NJMMA Newsletter – Spring Conference Cybersecurity Session Article

This 2017 Spring Conference session covered the challenges of cybersecurity. It was offered each of the two days. Marc Pfeiffer and Kurt Watkins spoke in both sessions, Jean-guy Lauture and Paula Cozzarelli each spoke at one session.

Kurt Watkins, an attorney with Scarinci Hollenbeck practices at the intersection of law and technology. He began the panel by discussing the various risks and threats of cybersecurity. He stressed the importance of a trained work force. Because cyber security threats can come from Microsoft Office (i.e., Word), PDF documents, e-mail links, e-mail attachments, USB drives, and more, the first line of defense is the end-user. Kurt explained that the wide variety of attacks requires that an end-user know the difference between risky and non-risky behavior.

Further, an end-user needs to be able to identify when something is wrong so that they either do not engage a potential attacker, or they report it to the appropriate internal authority. He urged those in attendance to consider electronic security the same way they consider physical security. There is no true way to overcome the many threats, but having everyone be familiar with what one looks like is the best way to prevent damage.

Jean-guy R. Lauture, the Township of Bloomfield's IT Director covered how to identify information security incidents and establish best practices for handling these incidents. He provided experience-based scenarios and recommended a step-by-step process for responding to incidents and developing an incident response plan and team.

He highlighted five elements for successful cybersecurity incident handling, and each requires different individuals responsible for taking the action. Depending on the structure of an organization, multiple individuals may be involved in performing the following:

- Identify the problem (all end users)
- Assess if it a cybersecurity incident (IT staff)
- Respond to the incident (technical staff and/or consultant)
- Report in accordance with the incident response plan (technical support staff and/or consultant)
- Review the overall effectiveness of the response procedures (responsible management official and technical staff)

It is critical to have a plan on how to recover from an incident in a timely and secure manner, and to minimize the impact on technology assets. It is important to establish an incident response policy, specifying necessary courses of action for dealing with a cybersecurity incident. The policy is a tool used to provide insight, guidance, and handling procedures. It specifies how to identify, respond to, and report a cybersecurity incident.

It is also important to consider the legal aspect of a cybersecurity incident and to have cyber insurance in place. This will help to expedite a response and avoid loss of time and resources should an event occur.

Paula Cozzarelli, the Administrator of the Borough of Little Ferry discussed her experience with a ransomware attack that came through a vulnerability found by an intruder conducting a brute force attack on borough servers.

Calls to the County Prosecutor's Office and Homeland Security found that there were no public decryption keys available for this ransomware variation (there are now thousands), but they advised not pay the ransom. After further discussion and filing a claim under the Borough's cyber insurance policy (through the MEL), they obtained professional computer forensic support, paid the ransom, and received the key to decrypt its files and eventually restored their files. Lessons learned from this experience include the following:

- Day-to-day information technology staff are best used for the operational needs of an organization. A system-wide ransomware attack requires the skills of computer forensic experts. This is best handled though a cyber insurance policy; be sure the organization has one and ransomware is covered.
- Proper back up is critical as it's the **ONLY** defense against attacks. No one will have the key to get files restored except the attacker.
- IT management is not a hobby or special interest; it's best left to IT professionals. Prior to the cyberattack the Borough's IT needs were managed reactively and not proactively.
- Educate staff. Cyber criminals are getting smarter by the second. This is a big business and growing exponentially.
- The forensic analysis determined that no personally identifiable information or protected health information was taken. The criminals' intent was to lock the files until payment was made.

Marc Pfeiffer, Assistant Director of the Bloustein Local Government Research Center at Rutgers discussed his technology management work for the Municipal Excess Liability JIF. Technology management and cybersecurity (one of several technology risks) are tough subjects, and very few municipal managers took courses in it.

The risks and threats are many and growing, and today they predominantly come from organized groups of criminals who conduct cybercrime. Thus, all municipalities must implement defenses to reduce their risks and enhance their ability to recover from a successful attack. He suggested of developing technology proficiency and focusing on technical competency, employee cyber hygiene, and sound technology management to help frame individual municipal solutions.

Using that model, he presented work that the MEL will recommend their members incorporate into their technology risk management practices. The guidance is based on a minimum, i.e., the "least-worst" policies you can have, and that higher levels should be considered. The key elements are as follows:

Become technically competent: *Backup!* Having a backup system that includes daily incremental backups with at least 14 days of versions on an off-network device, along with weekly backups of networked computers, and full backups of standalone devices. *Patch* – making sure that all operating systems and application software are tested and patched with the latest versions as released. Use *defensive software*, including antivirus, and enable firewalls on

all active devices and ports. Run antispam software on email servers, and ensure all unused network ports are closed. Employ *access control privileges* to ensure users have only those rights they need and limit administrator rights to the fewest feasible number of people. Make sure there are have *staff or contractors* on call to support agency technology and respond to security incidents.

Ensure employees understand and practice sound **cyber hygiene**. All computer users should have at least one hour of cyber hygiene *training* annually. That should include training on malware identification (email and websites), sound password/passphrase construction, how to identify security incidents, and understand social engineering attacks. The one hour can be spread over a year; not necessarily all at once. The organization should adopt *sound policies* covering government internet and email use. Also, *password protect or encrypt* files that include personally identifiable information. Finally, employees should be required to use *strong, unique passwords* (passphrases are even better), and be required to change them at least annually.

The third element covers **technology management** which includes technology planning, budgeting and decision making (i.e., governance). Here, the minimum standards expect that management has *access to expertise* that helps in making decisions. This can be staff, a consultant, or even citizen volunteers that support risk assessment/planning, decision-making, and budgeting. There needs to be a basic *cybersecurity incident response plan*. If the organization has cyber insurance (highly recommended), that plan should be tied to how that coverage is activated.

Marc also referred to his previous research on technology management that is online at http://blousteinlocal.rutgers.edu/managing-technology-risk. And because there was some leftover time, Marc also did an abbreviated presentation of his cyber hygiene training seminar for employees.