CHURCH PENSION GROUP
Passionate About Our Purpose

Paperless Workplace: Make a Safe Transition

Moving from paper-based to electronic systems in the workplace can make operations more efficient—but it can also induce anxieties about cybercrime. Concerns about exposure to hackers and privacy breaches are real, but there are ways to help protect your organization's data and finances while taking advantage of new technology.

What Could Happen

Some leaders of religious organizations are hesitant to make the transition to using electronic methods, especially for financial transactions, such as collecting donations and paying bills. According to Steve Follos, Vice President and General Manager, Church Insurance, they have a reason to be cautious. Cybercrime losses have increased in recent years as hackers get better at finding ways to fool users and bypass safety measures.

Losses that Church Insurance's Cyber Liability coverage has addressed come from attacks such as phishing schemes, ransomware, stolen computers, and even malicious acts perpetrated by disgruntled former employees.

Phishing is a technique used by hackers to steal information or funds by inducing users to provide passwords or other intelligence. Steve recalls one particular incident as being "quite sophisticated." A direct report received what appeared to be an email from a supervisor authorizing a large payment to a vendor. "The emailed wire transfer request said the supervisor was busy and didn't want to be interrupted or asked about the transaction, and to get it done by the end of the day," Steve recalled. The direct report fell for the scam, sending the funds to the hacker, and the organization made a cybercrime claim.

Ransomware schemes involve malicious actors tricking users into downloading programs that lock files on their computers. Users then receive a message or pop-up stating that the files will be unlocked only if the user sends money to the hacker. Steve says ransomware problems can sometimes be resolved by restoring from backups, provided that data has not also been compromised.

Viruses, payroll or gift card fraud, and other issues could also arise from moving to paperless systems, but it isn't necessary to avoid their use as long as you set up your technology environment properly.

Ways to Prevent Problems

Hazards associated with using technology instead of old paper systems may be mitigated by instituting training, working with professionals to set up secure systems, creating procedures where you might be vulnerable, and double-checking suspicious requests.

Training. Make sure any employees, interns, or volunteers who will be working with your organization's finances are aware of commonplace schemes, can recognize dubious requests, and know to double-check them. You may consider bringing in a local IT expert to educate workers.

Professional help. An IT expert can also help you create a secure technology environment. For example, Steve says, “The correct firewall could help prevent viruses.” Communicate your organization’s operations to the expert and follow his or her advice to set up adequate and ongoing protection.

Proactive procedures. Steve also recommends that organizations create procedures for off-boarding employees. “We had a claim where a former employee was suspected of gaining access to the organization’s system and deleting files,” he says. That can be prevented by cutting off access and changing passwords as part of the off-boarding process when an employee leaves the organization.

Double-checking. Requests that direct an employee to by-pass authorization procedures should be viewed with suspicion, Steve says. Financial transfers should always be done subject to policy and procedures that have been designed to mitigate fraud. He also advises that before clicking on a link in an email from an outside sender, hover over the link to see if the pop-up window shows a trusted destination website address.

What to Do If Something Happens

Cyber Liability insurance covers many issues that can occur when religious organizations use technology. Insureds have a $250,000 limit per occurrence, including several Third Party Liability and First Party Response Coverage Agreements. When you make a claim, Church Insurance assigns a breach attorney and performs an investigation and forensic accounting through its co-insurer, Navigant.

Steve suggests that religious organizations contact Church Insurance right away if something happens because “the experts will often be able to offer helpful advice.”

“Sometimes a privacy breach will mean that the organization has to notify those affected, and sometimes not,” he says. It depends on the applicable law and your particular circumstances and you will need to consult with an experienced advisor in this area.

Technology is meant to help individuals and organizations do things more easily. But if something does happen, contact Church Insurance for guidance.