CHURCH INSURANCE COMPANIES
Insurance for the Greater Good

Policy Factsheet

Cybersecurity Insurance

Overview

Cybersecurity insurance is becoming more important in the face of increasingly stealthy, sophisticated, and targeted attacks. A cyberattack is often a robbery, and the target is data.

The data can be anything that's meant to remain confidential—Social Security and driver's license numbers, health records, or other personal details of parish employees; the credit or debit card numbers of church preschool parents or parishioners who sign up for automatic donations; even information about vendors and service providers.

The risks are myriad—a former employee steals files; a pastor leaves their laptop (with no password protection) in a coffee shop; an employee accidentally shares a confidential file or inadvertently opens an email that downloads malware.

Churches can be among the organizations that criminals perceive as having less sophisticated cybersecurity systems—their software might not be up to date; they may use the same password across multiple accounts; they may lack robust firewalls; they may fail to regularly back up important files; or they have inadequate antispyware and antivirus software, leaving them vulnerable to phishing, worms, or Trojan horses.

What's Covered

Our coverage provides protection for data breaches that cause sensitive data to be divulged and, in the case of a ransomware attack, experts to negotiate with hackers.

And because many organizations that have been hacked can be criticized for the time it takes to notify those whose data has been compromised, we also provide response planning to help those impacted mitigate the effects of an attack.

FAQs

Q: What is the current coverage offering?

A: The policy carries a standard liability and nonliability coverage limit of $250,000 for each of the 10 common consequences of a cyberattack, including cyber extortion, the cost to protect a network, and defense for breach of privacy. In addition, we offer Cyber Crime coverage of $25,000.

Q: Are there additional coverage offerings?

A: You can increase your standard liability and nonliability coverage limits by $750,000 and increase the Cyber Crime coverage by $75,000 for $700/year.

Q: Is there a deductible?

A: The deductible is typically $5,000 per claim.

Q: Are those hurt by the hack covered as well as the policyholder?

A: The policy provides both first-party and third-party coverage for victims of cyberattacks.

First-party coverage insures for losses to the policyholder's own data or lost income or for other harm to the policyholder's business resulting from a data breach or cyberattack.

Third-party coverage insures for the liability of the policyholder to third parties—including clients and governmental entities—arising from a data breach or cyberattack.

Cyber Risk Management Tips

Work with IT professionals and cybersecurity experts to put in place the following:

- Require multi-factor authentication.
- Create unique questions that can't be answered using publicly available information and require long (16+) passphrases.
- Use antivirus protection.
- Back up data securely and often.
- Do not use personal devices or personal email accounts for work.
- Keep software patched and upto date.
- Avoid free/public Wi-Fi.
- Carefully analyze all emails by closely reviewing each sender's email address and checking for other signs of phishing.
- Never open any attachments or click on any links in suspicious emails.
- Carefully analyze any wire transfer request or unusual request.
- Confirm any nonstandard request via telephone from a known number, not the one provided in the email request.
- If infected by malware, **immediately** disconnect your computer from all networks and notify your IT resource.
- Lock or shut down your computer when the workspace is unoccupied.
- Never post passwords on or under a computer or in any accessible location.
- Never leave electronic devices unattended in public areas.