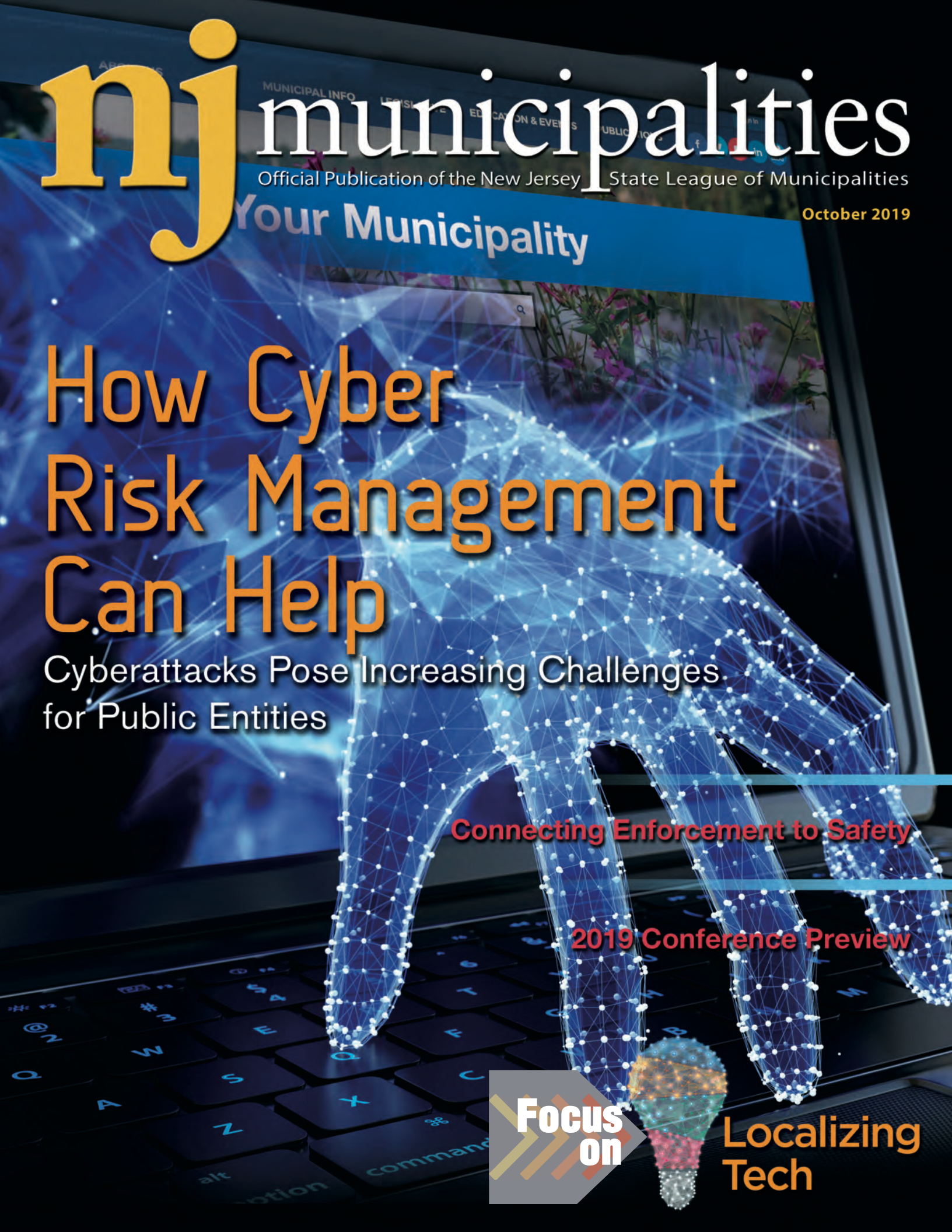
nj municipalities
Official Publication of the New Jersey State League of Municipalities
October 2019



How Cyber Risk Management Can Help

Cyberattacks Pose Increasing Challenges for Public Entities

Connecting Enforcement to Safety

2019 Conference Preview

Focus on Localizing Tech

How Cyber Risk Management Can Help

Cyberattacks pose increasing challenges for public entities

EDWARD COONEY, MBA, *Vice President, Account Executive/Underwriting Manager, Conner Strong & Buckelew, and MEL Underwriting Manager;*
JOSEPH HRUBASH, *Deputy Executive Director, MEL*

Only two years ago, cyber-attacks against public entities were rarer than tornadoes in New Jersey (less than 50 since 1835). A quick online search, and even conversations with colleagues who are not tech savvy, reveals a complete reversal of this trend that has cyber events growing exponentially more frequent and severe than ever before.

Verizon's 2019 Data Breach Investigations Report revealed that public entities topped the charts in 2018 for cyber-attacks, accounting for 16% of all breaches (out of the nearly 24,000 reported) and confidential information disclosed in over 300 of those incidents.

Cyber threats are quickly moving away from the category of something that "may happen" to something that "will happen," making it a higher priority for public entities to take active steps to prevent and prepare for cyberattacks.

Take a look at the current Cyber Statistics chart that illustrates an alarming rate of malicious emails, ransomware, and phishing incidents, and the skyrocketing costs involved with mitigating the devastation caused by cyberattacks.

Average ransom demands

Nationally ransom amounts range from hundreds of thousands of dollars to millions of dollars. Cyber criminals often demand ransom payments in Bitcoins or other cryptocurrencies. Today, each Bitcoin equals approximately $11,000 U.S. dollars.

For New Jersey Public Entities, ransom demands received at the end of 2018 and into 2019 are hitting around $300,000 each (25 bitcoins). These are only those that have been reported. So far, total losses paid have been nearly $2,500,000 (please note, many claims are still developing.

These facts point to a few key weaknesses that need to be addressed to help protect public entities from the growing plague of cyberattacks.

Eye-opening facts

Still think you are safe? Take a look at these New Jersey public entity cyber facts from 2013 to present:

540% Increase in Cyber Attacks

- About **80 events have been reported**, and there are another 50 we are aware of that were not formally reported.
- Less than 5 events were reported in each year from 2013-2016, with a jump to 19 in 2017 (375%), 32 in 2018 (68%) and **already 17 this year**.

Most Frequently Breached Department

- First: Administration with **over 50 events reported**
- Second: Police are ranked second with nearly **20 reported events**

Most Common Attacks

- Ransomware leads the type of attack with **over 35 events reported**
- The most common attack vectors being **Phishing** and **Supply Chain** (i.e., vendor access to your system).

So, what do we need to do?

The Municipal Excess Liability Joint Insurance Fund (MEL JIF), representing 65% of the public entities in New Jersey, has developed a model Cyber Risk Management Program for members that cover five key areas:

1) Defensive Software
2) Employee Training
3) Data and Software Backups
4) Technology Management
5) Polices & Procedures

Since there can be a big disconnect between the lingo of the Information Technology world and municipal leaders, this simple checklist has been created to outline what needs to be done and can be used by both parties for benchmarking their cybersecurity action plans and posture.

Why Defensive Software?

Antivirus programs, antispam filters and firewalls are common and effective first lines of defense. Antivirus programs provide protection from nearly all known malicious programs, while antispam filters are effective at blocking the majority of malicious SPAM. Firewalls help monitor network traffic and blocking malicious traffic. Microsoft Office users should utilize "Protected Mode" which blocks malicious programs from running when the documents are opened.

IMPORTANT NOTE:
These defensive measures are only effective if activated and applied to the correct locations on your network.

By the way, those annoying pop-up boxes that appear at the bottom of your screen are often patches to security gaps found in your software. While some pop-ups may be security related make sure to check with your IT professional before hitting the update button.

Why Employee Training?

Imagine your computer network as a house. You have numerous access points such as doors and windows. Locks are installed on the doors and a security system protects the home by requiring the use of a passcode. If someone gets your key or passcode, they can get in. Or, if someone comes to your door and tricks you into letting them in, you have walked them past all of that security. And that is what we see most often with phishing emails which trick people into clicking on malicious links or programs. So, when an attacker makes it past the defensive software, it is up to your employees to be able to recognize potentially malicious emails, links and documents, report them and NOT click or open them.

Why Data and Software Backups?

If our computers fail, or if data is accidentally deleted, or if information is manipulated by an attacker, how do we recover? Backups! When the defensive software and employees fail to protect your network, backups are your "Extra Life." If backups are set up correctly and information is backed up at least weekly, you can theoretically wipe your entire computer and reload the uncompromised version of the data within the same week. It is equally important to have backups of software programs, so they can too be reloaded.

While this sounds simple, there are a few key issues that can compromise the backup:

1) Backups on the same network that was attacked.
2) Backups not performed frequently enough (i.e., once per year).
3) Information stored locally on individual computers–this is NOT backed up.
4) Failure to check backups regularly for viability.

Why Technology Management?

Just as you wouldn't expect your insurance broker to be the town engineer, don't expect your staff to be technology experts. Having professional and experienced technology support, either on staff or outsourced, is critical. Not only should they be able to manage your network, but they should also be the quarterback for managing your cybersecurity posture. In addition to the defense mechanism already described, the technology manager should do the following:

1) Address physical security for your servers.
2) Limit employee access privileges across the network.

By the Numbers: Cyber Statistics for Public Entities

1 in every 302 emails are malicious
(Symantec ISTR 2019)

1 in 10 URLs are malicious
(Symantec ISTR 2019)

of successful hacks/breaches stem from phishing
(Cybersecurity Ventures 2019)

Successful ransomware attacks will occur every **11 seconds** by 2021
(Cybersecurity Ventures 2019)

Ransom demands range from **$100,000s to +$1,000,000s**
(NAS Cyber Report 2019)

Resource Center

Fortunately, there are a tremendous amount of free resources and links available both on the MEL JIF website, **www.njmel.com**, and through these organizations:

- New Jersey Cybersecurity Communications and Integration Cell (NJCCIC) **www.cyber.nj.gov**
- Stay Safe Online **www.staysafeonline.org**
- Center for Internet Security (CIS)/MS-ISAC **www.cisecurity.org**
- Stop.Think.Connect **www.stopthinkconnect.org**
- Cybersecurity and Infrastructure Security Agency (US-CERT/ICS-CERT) **www.us-cert.gov**

3) Password protect and encrypt confidential files/folders.

4) Require strong and regularly updated passwords.

FUN FACT:
The most commonly used password in cyber breaches is 123456.

Why Policies and Procedures?

Cyber Risk Management Practices are extremely effective, but they only work when everyone is aware of them and the rules and procedures are consistently followed.

Detail all of your technology plans in formal policies and procedures and show support from leaders by adopting them via resolution. In addition, an Incident Response Plan should be adopted that details exactly what to do and who is responsible for what during a cyber event. Countless times wrong and costly decisions have been made because no one knew what to do, or who to call.

The MEL JIF's Cyber Risk Management Program is both easy to follow and very cost-conscious regarding recommendations. Some critical items will require investment, such as backups; but many are free, such as requiring strong and frequently changed passwords.

Cyber risk is no longer theoretical, and cyber risk management is not something you can just put on your "to do" list. Cyber risk management must become as common as Workers' Compensation safety or storm preparedness to keep our towns, municipalities, and public authorities safe. Take action now!

At the League Conference

For more information on this topic, attend, "Your IT Systems Have Been Compromised: Now What?" on Thursday, Nov. 21 at 10:45 a.m. in room 309.

Focus on

Localizing Tech

Attention Elected Officials

Are your municipality's technology management practices putting it (and you) at risk?

MARC PFEIFFER, *Assistant Director, Bloustein Local Government Research Center, Rutgers University*

Today's technology is solidly embedded in most things that municipalities do. What's more, the public now expects technology-based services from its local government. However, as we have seen in recent headlines, technology presents risks that require sound management and ongoing mitigation.

To be clear: the IT systems in every municipality in New Jersey and around the country are under attack from cyber-criminals who want to steal and extort money, steal and resell data, or use hacked networks to attack and harass other computer users. These criminal networks target every computer user, from individuals whose computer is their smartphone, to tablets and desktop computers used in homes, governments, and business networks of every size.

If you don't already know this, you haven't been paying attention. The news has been full of stories about cybersecurity breaches affecting Equifax, the NSA, and the cities of Atlanta and Baltimore, with more places added to the list each week. You may even have heard rumors that three dozen or more New Jersey municipalities have been the victims of successful hacker attacks in the last two years.

If you are not proactively responding to these threats, you are putting your government, residents, and businesses in jeopardy and are effectively negligent in your responsibilities.

To help you understand what to do, here are some questions and answers about technology issues. As elected officials, you are ultimately responsible for your organization's cyber safety.

Day-to-day management

There are two things you absolutely must have in place:

1. A trusted employee or consultant who advises the town on technology management.

2. Tested back-up procedures that restore operating systems and data in the event your technology is compromised (e.g., ransomware). There are many backup solutions and yours must meet your specific needs.

That's why trusted expertise is a must. Your advisors can be vendors, employees, or even citizens involved in the computer industry.

If you don't have both, remedy that immediately. If you already have them, ask your expert to report on how secure your systems are, how often your data backup process is tested, and if there are other steps to take that would ensure adequate protection.

Check your procedures

Is it too late to protect my town from cyber threats? No, you are not too late because the threats are ongoing. But first, ask your technology staff one key question: what will your town do if its systems get infected by ransomware? If the answer does not give you confidence that recovery time will be reasonable, you need to revise your procedures.

Nevertheless, recovery from a successful ransomware attack doesn't happen overnight (even if a ransom payment is successful). Depending on the sophistication of the system, it will take at least several days or weeks to rebuild and restore systems. Do you have disaster recovery plans that allow critical operations to continue during that time?

If you have an expert and a sound and tested backup system. What else should you be doing?

Since every municipality has its own technology profile, each one must forge its own path to successfully mitigate its risks. However, there are three key elements needed to establish technological proficiency*:

Understanding Your Municipality's Technology Risks

There are six primary, inter-related technology risks:

Cybersecurity • Financial • Legal • Operational • Reputational • Societal

Cybersecurity threats present the most immediate, likely, and potentially damaging risk.

Technology risks can never be eliminated, but they can be mitigated. Mitigating cybersecurity risks requires ongoing management, technical attention, and support.

Today, system failures often stem from ransomware, when hackers encrypt software and data files and the key to unlock them requires payment over the internet (e.g., bitcoin). But beyond hackers, there are physical threats (e.g., broken HVACs, burst water pipes), power failures, and other disasters to consider.

Technology Management. This requires organizational leadership (proactive technology planning, budgeting, and decision-making processes), the development of sound incident response plans and technology policies that establish proficiency.

Cyber Hygiene. This means ensuring that all employees who use computers have had at least one hour of training in the last two years to stay safe from phishing attempts and social engineering when using their computer. Cyber hygiene also includes sound computer use policies, smart password construction, and appropriate data encryption practices.

Technical Competence. The more sophisticated the technology system, the greater the number of technical activities there are to do. However, there are some activities that apply to systems of all sizes. They include having sound backup practices, keeping software and hardware current with patches and updates, using defensive software (an anti-virus program at minimum) on all computers, procedures to control who has access to your systems; and maintaining a properly trained staff to manage those systems.

While this article focuses on cybersecurity, do not ignore the five other technology risks in the sidebar (left). Municipalities must address their complete technology "risk profile" as a management priority.

Looking to experts

No one expects every elected official or senior manager to be an expert in all

things municipal. That is why there are police chiefs, public works directors, engineers, finance officers, health officers and experts in every field. Today, technology managers need to be part of that list.

As a municipal leader, there is no excuse for your town not to manage its technology proficiently. Elected and appointed officials must make the security of their technology and their communities a priority and find ways to get it done well.

If your municipality is already there, kudos for having things under control! Most likely, you discovered that technology management takes more time, attention, and money than you thought it would. You were able to achieve proficiency because you invested in competent, trusted personnel to run your technology and you have supported them with sound decision-making processes. Keep up the good work. Share what you've learned with your peers. Staying cyber safe is a team effort.

Resource Center

For more information, visit the following websites.

- This collection of *NJ Municipalities* articles covers managing technology, **http://bit.ly/blousteinnjm**, developed by the Bloustein Local Government Research Center, Rutgers University.
- The Municipal Excess Liability Fund's Cyber Risk Management Program is an approach to implement sound cybersecurity: **http://bit.ly/njmelcrmprogram**. (The practices are available to anyone and not limited to MEL members.)
- MS-ISAC is a federally-sponsored resource center for states and municipalities on cybersecurity management: **https://www.cisecurity.org/ms-isac/**. It is free to join and each municipality should join.
- The NJ Office of Homeland Security and Prevention's point of contact for cybersecurity threats is **www.cyber.nj.gov** (aka, NJ-CCIC). Sign up for their (slightly technical) free weekly bulletin.
- Join GMIS the professional association of local government technology managers. Join as a municipality (low fees) and your staff and contractors can participate in a great local government technology management support group: **www.gmis.org**. Joining GMIS automatically enrolls you in the NJ chapter. Anyone can attend their annual Technology Education Conference.

Managing Technology Through Technological Proficiency is a report with implementation guidance. **http://blousteinlocal.rutgers.edu/managing-technology-risk/**