ENABLE MINISTRY PARTNERS

CYBERSECURITY CHECKLIST

CHECK THE BOX FOR EACH STATEMENT THAT IS TRUE OF YOUR CHURCH'S ENVIRONMENT

☐ SECURE PASSWORDS

You have an intentional password policy in place. Your policy includes requiring strong, unique passwords or pass-phrases and encourages the use of a password manager.

☐ MULTI-FACTOR AUTHENTICATION

You have enabled multi-factor authentication (MFA) for all users on all accounts for which it is available.

☐ PATCHING & UPDATES

All computers, systems, and software are on regular patching schedules that you audit regularly to ensure patching compliance.

☐ ANTI-VIRUS (ENDPOINT PROTECTION)

You use an organization-wide anti-virus solution on all Windows and macOS computers that provides advanced protections including anti-malware, network protection, and content control capabilities.

☐ FIREWALL & UTM

You have a firewall in place for all of your networks that segregates trusted and non-trusted networks, provides objectionable content filtering, and includes other unified threat management (UTM) features.

☐ BACKUPS & BUSINESS CONTINUITY

You have a robust local *and* cloud-based backup schedule. The technical portion of your broader business continuity plan is clear and understood by your IT team. Leadership is aware of recovery capabilities and timelines.

☐ USER MANAGEMENT

You regularly delete old user accounts that are no longer in use. You follow a standard process for new users that ensures 'least access' privileges with appropriate management approvals required for access level changes.

☐ SECURE WI-FI & NETWORK

You employ network segmentation. All private networks are password-secured, and client-isolation is enabled for all public/guest networks.

☐ ENCRYPTION

You have full-device encryption enabled on all Windows and macOS workstations. Users are trained on properly encrypting emails containing sensitive information.

☐ ANTI-PHISHING & EMAIL SECURITY

You have an organization-wide anti-phishing and email security solution, such as IRONSCALES, that provides added protection against phishing, name spoofing, and other email-based threats.

☐ SECURITY AWARENESS TRAINING

You consistently provide ongoing training for your staff (periodic online modules, webinars, group training sessions, etc.).

☐ ENDPOINT MANAGEMENT & SECURITY

You have tools and processes in place to accurately track your endpoints (computers). You utilize additional features of your management platform to implement security policies, security auditing, and ransomware monitoring and protections.

☐ ENDPOINT DETECTION & RESPONSE

You use an endpoint detection and response (EDR) tool, like Huntress, installed on all servers and workstations, to automatically scan for threats that anti-virus might miss.

☐ VULNERABILITY SCANNING

You conduct regular (monthly), automated vulnerability scanning of your organization's network.

☐ CYBERSECURITY INSURANCE

Unfortunately, this is no longer optional for a secure environment. You have assessed your cybersecurity insurance options with an expert and have an active policy for your organization.

☑ ARE YOU COVERED?

If you cannot realistically check all of these boxes yet, your environment is not as secure as it can and should be. If you would like help creating your comprehensive cybersecurity strategy, give us a call! We are passionate about helping churches and would love to partner with you.

This checklist is a great starting point for measuring your organization's level of security, but it is not a guarantee of protection. Rather, it is a guide to help move you in the right direction. In the cybersecurity world, things are always changing and new threats arise daily. Implementing all of these checklist items is a vital first step in the right direction, but you must continually be vigilant, stay aware, and regularly educate yourself and your staff.

WWW.ENABLEMINISTRY.COM | INFO@ENABLE.EMAIL | 866.397.2358