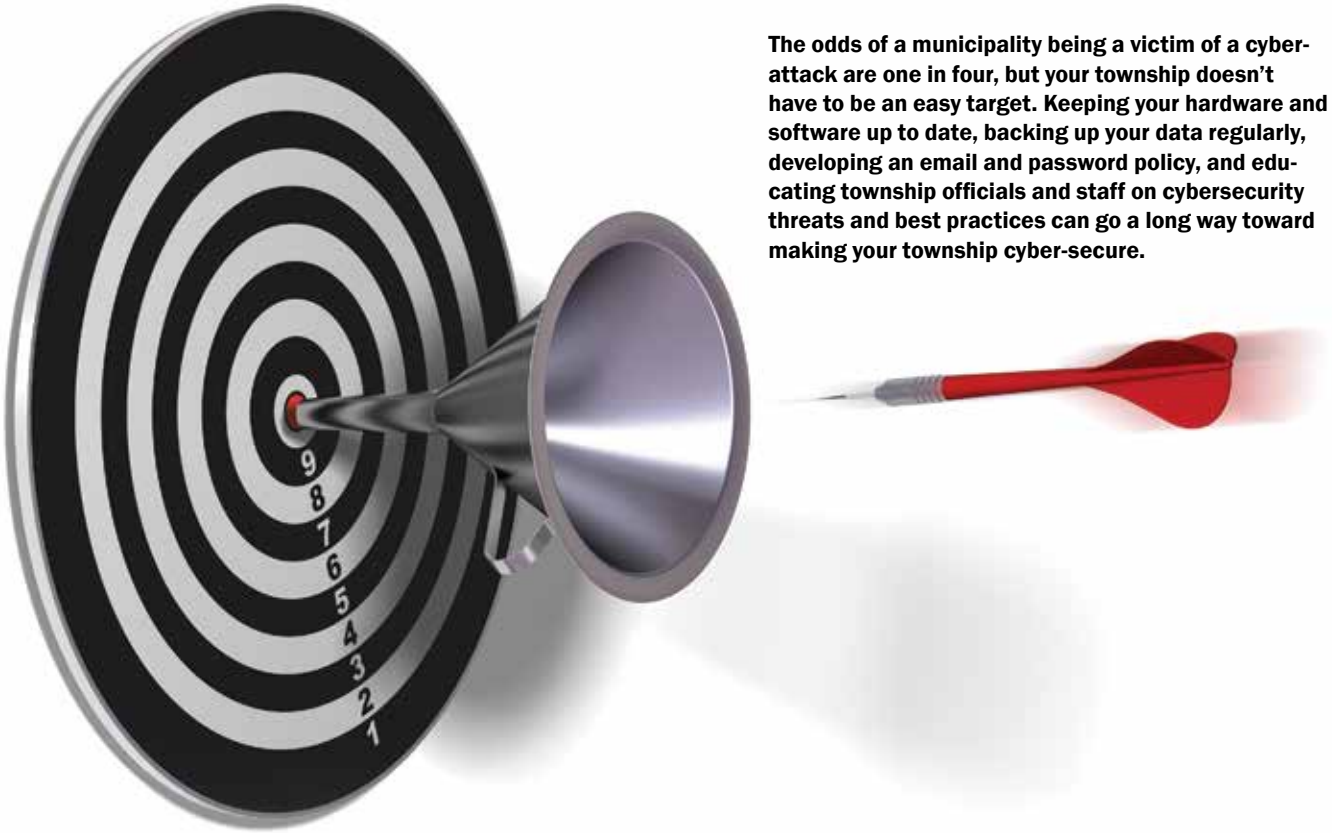
"If someone asks for information, we're probably going to give it to them," he says.

"Too many municipalities remain unprepared for today's threat environment, with inconsistent software updates, weak IT departments, and a pattern of selecting the insurance-paid option when confronted with the cost of restoring systems from the ground up," writes Kara Frederick in "The Rise of Municipal Ransomware" for *City Journal*, published by the Manhattan Institute of Policy Research.

In other words, they are paying the ransom to have their files released, adding to the lure for bad actors. Instead, Frederick says, municipalities should be proactive in preparing for cyberattacks and planning how they will respond. The time to do it is now.

"Local governments need to repli-

> "The problem is, **security is not a fixed line, it's a moving target.** These problems are going to continue to get worse."



The odds of a municipality being a victim of a cyberattack are one in four, but your township doesn't have to be an easy target. Keeping your hardware and software up to date, backing up your data regularly, developing an email and password policy, and educating township officials and staff on cybersecurity threats and best practices can go a long way toward making your township cyber-secure.

cate the private sector's urgent approach to cybersecurity," she says.

'Good backups saved the day'

Townships don't have to bust their budgets to be cybersecure. In fact, some best practices incur little to no cost.

First, townships should ensure that all data is backed up at least weekly, if not daily. In the case of a ransomware attack, you may be able to restore data from the backups, rather than paying to have files decrypted.

"Determine what your backup practice is and where the data is stored," Meade of Eckert Seamans says. "It's just good policy to know about your backups."

When East Hempfield Township got hit with ransomware, its backup enabled the township to restore its system without paying the ransom.

"Once we realized what was happening, we shut everything down so there was no access to or from the desktop computers," manager Cindy Schweitzer says. "Luckily, we do a backup every night through an outside vendor that stores it offsite. It took three to four days to restore 3 million files, and we were back up and running within a week."

It's a good practice to have a secondary backup stored offsite, such as on a thumb drive or external hard drive, in case cloud storage or the server housing the primary backup is compromised.

"We fought two nasty strains of ransomware over the past several months," Gembusia says of South Middleton Township. "Good backups saved the day."

It's a good idea to practice redundancy by having two copies of the backup, with at least one stored offsite. The Centre County Recycling and Refuse Authority found that out the hard way. When it was hit with ransomware in 2018, two separate hackers got into the system, executive director Ted Onufrak says. While one was encrypting files, the other was encrypting already encrypted files, including the backups.

The authority ended up paying

Don't assume that if you pay an outside vendor to back up your files to the cloud that you can forget about them. Check that the backups are occurring and run a test to ensure that you can restore your system from the backups.

two ransoms to free up its files: one for $1,500 and the other for $15,000. With broker fees, the total was about $18,000. *(You need a broker to purchase bitcoins, cybercriminals' currency of choice.)*

That doesn't include what it cost to restore the system, however, including a cybersecurity firm "scrubbing" the hard drives to remove all traces of the ransomware so the hackers couldn't return and do it again. It took a week to 10 days to get a couple of desktops up and running, Onufrak says, and about three months to restore all of them.

"The whole thing probably cost us $250,000," he says. "Now we use the cloud for our backups, and we back up everyone's desktop monthly on thumb drives that are stored offsite."

Tobyhanna Township in Monroe County was hit with ransomware in March 2018. The staff came in one morning to discover that none of the files could be accessed. When nothing they tried worked, they called the township's IT consultant, who confirmed that it was ransomware that originated in Russia.

> "Determine **what your backup practice is and where the data is stored.** It's just good policy to know about your backups."

The solution was to wipe the hard drives and restore the files from the backups. There was just one problem. Although the township's files were backed up regularly to the cloud, not all of them made it there.

"At one time, we had hit our maximum storage capacity and paid to increase it," says Julia Heilakka, the township's community engagement coordinator. "However, the vendor never activated the extra capacity so it continued to back up only the original amount."

Consequently, all the files from 2015 and earlier were retrieved, but everything from 2015 to 2018 was lost. The township had hard copies, of course, but the easily accessible digital files were gone.

"I started at the township in 2017 so I had nothing," Heilakka says.

Fortunately, the township had cyber liability insurance, which covered the cost of scrubbing the hard drives and scanning the documents that had been lost. The staff spent a Saturday at the office scanning minutes, land development plans, and more.

"We're still dealing with the fallout," Heilakka says. "Experience is the best teacher, though. Now our files are backed up to the cloud and local servers. Plus, several of us back up all our files onto thumb drives every few months to have a backup to the backup to the backup."

Tobyhanna Township's experience illustrates a crucial point: Talk to your

Townships should update all devices regularly and install all software security patches to ensure that their systems can ward off cyber threats.

IT vendor or whoever does your backup and ask questions.

"Ask how backups are done and when they were tested," Gembusia of South Middleton Township says. "How long would it take to do a complete system restore from the backup? I had one that took 48 hours."

"Check to make sure your backups really are in the cloud," Meade of Eckert Seamans says. "Don't assume your vendor is backing up everything. Make sure they are."

Meade says it is worthwhile to test the process of restoring your files from a backup.

"Recovering from backups is not just flipping a switch," he says. "It takes some time."

Townships should also ensure that their systems receive the latest updates and security patches. This process can be easily automated so that updates occur during off hours.

According to experts, local governments that do not regularly install security patches and software updates on all devices, hardware, and applications are vulnerable to attack. A single computer or device that has not been updated can be compromised and infect the entire network.

Along with installing updates and patches, townships should get rid of outdated hardware and software, particularly if it is no longer supported with updates. That goes for outdated data, as well. Purging files while complying with

regulations for record retention should be a regular practice.

"The more data you hoard, the greater your exposure," Meade says.

Addressing the human factor

Investing in hardware, software, and consultants goes a long way toward being cyber-secure, but often the greatest threat is human error. Most data breaches happen due to employee negligence, carelessness, or simple unawareness, such as clicking on a bad link or attachment to an email, Chwastyk of McNees Wallace says.

"There are also a lot of instances where an employee sends a file without encrypting it and checking to make sure the recipient address is correct," he says.

Employees should be educated on prevalent cyber threats, such as phishing and spear phishing, which often serve as the opening for ransomware attacks. Phishing involves sending emails that appear to be from reputable companies that ask the recipient to provide confidential information, such as passwords or credit card numbers. Spear phishing is similar, but the email appears to come from a known or trusted sender.

Gembusia suggests showing township officials and staff examples of the ways that hackers prey on unsuspecting users, from phishing emails to suspicious links.

"Show them how to hover the cursor over a link to see the address where it really goes," he says.

The ransomware attack on the Centre County Recycling and Refuse Authority was traced to an email an employee received several days after ordering flowers for her daughter from an online vendor. The employee clicked on a link in the email to view the order status.

Unbeknownst to her, the online vendor had been hacked, and clicking on the link opened a door for the crooks to invade the authority's system. *(See the box above for more on how to identify and respond to suspicious emails.)*

Adopting email and internet best practices is a good place for townships to start.

SPOTTING PHONY EMAILS

Follow these do's and don'ts to foil phishing attempts

The article "Cybersecurity: Protecting Your Township" from the Michigan Townships Association offers these tips for foiling phishing and other suspicious emails:

- **DO** look for spelling or grammar errors.
- **DO** check the sender's email address closely; it could be off by one letter or digit.
- **DO** be suspicious of any emails asking for a financial transaction.
- **DON'T** automatically send or transfer funds. Call the sender using the number you have on file or that you look up, rather than a number that appears in the email.
- **DON'T** just hit "reply" or click on any links if the email raises a red flag.
- **DON'T** click on a link in an email that asks you to change a password or update personal information. Visit the actual website and log in.
- **DON'T** click on the link in an email that appears to be from someone in your network and contains only the link.
- **DON'T** panic if you open an email that appears on second look to be a phishing scam. As long as you don't click on a fraudulent link, you're OK.

> "Townships should **develop a data security policy** for their employee handbook, just like a sexual harassment policy."

"Townships should develop a data security policy for their employee handbook, just like a sexual harassment policy," Chwastyk says. "It should reinforce the importance of treating confidential and personally identifiable information as classified and encourage employees to make good choices online. It should also direct employees to immediately report to their superiors when a potential cybersecurity issue has happened."

Another best practice is limiting access to certain systems and programs to only those individuals who need it to do their jobs.

Townships can also use hardware and software methods to help counteract the human factor. These include installing up-to-date firewalls on computers to help keep out viruses and malware, as well as antivirus software on every desktop, laptop, tablet, cellphone,

Passwords should be different for each account or site, contain a mix of upper- and lowercase letters, numbers, and symbols, and never be shared. Townships should institute the practice of changing passwords on a fixed schedule.

or other digital device that accesses township systems.

Another step townships can take is to establish and enforce a password management policy for all officials and staff. Everyone should create unique, hard-to-guess passwords for each account, computer, or digital device. A strong password has at least 10 characters, containing a mix of upper- and lowercase letters, numbers, and symbols.

The same password should never be used for more than one account or device, and passwords should not be shared. For added security, the township should require passwords to be changed regularly, such as every two or three months, and never repeated. Using the same password and simply tacking on a number or symbol won't cut it, either. The user should create a unique password each time it is changed.

Despite these practices, passwords can be cracked. Therefore, townships should consider using multifactor authentication to protect networks and systems. This two-step login process requires a user to supply additional information besides just a username and password to access an account or program.

Typically, in multifactor authentication, when a user logs in with their ID and password, they are prompted to provide a passcode or security code, usually a temporary number sent by email or text to the user. Sometimes, the user must simply tap a number or symbol on their phone to complete the login process. Multifactor authentication is especially important when supervisors or staff can access the township system remotely.

Making sure everyone who uses the township network or system is educated on cyber threats, what to look for, and what to do and not do are low- or no-cost best practices townships should take to help protect their data.

"Employees are the first line of defense against cyberattacks," Meade says. "You can spend lots of money, but if your employees aren't trained, hackers can get through. Also, make it clear that cybersecurity is everyone's responsibility, not just the IT department or consultant." ➤

HELP YOUR EMPLOYEES build a nest egg for retirement

JOIN THE PSATS 457 PLAN and give your employees a way to save for their retirement.

HIGHLIGHTS OF THE PSATS 457 PLAN

- Full- and part-time employees, as well as supervisors, solicitors, and engineers, are eligible to participate.
- Employees voluntarily contribute to their own pension portfolio. The township may contribute to or match these funds.
- Two investment approaches:

  "Do-It-for-Me" — Choose a Target Maturity Fund that coincides with your anticipated year of retirement. Funds are professionally managed by Vanguard. The asset allocation and diversification are done for you.

  "Do-It-Yourself" — Participants can select funds from a broad menu of options and build their own portfolio.
- Participants have access to their account balance 24/7 on the Internet and receive quarterly reports.
- Due diligence is performed regularly to maintain high-quality funds in all asset classes.
- PSATS and Summit Financial provide 457 Plan participants with investment education and personal assistance.

PSATS Trustees Insurance and Retirement Services SINCE 1959

PSATS MUNICIPALITIES PENSION TRUST

Call us toll-free at **(800) 382-1268** for enrollment information.

www.psatsinsurance.org

"Local governments that do not **assess their security weaknesses** on a regular basis are most vulnerable."

Assessing vulnerabilities

If a township does decide to commit dollars to cybersecurity, a good first step is to hire an IT security firm to conduct an audit or assessment of the system.

"An audit can detect any weaknesses or holes in your defenses or firewalls," Chwastyk says.

While a security audit is "incredibly valuable," Meade says, the township must be sure to take the actions that are recommended in the audit report to address its vulnerabilities.

In "Cybersecurity Best Practices for Municipalities," an article in the New Hamphsire Municipal Association's *Town & City* magazine, author and attorney Lisa Thompson says that a municipality that cannot identify its cyber vulnerabilities cannot effectively defend against them.

"Local governments that do not assess their security weaknesses on a regular basis are most vulnerable," she writes. "Oftentimes, hardware, network equipment, software, and wi-fi access points are weak [spots]."

Thompson says that an assessment should identify the types of sensitive information each department collects, where it is stored, and who has access to it. It should also include an inventory of all hardware and software and identify any potential risks to data.

Townships may also want to consider cyber liability insurance. Both East Hempfield and Tobyhanna townships had insurance to help cover the costs of recovering from ransomware attacks. Many insurance companies have attorneys and cybersecurity firms that it works with regularly.

"Our insurance company connected us to an attorney in New York, who connected us to an IT forensics company, which immediately started to investigate to see if any of our files had migrated out of the system," East Hempfield's Schweitzer says.

The township supervisors had been considering cyber insurance for a couple of years but balked at the cost, she says. As more government entities because victims of ransomware, they finally approved a basic $1 million policy last May. The township was hacked less than a year later.

The policy's $10,000 deductible and $5,250 premium are still a lot less than the $50,000 to $60,000 cost of the restoration after the ransomware attack, Schweitzer says.

"Townships should talk about their risk with their insurance agent or broker," Chwastyk says. "They may want to consider a cyber liability policy to cover the cost of a data breach as well as a crime policy to cover theft by deception."

It is important to have the right insurance company, preferably one that has experience with cyberattacks. At the time of its ransomware attack, the Centre County Recycling and Refuse Authority had insurance through a local agent who had never been down

Experts strongly urge townships to have an IT firm conduct a security assessment to determine the weaknesses and vulnerabilities in their IT infrastructure.

the ransomware road. Consequently, he really couldn't provide any advice or direction.

"We learned to have the right insurance coverage," authority executive director Ted Onufrak says. "Now, we have $25,000 coverage for hardware and software and $100,000 coverage if employee information is compromised."

Many insurance policies also pay for a year of ID monitoring after a cyberattack.

"Cyber liability insurance is like flossing and brushing your teeth," Meade says. "You don't think it's necessary until you get a cavity."

You don't want to scramble to find a cybersecurity consultant and other necessary helpers during a breach, he says. An insurance policy likely includes a bundled package of vendors at a guaranteed rate to handle investigations, credit monitoring, mail notifications, crisis communications, and more.

"There are lots of moving parts when recovering from a cyberattack," Meade says, "and most of it would be covered with a good policy."

When contemplating the expense of cyber insurance, townships need to consider all the costs of a cyberattack. In addition to restoration costs, there is the time the system is down, extra hours that may be required of staff, and a potential dip in the township's credit rating, which can affect bond issues.

Planning for the worst scenario

Adopting practices to educate the board of supervisors and staff, craft policies, and audit and secure systems are all good ways to deter cyber criminals. However, townships must take the next step and prepare and plan for a cyberattack.

"Just as local governments routinely prepare plans for the continuity of operations in the event of a natural disaster, they must also prepare plans to restore critical computer systems and networks as quickly as possible in the event of a cyberattack," writes Lisa Thompson in "Cybersecurity Best Practices for Municipalities."

Municipalities should proactively develop a comprehensive written incident response plan, she says. This is a set of actions the township will take

GET CYBER-SAVVY

Online resources provide information, tips for municipalities

Townships that want to learn more about how to keep their systems and data safe can turn to the following resources:

PUBLICATIONS

➤ "Cybersecurity Best Practices for Municipalities" — *Town & City Magazine,* New Hampshire Municipal Association, **nhmunicipal.org/town-city-article/cybersecurity-best-practices-municipalities**

➤ Municipal Cybersecurity Toolkit — MassCyberCenter, **masscybercenter.org/ municipal-toolkit**

➤ "Protecting Sensitive Data and Other Local Government Assets: A Non-Technical Cybersecurity Guide for Local Leaders" — Office of the New York State Comptroller, **osc.state.ny.us/localgov/pubs/cyber-security-guide.pdf**

WEBSITES

➤ Governor's Office of Homeland Security, **homelandsecurity.pa.gov/cyber-security**

➤ Pa. Office of Administration, **oa.pa.gov** *(Choose Information Technology under the Programs tab, then Cybersecurity, and finally, Local Government.)*

➤ Cybersecurity and Infrastructure Security Agency, U.S. Department of Homeland Security, **cisa.gov/cybersecurity**

- Stop.Think.Connect. Campaign, a national effort to raise public awareness of cyber threats, **cisa.gov/stopthinkconnect-toolkit; cisa.gov/publication/stopthinkconnect-government-resources**
- Cybersecurity training, **cisa.gov/access-fedvte-cybersecurity-training-today**
- Training exercises, **cisa.gov/cybersecurity-training-exercises**

➤ Cybersecurity Framework, National Institute of Standards and Technology, U.S. Department of Commerce, **nist.gov/cyberframework**

➤ National Cyber Security Alliance, StaySafeOnline, Common Cybersecurity Misconceptions for Small- and Medium-Sized Organizations, **staysafeonline.org/cybersecure-business/cybersecurity-misconceptions-smb**

Townships should not only have an incident response plan but also practice it periodically to make sure everyone knows what they are supposed to do when a cyberattack occurs. Experts say attacks on municipalities are not a matter of "if," but "when."

to identify, investigate, and respond to a cyberattack that reduces the impact and allows the municipality to return to normal as quickly and efficiently as possible.

"Your response plan should identify the external resources you will call upon after an attack," Chwastyk says. "Any actions should involve a law firm from the outset, whether retained by the township or an insurance company. If an attorney participates in all communications between the township and a cybersecurity firm and other involved parties, attorney-client privilege will apply."

A cyber incident response plan should include the names, phone numbers, and email addresses of everyone who needs to be involved in the recovery process, Meade says. The plan should also outline each person's responsibilities.

"Everyone assumes that everyone is going to be present in the case of an incident," Gembusia says. "It's good to spell out who does what, who to contact, and how to contact them."

Townships should think about various methods of communication during a cyberattack. Emails and address lists of outside parties may be unavailable if the system is locked up.

Once a response and recovery plan has been developed, the township should run a test with key players.

"Conduct a tabletop exercise, a hypothetical cyber incident to see how the team responds and then perform an analysis," Meade suggests. "Repeat the exercise until it goes smoothly. There is usually a big learning curve from the first to the second run-through. Just figuring out who needs to be involved can be challenging."

Chwastyk likes to refer to these exercises as "war games."

"Delegate the primary people and their assigned responsibilities," he says. "Review the risks that are out there and what you will do when you get that call."

Townships that think it's not necessary to develop a cyber incident response and recovery plan are wrong.

"If you don't have a response team or plan in place, you're going to be behind the eight ball," Meade says. "It's not a matter of 'if' but 'when.' No one is immune.

"Every municipality should take steps to protect its data and prepare for an attack," he adds. "Preparing is less expensive than paying for recovery." ✦

Peace of mind in uncertain times. That's what we work to provide to you by helping to ensure your annual premiums will not fluctuate from year to year, taking ownership of providing the most effective support services possible. This translates to MRM being able to offer the most cost effective Workers' Comp as well as Property and Liability insurance programs in Pennsylvania.

Contact us today to see why 500+ municipal entities trust MRM.

John McConaha | jmcconaha@mrmtrust.com
Chuddy Carless | Chuddy.carless@hubinternational.com

OUR BEST REFERENCES ARE YOUR NEIGHBORS ... MEMBERS OF THE TRUSTS.

ACROSS 60 COUNTIES IN PENNSYLVANIA, MORE THAN 500 MUNICIPAL ENTITIES INCLUDING BOROUGHS, TOWNSHIPS, COUNCILS OF GOVERNMENT, REGIONAL POLICE FORCES AND AUTHORITIES HAVE BECOME MEMBERS OF THE MRM TRUSTS. THEIR TRUST HAS BEEN REWARDED BY OVER $150 MILLION IN CUMULATIVE ANNUAL DIVIDENDS RETURNED.

For more information, please visit www.mrmtrust.com