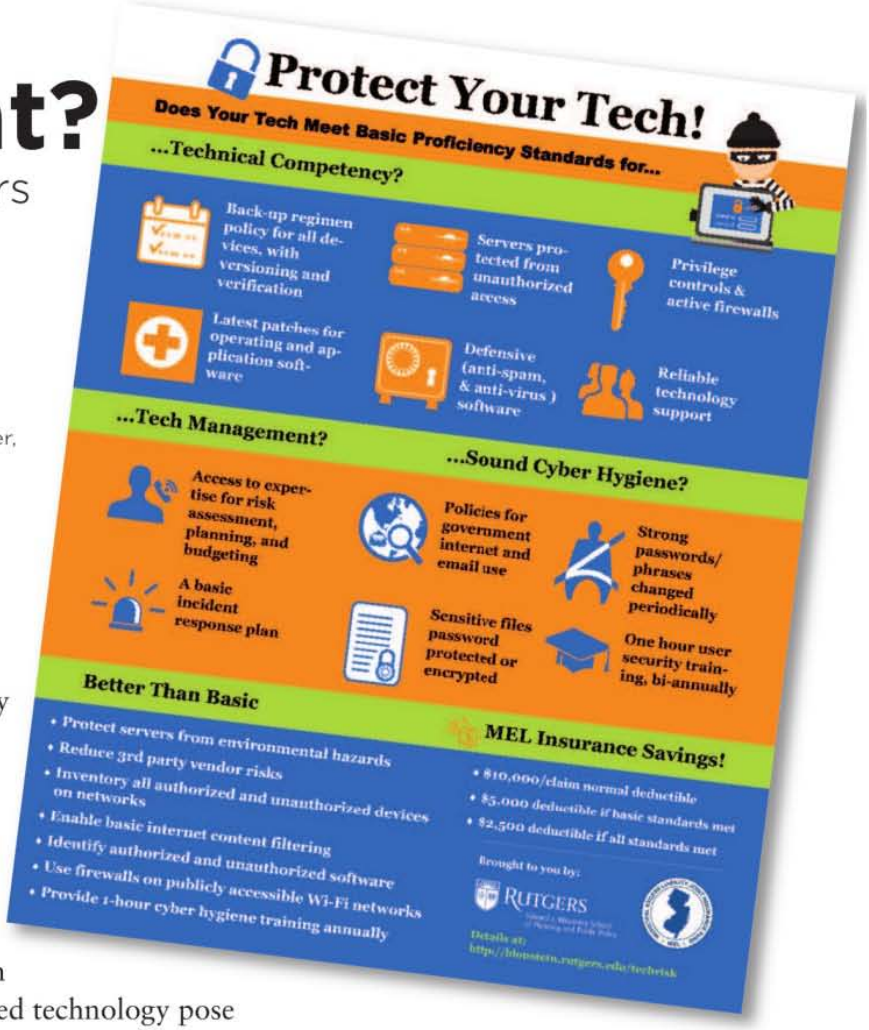
Know What?

What government leaders need to know about cybersecurity and technology

By Marc Pfeiffer, Assistant Director, Bloustein Local Government Research Center, and Technology Consultant, NJ Municipal Excess Liability Fund



It is clear to any observer of municipal government operations that technology has become an integral part of most municipalities. The problem is, it is constantly evolving; this requires organization leadership to pay close attention. Unfortunately, many government leaders don't fully understand technology, the speed at which it changes, or the risks that poorly managed technology pose to the government and the public.

Lucrative and low-risk crime

Criminals have found that attacking computer systems is a lucrative and low-risk activity. Ransomware encrypts individual computers and networks, and requires payment to get the decryption key; hackers can infect systems to find personally identifiable data and sell it on the "dark web"; there are convincing-looking, but fraudulent emails designed to mislead recipients into unwittingly helping hackers compromise financial controls or steal user and banking credentials. In short, all users, their computers, and their networks are under attack, all the time.

Since 2016, the Municipal Excess Liability Fund (MEL) had 14 reported claims filed against their cyber insurance policies.

Many municipalities have been successfully attacked. Those attacks shut down entire municipal systems for days. In addition to the successful attacks, there are dozens of other, less catastrophic incidents when an agency's IT staff detected the attack, responded to it, then limited and recovered from the damage.

Elected officials and senior managers need to put technology management on their agendas; it needs their time and attention. All municipal activities, such as police, land use, fire, housing and development, labor relations, etc., require advice from experts to help them determine what must be done now, and what will be required down the road. In addition, these experts can help them decide how to get there.

Minimum technology actions to protect yourself

There are a lot of experts offering lots of advice on technology management. Much of it is confusing to people who don't regularly deal with it, and frequently it is targeted to large organizations who have full-time, highly trained technology

professionals on staff. For municipal officials whose experience lies in other areas, making technology decisions is complicated.

Over the last three years, working with the Rutgers Bloustein Local Government Research Center, the MEL has studied the risks and challenges of managing technology, with the goal of providing municipalities with practical guidance. These studies concluded that there are two key elements. The first is understanding technology risks. The second is a standard outlining the bare minimum a municipality must do to proficiently manage its technology.

There are professional organizations that can help municipalities understand and manage their technology risks:

- NJ-GMIS, the association of local government technology managers; njgmis.org.
- NJ Cyber Communications and Information Cell, cyber.nj.gov. (Free)
- MS-ISAC, a US Homeland Security funded national group, cisecurity.org/ms-isac (Free)

Technology risks fall into six categories: cybersecurity, operational, financial, legal, reputational, and societal. These issues are detailed in a Bloustein Local report, available online at **blousteinlocal.rutgers.edu/managing-technology-risk/**.

Identifying a minimum technology means a municipality should meet a standard to protect and manage its technology assets. NOT meeting these minimum standards exposes a municipality to unconscionable risks that can result in the loss of data and the inability to deliver services; it can also make the organization vulnerable to legal and financial repercussions. Some municipalities already safeguard their technology assets by doing more than the minimum. Doing more reduces risk and is in everyone's best interest.

The following summarizes the three areas of technological proficiency. More detailed information about the standards can be found online at **bloustein.rugers.edu/techrisk**.

The first, technical competency, is composed of six actions:

1. Networks must have a competently designed backup system that permits recovery from ransomware or other forms of malware, mechanical failure, or any kind of disaster. The system also requires that backups are regularly verified and tested.

2. All devices must have actively maintained defensive software, i.e., anti-malware, anti-virus, anti-spam, and firewalls.

3. All servers must be protected from unauthorized access and secured from tampering. They cannot simply be left on a table in an unlocked basement or closet.

4. Access to applications must be limited to only those employees who need it, and access must be updated when jobs change or the individual leaves the organization.

5. System and application software must be patched with manufacturer recommended updates as soon as they are released; this takes technical expertise, testing, and good system management to ensure that updates are properly installed.

6. Experts must be available to support the deployment of technology and respond to security incidents.

Cyber hygiene and technology management

Cyber hygiene, or practicing safe computing, is the second area. Municipal staff members represent a critical line of cybersecurity defense. All computer users must understand that they will be attacked at some point; they need to protect themselves and the organization by knowing how to recognize and respond to attacks. They need to be trained to identify and respond to cybersecurity threats. This requires at least an hour of employee training spread over two years, although an hour of training every year is preferred to guard against ever-evolving cyber threats.

Municipalities must adopt and enforce sound internet and email use policies so that staff members understand their responsibilities and the risks they face if they violate them. Many municipalities have already done this; those that have not, need to. Today, it is as essential as employment practices liability training.

Many criminals focus on personal information. They invade vulnerable networks and look for files containing personally identifiable information or personal health information. These files need password protection or, even better, they should be encrypted.

Finally, systems and applications need a password policy that requires strong, unique passwords or pass phrases (an even more secure option) that are changed at least annually.

Managing technology and testing plans

Technology management is the final area. Every municipality needs a cybersecurity incident response plan, and it should be tested periodically. In addition, all municipalities need a process to assess technology risks, develop plans, make decisions, and fund their technology programs. The sophistication of the plan and its implementation need be relevant to the organization's technological needs. This can include any combination of staff members, volunteers, or contractors working to guide and help make decisions.

Recognizing the importance of these standards, the MEL is providing an incentive to its members to meet them. The incentive is that the usual $10,000 deductible for a cyber insurance claim will be cut in half if the basic standards are in place when a cyber incident happen, and that $5,000 will be cut in half again if a slightly higher standard is met. In most cases, the cost of meeting the standards should pay for itself if a claim is made against the policy.

Municipal leaders must understand that they need to pay ongoing attention to their technology assets as they evolve and their organizations provide more tech-based services. If your municipality (or any other organization) is not managing its technology proficiently, bring it up to speed. If it is, strive for improvement; there is always more to do. Remember, the criminals are smart and sophisticated; they only need to penetrate a network once; a successful technology program has to be successful 100% of the time.

Could This Happen to You?

Imagine walking into to the borough hall of a town of 10,000 people, turning on a computer, and seeing a screen that says that the computer's files have been encrypted; to restore them, the town must pay a ransom of $2,500 has to be paid in bitcoins, whatever those are. Then, you discover that every computer on the municipal network is affected. An uneasy feeling sets in. You call the local guy hired to manage the network and although he tries try to restore the computers to the way they were before the ransomware attack, you discover that the backups are also encrypted. As it turns out, they were on the same network.

Calls to law enforcement have no result; they couldn't do anything because there is no way to identify the attacker or locate the source of the attack. However, someone remembers that the municipality has cyber insurance through their Joint Insurance Fund. After contacting the risk manager who notified the insurer, a cyber breach coach is assigned to manage the crisis. The coach in turn, brings in a national cybersecurity firm to work its technology magic. The malware that caused the problem is identified, but because the backups are bad, the ransom to restore the data must be paid anyway. Finally, in spite of several false starts resulting in days of downtime, the network is disinfected and data is restored, at the cost of agency productivity, unplanned spending, and several sleepless nights.

Once the network is restored, it is easy to conclude that the agency's technology needs an upgrade. The town has several generations of computers, different versions of software, limited network support, and a poor backup system. Now, municipal officials see the importance of investing in technology, developing a management plan, and protecting the system from criminal intruders. But the damage has already been done.

Don't let a crisis determine your town's technology policies. Planning and preventive measures will save both time and money, with a reward of fewer unexpected problems.