Cyber Security Best Practices for Vermont Municipalities

Municipalities often ask for a list of the most important things they can do to reduce the likelihood of a successful cyber attack, security breach, or system disruption from an external cyber event. We’ve compiled this list of best practices to help members understand exactly what they need to reduce their risk of an adverse cyber event.

For members who use NEMRC, specific recommendations include:

- The existing NEMRC version should be updated to the most current version, if not already completed. There are two specific patches that must be installed to address an identified vulnerability in the software. One is dated 7/18/18 and the other 12/18/18.
- The NEMRC “share” setting should never be left with “FULL, EVERYONE or ANONYMOUS” share/file permissions.

Beyond updating NEMRC, the following are some suggested best practices that apply to IT system management, users, and cyber security practices in general. These include the following:

**Hardware, Software, & Systems**

1. Complete a security assessment from a competent, independent IT vendor. The assessment should include file level scanning for PII.
2. Practice the principle of “least privilege” which provides system access to only the few individual end-users who must have it to perform their duties.
3. Maintain up to date anti-virus, malware and firewall defenses.
4. Perform regular scanning, monitoring and auditing of systems, communication ports, and applications via qualified IT personnel.
5. Separate publicly accessible computers from the office business network.
6. Carefully review software chosen to hold, store, and transmit municipal data to ensure that it meets current requirements for data security. As a rule, all data should be encrypted in transit and at rest.
7. Make sure that ALL software is updated and current. Software which is no longer supported by vendors (for example Windows 7), will pose a security risk and should be evaluated for replacement with a more current product as soon as possible.
8. Maintain physically segregated system backups that cannot be accessed via electronic administrator privilege. Backups should be periodically tested for integrity and function. Hackers that gain access to systems are encrypting back up files – as well as the primary data and systems - and then extorting the entity for the decryption key.
Work Practices

1. Provide regular and ongoing cyber security awareness training to employees to help them identify social engineering-based attacks such as phishing and business email compromise scams that will likely make their way into your email environment. Recent claims data confirms that humans are the weakest link in your cyber defense.

2. Always cross check and verify financial transactions to eliminate the potential for deception by spoofed invoices and bogus fund transfer requests. Employees should not click links in emails if it gives any cause for suspicion - and should instead pick up the phone to verify a funds transfer or other transactional request.

3. Never accept payroll or other payment changes by email or phone. Always require a form signed by the requestor.

4. Implement two-factor authentication for logins to improve overall security.

5. Use strong passwords and require a new password every 90 days.

Implementing all of these measures will substantially reduce your risk of a cyber loss!