CAPINTECH

# Cyber Insurance for Nonprofits: What it Looks Like, How it's Priced, and What to Expect

By James Dick, Advisor – Nonprofit & Religious Practices, Gallagher

*This article was provided by a subject matter expert who is not affiliated with CapinCrouse and is intended to provide important, timely, and useful information. Although it may include recommendations by the author, any actions or conclusions by the reader are solely those of the reader.*

---

Cyber incidents can occur in any organization, and the effects can be significant, costly, and long lasting. While cyber insurance won't prevent a cyber incident, it can help organizations manage the impact if one occurs.

There have been many changes in cyber insurance over the past few years. Let's take a look at what cyber insurance entails, how it is priced, and what to expect as you explore options for your organization.

**Cyber Insurance Overview**

Policies vary widely, but a comprehensive cyber insurance policy can cover areas such as:

- Crisis management costs (attorneys, IT forensic investigators, credit monitoring firms, mailing and call centers, public relations experts, etc.)
- Extortion costs, with immediate access to Bitcoin and trained negotiators
- Lost income due to interruption of your operations
- Data asset restoration
- Third-party liability coverage for lawsuits from regulators, business partners, and affected individuals

A cyber insurance policy can transfer some of the risk and cost of a cyberattack to the insurer.

**How Cyber Insurance is Priced**

Cyber insurance has undergone significant changes over the past few years. When it was first introduced to the insurance marketplace, many in the industry described it as "priced by spreadsheet." The rating system would ask a few questions about the size of the organization (revenue, employees, industry, and website), make sure it was an information-only site (i.e., not eBay), and generate a premium. Very little consideration was given to the IT security of the organization applying for coverage.

Although that may seem implausible, there was no other way to start. Fair insurance premiums are based on years of credible loss data — and that data did not exist when cyber insurance was first brought to market.

Now that data breaches, malware attacks, and other cyber-related damages have become commonplace, however, there is credible loss data. Unfortunately for nonprofit organizations' budgets, this data showed that insurers were not charging enough in premiums to cover the losses they were paying out. Attacks were increasing in frequency and severity, and cybersecurity protocols were inconsistent.

These issues came to a head in 2022 when almost all cyber insurance companies drastically increased their pricing (sometimes by 30% to 40% or more) and started implementing cybersecurity requirements that must be met prior to insurance being offered. For example, most organizations had to implement multi-factor authentication (MFA) or risk losing their coverage.

The top cyber insurance underwriting requirements in 2022 included:

- MFA implemented for employee email, privileged access, and remote access
- A written patch management plan to remediate vulnerabilities as they become known
- Endpoint detection and response controls
- Encrypted, air-gapped data backups that can be recovered within 30 days (seven days for critical data), with recovery tested annually
- Employee cybersecurity training, including training on phishing and other current threats
- Privileged access management, with advanced levels of protection for users with higher levels of access

- Incident response planning, with a written plan identifying roles and responsibilities for post-incident procedures

So far in 2023, last year's cost increase and security demands seem to have stemmed the tide of larger and more frequent claims. Underwriters are starting to feel more comfortable looking at a nonprofit's IT network and security protocols and feeling some level of confidence that they will provide the needed protection. In turn, many nonprofits have increased their investment in IT security. More importantly, more and more nonprofit leaders appreciate that IT security can be a worthwhile investment in protecting their organization's mission and services.

In the immediate future, premiums are relatively flat for nonprofits that already have cyber insurance in place and have not experienced any claims or cyber-related losses. Some nonprofits may even see a premium decrease, often by finding that a better value is available from a specialty insurer rather than their primary liability insurer. Many nonprofits that do not have coverage, especially those with annual budgets under $10 million, can find affordable coverage for $5,000 or less annually. There is even a growth of "insurance-plus" service offerings that combine an insurance policy with an IT security software solution. If implemented correctly, this can be a great value for a nonprofit without the budget to regularly work with a qualified IT security provider or consultant.

**What to Expect When Applying for Coverage**

When looking for a cyber insurance provider, it's important to ensure that you understand the policy and what it covers. Research:

- The types of incidents that are covered. There are many different types of cyber incidents, including ransomware and other malware, distributed denial-of-service (DDoS) attacks, and the deletion or corruption of data, to name just a few. Policies may stipulate what specific types of incidents are covered.
- The type of coverage included. Consider obtaining coverage for legal fees and penalties, forensics or incident investigation services, notification of affected parties, incident response, and loss of income due to operational disruption.
- How to file a claim. Make sure you know the minimum requirements that must be met to make a claim and the required documentation. Some policies may require certain data and evidence for a claim.

It's also vital to make sure you understand what information security controls the insurer requires and address them before seeking coverage. Many cyber insurers will require you to complete an extensive questionnaire about your controls and policies, and many have stipulations for baseline controls that need to be met.

Finally, keep in mind that cyber insurance can be a crucial component of your organization's information security strategy, but it should be part of a layered control framework.

**Additional Resources:**

CapinTech Cyber Series: The Evolution of Cyber Insurance for Nonprofit Organizations Recorded Webcast

Top Cybersecurity Myths: We Can Just Get Cyber Insurance

## About the Author

**James Dick, Advisor – Nonprofit & Religious Practices**
Gallagher

James Dick serves Gallagher's Religious & Nonprofit Practices in the U.S. and works closely with a variety of nonprofit organizations around the country on implementing their chosen risk management and insurance programs. Additionally, he co-manages Gallagher's insurance program for the Citygate Network, an association of faith-based life transformation ministries that serve the homeless and addicted. He holds a Chartered Property and Casualty Underwriter (CPCU) and is an Accredited Advisor in Insurance (AAI).

## About CapinTech

CapinTech, a CapinCrouse company, provides information security services, including cybersecurity assessments, consulting, and training services, to financial institutions, nonprofit organizations, medical entities, professional services firms, and other organizations. Each year the firm performs hundreds of assessment, 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. For over 50 years, 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.