CharityFirst

Addressing Cybersecurity and Privacy Risks

FOR NONPROFIT ORGANIZATIONS

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**

Introduction

It's easy to assume that nonprofit organizations aren't exactly prime targets for a cyberattack. The truth is, cybercriminals don't have a guilty conscience about targeting charities, foundations, and other nonprofit organizations that have made it their mission to help make the world a better place. In fact, because nonprofits collect and store sensitive financial and personal data — including donor and member information and lists of program beneficiaries such as children, students, seniors, patients, and grantees — they are particularly attractive and vulnerable targets.

> The average number of **records seized in a cyberattack** on a nonprofit in 2016 was more than 12,000.
>
> – NetDiligence Cyber Claims Study

A NetDiligence Cyber Claims Study[1] ranked nonprofit organizations as one of the top five industries affected by cyberattacks — a problem that will only continue to grow. Organizations that think the damage hackers can inflict won't be significant — or worse, are under the impression that cybercriminals won't make them a target — may be in for a shock. In this whitepaper, we'll look at the growing problem of cyberattacks and privacy risks facing nonprofits and why it is critical for organizations to be educated about cybersecurity and the importance of developing an organizational strategy and best practices to prevent a cyberattack.

Why Have Nonprofits Become Prime Targets for Hackers?

According to Giving USA[2], Americans donated $410 billion to nonprofits in 2017. Most of this money is collected online through nonprofit websites, while major platforms such as Google and Facebook have added a donate button to make it easier to give. Unfortunately, this also has provided more opportunities for hackers.

In addition to collecting donations, nonprofits also collect and store large amounts of sensitive personal information, including donor postal and email addresses, contact numbers, employer information, and a variety of data about family members, friends, and interests. For donors who contribute regularly or on a recurring basis, bank and credit card numbers are often stored on the nonprofit's database. For those who donate by phone or mail, payment information and personal data are entered on a spreadsheet or the organization's donor management system.

> Websites that end in .org tend to rank high on Google, making nonprofit and charity organizations more visible to donors — **as well as to hackers.**
>
> – Giving USA

Hackers also know that many nonprofits use basic operating systems and software with weak cybersecurity defenses. They are aware that nonprofits tend to operate with limited staff, rely heavily on volunteers who have the organization's trust and confidence, and may lack adequate information about cybersecurity resources that are used to protect large companies.

Insurance specialists like Charity First who provide employment practices coverage, utilize carriers that offer critical pre-claim assistance. A free helpline offers unlimited consultation with human resources professionals. Online resources such as policies and procedures are available, as well.

Compliance with Data Protection Laws

Several U.S. states have recently introduced and passed legislation to expand data breach notification rules and to mirror some of the protections provided by Europe's newly enacted General Data Protection Regulation. In particular, the California and Vermont laws go beyond breach notification and require companies to make significant changes in their data processing operations. In 2018, California enacted some of the country's toughest and most comprehensive privacy legislation, which applies broadly to businesses that collect personal information about California consumers and is aimed at expanding new consumer privacy rights. As such, it has created significant new obligations for businesses. The California Consumer Privacy Act of 2018 is essentially an expansion of the state's existing Shine the Light law.[3]

Currently, the U.S. lacks uniform and comprehensive data protection laws, though it maintains a number of sector-specific laws that are aimed at helping organizations better understand compliance rules and regulations. They include:

- **The Health Insurance Portability and Accountability Act of 1996**
- **The Children's Online Privacy Act**
- **The Electronic Communications Privacy Act**

Moving forward, data breach laws in California and other states will begin to expand data privacy laws for businesses on both the federal and state levels, imposing additional obligations on organizations that handle personal data. With so many data protection laws under development and amendments to existing laws, it is increasingly important for nonprofits to stay informed regarding the regulatory landscape and continually reassess risk mitigation.

Top Six Cybersecurity Threats and Risks Facing Today's Nonprofits

Cybersecurity incidents are often difficult to detect. Microsoft security researchers have shown that on average, attackers spend 146 days (20+ weeks) on a network before being detected.[4]

Malware

Short for malicious software, malware works by infecting a computer to disable a system, prevent user access, or steal sensitive or valuable data. It is typically hidden in an email attachment, link, pop-up, or webpage. It works by breaching a network through a vulnerability, such as when a user downloads an email attachment or clicks on a dangerous link that installs risky software. An example of this type of cybercrime against a nonprofit is the November 2018 attack on the Make-A-Wish Foundation's international website, where a cryptojacking malware attack affected anyone who visited the infected webpage, allowing attackers to generate cryptocurrency by using the users' computer processing power. The attack severely compromised the charity's website operations and fundraising.[5]

Phishing

Of those surveyed, 45.6% of nonprofits said they have no internal procedures or policies in place for managing how data is shared with external agencies, making them vulnerable to a phishing attack.[6]

In a phishing attack, someone masquerades as a trustworthy source in an attempt to bait users to surrender sensitive information, such as a username, password, or credit card number. Imagine a door where a hacker picks the lock and a phisher convinces the user to let them in. The attacker may mimic a charity's brand to get donors to click on a fake donation link, exposing donors' financial information.

An example is the increased number of phishing scams after Hurricane Harvey in 2017. In this instance, the U.S. Department of Homeland Security warned charitable organizations about scammers using emails to send fake donation links that promised to help victims, when, in fact, the links led to fake websites asking for personal payment information.[7]

Take Note!

Because a phishing attack requires human intervention, the best way to prevent one is with human intervention. This includes implementing an organizational security policy for any sensitive transactions involving account/password changes or financial

Nonprofit organizations with 1,000 or more people have the highest percentage of "phish-prone" employees.

Four types of phishing targeting nonprofits:

- **Whale phishing.** Users are typically board members, directors, or other high-value targets.
- **Deceptive phishing.** Users receive an email that claims to come from a recognized source and asks a user to reenter sensitive information or make a payment.
- **Spear phishing.** Users receive emails that look legitimate and may have information such as name, position, company, work phone number, etc., to trick them into believing the sender is trying to help. This is especially prevalent on an organization's social media platform.
- **Pharming.** Criminals send users to a fraudulent website that looks legitimate. Unlike a typical phishing attack, victims don't have to click a link; instead, hackers use a computer to redirect the user to a fake URL.

– Source: KnowBe4, 2018 Phishing Benchmark Data press release.

transactions such as online donations. For example, organizations may require direct verbal acknowledgment from the person making the request to the person with the power to execute it.

Denial-of-Service (DoS) Attack

A DoS attack is designed to infiltrate entire systems, servers, or networks. It directs traffic to a website or sends so many requests to a database that it exhausts the system's resources and bandwidth, rendering them unavailable to the organization and resulting in lost money because of internal unproductivity or denial of access to customers. 60% of organizations surveyed estimated downtime cost of a denial-of-service attack at around $500 per minute.[8]

Structured Query Language (SQL) Injection

The Open Web Application Security Project[9] lists SQL injection vulnerability as one of the most dangerous issues for data confidentiality and integrity in web applications, and it is one of the 10 most common and widely exploited vulnerabilities facing organizations today. Simply put, a hacker inserts a malicious code in a server that uses SQL to get access to the organization's database.

Man-in-the-Middle (MITM) Attack

The Symantec Corporation describes an MITM attack as having three players: the victim, the entity with which the victim is trying to communicate, and the "man in the middle" who's intercepting the victim's communications. Also known as the eavesdropping attack, it lets hackers secretly put themselves between users and a web service they're trying to access, allowing the attackers to filter and steal personal data. After intercepting a network connection, they also can take advantage of session hijacking that compromises the web session by stealing the session token.

The primary goal of an MITM attack is to:

- Steal personal information for identity theft
- Gain login credentials from a user
- Get a credit card number or other payment information

Day-Zero Exploit

Symantec Corporation defines a day-zero vulnerability as a software security flaw that the software vendor knows about but doesn't have a patch in place to fix. It occurs when a

network's vulnerability is revealed but a patch or solution has yet to be implemented. During this time, attackers have a small window of opportunity to sneak in and do harm. The term "day zero" refers to the fact that the developers have zero days to fix the problem that has just been exposed and perhaps already exploited by hackers.

Cybersecurity Best Practices

Of nonprofit organizations surveyed, 62.8% don't have documented policies to handle a cyberattack.[10]

"Nonprofits that accept online donations, event registrations, and newsletter subscriptions and/or store data about their donors and supporters must assess the risk involved and develop an effective cybersecurity plan."

– Maureen Dyson, Area Executive Vice President, Charity First

The State of Nonprofit Cybersecurity 2018 recent report from the Nonprofit Technology Network (NTEN) and Microsoft surveyed more than 250 nonprofits.[11] While 58% of respondents said their nonprofit had policies on equipment usage and data privacy, only 20% had documented policies in case of a cyberattack.

Today's nonprofits need a variety of effective and efficient controls, liability coverage and work practices to improve mitigation efforts and better respond to cybersecurity and privacy threats.

- **Secure the right cyber liability insurance.** The U.S. cyber insurance market has almost doubled in size since carriers began submitting premium data to the National Association of Insurance Commissioners in 2015, and it has become a critical component of cybersecurity management. Today's policies cover both first- and third-party costs as well as business interruption if a cybersecurity breach forces the nonprofit to suspend operations. Examples of specific coverages available under a cyber liability policy include notification expense, crisis management, regulatory investigation expense, data breach liability, content liability, data loss and system damage (data restoration) and business interruption.

Take Note!

Before organizations purchase coverage, the Nonprofit Risk Management Center advises them to be sure they understand how a breach of privacy claim could affect them and to partner with a knowledgeable insurance broker/agent with an in-depth understanding of the nonprofit's operations and activities to better identify their specific potential exposure.

- **Train employees, board members, and volunteers in cybersecurity risk prevention.** It's important to establish a regular training program for staff, board members and volunteers on cybersecurity and internet safety issues and risks, and to include information on spotting malicious or suspicious emails, not opening links in emails, use of the internet, and safeguards when installing new programs and downloading documents.

Of nonprofits surveyed, **52.9%** said they don't provide any type of cybersecurity training for their staff.

- **Restrict the use of personal and business computers, mobile devices, and email accounts to access organization information.** Enforce strict policies regarding the separation of personal electronic devices when conducting sensitive business activities on behalf of the organization. For example, prohibit sending sensitive business information to a personal email address.

- **Conduct password management policy/training.** Cybersecurity training should include password management that covers best practices in how to create strong passwords using a combination of numbers, letters and symbols.

- **Implement multifactor authentication.** This uses factors such as a rotating PIN in addition to a password to verify a user's identity when accessing email or a network, providing an additional level of protection even if a user's password has been compromised.

71% of nonprofits surveyed said they allow staff and volunteers to use some form of unsecured wireless technology — including personal devices — to access organizational emails and business files

- **Control access to networks.** Establish access control procedures that limit access to only what staff and volunteers need to perform their jobs. Establish a process for immediately revoking user access and changing passwords when an individual leaves the organization.

Only one-third of survey respondents said they use a password management tool, and half of those make its use optional.

- **Assess data risks.** NTEN suggests that nonprofits take an inventory of all the data they collect and identify where it is stored and for how long. For example, organizations may find that the data they are currently asking for and retaining doesn't need to be collected or kept. This process can help reduce or limit the data a nonprofit collects and stores, and is a simple first step in risk mitigation.

- **Educate staff on PII.** Nearly 62% of nonprofits surveyed said they don't have clearly defined policies on what is considered personally identifiable information, or PII, in the data they collect. Everyone at the organization should know what PII is and how to safely handle it.

Over 55% of organizations reported not using multifactor authentication to log in to the nonprofit's online accounts.

- **Encrypt cloud data.** The encryption process transforms data into ciphertext, which is nearly impossible to use without decryption. When storing data in the cloud, organizations should ensure data is secure and encrypted, including restricting data to authorized users and encrypting data before sending it to the cloud.

- **Protect the wireless network.** Safeguard routers by changing the default name and password, disabling remote management, and logging out as the administrator once the router has been set up. Be sure that routers use WPA2 or WPA3 encryption (a certified Wi-Fi hardware technology) to ensure outsiders can't read information sent over the network.

- **Prohibit connecting personal or untrusted storage devices or hardware to computers, mobile devices or networks.** USB drives and external hard drives should not be shared between personal and business computers or devices, and no unknown or untrusted hardware should be connected to the system or network. No unknown CD, DVD,

or USB drive should be used. Disabling the autorun feature for USB ports and CD and DVD drives can help prevent malicious programs on an organization's system.

- **Establish a recovery plan.** After a cybersecurity incident, organizations must begin recovery efforts as soon as possible to resume normal operations. A recovery plan helps expedite the process by making it easier for an organization to restore capabilities and services that may have been impaired or lost. It can also help reduce the severity of the impact.

Conclusion

A cyberattack can have a serious financial impact on a nonprofit or charitable organization and can mean the difference between being able to provide services and closing the doors for good. Staying informed on key issues, regulatory changes and laws, as well as implementing proper safeguards and best practices, makes it much easier to prevent a breach and detect anomalies or security events that may impact information systems.

About Charity First

Charity First is a wholesale brokerage, underwriter, and program manager specializing in serving 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 Department of Homeland Security, NetDiligence Cyber Claims Study, Cyber Infrastructure, Potential Hurricane Harvey Phishing Scams, August 2017.

2 Giving USA, A Fundraising "High Five:" Graham-Pelton's Top Five Takeaways and Actions from the Giving USA 2019 Report, July 2019

3 California Legislative Information, Civil Code 1798.83.

4 Microsoft "Advanced Threat Analytics Data Sheet," Available at https://www.microsoft.com/en-us/cloud-platform/advanced-threat-analytics, 2017.

5 Block Chain Reporter, Hackers Inject Cryptojacking Malware into Make A Wish Website, Nov. 20, 2018.

6 NTEN, State of Nonprofit Cybersecurity Report, 2018.

7 KnowBe4, Phishing Benchmark Data press release, Tampa Bay, FL 2018.

8 Netscout, 14th Annual Worldwide Infrastructure Security Report, 2018.

9 OWASP Foundation, Open Web Application Security Project.

10 NTEN, State of Nonprofit Cybersecurity Report, 2018.

11 Nonprofit Risk Management Center: https://www.nonprofitrisk.org/

Disclaimer

CHARITY FIRST INSURANCE SERVICES, INC.

1255 Battery Street, Suite 450
San Francisco, CA 94111

Tel: 800.352.2761
Fax: 415.536.4033

charityfirst.com

FRANK TARANTINO

Marketing

frank_tarantino@charityfirst.com

SUBMISSIONS TO:

cfsubmissions@charityfirst.com

CA License No. 0B39059