MONTANA MUNICIPAL INTERLOCAL AUTHORITY
RISK MANAGEMENT BULLETIN
Please distribute to all appropriate personnel.

Date:	May 29, 2020
To:	MMIA Member Cities and Towns
Re:	Cyber Security Practices

According to the 2019 Data Breach Investigations Report by Verizon Business, 69% of cyber-attacks are perpetrated by outsiders. No organization is too large or too small to be avoid being susceptible to an attack. In fact, 16% of breaches occurred in public sector entities, with experts estimating this sector will see increased attacks in the future.

The best outcome for a cyber-attack, is to not have one. Follow these cyber security readiness protocols to help protect your organization from an attack, and to be able to quickly recover if an attack does occur.

Plan and protect

- Make sure you have a cybersecurity plan in place, and periodically review and update it to stay current with the latest security issues.
- Encrypt your devices to prevent breaches from lost or stolen devices.
- ***Back your data up regularly***. If your files are backed up, you can copy them back to your computer and bypass any ransomed files. Use the 3-2-1 rule. Keep three backups of your data, on two different storage types, and at least one backup offsite.
- Update your software regularly.
    - Automate patch management to ensure regular updates.
    - When Microsoft or another vendor sends out a patch, install it immediately. Many attacks are only possible because someone did not take this simple precaution.

MONTANA MUNICIPAL INTERLOCAL AUTHORITY
RISK MANAGEMENT BULLETIN
Please distribute to all appropriate personnel.

Date:	May 29, 2020
To:	MMIA Member Cities and Towns
Re:	Cyber Security Practices

- Use the "Controlled Folder Access" feature in Windows 10 to prevent ransomware from encrypting files and holding them for ransom. Controlled folder access works by only allowing apps to access protected folders if the app is included on a list of trusted software. If an app isn't on the list, Controlled Folder Access will block it from making changes to files inside protected folders.
- Password protect your data.
    - Require strong passwords and educate your employees on how to create strong passwords or passphrases.
    - Passwords should be at least eight characters.
    - Arbitrary password expiration is not recommended.
    - Passwords should be changed immediately if there is any reason to suspect they were compromised.
    - Longer is better. Using four unrelated words can create a strong, memorable password.
    - Do not re-use passwords.
    - Use a password manager to create and keep track of strong, unique passwords.
    - Use two factor authentication (2FA) where available.
- Be alert to phishing – educating employees is key.
    - Check the address the email is from, not just the name.
    - Do not open any email attachments or click on links unless you are sure of the sender.

MONTANA MUNICIPAL INTERLOCAL AUTHORITY
RISK MANAGEMENT BULLETIN
Please distribute to all appropriate personnel.

Date:	May 29, 2020
To:	MMIA Member Cities and Towns
Re:	Cyber Security Practices

    - If an email is unexpected or even slightly questionable, call and request verification that the email is legitimate. Do not use information in the email to contact the sender, get their information from an independent source.
    - Beware of very general, vague emails.
    - **Phishing does not stop with email**! Be aware of odd phone calls requesting personal or company information.
- Avoid open Wi-Fi networks or use a VPN.
- Avoid questionable sites; advertisements from disreputable sites are more likely to contain viruses and malware.
- Train all employees on these cybersecurity best practices, and educate them on suspicious behaviors.
- Make cyber security a focus of your third-party contracts.
- Don't wait until it's too late. Make cyber security a focus.

Response

- Disconnect the infected machine(s) from the network, but do not unplug the machine(s).
    - These practices help preserve evidence for forensic analysis.
- Report the claim to MMIA at 800-635-3089 option 5 or liability@mmia.net
    - If the incident happens outside of the business hours of 8 am to 5 pm Monday – Friday, MMIA property program members may report the claim directly to Beazley at 646-943-5912 or tmbclaims@beazley.com before reporting it to the MMIA.
    - If you are not in the MMIA property program, notify your cyber carrier.

MONTANA MUNICIPAL INTERLOCAL AUTHORITY
RISK MANAGEMENT BULLETIN
Please distribute to all appropriate personnel.

Date:	May 29, 2020
To:	MMIA Member Cities and Towns
Re:	Cyber Security Practices

- Don't pay ransom demands. You are probably not going to get your data back anyway, and if you do, they may have left themselves a way to access it again. Just use the backup you so wisely created.

Need assistance in developing a cybersecurity plan?

MMIA property program members have access to sample cybersecurity plans, an online e-learning platform where your employees can receive the latest training on cybersecurity best practices, and more! For more details, contact the MMIA risk management department at 800-635-3089 or riskmgmt@mmia.net