CHURCH PENSION GROUP

Protection Against Cyber Crime Now Included

When you think of computer hacking or data breaches, what comes to mind? Sony? Equifax? Only big companies? True, big companies are often the target of hackers. But, according to the 2016 NetDiligence Cyber Claims Study, 49% of the organizations that submitted claims had revenues of less than $50 million.

For example, in 2011, St. Ambrose Cathedral in Des Moines, Iowa, was the victim of a cyberattack. The hackers stole more than $680 thousand that had been collected to help homeless and abused women.

Because these types of problems have become more common, we have architected a new program. As of September 1, 2017, Church Insurance Company of Vermont (CIC-VT) and Church Insurance Company of New York (CIC-NY) have enrolled all participants in a separate master policy that covers Cyber Liability. Churches have a $250 thousand limit, including several Third Party Liability and First Party Response Coverage Agreements. The cost is built into insureds' current premiums.

What Cyber Liability Prevents and Protects

Anthony Manna, RPLU+, Account Executive for NIF Group, Inc. and the broker for CIC-VT's and CIC-NY's Cyber Liability coverage, says the coverage is valuable because, "It protects the insured for data and privacy breaches of their system." These breaches can lead to internal losses or liability claims from members whose information has been stolen and misused or released. "It also has a media component that can help protect the insured's presence online," he says.

Data breaches

Churches may keep member lists with addresses or employee lists with Social Security numbers. They may have personal data, including healthcare and financial information, on file for members. If someone obtains that information, it could potentially be misused, but, as Anthony says, "It could also be a breach of privacy."

When a church is the target of a cyberattack and subsequent data breach, it must take certain steps to comply with privacy laws. "Anyone whose data is breached may have legal obligations to notify all the people who are affected and possibly create a call center and offer credit monitoring services," Anthony says.

Cyber Liability coverage can help you respond to a breach, once you make a claim. "The carrier uses the top cyber-response teams available in the country," Anthony says. "They help you prevent further damage." And, if a member who is adversely affected by a data breach brings suit against a church, Cyber Liability coverage can help with that, too.

Ransomware and fraudulent transfers

Cybercrime is not just about hackers breaching an organization's system to find and release or use lists of information. Some hackers will trick users into clicking on a link or opening an attachment that downloads malicious software onto their computers. The software locks users out and holds their files hostage until they pay the hacker. This is called ransomware. This situation happened at First Presbyterian Church in Birmingham, Michigan, in 2014.

Users might also receive an official-looking email that asks them to provide something, such as a bank account number, only to learn that the email was a fake, and they gave away important information to a hacker. Or, they might receive a desperate message from a church member who needs money wired to them immediately. After sending the money, they discover that the church member's email had been hacked, and the money was wired to a criminal instead.

Cyber Liability covers both ransomware extortion as well as fraudulent transfers.

Media liability

Cyber Liability coverage also handles media liability, which includes **copyright infringement**, trademark infringement, and libel.

"Churches are tempting targets for hackers because they often lack sophisticated security," Anthony says. As churches use the internet to reach more people, they are at greater risk. The new Cyber Liability coverage helps protect churches from the risks associated with embracing technology.