Summer, 2022

THE STEWARD

Trustworthy Insurance Insights for Churches and Ministries

"No weapon that is formed against thee shall prosper...saith the LORD"
Isaiah 54:17

- Cybersecurity Resources for Houses of Worship
- Cyber & Finance for Seniors and Older Adults
- Cybersecurity Claims Lessons Learned
- Cyber Hygiene Best Practices
- Agent Corner & Insurance Board Is Going Green
- CEO Corner

INSURANCE BOARD
Partners in Protection

Cybersecurity Resources for Houses of Worship

Susan Schneider, Office of Security Programs, Infrastructure Security Division, Cybersecurity and Infrastructure Security Agency

The internet is a great tool for faith-based organizations to connect with members and potential members, but it is also an attractive tool for malicious actors who may exploit information that is readily available. The Cybersecurity and Infrastructure Security Agency (CISA) provides a wealth of security and awareness resources to assist houses of worship to continue to use the internet safely. CISA's *Mitigating Attacks on Houses of Worship Security Guide* provides an analysis of ten years of targeted attacks against houses of worship and potential risk mitigation solutions designed to achieve a robust and layered approach to physical and cyber security. Within this guide, houses of worship can find information written specifically for them on creating a culture of cyber readiness, cyber hygiene, online safety, and resources to build a robust security program.

CISA provides a Cyber Essentials Guide and Starter Kit for organizations to begin implementing organizational cybersecurity practices. Houses of worship are encouraged to make backups of their data to avoid the loss of information critical to operations in the event of a ransomware attack. Important files that need additional back up and protection might include financial records; congregant lists, addresses, and personally identifiable information; property records; employee and volunteer files; online donation records, etc.

Additional cybersecurity best practices include requiring multi-factor authentication (MFA) for accessing systems by all users, but especially by privileged, administrative, and remote access users. MFA is a layered approach to securing online accounts and the data within them. MFAs are essential to put into place because there are two or more authenticators to verify your identity before you are given access to protected data. Even if one authenticator, like your password, is compromised, unauthorized users will be unable to access your accounts. This CISA action plan for small businesses has great information to consider with additional details about MFA and is informed by the way cyber-attacks happen. The tasks are broken down by role to lay the groundwork for building an effective security program.

In addition to these best practices, CISA develops *CISA Insights*, to discuss specific cyber and physical threats to the nation's critical infrastructure, along with mitigation strategies stakeholders can implement. If you would like to subscribe to the CISA cybersecurity mailing list to learn more about best practices for cybersecurity network to action visit cisa.gov/uscert/mailing-lists-and-feeds. Finally, CISA Cybersecurity Advisors (CSA) are located across the United States who offer assistance and front-line support to help prepare and protect stakeholders from cybersecurity threats. To contact your local CSA visit cisa.gov/cisa-regions or email central@cisa.dhs.gov.

Cyber & Finance for Seniors and Older Adults

Insurance Board, Loss Control

Seniors and vulnerable adults in your congregation may be at greater risk of becoming victims of financial abuse or cyber-crime due to sophisticated schemes that target people within vulnerable populations. A safety net should be used to help protect people from becoming victims.

Cyber Crime

There is a running joke about the emails people receive in their spam folders from the king of a far-off country offering an inheritance if we would only send money to claim the reward. The joke ends when a vulnerable party is duped into sending thousands of dollars to an offshore account guaranteeing their life savings is gone forever. Victims may not be familiar with the dangers of the internet or the ominous "Dark Web." Education, awareness, and advice are the keys to prevention.

Teaching seniors and vulnerable adults how to practice cyber safety can go a long way toward protecting their identity, sensitive personal information, and financial resources. Providing resources and training, or a cyber resource help line (supported by church members with a technical background) can make all the difference between a positive online experience for someone or a complete disaster.

Please see the tips below regarding tactics that can be used to protect seniors or vulnerable adults while online:

1. Passwords: Use passwords, including one to lock a device, and close out internet or computer sessions when done. A strong password is at least 12 characters long with a mix of letters, numbers and symbols (and should not include personal information).

2. Secure access to accounts: Since passwords can be stolen, adding two-step authentication (a system to provide a onetime access code) to accounts provides a second layer of protection. Many online services, including apps and websites, offer free options that could help you protect information and ensure that the proper person is trying to access an account – not just someone with a password.

3. Think then act: Communications that create a sense of urgency, such as a problem with a bank account or taxes, are likely scams. Consideration should be given to reaching out directly to the company by phone to determine if the email is legitimate or not. A help line with qualified congregants could offer assistance and answer questions for seniors or vulnerable adults.

4. Delete it: Clicking on links in emails is often how scammers get access to personal information. If an email looks unusual, even if the person knows the party who sent it, it's best to delete it. Scammers can use a friend's email address and send someone messages acting as them. It is best to turn on spam filters for an email account to help filter out unwanted or suspicious messages and senders.

5. Online sharing: One should be careful of what is shared publicly on social media sites. Adjusting the privacy settings on the site can limit who can see information and avoid giving a location.

6. Security software: Install security software from a reliable source on devices and keep it updated. It is best to run the anti-virus and anti-spyware software program regularly. Avoid security updates from pop-up ads or emails, as they could be malware that could infect a computer.

Hosting an information session where people can bring in their personal devices to have someone assist them with security measures, or even scheduling appointments with individuals to offer assistance may be helpful.

Cyber & Finance for Seniors and Older Adults

Insurance Board, Loss Control

7. Browser safety settings: If someone searches for news, information, or products by using an internet browser, adjust the settings in each of those browsers to select the options for optimal security. The menu choices can often be found in the upper right corner of the browser. Consider clearing the browsing history at the end of a session to avoid leaving a trail of sensitive data.

8. Firewall security on a computer: The computer's operating system (OS) likely has a default firewall setting that will protect a computer from outsiders without needing adjustment. An antivirus software program can include additional firewall protection that can be adjusted separately-consider contacting a computer professional for assistance.

9. Logging out: Remember to log out of apps and websites when they are not being used. Leaving them open on the computer screen could make a system vulnerable to security and privacy risks.

10. Support: If a trusted person (family member or caregiver familiar with computers) is not available to assist with questions, consideration should be given to hiring a service to serve as a trusted source and to act as a second set of eyes and ears.

Financial Crime

The first step in protecting at-risk individuals is identifying those congregants who may be susceptible to exterior influences. Changes in behavior and their emotional state may help identify who may need assistance. If someone is becoming withdrawn, it can be a sign of a changing mental or emotional state. If someone is limiting a person's ability to interact with others, their motives may be nefarious.

The second step is determining what assistance can be provided to create a safety net for those who need it. A program that creates awareness of issues and available assistance without causing shame can be a saving grace for seniors and vulnerable adults.

Protecting Against Financial Abuse

- Develop program that helps build awareness and identifies people in your congregation who may be at risk for financial abuse.

- Provide helpful resources to help people recognize when someone may be trying to manipulate or take advantage of them.
- A ministry can provide resources offering financial guidance through regular meetings or seminars conducted by qualified church members who could also be enlisted as a direct contact for those needing advice.
- Sadly those who are closest to a vulnerable party and have access to them (caregivers, neighbors, or other family members) are often the same people that exploit seniors and vulnerable adults for financial advantage.
- Financial records can provide a window into possible abuse. A simple act such as reviewing a checkbook or banking statement may provide clues.
- Clues may include an abnormally large amount of cash withdrawals or small checks written on a regular basis to one person.

Other signs of financial abuse can be:

- Changes in bank accounts
- Altered financial documents (such as a will or power of attorney)
- Unusual changes in spending habits
- Secretive financial discussions
- Often, legal action is needed to protect the victim of exploitation from a predator. This can involve contesting a trust agreement or will.

Please consult experts, an attorney and/or licensed financial or computer professionals for specific advice on any program to protect your ministry and its members.

Also see these resources:

- U.S. Department of Justice Office of Justice Programs
- Insurance Board's Cybersecurity 101

Cybersecurity Claims Lessons Learned

Monroe Moore, Insurance Board Senior Claims Analyst

In today's fast-paced, electronic world, security for modern-day organizations can feel almost impossible. Cybercriminals will stop at nothing to access vital systems within your organization. Now more than ever, it is imperative that we stay vigilant in keeping our organizations protected from such breaches of security. It is essential to have safeguards in place to ensure that should a breach occur, it is identified quickly, and the necessary steps are taken to ensure that the breach will not happen again.

With so many ways that a cybercriminal can infiltrate your systems, what preventative steps can you take to ensure that you and your organization are protected? Here are some basic measures that you can take to minimize your exposure:

- Make sure that your work and personal laptops are always locked when you step away from them;
- Do not utilize public WIFIs -- you never know who else might be logged on to that same public network;
- Conduct employee awareness training, email filtering, and web security;
- Be careful with how you dispose of old computers and laptops as they may still contain vital organization information;
- Be suspicious of emails with addresses you do not recognize and those that are poorly written;
- Smartphones should be password protected and not left out in the open. A few moments with an unattended computer, smartphone or tablet can allow a criminal the opportunity to steal all sorts of personal information such as call logs, address books, saved logins and passwords, financial and banking apps, credit card numbers, etc.

It is important to consider all the ways that you and your team access the internet. Strong passwords and cyber policies for all devices including servers and routers will help keep your data safe and secure. It is imperative for passwords to be strong - meaning they should be of a longer length and utilize unique characters. The same or similar passwords should not be used across all their devices and apps. These security vulnerabilities allow bad actors to access devices and download data. Password managers can be very helpful when working with longer, unique, and complex passwords.

When a Cyber breach occurs at your organization, whether it be sophisticated ransomware events, business email compromises, or social engineering attacks, please get in touch with Insurance Board immediately. Promptly filing a claim will ensure that Insurance Board can coordinate the engagement of vendors to determine where and when the breach occurred and the necessary steps to terminate the threat to your organization and mitigate any damages. Insurance Board will also contact an approved privacy attorney to consult and assist in engaging other vendors, including forensic investigators, if necessary.

In summary, the best way to protect your organization from cyber threats is for you and your staff to be well versed in Cyber security and remain vigilant in looking for the red flags that indicate someone is trying to infiltrate your network. Should an actual data breach occur, please contact your partners at Insurance Board to mitigate damages and restore your ministry's operations.

Cyber Hygiene Best Practices:

By: The Cincinnati, Insurance Companies

As cyberattacks become more frequent and severe, it's increasingly important for organizations to practice good cyber hygiene—habitual practices ensuring critical data and connected devices are handled safely—to minimize their exposure to risk. Some consequences of poor cyber hygiene include:

Security breaches

Data loss

Software vulnerabilities

Antivirus weaknesses

The following are essential parts of cyber hygiene:

Passwords — Users should create strong and complex passwords, and avoid sharing passwords or using the same password across different accounts.

Security software — A high-quality antivirus software can perform automatic device scans to detect and remove malicious software and provide protection from various online threats and security breaches.

Data backups — Essential files should be backed up in a separate location, such as on an external hard drive or in the cloud.

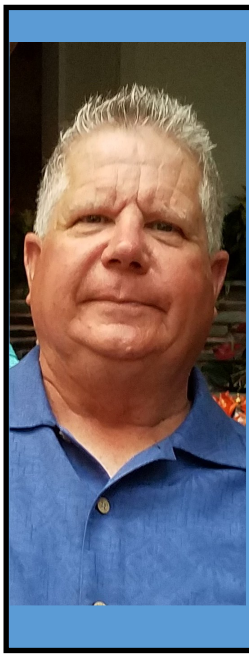
Firewalls — Organizations should have a network firewall to prevent unauthorized users from accessing company websites, email servers and other sources of information.

Multi-factor authentication — Important accounts should require multi-factor authentication to limit the opportunity for cyber-criminals to steal data.

Employee education — Workforce cybersecurity education is essential to teach employees to identify phishing attacks, social engineering and other cyberthreats.

Daily routines, good behaviors and occasional checkups can make all the difference in ensuring an organization's cyber health is in optimal condition.

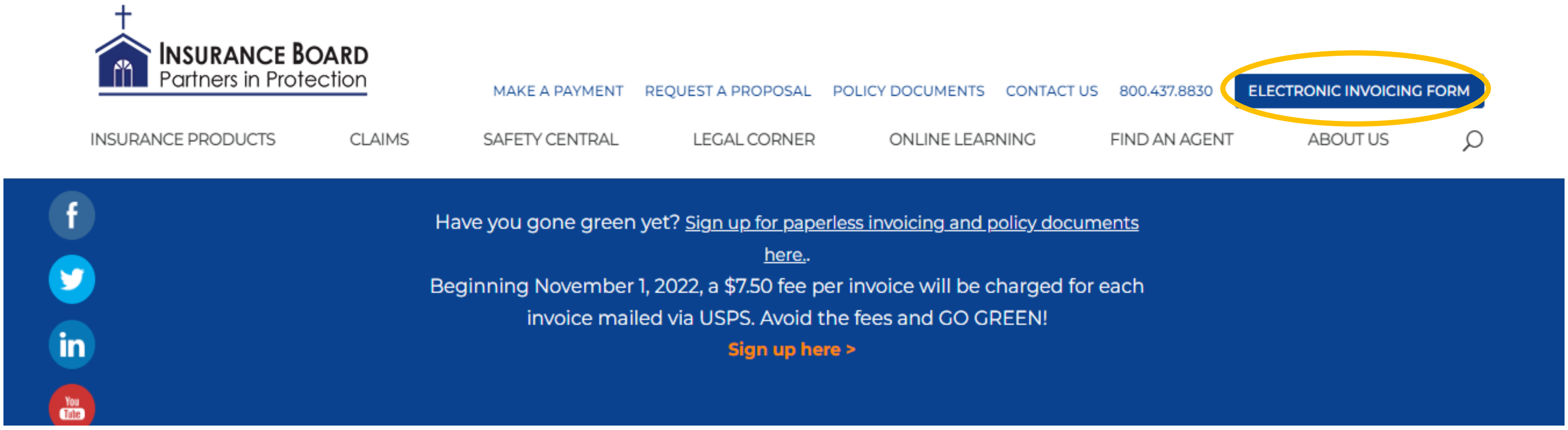
Agent Corner



Matthew "Matt" Huntington has been an Agent with Insurance Board since 2004 and has been in the insurance business for over 40 years. In relation to cybersecurity, Matt says: "It's an important topic. I tell my churches, just like they would with any other claim or issue to stay vigilant no matter what's going on at the church. Just like water damage issues, everything starts small and then becomes bigger. Consider getting cybersecurity protection and if something occurs, react right away. Just like a little leak on the ceiling, if not addressed, a year later it's a huge problem; cybersecurity is the same." Matt suggests that you have a policy in place to not wire transfer money to anyone. When Matt was the Treasurer of the Rocky Mountain Conference, he received phishing emails every week asking to help someone out as they were in trouble and needed money wire transferred to them immediately. Most of those emails looked like they came from the conference minister or the moderator of the conference. "I hope churches never fall for this but just last week I had a church say that they wired $500 to someone in need and it was not who they thought it was."

Matt also shared that he forwards all his churches the information from Insurance Board's website including articles and workbooks with helpful information on cybersecurity. He also mentioned the webcast handouts for example: Cybersecurity 101, and the policy samples from (CISA) Cybersecurity & Infrastructure Security Agency & (DOD) Department of Defense. Matt emphasized that churches should "Stay vigilant, know what's going on at your church, and have controls in place to prevent fraud, including financial controls, property damage controls, and computer access controls as well."

Insurance Board Is Going Green!



Have you gone green yet? Sign up for paperless invoicing and policy documents here..

Beginning November 1, 2022, a $7.50 fee per invoice will be charged for each invoice mailed via USPS. Avoid the fees and GO GREEN!

Sign up here >

We're going green beginning November 1, 2022!

All invoices will be sent electronically via email, please complete the following steps to go green:

1 Go to InsuranceBoard.org and click on the electronic invoicing button on the home page;

2 Fill out the form with the required info and submit it. Please allow ten business days for processing.

You can go paperless with payments, too! ACH payment processing (electronic payments) is available through our website at InsuranceBoard.org/make-a-payment/

Contact: Insurance Board
1468 W. 9th Street, Suite 350 Cleveland, OH 44113
Phone: 800.437.8830 Fax: 216.736.3239
www.InsuranceBoard.org

INSURANCE BOARD
Partners in Protection

CEO CORNER

TIMOTHY S. HARRIS, CPCU
PRESIDENT AND CEO

Basic Cybersecurity Practices

Cybersecurity continues to emerge as a significant challenge for all organizations as transactions are increasingly performed online. Numerous cybersecurity resources cite the rise in cyber related attacks during the pandemic when many people and businesses (including churches) across the globe were forced to transition to online resources in an effort to ensure business continuity. That trend has persisted. Previously, cyber thieves often focused on larger, more sophisticated organizations where the perceived bounty was greater. However, increasingly, cyber criminals have realized that cyberattacks on smaller, less sophisticated organizations can prove just as fruitful.

The Cybersecurity and Infrastructure Security Agency (CISA) highlighted a surge in sophisticated ransomware attacks during 2021. Ransomware incidents are where a hacker infiltrates the computer network of an individual or organization and encrypts data so that the only way the individual or organization can access their data is by paying a ransom. While these attacks are not all that common for churches and ministries, the methods by which they gain valuable information are quite common. Two very frequently used techniques include:

- Hacking simple passwords – organizations should implement a password policy that requires longer passwords and multi-factor authentication (MFA) to verify a user's credentials

- Social engineering – using deceptive techniques to manipulate individuals into giving up sensitive, confidential information for fraudulent purposes

A sophisticated hacker can employ software able to easily crack simple passwords within days or even hours. The longer the password, the more difficult it is for a hacker to decipher. In fact, the FBI suggests that the length of a password, even if a simple passphrase, is more difficult to crack than a shorter, complex one with a combination of upper and lowercase letters, numbers, and special characters. Of course, using both a longer and complex password provides the best protection.

Cybercriminals don't have to be sophisticated IT experts to extract valuable information and assets from their victims. Oftentimes, their victims give this information up willingly. They do so by clicking on unknown links in emails (sometimes being deceived into thinking those links are coming from a reliable source) or being instructed to send information to a fraudulent person including being asked to send or wire funds to a new bank account. My staff members regularly get emails from individuals purporting to be me, asking them to carry out some action or transaction on my behalf.

Claims alleging cyber theft or breaches are often complex, may involve outside investigations or forensic analysis, occasionally require law enforcement, and can take many months to resolve. Also remember that while insurance coverage for cyber events is very important, it does not protect against all cyber related incidents. For instance, coverage for the voluntary parting of funds or wiring funds to fraudulent accounts may be limited or not covered at all. Churches should be very vigilant when wiring funds, confirming wiring instructions and the recipient. Sometimes, this can be achieved by simply calling the recipient at their known phone number. We have experienced church claims involving fraudulent wires from the thousands of dollars into the millions. Consequently, these cybercrimes can have substantial financial consequences.

This material may include a general description of insurance coverages and does not include all terms, conditions, and limitations found in Insurance Board policies. Only the insurance policy will form the contract between the insured and Insurance Board. Neither Insurance Board nor its employees, representatives, or agents shall be liable for the use of any information of statements made or contained herein. The information contained in these materials is intended solely to provide general guidance. Insurance Board disclaims all liability for any errors or omissions or for any actions you take or fail to take based on these materials. The information provided may not apply to your particular facts or circumstances; therefore, you should seek professional advice prior to relying on any information that may be found herein.