Cybersecurity Must-Haves & Specialized Insurance ***For Churches***

WHAT YOU NEED TO KNOW TODAY

ENABLE MINISTRY PARTNERS

Contents

Cybersecurity Must – Haves

Cybersecurity is a crucial issue that requires the attention of anyone charged with leadership of a church, ministry, school, business, or any other type of organization. The reality is that threats and risks associated with cyberattacks are rising exponentially. While it may not seem evident initially, churches are a popular target of cybercriminals. Why are churches targets? First, churches are attractive targets because they often maintain members' valuable personal and financial information. Second, most churches are not prepared to protect themselves against cybercriminals who seek to do them harm.

Increasingly, church leaders must prioritize implementing comprehensive, effective cybersecurity plans, procedures, and training. These "non-negotiables" are for anyone involved in a technology-enabled ministry environment. While most leaders understand their responsibility in this area, many do not know where to begin planning their strategy and often approach the topic with confusion.

At Enable, we work with these leaders daily. Our clients regularly ask us the same two introductory questions:

“What steps should I be taking to protect our church?”
and “What should I tackle first?”

We have created the Enable Cybersecurity Checklist to help leaders assess the security level of their church's technology environment. This checklist provides a roadmap for implementing vitally important security measures within your specific church environment.

1. INVENTORY

To protect something, you must be able to account for it. It’s vitally important that you have a complete inventory of all network and computer equipment owned by your organization, and that you are cognizant of every place where data is stored (local servers, workstations, cloud services, etc.). You can’t protect systems or data that you aren’t aware of.

2. USER MANAGEMENT

Ensuring that only current, active employees have access to your computers and network environment is of vital importance. You must also limit employee and volunteer access to only the systems and data needed for them to perform their job functions. You must regularly delete old user accounts and follow a standard process for new user setups that ensures 'least access' privileges with appropriate management approvals required for access level changes.

3. SECURE PASSWORDS

Accounts with weak, easy-to-guess, or reused passwords are “low-hanging fruit” for cybercriminals. A password policy that requires strong, unique passwords and encourages using a password manager is one of the most crucial security measures an organization can take.

4. MULTI-FACTOR AUTHENTICATION (MFA)

The goal of multi-factor authentication is to verify identity and ensure that the person logging into an account genuinely is the person they claim to be. MFA is necessary because passwords alone do not deter security breaches and cybercrime. On top of secure passwords, MFA provides a second layer of protection and security. It strengthens security during login and is an accessible, helpful, and easily implemented solution.

5. PATCHING | UPDATES

One of the most valuable and straightforward ways to keep your technology environment secure is to stay up-to-date with software and firmware patches. Patching is simple; it just takes disciplined, consistent attention. In most successful cyber breaches, hackers obtain access to data or systems via well-known software bugs for which patches already exist but which IT administrators have never applied!

6. FIREWALL WITH UNIFIED THREAT MANAGEMENT (UTM)

Basic firewalls have been a "must-have" for years, but rising security threats call for firewall platforms with enhanced protection. Today's firewall platforms include UTM features such as Intrusion Detection and Prevention, Gateway antivirus, Geo-IP filtering, and objectionable content filtering. A basic firewall doesn't do enough to protect you without these advanced capabilities.

7. SECURE WI-FI & NETWORK

When it comes to Wi-Fi, there is no one-size-fits-all solution. Still, church IT staff must properly segment/isolate traffic across the church's wired and wireless networks. It must encrypt all sensitive Wi-Fi traffic to the highest available standards. A secure wireless environment will utilize strong user authentication for staff network access, will have a separate guest network with client isolation enabled, and should work in tandem with a UTM firewall solution as described above. Additionally, Internet of Things (IoT) devices like building automation controls (e.g., HVAC, door access controls, lighting systems, security cameras, etc.) should each have their own network segments, isolating each system type from talking with other network devices.

8. DEVICE ENCRYPTION

Disk encryption is vital to protecting your systems and thwarting those determined to misappropriate your data. It enables you to store information on your technology devices in a state that an unauthorized user cannot easily access. So, if a cyber thief physically steals your computer, it will be difficult for him to read and utilize this data.

9. ANTI-PHISHING | EMAIL SECURITY

Email is, far and away, the preferred method for hackers who desire to steal information, money, and access. We recommend implementing a system that focuses explicitly on stopping phishing attempts and goes beyond the traditional spam filtering provided by your email provider. This one move is a significant first step in protecting against vulnerability in this area. Solutions that provide much more protection and power than those supplied with your email hosting platform are available and affordable. However, anti-phishing solutions are not enough in and of themselves. Fraudulent email schemes are becoming increasingly more sophisticated, and we must train our staff members to recognize and avoid common email attacks.

10. SECURITY AWARENESS TRAINING

The most vulnerable link in all churches' cybersecurity prevention efforts is the human element – the staff. The staff? Why? The reason is almost always because the staff has not received adequate training to recognize security threats, how these threats may manifest, and how to respond to an attack. As humans, staff members can and do make mistakes! They trust fake identities, fall for alluring "clickbait," and can become entangled in many other sneaky cybercriminal schemes. The best protection for cyberthreats is a combination of the right tools, practices, and staff training. Training should include all staff, regardless of role. It should be ongoing, perpetual, measurable, and delivered in various formats tailored to the specifics of your church staff.

11. ANTIVIRUS | ENDPOINT PROTECTION

Implementing a robust, organization-wide antivirus solution on all Windows and macOS computers provides centralized reporting and advanced protections, including anti-malware, network protection, and content control capabilities. Enabling such a solution is a non-negotiable that strengthens your environment's security.

12. VULNERABILITY SCANNING

Identifying open weaknesses in your environment is critical to helping you know what you need to fix and protect. You should perform vulnerability scanning internally and externally and repeat it regularly to identify new threats. A good vulnerability scan will identify the systems with known problems that you can fix by installing appropriate patches, adjusting security parameters, or isolating the affected equipment so other network devices can't reach it.

13. IDENTITY THREAT DETECTION & RESPONSE

You can control access to your church's most important data by carefully assigning appropriate access permissions to your trusted users. But what happens when an attacker takes over the digital identity of your user? Now your 'trusted user' is anything but trustworthy. So, it's vitally important that you always protect the digital identity of your users. You need to know the minute a user's online accounts are compromised and a "fox has entered the henhouse." Ideally, if you believe someone's account has been compromised, you will also want to immediately disable access to that account. This is exactly what an Identity Threat Detection and Response service does. They proactively monitor your online accounts and look for indicators of a compromised account. If they find suspicious activity, they can immediately disable access while notifying IT administrators so they can further investigate and remediate the threat.

14. ENDPOINT DETECTION & RESPONSE

A good cybersecurity defense program includes multiple layers of protection that work together to prevent, detect, and respond to attacks by malicious actors. Firewalls and traditional antivirus are great prevention layers, but it's essential to have other tools to detect and respond when cyber criminals successfully breach your preventative layers. Endpoint Detection and Response (EDR) or Managed Detection and Response (MDR) tools help cover the detect and respond phases by identifying threats that make it past your preventive defenses and providing steps to recover from a successful attack. You should install EDR tools on all servers and workstations.

15. CYBERSECURITY INSURANCE

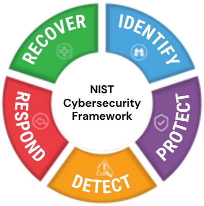
Cyber insurance, also called cyber risk insurance or cyber liability insurance, is a policy designed to help organizations mitigate risk exposure by offsetting costs involved with recovery after a cyber-related security breach or similar event. It covers scenarios generally not included in General Liability and Professional Liability policies. Given the environment in which they operate today, this is no longer optional for churches utilizing technology in ministry operations.

16. BACKUPS | BUSINESS CONTINUITY

A robust ministry continuity plan involves the backup of data, systems, and servers. Such a plan ensures you back up data and machine images in geographically diverse sites. Your plan will allow you to avoid paying a "ransom" for your data and ensure you have good data backups. It will also provide for redundant capacity to continue the technology, reporting, data, and back-office ministry operations while you are recovering from any attack, incident, natural disaster, etc.

The items on this checklist are a great starting point for measuring your church's level of security, but the checklist is not a guarantee of protection. Instead, it is a guide to help move you in the right direction. In the cybersecurity world, things are constantly changing; new threats arise daily. **Implementing 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.**

THE ENABLE CYBERSECURITY CHECKLIST



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.

These recommendations are aligned with the NIST Cybersecurity Framework, which you can learn more about here: https://www.nist.gov/cyberframework.

Check the box for each statement that is true of your church's environment

- □ **Inventory**
  You maintain accurate, up-to-date inventory lists of all IT equipment, software, and services to ensure you know what you are responsible for protecting.

- □ **User Management**
  You regularly delete old/retired user accounts. All generic email addresses use delegated access techniques (no shared logins). You follow a standard process for new users that ensures 'least access' privileges with appropriate management approvals required for access level changes.

- □ **Secure Passwords**
  You have an intentional password policy in place. Your policy reminds users that longer passwords or passphrases are more secure and encourages the use of a personal password manager.

- □ **Multi-Factor Authenticator**
  You require multi-factor authentication (MFA) for accessing all systems that support it (Microsoft 365, Google Workspace, church management system, etc.).

- □ **Patching & Updates**
  All computers, systems, and software are on regular patching schedules that you audit regularly to ensure patching compliance. You work with HVAC, security camera, and other vendors to ensure their products stay patched as well.

- □ **Firewall & UTM**
  You have a firewall in place that segregates trusted and untrusted networks, provides objectionable content filtering, and includes other unified threat management (UTM) features.

- □ **Secure Wi-Fi & Network**
  You employ network segmentation. HVAC controls, security cameras, Internet of Things (IoT) devices, etc. are restricted to their own isolated network segments. All private networks are password protected, and client isolation is enabled for all public/guest networks.

- □ **Device Encryption**
  You require full-device encryption on all user-issued Windows and macOS workstations.

- □ **Anti-Phishing Email Security**
  You have an organization-wide anti-phishing and email security solution that provides added protection against phishing, name spoofing, and other email-based threats.

- □ **Security Awareness Training**
  You consistently provide ongoing cybersecurity-related training for your staff (periodic online modules, webinars, group training sessions, etc.).

- □ **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.

- □ **Vulnerability Scanning**
  You conduct regular (monthly), automated vulnerability scanning of your organization's network.

- □ **Identity Threat Detection & Response**
  You proactively monitor user activity in Microsoft 365, looking for potential indicators of compromise with a security operations center (SOC) helping analyze and remediate identified threats.

- □ **Endpoint Detection & Response**
  You use an endpoint detection and response (EDR) tool partnered with a security operations center (SOC) to identify threat-actor activity on your endpoints. This protection is installed on all servers and workstations in your environment.

- □ **Cybersecurity Insurance**
  You have an active cybersecurity insurance policy that you've reviewed with your insurance provider to ensure it covers your risk exposure adequately. You're confident that if you experience a cybersecurity incident, your insurance provider will help you respond and recover.

- □ **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.

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.

Download your copy here!

Specialized Cyber Liability Insurance

A Non-Negotiable for Churches Today

AN ALL-TOO COMMON SCENARIO

You hear a new story almost every day. Cybercriminals use social engineering to bypass technology safeguards and security protections to infiltrate email systems, bank accounts, credit card accounts, member databases, and other areas containing sensitive data. The criminals then utilize the data to steal money and identities, create access for future attacks, or obtaining compromising personal data as the basis for extortion attempts. The financial and reputation results can be devastating.

HOW DOES THIS HAPPEN?

Cybersecurity attacks can happen in a variety of ways and are limited only by the attacker’s creativity. But common themes do exist. In one widespread social engineering scenario, hackers may first get into someone’s email account and start watching conversations for things like due dates on project payments or bills, amounts owed, and the specific discussions in the emails. Then, because they have obtained such precise information, they can represent themselves as a trusted person making a request that seems absolutely legitimate. They may utilize fear as a trigger to induce the person “to act right now” to avoid consequences for the church or the employee. For example, “Since you haven’t paid your bills, we are going to penalize you, expose your negligence, or impose embarrassing delays or restrictions, etc.”

For example, a Catholic church in Ohio fell prey recently to this exact type of attack and was induced to send $1.75 million to cybercriminals. Amid a large construction project, the church was contacted by the general contractor, who expressed concern that the church had missed its last two monthly construction payments. The church staff in charge of the project was horrified as they were very conscientious in paying everything on time and even had proof that the disputed wires had gone through.

FBI investigators later were able to discern that the hackers had penetrated the church's email system and were able to then pose convincingly as the construction company principals. In this place of trust, the hackers communicated to the church that their bank routing and account information had changed. Accordingly, the church sent the money to the criminals' accounts rather than to those of the general contractor.

What happens when a church suffers this type of loss? Sadly, most general liability and professional liability policies do not cover this type of increasingly common injury. This is where cyber insurance comes into play.

WHAT IS CYBER INSURANCE?

Cyber insurance, also referred to as cyber risk insurance or cyber liability insurance, is a policy designed to help an organization mitigate risk exposure by offsetting costs involved with recovery after a cyber-related security breach or similar event. Malware, ransomware, and distributed denial-of-service (DDoS) attacks are conventional methods used to compromise networks and sensitive data sources.

DOES MY CHURCH REALLY NEED CYBER LIABILITY INSURANCE?

Yes, absolutely, without a doubt you do.

Cybercrime is on the rise; this is no mystery to anyone today. The frequency and ingenuity of cybersecurity incidents are increasing exponentially. As churches utilize an increasing number of applications, devices, and other technology components and services to enable ministry, they become more vulnerable to attacks. Just as businesses insure against business problems, natural disasters, and physical risks, churches need insurance coverage for cyber threats as well. And if you are like many churches, your General Liability and Professional Liability policies likely do not address your exposure to cyber risks.

In the church context, Errors and Omissions Insurance (also known as Professional Liability Insurance or Malpractice Insurance) is designed to protect church staff or pastors accused of errors and negligent acts committed in the course of ministry activities. Because this type of coverage is not offered under a general liability policy, E&O is vital to churches looking for protection from incurring the full cost of defense and damages that may arise in a lawsuit. But merely obtaining a standard E&O policy may not be sufficient.

Typically, E&O insurance in the church context is provided to insure against exposure in such areas as pastoral liability (damages that may arise from pastoral counseling such as sexual misconduct, invasion of privacy and defamation), counselor's liability (neglect or omissions that may occur due to vocational counseling, educational or even learning disability, therapy), or abusive acts liability (coverage for staff or volunteers who are acting on behalf of your church or religious organization that may be accused of actual or threatened abuse).

It is important to note, however, that many E&O policies do not cover the types of cybercrime exposure that are becoming increasingly common. Church leadership must confer with their insurance counsel to ensure that they have obtained proper coverage for the types of cyber-attacks to which they vulnerable.

In a recent Enable blog series, we have covered numerous ways to protect your staff, systems, and data. If implemented conscientiously, items such as multi-factor authentication, password management, security training for staff, enforcement of security policies, email security practices, business continuity, managed firewalls, disk encryption, consistent patching, and sophisticated SIEM tools can all significantly reduce the likelihood that a church is going to fall prey to the kind of cyber-attacks we have been discussing. Nevertheless, in the rapidly changing environment of cybercrime in which we all now operate, we believe that churches who desire to be faithful stewards must consider the available cyber insurance options carefully.

SOME PRACTICAL CONSIDERATIONS

Most insurance providers can individualize policies based on need and size.

- **Theft and fraud** – Covers loss of the policyholder's data as the result of a criminal or fraudulent cyber event, including theft and transfer of funds.
- **Forensic Investigation** – Covers the legal, technical, or forensic services necessary to assess whether a cyber attack has occurred, to determine the impact of the attack, and to stop an attack.
- **Business Interruption** – Covers lost income and related costs where a policyholder is unable to conduct business due to a cyber event or data loss.
- **Extortion** – Provides coverage for the costs associated with the investigation of threats to commit cyber attacks against the policyholder's systems. The coverage extends to payments to extortionists who threaten to obtain and disclose sensitive information.
- **Computer Data Loss and Restoration** – Covers physical damage to, or loss of use of, computer-related assets, including the costs of retrieving and restoring data, hardware, software, or other information destroyed or damaged as the result of a cyber attack. Many carriers have an absolute exclusion in their policy form for the replacement, reproduction, and restoration of data lost or damaged during a security breach or other error or omission.

There are many additional coverage options as well, e.g., rogue employee coverage, privacy liability, media liability, privacy notification costs, etc. Some of these may apply to your specific church situation, and some may not. Your insurance counsel should be able to guide you into those choices that make sense for your circumstances. As with all financial decisions, stewardship demands a prayerful consideration of the costs and benefits derived.

COMPARING POLICY FORMS AND WHAT TO LOOK OUT FOR

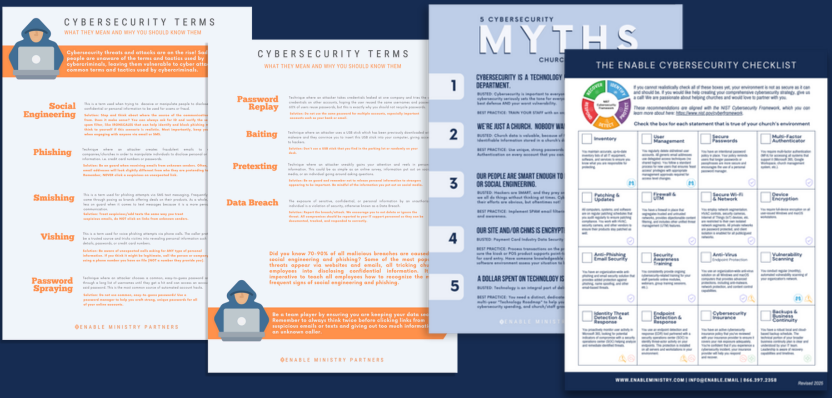
- Identify your unique risks. The first step in buying cyber insurance is to understand the nature and the extent of the risks facing your organization.
- Identify the limit structure (coverage, aggregate policy, sub-limits imposed).
- Are data breach expenses inside or outside the policy limit? Are they included?
- Is there coverage for inadvertent disclosures (i.e. lost or stolen cell phone or laptop with unencrypted data)?
- Understand the “triggers.” It is essential to understand what activates coverage under your cyber policy.
- Is there coverage for violation of the insured’s privacy or data handling policies?
- What coverage restrictions are imposed?
- What are the proposal’s subjectivities or conditions (underwriting requirements)?
- Does the application contain a warranty statement?
- Available risk management services: what loss prevention tools are available? Are there any fees associated with these services?

Other **Tools and Resources**

Cybersecurity Tips ‘N Tricks

Help keep your organization cybersafe!

As your trusted IT provider, we encourage you to remain vigilant in keeping your data safe. Since the pandemic in 2020, cybercrimes have increased nearly 600%! These types of crimes include identity theft, email scams, social engineering ploys, and others, all of which can cause significant financial and reputational loss. We’ve assembled a variety of resources that can assist you and your staff in keeping your organization cybersafe. Our hope is that you will use these resources and apply as many of the recommendations as possible.



CYBERSECURITY TERMS
WHAT THEY MEAN AND WHY YOU SHOULD KNOW THEM

Social Engineering
Phishing
Smishing
Vishing
Password Spraying

ENABLE MINISTRY PARTNERS

CYBERSECURITY TERMS
WHAT THEY MEAN AND WHY YOU SHOULD KNOW THEM

Password Replay
Baiting
Pretexting
Data Breach

ENABLE MINISTRY PARTNERS

5 CYBERSECURITY MYTHS

1 CYBERSECURITY IS A TECHNOLOGY DEPARTMENT.
2 WE'RE JUST A CHURCH. NOBODY WA
3 OUR PEOPLE ARE SMART ENOUGH TO OR SOCIAL ENGINEERING.
4 OUR SITE AND/OR CHMS IS ENCRYPT
5 A DOLLAR SPENT ON TECHNOLOGY IS

THE ENABLE CYBERSECURITY CHECKLIST

Check the box for each statement that is true of your church's environment

□ Inventory
□ User Management
□ Secure Passwords
□ Multi-Factor Authenticator
□ Patching & Updates
□ Firewall & UTM
□ Secure Wi-Fi & Network
□ Device Encryption
□ Anti-Phishing Email Security
□ Security Awareness Training
□ Anti-Virus
□ Vulnerability Scanning
□ Identity Threat Detection & Response
□ Endpoint Detection & Response
□ Cybersecurity Insurance
□ Backups & Business Continuity

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