Cybersecurity Issues Councils Should Consider

Michael Kirk, General Counsel, Legal Services Department
David Dinkel, Associate Director of IT, Information Technology
Administrative Services Group, Presbyterian Church (U.S.A.), A Corporation

Data breach. Two words that cause palms to sweat and send shudders up and down the spine. Churches and councils are not immune from hackers, intrusion, and data breaches. Electronic files and systems owned by churches often have information, such as bank account numbers and credit card information, that hackers covet and can use for their benefit or sell on the dark web. Such systems also contain employee information such as social security numbers that cybercriminals can use for financial gain. Churches and councils should take all reasonable steps to make their systems secure and to protect data of employees, members, and donors.

Most security risks can be relatively easily addressed. Employee mistakes often contribute to many security problems. Cybersecurity experts point out that employees are often the biggest cyber security risk because: (1) they are prone to make mistakes and are not properly trained to secure data; (2) they do not adequately protect the physical security of their employer-issued computers and devices; (3) they do not passphrase protect devices so if they are stolen, it is more difficult to access information on them; and, (4) they respond to emails from hackers in ways that allow hackers to compromise employer computer systems. This article will provide guidance to help avoid such risks.

Why Do We Need It?

One question congregations and councils need to ask to start an analysis of cybersecurity risks is: what confidential and personal information do we hold in hard copy or electronic form for employees, members, and donors? Once you have clearly identified all sources of risk and whether items are retained in hard copy or electronic format then you can ask another very important question: WHY DO WE NEED IT?

Some organizations gather potentially sensitive information, and it lingers on their systems for no reason. The information is not used and is not necessary, but no one thinks to shred it, burn it or delete it from electronic systems. Conduct an audit. If you do not need some of the information/data that you find in hard copy or electronic storage– GET RID OF IT!! Of course, get rid of it securely by shredding hard copies (not putting them in the trash or recycling) and talk to your cyber advisor on how to safely and effectively delete electronic records.

Physical Security

Many businesses ignore physical security while making extraordinary efforts to protect their computer and online systems. It is easier for a burglar to kick in a door or break a window to get at physical files, laptops or hard drives than it is for a hacker to get at electronic files. Suggestions for physical security:

1. Put as many locks as you can between a thief and the desirable paper files. Locks on building doors, locks on office doors, and locks on cabinets where confidential data is stored.
2. Similarly, lock up your servers, external drives, and equipment.
3. If you can afford a security system, have one installed in your offices and buildings.
4. Do not share with non-employee, non-member third parties or inquirers the location of confidential information in your offices.
5. Have policies and procedures for all staff so that when they remove phones, devices, and laptops from church or council property they must do all they can to protect them and know where they are at all times. Examples of policy provisions:
    a. Never leave devices unattended at coffee shops, restaurants, or airports or ask an unknown third party to watch them while you go to the restroom or check on a flight.
    b. Never lock devices in car trunks except in emergencies. If you take them home always locked them in the residence or, if traveling, in your hotel room.
    c. Never leave devices in plain view in cars or at home.
6. When employees retire, resign or are terminated, immediately lock them out of your email and other systems so they cannot access confidential and sensitive information, especially if the employee is terminated or leaves under unpleasant circumstances. When someone is no longer an employee there is never a good reason not to lock them out of your offices and your systems.

<u>Device Security</u>

Device security programs and system software security programs are a MUST. Enable your firewalls and regularly update your PCs, Macs, iPhones, and all devices. All such security programs should be activated, monitored, and kept up-to-date. Often, devices have an auto-update feature so that the programs are automatically updated and patched 24/7.

Employees should also be required to passphrase protect their devices. Many employees do not protect their phones or devices with passwords so that anyone can pick up an employer-issued device and immediately access the contents. This becomes a significant problem if the employee has emails and documents on the phone or device that contain confidential information from members and donors. Employees may not think they have confidential information, so they need to be reminded. For example, if a parishioner has contacted a pastor with a confidential personal problem seeking pastoral care, that is confidential. A device that houses donor information holds confidential information.

Even when employees create passwords, they do not make them adequately complex and they are easily breached. Employees sometimes use silly numerical combinations such as 123456 or personal information like the name of their children or dog. All a thief needs to do is visit an employee's Facebook page, conduct some research on their personal life, and the thief can try a few likely passwords and quickly access a stolen phone or device.

Passphrases are longer, more secure, and are much easier to remember than passwords. Employees should select phrases they can remember, such as combinations of their favorite books, plays or songs. For example, TheTempestBennie&TheJets2019 is stronger than Jane or Fluffy. For devices or external drives that hold confidential information, it is desirable to encrypt that information when it is removed from work so that if a thief steals the device it is difficult to access the confidential information it contains.

One last instruction/order to employees concerning passwords and passphrases: employees NEVER share them with anyone.

Phishing and Spoofing

Phishing is a strategy in which a victim is contacted by email or text message by someone posing as a legitimate person or institution to lure the victim into providing personal and confidential information such as bank account numbers, credit card details or passwords. One of the common ways that phishing is used against employees is for a hacker to study the website of an organization. They identify the leadership of an organization and may even contact someone in the organization by email to see what a legitimate organizational email looks like. The hacker then manufactures what looks like a legitimate email from the Executive Director or Head of Staff to someone in HR or finance (spoofing) and makes a request for a list of employee social security numbers or donor bank account information. Without checking, the employee responds. After all, the boss asked for the information. But the information ends up being sent to a hacker outside the organization. This type of targeted email attack is called spear phishing and is one of the most common and fastest-growing types of cyberattacks. Because of this, employees must be extra diligent when reviewing their email, particularly when the sender requests personal, confidential or financial information.

Another more recent spear phishing scam is a phony email allegedly sent by an employee to someone who handles finances or benefits asking to change the direct deposit bank account information in the employee's personnel records. The change is made, and funds are sent to the phisher's offshore account before the problem is discovered.

Another example of spear phishing is what looks like a legitimate email from someone in leadership, such as a pastor/head of staff, asking someone in finance to immediately wire or send money to someone or some business. The email looks legitimate and the employee promptly takes care of the assignment. But the money has actually been sent to the phisher's account.

A final tactic about which churches and councils should be aware. A donor sends a frantic email. The donor alleges that he or she made a donation but missed the decimal point ($1,000 instead of $100.00) and asks the church to refund the overage. Church staff check and discover the donation and refund the overage. Days later staff find out that the phony donor's original donation was rejected by the bank due to insufficient funds. Staff try to contact the donor and receive no response. It was a scam; the church sent a refund that was not owed for a donation that was fake.

There are ways to try to avoid such mistakes:

1. Have a policy or practice that no employee should respond to an email request for confidential personal information. Requests can only be made in person within the church office or council office.
2. If you allow people to respond to email requests, the policy should require that they contact the requestor in person or by phone to confirm the request before responding (pastor – did you send me an email asking me to send $10,000 to organization X?).
3. Train employees to check the email address in requests for money transfers or the sharing of confidential information. Often if the employee hovers their cursor over the email name it will show the actual email address. So, for example, if the email address of the employee's boss is Boss@firstpresanywhere.org and the employee hovers over the email name (Boss) and it says something else (for example r45677@gmail.com), they should not respond – they should delete the email. They should immediately notify their boss and all other employees to be aware if they get similar emails.
4. Train employees to be suspicious of all emails, especially those that ask them to click on a link or open an attachment. If the email is from a hacker, it is common for them to insert malware or ransomware on the employer's system to steal information or shut the system down until a ransom is paid.

The Federal Trade Commission has a helpful webpage on phishing.

https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams

Back It Up

Finally, make sure you have a back-up system. If disaster strikes you want to be able to go back at least 30 days to recover all data stored within that time.