STREAMLINE

2024 Cybersecurity Checklist for Special Districts

Protect against impersonation

- □ **Enable 2-factor (MFA)** - Enable multi-factor authentication and/or other tools like Single-Sign-On (SSO), security keys, and/or passkeys on your main web-accessible systems.
- □ **Get a .gov URL** - Register a .gov URL for your district (bonus points if you use it for your email).
- □ **Authenticate email -** Enable DMARC email authentication, implement a strict policy, and test your setup on mxtoolbox.com so no one can send mail on your behalf.
- □ **Prepare for AI-enabled phishing** - Implement security awareness training for employees that includes information for preventing AI-enabled social engineering attacks. If you can't train in person, VC3, Breach Secure Now, and/or Bullphish ID are good automated solutions to consider.
- □ **Confirm wire transfers** - Put a confirmation process in place for wire payments where you call only trusted, verified numbers. Create a separation of duties for oversight. (e.g., one initiates, one approves). Utilize tools like iMessage Contact Key Verification to ensure text messages can be trusted between key district contacts.

Protect network and infrastructure

- □ **Conduct network security testing** - Work with a third party to audit the security of your network on a very regular basis (especially essential if you have SCADA/ICS/IoT devices.)
- □ **Password-protect all devices** - Require passwords and/or device-level authorization (biometrics, etc.) on all devices. Consider mobile device management (MDM). (It sounds simple, but one employee who doesn't have a protected device can allow your entire network to be compromised.)
- □ **Consider a password manager** - When logging in through district Office365 or Google Accounts isn't possible, require all staff to use a password manager. Good options include 1Password, Dashlane, Bitwarden.

Other best practices

- **Consider a secure intranet** - sharing documents over email alone is not as secure as using a secure intranet product that has been audited by a third-party
- **Consider integrated payments** - being able to collect payments on your own .gov improves trust. Be sure to know who has the power to redirect your payment page to a lookalike site.
- **Consider integrated agreements and forms** - allowing people to e-sign on your website is better than having people scan and email forms to your office
- **Consider grant funding** - programs like the SLCGP can cover 60%-100% of the costs to tackle all the above. Managed service providers (IT consultants) and other vendors with knowledge of local government should be able to help you apply!
- **Consider having a Managed Service Provider** - Hire a 3rd party that ensures hardware and software is upgraded and patched as necessary, monitored 24x7x365 (with endpoint detection response/EDR), that key systems are backed up in perpetuity, and that manages your technology roadmap, inventory, and lifecycle.

Questions? Contact Mac Clemmens <mac@getstreamline.com>