Coalition

THE CYBER SAVVY BROKER'S GUIDE

Cyber Insurance for the Nonprofit Industry

Nonprofit organizations play a valuable role in advocating for their clients, improving communities, and positively impacting the lives of many. They also face unique cyber risks due to their handling of sensitive individual data and reliance on donations. The type and volume of sensitive financial and personal data typically handled by nonprofits make them an attractive target for attackers seeking to exploit the valuable data for monetary gain.

Nonprofits often have limited resources and tight budgets, which can hinder their ability to invest in comprehensive cybersecurity solutions and staff training. As a result, they may not have the necessary expertise or systems to detect and respond to cyber threats effectively.

A cyber attack targeting a donation system or website can severely impact a nonprofit's ability to raise funds and even expose donors to becoming victims of scams or fraud. Cyber incidents involving technology, like client intake or case management systems, could expose sensitive data and lead to costly data breaches, not only damaging the reputation and credibility of the organization but also resulting in significant financial losses.

Claims Insights

It's just a little security incident. How bad could it be?

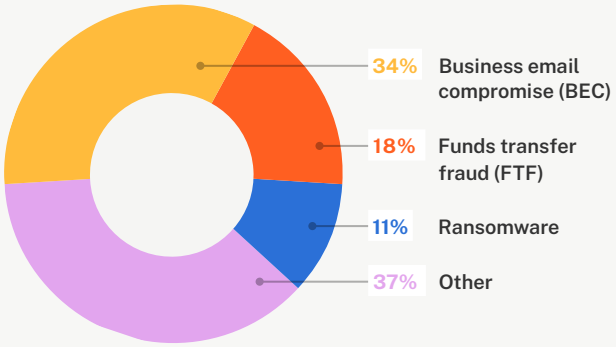
$110,000

Average cost of a cyber insurance claim for nonprofit organizations

Claim Examples

ORGANIZATION	INCIDENT	LOSS
Veterans Charity	Funds Transfer Fraud	$125,000
Social Services	Business Email Compromise	$155,000
Rehabilitation Center	Ransomware	$962,000

Cyber Claims by Event Type



Source: Coalition claims data

KEY INSIGHT —— Although it's not the leading event type, the average ransomware loss for nonprofit organizations is more than $365,000.

Coalition, Inc. · 55 2nd Street, Suite 2500, San Francisco, CA 94105 · coalitioninc.com

Coalition

Unique Exposures

Most nonprofit organizations use data and technology. Why is that risky?

Essential Technologies Can Create Cyber Risk

Online fundraising platforms

These platforms enable nonprofits to collect donations online, which is vital to the health of an organization. However, if a platform is compromised, cyber attackers can gain unauthorized access to donor information and potentially steal funds.

Donor management systems (DMS)

These systems store valuable donor information, including personal data, financial data, donation amounts, and transaction histories. Cyber attackers can target DMS to conduct identity theft or carry out spear-phishing attacks on donors and staff.

Cloud computing

Cloud computing allows organizations to store and process large amounts of data while reducing overhead. However, risks include unauthorized access to sensitive data, data breaches due to misconfigurations, and lack of control over security measures implemented by cloud service providers.

Email

Business email compromise (BEC) is the leading cause of cyber insurance claims among nonprofit organizations, triggering data breaches, business interruption and even reputational damage.

Websites

Nonprofit websites provide information about the organization's mission, its projects, and collect user data. But if they lack proper security, websites can become vulnerable to hacks and expose sensitive user information.

End-of-life software & hardware

Organizations may use outdated technologies with the belief that upgrading would be expensive, time-consuming, and disruptive. However, technologies no longer supported by the manufacturer often have known security vulnerabilities and may lack important security features to protect against modern threats.

Social media

Nonprofits utilize social media platforms for outreach, fundraising, and creating awareness. However, cybercriminals can exploit this increased online presence of nonprofits through social engineering techniques to steal sensitive information or launch phishing attacks.

Client intake and case management software

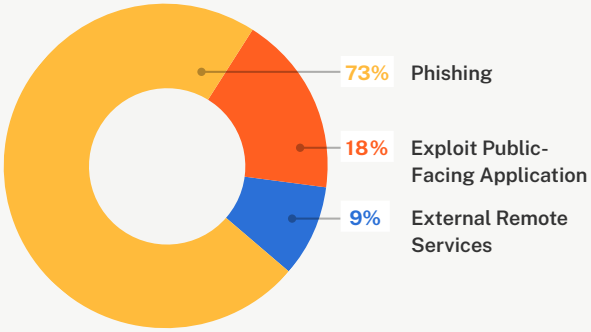
Many nonprofits provide services directly to their clients and use tools to determine eligibility, needs and track services delivered and progress over time. These types of systems are not only essential to the operations of the organization but often contain sensitive personally identifiable information about clients receiving services.

Mobile applications

Some nonprofits deploy mobile apps to reach wider audiences, facilitate donations, and raise awareness. If the applications are not secure, they can provide an entry point for hackers to access user information or perform unauthorized transactions.

Cyber Claims in the Nonprofit Industry by Attack Vector

KEY INSIGHT —— Phishing isn't associated with one event type; it's simply how attackers get into a system. Once inside, they can pursue all sorts of malicious activities, which is why **phishing is the leading attack vector for all cyber claims.**



Source: Coalition forensics survey data

Coalition

Sensitive Data Can Increase Business Liability

Sensitive personal information

Nonprofits may collect or process sensitive information about program beneficiaries, clients, patients, or students. This data could include protected health information (PHI), personally identifiable information (PII), or other data that could be used to identify an individual. A breach of this data could expose a nonprofit to legal or regulatory action, including fines and penalties. Unauthorized access to this data could also lead to identity theft, fraud, or other attacks targeting individuals the organization is dedicated to serve.

Donor information

Nonprofits typically maintain records about their donors, including names, addresses, contact information, and donation history. This data can be targeted and used for identity theft or sold on the dark web.

Financial data

Nonprofits may handle financial information, such as bank account details, credit card information, and transaction records. Cybercriminals can exploit vulnerabilities to gain unauthorized access to these records and conduct fraudulent activities.

Sensitive employee records

Most organizations collect and store information about their employees, such as social security numbers, addresses, and tax records. Unauthorized access or disclosure of this data can cause direct harm to employees.

Volunteer information

Nonprofits often collect personal information about volunteers, including names, addresses, and background checks. Cyber attackers may use this information for identity theft or to glean additional details about people affiliated with the organization.

Board member information

Cyber attackers may target data pertaining to board members or other nonprofit leaders to gain unauthorized access to personal details, including contact information, professional backgrounds, or financial holdings. This information can be used for spear-phishing attacks or extortion attempts.

Grant applications

Cybercriminals may target grant applications to gain access to sensitive information about a nonprofit's plans, finances, or projects. This data can be used for corporate espionage or sold to competitors.

Non-sensitive personal information

Some data may be publicly available and not considered protected, but a breach can still impact trust and public image if it appears the organization did not handle the situation appropriately.

Examples of Legal & Regulatory Compliance

- Data privacy & security contractual obligations
- International data privacy and consumer protection regulations (e.g. GDPR)
- Health Insurance Portability and Accountability Act (HIPAA)
- State data privacy & consumer protection laws (e.g. CCPA)
- State notification requirements
- Payment Card Industry Data Security Standard (PCI DSS)

$2.6 million

Average total cost of a **data breach** for nonprofit organizations[1]

1. IBM Security, Cost of a Data Breach Report 2023

Coalition

Business Impacts

What can nonprofit organizations expect after a cyber incident?

Direct costs to respond

Responding to a cyber event typically requires numerous direct costs, also known as first-party expenses. If a nonprofit organization experiences a data breach involving PII, it will require a prompt response and the need for additional legal counsel, forensic investigation, victim remediation, and notification to comply with regulatory requirements. Simple investigations can cost tens of thousands of dollars, while more complex matters can increase costs exponentially. Relevant insuring agreements may include:

- Bodily Injury and Property Damage - 1st Party
- Breach Response
- Crisis Management
- Cyber Extortion

Liability to others

Navigating the patchwork of laws and regulations after a security incident or data breach is especially difficult for organizations that operate in a highly regulated industry. A data breach or security failure can trigger liability to third parties and cause bodily harm or injury, even if the management of financial records is outsourced and the organization is otherwise in compliance with applicable regulations. Relevant insuring agreements may include:

- Network and Information Security Liability
- Regulatory Defense and Penalties
- PCI Fines and Assessments
- Pollution
- Multimedia Content Liability
- Bodily Injury and Property Damage - 3rd Party

Business interruption and reputation damage

A cyber event that impacts essential technology can have a significant impact on a nonprofit's ability to operate and can be highly visible to donors, beneficiaries, and other stakeholders. Even short periods of disruption can lead to direct loss of revenue and inhibit an organization's ability to champion a cause, negatively impacting not only donor retention but also the delivery of essential services. Relevant insuring agreements may include:

- Business Interruption & Extra Expenses
- Reputation Repair

Cybercrime

Beyond ransomware and data breaches, cyber events can result in financial theft for a nonprofit or its supporters — often without an actual breach. If an attacker dupes someone in the billing department to alter payment instructions, an organization can lose tens or hundreds of thousands of dollars almost instantly. Attackers can also gain access to email accounts and send fraudulent invoices or payment instructions to donors, beneficiaries, and other third parties. Relevant insuring agreements may include:

- Funds Transfer Fraud
- Invoice Manipulation
- Phishing (Impersonation) and Proof of Loss Preparation Expense Endorsement
- Service Fraud

Recovery and restoration

After a cyber event, resuming operation is no easy task. If an attacker damages or destroys essential technology, data, or physical equipment, an organization may need to bring in external support or purchase new equipment to re-secure systems. Full remediation, restoration, and recovery can take a significant amount of time, when possible, and may require purchasing new software, systems, and consultants to rebuild the network. Relevant insuring agreements may include:

- Computer Replacement
- Digital Asset Restoration

Coalition

Cyber Insurance Reimagined

How does Coalition perform?

1.87%
Coalition 2022 overall claims frequency

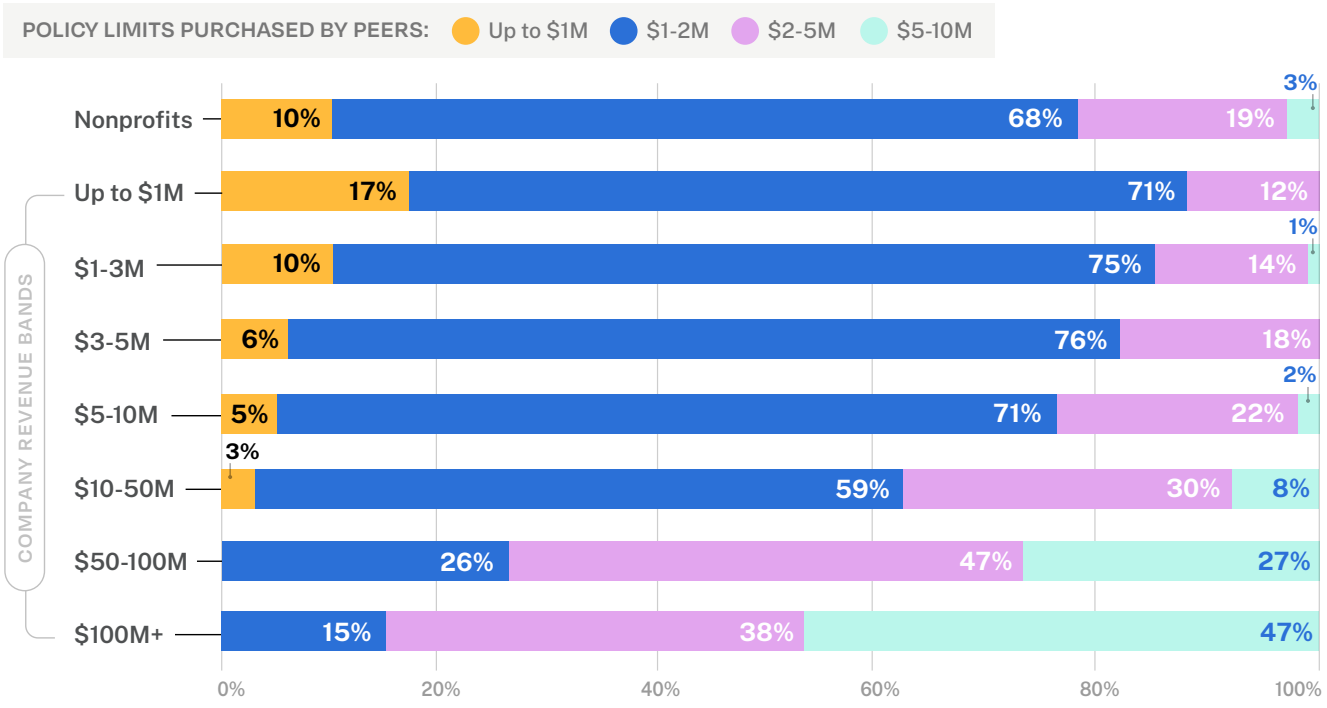
↓ 22%
Year-over-year decrease in claims frequency

64% fewer
Coalition claims vs. cyber industry average

Peer Purchasing Insights

Primary limit amounts purchased by others in the nonprofit industry

PEER PURCHASING HABITS BY REVENUE



Source: Coalition policyholder data

KEY INSIGHT —— Most small and medium-sized businesses in the nonprofit industry purchase $1M-2M in limits, while many mid-market organizations purchase $5-10M in limits. For those needing more than $10M in limits, Coalition offers primary and excess terms for businesses up to $5B in revenue.

Coalition

The Power of Active Insurance

Why do nonprofit organizations choose Coalition?

47%

Reported cyber events handled with no cost to policyholder

43%

Reduction in critical vulnerabilities among policyholders in 2022

5 minutes

Average response time to a cyber incident

Active Insurance* is designed to help mitigate digital risk before it strikes. Our new approach to managing digital risk provides **three layers of support**:

Active Protection

Monitoring and alerting to identify and prevent risk before it strikes

Active Response

Access to in-house resources that accelerate response and coverage if an incident occurs

Active Risk Assessment

Underwriting, quoting, renewals, and digital risk scores powered by real-time data

Insurance as active as digital risk

In the digital economy, Coalition wants to ensure that all organizations can thrive by helping to protect them from the threat of emerging risks. We've built an expert team across incident response, claims, and our panel vendors. In the event of a claim, Coalition helps organizations respond and recover so they can get back to business.

Brokers

Get appointed today at signup.coalitioninc.com

Nonprofit organizations

Get a free risk assessment at control.coalitioninc.com

Coalition, Inc. · **55 2nd Street, Suite 2500, San Francisco, CA 94105** · **coalitioninc.com**