NOT-FOR-PROFIT RESOURCE

CYBERSECURITY & DATA MANAGEMENT BEST PRACTICES

Use this checklist to secure your not-for-profit organization against cybersecurity attacks that could compromise your customer and donor data while working remotely or on-site.

□ **Use up-to-date technology**
Make sure that your organization is using the latest version of Windows and keeping application software updated.

□ **Patching**
Utilize automated patching software and prevent "unpatched" workstations from accessing your network.

□ **Create and utilize strong passwords**
Create a password policy that requires strong passwords (minimum 8-10 characters and complexity requirements). Also consider utilizing two-factor authentication.

□ **Ensure device security**
Encrypt all hard drives and secure mobile devices through Mobile Device Management (MDM) software and also ensure a commercial grade antivirus software on all PCs and servers.

□ **Train your employees**
Cybercriminals often take advantage of unsuspecting employees to gain access to your systems. Develop a formal training program for your employees that includes "red flags" they should look for in phishing emails.

□ **Secure home environment**
Enable encryption on your home wireless networks and enforce the use of Virtual Private Network (VPN) software for remote access.

□ **Electronic file storage**
Create a formal policy outlining the permissible storage locations which should be within the organization (e.g., your on-premise file servers or your Office 365 instance). You should prohibit personal Drop Box or Google Drive solutions.

□ **Secure documents**
Create a document security policy that includes what documents you consider confidential, how to securely store them, and dispose of them.

□ **Backup data**
Data should always be backed up to an alternate location from your primary data storage on a nightly basis. Regularly test your back-ups to ensure your team can actually restore backups if necessary.

□ **Incident response plans**
Develop and then test an incident response plan that outlines what to do in the event of a breach or infection.

□ **Purchase cyber insurance**
Talk with your insurance provider about the proper level of cyber insurance based on your risks and the costs associated from a data breach or ransomware attack.

CPAS / ADVISORS
blue

Questions about how to implement these cybersecurity best practices at your not-for-profit organization? *Contact our expert.*

Tom Skoog *Cybersecurity & Data Management Practice Leader*
tskoog@blueandco.com | 614-220-4131