CAPINTECH

Cybersecurity Best Practices for Churches

By Lisa Traina, Partner

A church in Iowa lost more than $680,000 raised to help homeless and abused women after a phishing email allowed hackers to gain access to the church's online bank account.

Another church in Iowa had seven years' worth of files encrypted in a ransomware attack after an employee clicked on an email titled "job application – please see attached CV." Churches in Bristol, England were victims of a similar attack.

And earlier this year, two arrests were made in a widespread cyber attack that compromised communications of prominent Italian individuals and institutions, including the Vatican.

Cybersecurity is no longer an "IT issue." It's a critical operational issue. Church leaders need to understand the risk and ensure they are devoting the proper resources to addressing it.

The following best practices will help you tighten up your church's cybersecurity defenses.

Church leaders need to understand the risk and ensure they are devoting the proper resources to addressing it.

Accept that your church is at risk.

Many churches believe that they are too small to be at risk of a cyber attack, or that they don't have data a hacker would want. As the examples above illustrate, however, all churches are at risk.

Many cyber attacks are random, meaning that churches of all sizes are equally vulnerable. Other cyber attacks are targeted, with criminals often focusing on small and medium-sized organizations because they assume these organizations lack the resources to maintain strong information security controls.

Additional factors that make churches vulnerable to a cyber attack include:

- Highly desirable data, including user names, passwords, and personally identifiable information such as names, addresses, dates and places of birth, and Social Security numbers
- A diverse group of network users — staff, volunteers, members, and visitors with their own devices
- Online bank accounts
- Electronic connections to vendors and other organizations
- The growing threat of hacktivism — a form of hacking that occurs for socially or politically motivated purposes

Depending on the type of cyber attack, your church could lose data, be locked out of your network, or have personal information about employees and members compromised. This can result in significant financial and reputational damage.

Understand the threat.

Cybercriminals typically target common technical weaknesses. Three of the most prevalent threats are malware, phishing, and technical vulnerabilities.

Malware is malicious software installed without a user's knowledge, typically when a user clicks on a link in a phishing email or visits an infected website. This includes ransomware, which cybercriminals use to encrypt data and demand money to unlock it, or threaten to leak data unless a ransom is paid.

Malware can be dormant for quite some time before the hacker uses it to exploit a vulnerability or system weakness. All systems are vulnerable to malware, so it's crucial to have appropriate controls in place to protect all

your systems. This includes servers, desktops, laptops, networking equipment, networked printers, and mobile devices. It also includes the increasing number of "smart" devices such as alarms and thermostats that can connect to the Internet and operate like mini computers.

Phishing emails are fraudulent emails designed to entice the recipient to click on a link or attachment that opens the door for hackers to infect systems with malware or steal data. These emails can take many forms, from typo-ridden messages that are fairly easy to spot, to package shipments or credit card fraud alerts from what look like legitimate sources. Although your church may use filtering to stop many of these emails, some slip through in even the best systems.

Spear phishing emails look like they are from a person or business you know. These often include personal details that can be gleaned online, such as through social networking sites.

Vulnerabilities are holes in software code that can allow cybercriminals to gain unauthorized access to a system. These can exist in all software, including operating systems and applications (e.g., Java and Adobe Flash). While the holes can be closed by applying patches or updates, many times a patch or update isn't available at the time a vulnerability is discovered. These are known as zero-day vulnerabilities.

Appoint a cybersecurity champion.

Whatever title you give them, it's vital to have an individual who is responsible and accountable for ensuring the security of the church's systems and data. This will likely be someone outside your IT department who has the authority to ensure the appropriate resources are devoted to information systems security.

Implement — and maintain — network and work station controls.

You can't manage what you can't measure, so start by creating a complete inventory of all your systems. This should include servers, computers (desktop and laptop), mobile devices, switches, routers, firewalls, and peripherals.

Then, use an IT specialist to help your church:

- Ensure you have a properly configured firewall to monitor incoming and outgoing network traffic
- Block spam to reduce phishing emails reaching end users
- Keep anti-virus and anti-malware software running around the clock on *every* system
- Continually patch and update all systems

While it can be time-consuming to update your systems, it's a critical step. It's also important to periodically review who has access to data and systems, and limit it to those individuals who need access to carry out their responsibilities.

Use strong passwords.

One employee with a weak password can put your whole network at risk. Require complex passwords with a combination of letters and numbers, which are more difficult to hack, and set them to expire periodically.

Create a culture of security that includes ongoing training.

It's vital for all employees and volunteers with access to your network to understand the importance of cybersecurity. You may be surprised how many people do not understand that clicking on just one fraudulent email can result in a major cyber breach.

This culture of security should include frequent training and communication on:

- The latest cybersecurity threats
- The importance of using, and regularly changing, complex passwords
- Why you shouldn't use the same password for multiple sites
- How to detect phishing emails
- The dangers of visiting unsafe websites
- The risks of using public Wi-Fi networks

Present this information in a simple, direct way that is easy for those with a range of technical knowledge to understand.

Test to identify ongoing risks.

While the steps above can help your church minimize risks and vulnerabilities, it's also important to identify any existing issues through periodic independent testing.

This should involve:

- Information security controls testing, which helps determine whether the appropriate information security controls are in place and functioning as designed. This testing should be performed annually.
- Vulnerability scanning, which uses specialized software to scan your internal network and external Internet-facing systems to identify any potential weaknesses. This should be done regularly, such as quarterly.

Because this is such a key issue, it's important for someone outside the IT department to follow up and ensure that all identified issues are addressed.

Remember that cybersecurity is an evolving process.

Cyber threats change constantly, and an astounding number of new vulnerabilities are discovered every day. After you have the appropriate controls and processes in place, it's crucial to ensure they are maintained consistently, and that new risks are being identified an addressed.

Cybersecurity is like cake — the more layers, the better. The best practices above will help you implement multiple controls in a layered fashion so that if one control fails, others exist to protect your church.

This article first appeared in the Summer 2017 issue of INSIGHT, a journal of The Church Network®.

About the Author

Lisa Traina, Partner
CapinTech
ltraina@capincrouse.com
o 505.50.CAPIN ext. 2000

Lisa uses her more than 30 years of experience to assist organizations in implementing measures to secure data and manage risks efficiently and effectively. She is a nationally recognized speaker and author, and serves on the AICPA Cybersecurity Task Force. Lisa founded Traina & Associates in 1999 to provide IS security services to a broad range of industries. Traina & Associates joined CapinCrouse in January 2017.

About CapinTech

CapinTech, a CapinCrouse company, provides information security services, including cybersecurity assessments, consulting, and training services, to nonprofit organizations, financial institutions, medical entities, professional services firms, and other organizations. Each year the firm performs hundreds of assessments, consulting, and speaking engagements with a team of experienced professionals retaining numerous certifications, including CPA, CISSP, CISM, CISA, CITP, CGMA, and CTGA. Each engagement is tailored to fit the unique needs of the organization, and information and reports are presented in a clear, concise manner intended for an audience with varying information systems (IS) knowledge. More information is available at capintech.com.

About CapinCrouse

As a national full-service CPA and consulting firm devoted to serving nonprofit organizations, CapinCrouse provides professional solutions to organizations whose outcomes are measured in lives changed. Since 1972, the firm has served domestic and international outreach organizations, universities and seminaries, foundations, media ministries, rescue missions, relief and development organizations, churches and denominations, and many others by providing support in the key areas of financial integrity and security. With a network of offices across the nation, CapinCrouse has the resources of a large firm and the personal touch of a local firm. Learn more at capincrouse.com.

CapinCrouse is an independent member of the BDO Alliance USA.