CharityFirst

Why You're Not Selling More Cyber to Nonprofits

AND WHAT TO DO ABOUT IT

WHITE PAPER

CHARITY FIRST INSURANCE SERVICES, INC.
1255 Battery Street, Suite 450, San Francisco, CA 94111 Tel: 800.352.2761 Fax: 415.536.4033 **charityfirst.com**

Why You're Not Selling More Cyber to Nonprofits—and What to Do About It

If you're looking for proof that cyber insurance is essential for nonprofits as well as for-profit companies, there's no shortage of recent case studies in the news.

In 2017, a global ransomware attack struck computer systems all over the world; among the victims were more than one-third of the healthcare trusts in Britain.[1] In 2016, WikiLeaks published almost 20,000 emails leaked from the Democratic National Committee—a high-profile breach most likely committed by Russian intelligence hackers.[2] This may have been one of the most influential cyber-hacks in history.

Most nonprofits are not aware of the risks. Yet many still believe it can't happen to them. In addition, agents hear a range of objections and misconceptions about cyber insurance in the nonprofit market. These keep agents from selling as much cyber insurance as they could—and keep nonprofit organizations dangerously exposed to risk.

Why Nonprofits Are Especially at Risk

All organizations are at risk of a cyber attack. But there are a few factors and behaviors that make nonprofits especially vulnerable. These include:

Skimping on software and hardware

It's not uncommon for nonprofits to satisfy their technology needs on the cheap. Many use donated computers and hardware, as well as older, unsupported versions of software and operating systems. The older a system is, the more vulnerable it is to data breaches.

In addition, it's not unusual for nonprofits to save money by using open-source software—which is often more vulnerable to cyber attacks than the proprietary version.

Collecting payment and contact information

Many companies and organizations collect contact information and take payments online—but nonprofits live and die by their member mailing lists, while collecting donations and membership dues online. This presents an obvious vulnerability for hackers to exploit.

Having lax cyber security policies

Many smaller nonprofits can't afford elaborate security measures or to keep a dedicated IT professional on staff. This makes them an easy target for hackers. Lack of basic security measures such as two-factor authentication and password complexity requirements can make them even more vulnerable.

Employees and volunteers

One of the biggest threats to cyber security in most organizations—including nonprofits—is the people who work for them. A disgruntled employee or volunteer can easily steal a laptop and wreak havoc with the data. And anyone can misplace an important thumb drive or laptop, or have it stolen.

Myths That Keep Nonprofits from Buying Cyber Insurance

Retail agents hear a number of excuses when suggesting cyber insurance to nonprofits—despite the clear need. And agents have their own misconceptions, which can keep them from entering this sector. Here are some of the most common:

“Hit rates are too low for cyber insurance.”

This objection is usually held by retail agents, not the nonprofits themselves. It’s not untrue, but it’s based on outdated information. As recently as two years ago, low hit ratios were endemic—for very specific reasons. But cyber insurance changes as rapidly as the tech industry as a whole, and it’s no longer the case today.

Cyber insurance is still new. In the recent past, carriers were more uncertain of the risks than they are now—and their applications were long and onerous, requesting information that nonprofit employees didn’t have. Most retail agents faced a huge challenge to produce applications that were acceptable to carriers.

This isn’t the case today. Some programs have applications with as few as four questions—easy for retail agents to ask and nonprofit employees to answer. Once the agent submits the risk, the hit ratios are high.

“Interestingly, we’ve found that the charity and nonprofit class of business has a 51% hit ratio, which is one of the higher classes of business,” says Ryan Collier, chief digital officer at Risk Placement Services, Inc. “Clearly they are understanding the need, see the prices are very competitive, and realize that all entities will be hit eventually.”

“So much was unknown in this area of business up until recently,” adds Riley Binford, executive vice president of Charity First Insurance Services. “The insurance carriers continue to figure out their true liability. But there are programs in this space that have very streamlined application processes, and the hit rate is high for retail agents to present to their customers.”

“We don’t do transactions over our website, so we don’t need cyber insurance.”

Just because a nonprofit doesn’t take donations or membership dues online doesn’t mean they aren’t exposed to cyber-related losses. As a cost-saving measure, many nonprofits have employees or volunteers design their websites for free by people with lots of dedication but not always a high level of professional knowledge.

Under these conditions, a well-meaning developer could include images, music, and other material on the nonprofit website without the proper permission, which could result in copyright infringement charges for unauthorized use. In addition, online bulletin boards and testimonials can attract defamation claims and result in damages.

General liability policies specifically exclude copyright, patent, and trademark infringement, as well as personal injury arising from bulletin boards and chat rooms. The only way to get this coverage is through cyber liability insurance.

"We don't keep or store sensitive information."

This isn't an unusual claim, but often, nonprofits that make it don't realize exactly how far-reaching the definition of "personally identifiable information"—or PII, as referred to in privacy law—really is.

In fact, PII includes any information that can be used to identify, contact, or locate an individual, including: cell phone numbers, email addresses, social security numbers, driver's license information, and health information.

Mailing lists of donors, volunteers, and members are essential to any nonprofit's fundraising and operations. It's difficult to imagine any organization that doesn't maintain some way to identify and contact the people it depends on.

"We don't store our data on a computer; we have paper files only."

Data doesn't have to be digital to be stolen. Paper files can also be the target of a data breach, and this can wreak as much havoc on an organization as a digital hack. A number of cyber policies will cover this type of occurrence.

"We only use our computers for email."

Email is one of the most vulnerable points of any organization, due to an attack known as "phishing."

The term refers to emails sent by hackers to get the reader to give up sensitive information. These attacks can be surprisingly sophisticated, with emails and websites that cleverly mimic trusted organizations such as the recipient's bank or a social media site they use.

According to a 2016 study by PhishMe, a whopping 91% of cyber attacks start with a phishing email. One reason why these are so pernicious is that these emails bypass even the strongest cyber security defenses—and thrive on human curiosity and error. According to the survey, almost one-third of employees will respond to phishing emails even after receiving training in cyber security awareness.[3]

"We don't have a website or social media presence; therefore we aren't vulnerable."

Hackers don't have to rely on websites or social media presences to gain access to a nonprofit organization's systemn. All an employee has to do is click on the wrong popup, get taken in by a phishing email, or unknowingly download an infected file to bring a cyber threat into a nonprofit organization.

"We're a small nonprofit; hackers wouldn't be interested in us."

There are plenty of examples of small organizations that thought the same thing—and were proven wrong.

For instance, the Red Barn, a small nonprofit that uses horses to help those with physical and cognitive disabilities, had its website hacked in 2015 by a group of terrorist sympathizers. The event made national news, damaged the nonprofit's reputation, and left them without a website in the middle of a fundraising effort.[4]

Far from being less vulnerable to attack, small organizations are low-hanging fruit for hackers. While larger organizations have more to lose, they also have stronger security measures. Smaller nonprofits frequently can't afford these measures, leaving the door wide open to cyber attacks. The truth is that smaller nonprofits need cyber insurance just as much as larger organizations do—if not more.

Why It Pays to Work With a Specialized Broker

Wholesale brokerages with specialized expertise in cyber liability can be of immense help to insurance agents looking to place nonprofit risk.

It isn't unusual for nonprofits to go without this coverage if the insurance agent they work with doesn't have experience in this area. This leaves the nonprofit dangerously exposed.

A wholesale broker with knowledge in this area can be immensely helpful in assessing the risk, guiding the conversation, responding to objections—and ensuring the nonprofit gets the full coverage they need.

About Charity First

Charity First is a wholesale brokerage, underwriter, and program manager specializing in nonprofit organizations, social service agencies, and religious institutions.

For additional information about Charity First, please contact Frank Tarantino at frank_tarantino@charityfirst.com or (800) 352-2761.

Notes

[1] "Ransomware Hits NHS Trusts." *Out-Law.com*, February 6, 2017.

[2] Nakashima, Ellen. "Cyber Researchers Confirm Russian Government Hack of Democratic National Committee." *Washington Post*, June 20, 2016.

[3] "Phishing Emails Used in 91% of Cyber Attacks." *HIPAA Journal*, December 14, 2016.

[4] Segedin, Andy. "Hacked! Crooks are Grabbing Nonprofit Websites and Demanding Ransom." *The Nonprofit Times*, March 30, 2017.

Disclaimer

This whitepaper is for educational purposes only and does not purport to provide legal advice. If you require legal advice, you should consult with an attorney. The information provided here is for reference use only and does not constitute the rendering of legal, financial, or other professional advice or recommendations by Charity First. The listing of an organization or website does not imply any sort of endorsement and Charity First takes no responsibility for the products, tools, and Internet sites listed.

CHARITY FIRST INSURANCE SERVICES, INC.

1255 Battery Street, Suite 450
San Francisco, CA 94111

Tel: 800.352.2761
Fax: 415.536.4033

charityfirst.com

CONTACT

FRANK TARANTINO

Marketing

frank_tarantino@charityfirst.com

SUBMISSIONS TO:

cfsubmissions@charityfirst.com

CA License No. 0B39059