Wisconsin Elections Commission
212 East Washington Avenue | Third Floor | P.O. Box 7984 | Madison, WI 53707-7984
(608) 266-8005 | elections@wi.gov | elections.wi.gov

DATE: May 13, 2021

TO: Wisconsin Municipal Clerks
City of Milwaukee Election Commission
Wisconsin County Clerks
Milwaukee County Election Commission

FROM: Meagan Wolfe, Administrator
Robert Kehoe, Technology and Training Director

SUBJECT: Elections Security: Ransomware in the News

1. **Purpose**. This memorandum provides important information regarding the recent ransomware attack that shut off the flow of 100 million gallons of fuel daily to the U.S. East Coast. While this attack did not involve election officials or systems, it is a powerful reminder that basic practices are vital to our collective security.

2. **Background**. A major fuel transportation company in the United States recently shut down due to a ransomware attack. After gaining initial access to the pipeline company's network, the attackers deployed ransomware against the company's IT systems. In response to the cyberattack, the company has reported that they proactively disconnected certain systems to ensure the systems' safety. This company's shut down is causing fuel shortages on the East Coast and is likely to have a significant impact on the U.S. economy.

A. **Who Did This?** The FBI is attributing the attack to a group of people who call themselves "DarkSide." According to open-source reporting, since August 2020, DarkSide actors have been targeting multiple large, high-revenue organizations, resulting in the encryption and theft of sensitive data. The DarkSide group has publicly stated that they prefer to target organizations that can afford to pay large ransoms instead of hospitals, schools, non-profits, and governments.

B. **Since DarkSide is targeting wealthy corporations does that mean local governments are safe?** No. Ransomware can affect anyone and DarkSide is just one criminal actor among many. People who are not the intended target can also become victims of ransomware. Local governments can and do fall prey to ransomware attacks.

C. **How do cyberattacks affect local governments?** These attacks affect people both professionally and personally. From a professional standpoint, cyberattacks can shut down an office and prevent it from providing services to the public. Public records may be destroyed. Sensitive personal information

can be leaked to others and both members of the public and local officials may become victims of identity theft. The average cost of a data breach is approximately $150.00 *per record compromised*. Thus, a municipality of just 1,000 people could see recovery costs of $150,000.

3. **What to Do?** In nearly all cases the attack is successful because someone failed to follow very basic security practices. Ensure you and your organization are following these best practices:

A. **Strong Passwords** Use complex passwords (i.e. use a long phrase, instead of a word). Do not reuse the same password in multiple places. Consider using a password manager, but do not store passwords in a browser or any other application not specifically designed for it. For instructional videos on these topics, please see the resources section of this memo.

B. **Multi-Factor Authentication**. This means using something *in addition to* your password to complete authentication. For example, many banking sites may text a code to your cell phone as the second factor. You are not given access to the website until you enter your password and the numeric code. Similarly, WisVote requires use of a physical USB key for access even after entering your password. This additional factor makes it much more difficult for someone to access an account without permission. Whenever you are given the option to activate multi-factor authentication, do so.

C. **E-Mail Safety**. E-mail is the most common entry point for cyber-threats.
   1) Use caution opening emails from people you do not recognize, or emails with suspicious subject lines, links, or attachments. Human nature is generally trusting so being skeptical may mean going against your first instinct.
   2) Avoid clicking on links or attachments that come from sources you do not recognize or are not expecting. If someone responds to your three-month-old email by sending a link or an attachment, call them before clicking.
   3) Check with your email provider to see if you can use Multi Factor Authentication (MFA) to protect your email account.

D. **Regular Backups**. Backing up your computer is the best defense against ransomware. Backup or copy any data/documents onto a separate drive that is then disconnected from your computer and stored in a safe place. For Windows users, type "backup" in the bottom left corner of your screen's search box or see the additional resources page for a collection of how-to resources. You may want to work with your IT provider for assistance.

E. **Update Software & Restart Frequently**. Software updates protect you from known vulnerabilities.
   1) Protect your computer by turning on automatic updates. Since some updates are not applied until your computer restarts, it is a good idea to shut your computer down when you are done

using it for the day or restart it regularly. Leaving a running computer unattended for days or weeks hampers your ability to contain or notice an incident. Restarting your computer also protects it by clearing certain items such as typed usernames and passwords that remain in memory until a restart.

2) Update any and all software that is on your computer. Outdated software such as internet browsers (even programs you don't use) are entry points for attackers to compromise your system. A link to Microsoft's guidance on updating software is on the following page.

F. **Use a Supported Operating System**. Microsoft Windows users should upgrade to Windows 10. As of January 14, 2020, Microsoft no longer provides free security updates and support for the Windows 7 operating system. If you continue to use Windows 7 your device is at serious risk for security threats and viruses. Systems using Windows 7 or other operating systems are no longer supported by their developers are not authorized to access WisVote. There is additional information about this change in the clerk communication dated August 28, 2019.

G. **Consult with your IT service provider** regarding technical mitigations such as restricting RDP (remote desktop protocols), disabling macros, blocking TOR, and implementing application allow listing (a/k/a whitelisting).

4. **Where Can I Learn More?** The Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) have published a public alert on the attack that may be found on the CISA website here:

https://us-cert.cisa.gov/ncas/alerts/aa21-131a

5. **Resources.** For additional information on the actions above, you may wish to visit these links from Microsoft and the Global Cyber Alliance. As well, there are attachments about Distributed Denial-of-Service and acquiring services from the Department of Homeland Security (DHS).

Microsoft's instructions on how to enable automatic updates for your computer:
https://support.microsoft.com/en-us/help/17154/windows-10-keep-your-pc-up-to-date

Wisconsin Elections Training video on password complexity: (requires login)
https://electiontraining.wi.gov/mod/scorm/view.php?id=367

The Global Cyber Alliance's toolkit for password complexity, password managers and Multi Factor Authentication: https://gcatoolkit.org/smallbusiness/beyond-simple-passwords/

The Global Cyber Alliance's toolkit for how to back up your computer:
https://gcatoolkit.org/smallbusiness/defend-against-ransomware/

6. **Questions**. If you have any questions, please contact the WEC Help Desk. Call 608-261-2028 or e-mail elections@wi.gov.