nten

CONNECT ▸ LEARN ▸ CHANGE

Cybersecurity for Nonprofits
A Guide

Written by Afua Bruce

February 2020

Table of Contents

Supporting Nonprofit Staff
Investing in the Nonprofit Sector

Last year, Microsoft and NTEN published the first State of Nonprofit Cybersecurity report and found that 59% of nonprofit respondents did not do any cybersecurity training for their staff. None at all. In the 2018 State of Nonprofit Cloud report, also from Microsoft and NTEN, 56% of nonprofit respondents noted that their organization had decided to implement a new cloud service in just the last year.

As a nonprofit, NTEN understands firsthand the opportunities and challenges that come with engaging in a digital world. With organizations making decisions about technologies at the same time that staff training is lagging, the vulnerability of data, service delivery, and effectiveness is increasing.

We know that the research is only part of the need. It helps benchmark where the sector may be and direct us in providing support where most appropriate. Microsoft has invested in NTEN this year to provide resources about the cloud, cybersecurity, and artificial intelligence to increase the capacity of all nonprofits to understand these topics, make plans, and train staff.

Please share these resources with everyone on your team, use the checklists and guides in meetings and to support planning, and let us know how we can help you further.

Amy & Jane

Amy Sample Ward
CEO, NTEN

Jane Meseck
Senior Director, Global Programs &
Partnerships, Microsoft Philanthropies

Introduction

Experts predict that financial damages from cybersecurity attacks will hit $6 Trillion by 2021.[1] On a nearly weekly basis, reports of a cyberattacks against private companies or government entities surface. Although news headlines may not be filled with the vulnerabilities nonprofit organizations face, nonprofits are not immune.

In fact, because many nonprofits store personally identifiable information (PII), including full names, addresses, social security numbers, medical information, driver's license numbers, email addresses, and more, their IT systems are a target-rich environment. Adversaries opposed to the mission of nonprofits may seek to attack a nonprofit's system, either to disrupt the nonprofit's operations or gain information to target the nonprofit's client or volunteer base. Nonprofits that have particularly sensitive data (healthcare, high-value donor info, financial info), that are doing high-profile controversial work, or organizations that might be working against nation-states on issues like human rights or immigrant rights, should expect to be targeted at some point. Smaller nonprofits that work with bigger nonprofits, or any nonprofit that works with a government entity, is also vulnerable; these institutions may be targeted because they are seen as an easy entry to larger nonprofits or government entities.

Nonprofits must implement cyber safety as well. Internet surveillance and cyber bullying impact many of the people nonprofits support (survivors of domestic violence, individuals, activists, economically disadvantaged individuals, and targets of racial violence, for example). Nonprofits have a responsibility to communicate with and support clients in ways that do not put them at greater risk. Additionally, when PII or other data held by nonprofits is compromised, it is easier for employees, volunteers, and clients to be personally attacked – digitally and physically.

By understanding what cybersecurity is, performing a risk assessment, and implementing simple strategies, nonprofit organizations can protect themselves from cyberattacks.

Cyber Security vs. Cyber Safety

Cybersecurity, simply put, is "the practice of protecting systems, networks, and programs from digital attacks. These cyberattacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money from users; or interrupting normal business processes."[2]

When organizations first begin discussing creating a safe cyber environment for employees, clients, and volunteers, however, they may begin by having first level conversations about cyber safety, or the use of "technology to help protect the physical and emotional well-being."[3] Tactics to protect cyber safety within an organization include installing filters to prevent objectionable or dangerous material, applying automation technology to flag suspicious behavior by and towards individuals, and discouraging cyberbullying activities. Further, nonprofits may encourage their employees, clients, and volunteers to practice internet safety remember to exercise caution and restraint when interacting online, just as they would in face-to-face interactions. While important to reinforcing a culture of respect and awareness of online interactions, although cyber safety can be a start to safe online practices, it is not sufficient to protect an organization's IT systems.

Cybersecurity attacks come in many forms, but always require adversaries gaining access to an organization's systems. Individuals who perpetrate cyberattacks are often referred to as "adversaries," "bad actors," "attackers," or "hackers." When a cyberattack has been successful, the IT systems are often described as "compromised" or "infected."

[1] *Cybercrime Magazine.* Cybercrime Damages $6 Trillion by 2021. https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/

[2] *Cisco.* What is Cybersecurity? https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html

[3] *DZone: Security Zone.* Cyber Safety vs. Cyber Security: What's the Difference? https://dzone.com/articles/cyber-safety-vs-cybersecurity-whats-the-difference

Cyber Security vs. Cyber Safety

(cont'd.)

It is often said that humans are the weakest link in cybersecurity because efforts to protect systems, networks, and programs can be compromised by individuals unknowingly – or knowingly – providing unauthorized parties with access to secure systems. Social engineering is the act of tricking someone into divulging information or taking action; it takes advantage of a potential victim's natural tendencies and emotional reactions.[4] Many of these attacks install malware, a type of malicious software installed onto a computer or system without the consent or intent of the user. Viruses (code that is injected into a system when a user takes an action, such as clicking on a link in an email) and worms (self-propagating malicious code that spreads across networks and computers) are examples of malware. Four major types of social engineering attacks to educate employees against are:

Baiting – Use of a false promise that appeals to an individual's curiosity and instead steals user's information or injects malicious software that into the IT system. Baiting often involves hardware; an attacker could leave a USB flash drive in a place for an employee to find. When the employee inserts the USB flash drive into a computer, the system is then compromised.

Phishing – The act of sending emails sent en masse to trick users into divulging passwords or PII to cyber attackers. Employees may receive a generic "Dear user, please update your password at this link," email; the link is to a site controlled by the hacker.

Scareware – Convincing users that their systems have been compromised and that the way to protect or clean their system is by installing (malicious) software. A pop-up box may appear on an employee's screen stating that their system has been compromised and they must take an action, such as removing malware from the computer, immediately.

Spear Phishing – A specific form of phishing, targeted towards a specific individual, organization, or business.

[4] *Norton by Symantec.* What is Social Engineering? Tips to Avoid Becoming a Victim. https://us.norton.com/internetsecurity-emerging-threats-what-is-social-engineering.html

[5] *Brooks, Sean.* Defending Politically Vulnerable Organizations Online. https://cltc.berkeley.edu/wp-content/uploads/2018/07/CLTC_Defending_PVOs.pdf

[6] *National Initiative for Cybersecurity Careers and Studies.* Explore Terms: A Glossary of Common Cybersecurity Terminology. https://niccs.us-cert.gov/about-niccs/glossary#D

Cyber Security vs. Cyber Safety

(cont‘d.)

However, cybersecurity threats are not limited to social engineering attacks. Organizations must also protect their systems from a variety of threats designed to disrupt operations or compromise data. Examples of these types of cyberattacks include:

Advanced Persistent Threat – A sustained, embedded attack that strives to remain undetected, enabling surveillance, service disruptions, and data theft over a long period of time.[5] Attackers can surreptitiously collect sensitive data the organization stores or shares over its network, and can disrupt network services.

Denial of Service – An attack that prevents or impairs the authorized use of information system resources or services.[6] Individuals trying to access the site will instead be met with "403: Access Denied" or "You don't have permission to access <website name>" messages.

Man-in-the-Middle – Occurs when a hacker itself between the communications of a client and server.[7] For example, a hacker could insert itself in-between a Wi-Fi hotspot and an individual's computer; whatever information an individual then sends over the wi-fi network, the hacker is able to see and collect.

Data Extraction Attack – Occurs when a bad actor executes a SQL query to the database via the input data from the client to server.[8] If successful, the attacker can read all information stored in the organization's database, modify the information in any way, and even complete delete the database.

Protecting against these attacks requires preventing access to data, IT systems, and programs an organization maintains.

[7] *Netwrix Blog.* Top 10 Most Common Types of Cyber Attacks. https://blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks/#Man-in-the-middle%20(MitM)%20attack

[8] *Netwrix Blog.* Top 10 Most Common Types of Cyber Attacks. https://blog.netwrix.com/2018/05/15/top-10-most-common-types-of-cyber-attacks/#SQL%20injection%20attack

Cybersecurity is Part of Organizational Security

Most nonprofit organizations regularly review the physical safety of their buildings and operations, and communicate to employees organizational safety standards and procedures; cybersecurity must be treated in the same manner.

Organizations often have physical security plans with multiple layers – perhaps there is someone who educates employees and volunteers on responsible actions to take and someone else responsible for addressing basic precautions, in addition to locks and an alarm system. An organization's approach to cybersecurity should be no different. Both IT support and employees should regularly install software updates, which often patch recently discovered security holes in software. While IT may be responsible for software upgrades on enterprise-wide software, employees should understand that installing the recommended software updates on their computers and other devices is part of the organization's security plan. Additionally, organizations should educate employees on what cybersecurity is and how they should interact with emails, passwords, and organization software.

Organizations also ensure that there are physical locks on doors to their buildings and restricted spaces, that only a list of verified individuals have the ability to access buildings, and that trusted individuals determine who else can access what parts of an organization's physical space. In a similar manner, organizations must secure their digital information and IT systems. Data and IT systems accessible online should be encrypted, or essentially be digitally locked and protected from unauthorized sources. Encryption is the act of converting data into a form that cannot be understood by unauthorized people.[9] When purchasing new software or storing data in a system (whether in the cloud or in an internally networked system), organizations should encrypt their digital assets. Fortunately for individual IT departments, in practice encrypting data often means ensuring that software

[9] *National Initiative for Cybersecurity Careers and Studies.* Explore Terms: A Glossary of Common Cybersecurity Terminology. https://niccs.us-cert.gov/about-niccs/glossary#E

Cybersecurity is Part of Organizational Security (cont‘d.)

providers and cloud providers encrypt the systems – and that organizations select and pay for this feature if it is optional. Organizations must take care to encrypt both data at rest (information stored in a database) and data in transit (information as it is sent over a communication system such as the internet). Organizations should ensure data on devices that leave their offices or are in public parts of their offices are encrypted; this technology is built into all modern workplace-caliber devices and can be enabled with a single click.

Just as organizations may hire security to periodically check that their buildings and people are safe, organizations must realize that implementing good cybersecurity practices is an ongoing effort. Cybersecurity trainings should be administered at least annually, and encryption settings confirmed and updated. The National Initiative for Cybersecurity Careers[10] and Studies and the Federal Trade Commission[11] have free cybersecurity awareness materials that organizations can use with their employees. Organizations can also consider purchasing and installing cybersecurity monitoring tools to continuously scan their networks for vulnerabilities.

[10] National Initiative for Cybersecurity Careers and Studies. Cyber Security Awareness Training. https://niccs.us-cert.gov/training/search/aziksa/cyber-security-awareness-training

[11] Federal Trade Commission: Protecting America’s Consumers. Cybersecurity for Small Business. https://www.ftc.gov/tips-advice/business-center/small-businesses/cybersecurity

Framework to Implement a Cybersecurity Plan

Once organizations understand what cybersecurity is and recognize that it is a threat to their operations, the next step is to assess what cyber risks the organization has. By conducting risk assessments and implementing appropriate protections, organizations can decrease the likelihood of a cybersecurity attack. Additionally, the risk assessment process often increases communication within an organization, at least temporarily, since those facilitating the assessment must speak to employees throughout the organization.

Although many risk assessment guidelines exist, standards based on the National Institute of Standards and Technology (NIST) guidelines are generally considered the best. The NIST Cybersecurity Framework includes five functions[12]:

Identify cybersecurity risks

Protect against potential cybersecurity events

Detect cybersecurity events

Respond to a cybersecurity incident

Recover from a cybersecurity incident

Nonprofits, especially, should be concerned about three categories of risks and threats:

- Reputation – that an account will get compromised to send spam
- Financial – an employee, volunteer, or donor will be tricked into sending money
- Distraction – an employee's system will be compromised through automated tooling, which can cause organizations to deal with disabled systems, ransomware, or wonder what was actually accessed; this all costs a great deal of work and money

To further understand what risks an organization may face, the organization must first began by identifying the data it collects. NIST defines risk assessments as tools "used to identify, estimate, and prioritize risk to organizational operations (i.e., mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation and use of information systems." To perform a risk assessment, begin by listing all data the organization collects and uses, and then asking who,

[12] Cybersecurity Framework: The Five Functions. https://www.nist.gov/cyberframework/online-learning/five-functions

Framework to Implement a Cybersecurity Plan (cont'd.)

where, what, and how. For each data type, determine 1) who owns the data, 2) where the data is stored, 3) what the level of sensitivity or confidentiality of the data is, and 4) how access controls and security measures are implemented on the data. Organizations will need to repeat this process for other digital and physical assets, including websites and servers; these assets are vulnerable to cyber attacks as well. The next step in this process is, for each item on the list, to determine the impact of a cyber breach or attack, and the likelihood of an attack.

The protect step of the framework "supports the ability to limit or contain the impact of a potential cybersecurity event."[13] This includes activities such as training staff on cybersecurity awareness, creating polices and procedures to protect systems and data, and strengthening access control by requiring strong passwords and controlling who has access to data and when. Protecting against potential cyber events translates to proactively implementing security protocols to make an organization's systems and data more difficult for attackers to access. Detecting cybersecurity events is more challenging, as "cybersecurity incidents are often difficult to detect."[14] In fact, attackers reside within a system on average 146 days before being detected.[15] To effectively carry out this function, organizations should implement continuous monitoring software to alert organizations of any anomalies in the system.

Should an organization fall victim to a cybersecurity attack, the primary goal in responding to the incident is to contain, or prevent the spread and impact, of the attack. Organizations will need to communicate with a variety of internal entities, including legal, HR, and IT, and external entities, including law enforcement, clients, and donors, as appropriate. Organizations must also analyze how hackers were able to access the system, and update protocols to prevent future attacks. Recovering from a cybersecurity attack requires organizations to restore functionality to the pre-attack state. Organizations that regularly backup data and systems will have an easier time restoring information and operations.

The NIST Cybersecurity Framework is intended to scale with an organization's resources. All organizations should develop the capability to periodically conduct cybersecurity risk assessments, and identify, at least theoretically, steps to be taken if any data or systems are compromised. Using the risk assessment to guide conversations between an organization's IT, finance, programs, and executive leadership, will allow the organization to understand its vulnerabilities and make informed decisions about how much risk to absorb, and how many resources should be expended to mitigate the remaining risks.

[13] Cybersecurity Framework: The Five Functions. https://www.nist.gov/cyberframework/online-learning/five-functions

[14] Microsoft Inc. Nonprofit Guidelines for Cybersecurity and Privacy. https://download.microsoft.com/download/1/D/4/1D494A7D-D153-40FC-BC18-F4C2F800E752/Nonprofit_Guidelines_for_Cybersecurity_and_Privacy.pdf

[15] Microsoft Inc. Advanced Threat Analytics. https://www.microsoft.com/en-us/microsoft-365/enterprise-mobility-security/advanced-threat-analytics

Almost Everything Is Cyber

For many organizations today, the reality is that almost all of the organization's activities are vulnerable to cyberattacks because almost everything is cyber. As has been discussed, bad actors may want to gain access to and exploit the PII an organization collects. Other bad actors may want to disrupt operations by taking down an organization's website or access to its online services. Even organizations that simply have an informational page as their website can be vulnerable to a bad actor gaining control of the site and changing its contents to negatively affect the organization's reputation—or worse, inflict harm on clients who visit the website. The number of potential risks can make developing a cybersecurity plan seem to be a daunting task.

Luckily, there are some ways to mitigate this. Organizations can conduct all five functions of the NIST Cybersecurity Framework on their own, or seek help from a variety of sources that provide cybersecurity services to nonprofit organizations. In additional to traditional services, ie: consultants and businesses, innovative new methods such as the University of California at Berkeley's Cybersecurity Citizen Clinic ensure nonprofit organizations can be cyber secure, and can respond to cyber incidents if needed. Additionally, many cloud-based services provide cybersecurity protections as well. By taking advantage of encryption, protection, monitoring, detection, and recovery capabilities that some cloud-based services provide, organizations can alleviate some of the burden of its staff in creating and maintaining a safe cyber environment. Using cloud-based services is not a panacea, as organizations must ensure the connections to the services are also secure.

Extremely risk averse organizations with extremely sensitive information that are willing to devote significant resources to cybersecurity may decide to do penetration testing on their systems. Usually done on sensitive systems for private businesses or government agencies, pen testing "is a controlled attack simulation that helps identify susceptibility to application, network, and operating system breaches."[16] The outcome of a pen test is a detailed report that clearly identifies an organization's cyber vulnerabilities. For many small to mid-sized nonprofits, however, this testing is more than what is needed.

Organizations can also choose to buy cybersecurity insurance. The financial and human capital costs to respond to cybersecurity attack can be significant. Cybersecurity insurance can cover "the cost of notifying all the folks whose information may have been comprised; to the cost of content repair, such as repair to a hacked website; to the cost of hiring a PR whiz to help your nonprofit recover its reputation after a severe security breach."[17] Given that almost everything is cyber within an organization, depending on the level of risk assessed, organizations should seriously consider obtaining cybersecurity insurance. Nonprofit support entities, such as state-level associations of nonprofits, may offer more detailed training in when and how to purchase cybersecurity insurance. Larger nonprofits, or any nonprofit with a large cybersecurity budget and at high risk for a cybersecurity attack, may choose to hire a specialized Managed Security Provider (MSP) that provides a Security Operations Center (SOC) to continually monitor an organization's environment for threats and compromises.

[16] U.S. Department of Interior. Penetration Testing. https://www.doi.gov/ocio/customers/penetration-testing

[17] Council of Nonprofits. Cybersecurity for Nonprofits. https://www.councilofnonprofits.org/tools-resources/cybersecurity-nonprofits

Common Baselines and Techniques

Implementing basic cyber safety precautions will begin to create a safe environment in an organization. Providing employees cybersecurity awareness training, especially focused on social engineering methods, can decrease an organization's vulnerability to attacks. Developing a comprehensive cybersecurity strategy by performing a risk assessment and determining how an organization would respond to a cybersecurity attack can raise an organization's overall preparedness level. However, there are a number of procedures and policies organizations to actively protect against basic cybersecurity attacks. Below are guidelines for organizations to follow to create a solid cybersecurity foundation.

- **Use strong passwords and change them often**. Passwords are the simplest digital lock on data and systems organizations own. Secure passwords are unique and complex, and cannot be easily guessed by hackers or cracked with software tools. Secure passwords are at least 8 characters (although, the longer the better), and use a combination of uppercase, lowercase, symbols, and numbers; they are not words, birthdates, or names of friends, family, or places. Additionally, because volunteers and employees with access to a nonprofit's system may be constantly joining and leaving the organization, nonprofits especially need to frequently change passwords to major systems and programs.

- Organizations should consider **using password managers,** such as 1Password, DashLane, or LastPass. Password managers generate secure and unique passwords for many applications, and automatically login users to their applications. This removes the challenge of coming up with passwords and memorizing several passwords from individuals.

- **Use multi-factor authentication (MFA)** on sensitive systems such as email and banking. Multi-factor authentication essentially requires users to provide two different credentials – such as a known password and an authentication code generated and delivered in real time via text or authentication app – to gain access to a system. "MFA helps protect you by adding an additional layer of security, making it harder for bad guys to log in as if they were you. Your information is safer because thieves would need to steal both your password and your phone." Many programs come with an option to enable MFA, so in most cases, organizations do not need to develop and maintain their own MFA system.

- Practice safe online browsing by only **transmitting information over https websites,** and using a virtual private network when on a public wi-fi network. Websites begin with either "http" or "https." The "s" indicates the site encrypts data and has additional security protocols. Employees and volunteers may access an

Common Baselines and Techniques

(cont'd.)

organization's system outside of the office, by taking advantage of public wi-fi networks at coffee shops, in hotel rooms, at conferences, and more. While convenient to access, public wi-fi puts individuals at risk to cyberattacks; it is easy to use a wi-fi network to do legitimate work, but it is also easy for hackers to steal information transmitted over a public wi-fi network. To protect against this, individuals should use a virtual private network (VPN), which protects and anonymizes the individual's data sent through the wi-fi network.

- **Regularly update hardware and software.** Because technology evolves, as do attacker's ways of exploiting vulnerabilities. Technology manufacturers and providers fix discovered vulnerabilities and provide these fixes to customers through updates. Organizations, then, must install updates when they are received to protect against known cybersecurity attacks. Manufacturers and providers may eventually stop issuing updates for older technology, and only support newer versions of hardware or software. Nonprofits must plan for this evolution, and periodically purchase new technology to ensure safe systems.

[18] Norton. *How to Choose a Secure Password.* https://us.norton.com/internetsecurity-how-to-how-to-choose-a-secure-password.html

[19] *National Institutes of Standards and Testing.* Back to Basics: Multi-factor Authentication (MFA). https://www.nist.gov/itl/tig/back-basics-multi-factor-authentication

[20] Norton. *The Dos and Don'ts of Using Public Wi-Fi.* https://us.norton.com/internetsecurity-wifi-the-dos-and-donts-of-using-public-wi-fi.html

Conclusion

Cybersecurity presents real risks to a nonprofit organization's ability to carry out its mission and serve its clients. There are myriad ways for attackers to maliciously gain access to a nonprofit's information, and protecting against and anticipating cyberattacks is a never-ending process. However, nonprofits can implement basic cybersecurity measures to start, and work over time, if resources allow, to develop and implement a large-scale cybersecurity plan. By starting with regularly educating employees on cybersecurity and social engineering, conducting risk assessment, and implementing simple security policies such as strong passwords and secure browsing, nonprofits will be well on their way to ensuring the security of their organization, and their operations. Applying strong cybersecurity practices on top of cyber safety practices will allow nonprofits to meet the goal of supporting their clients and keeping their clients safe.

nten

CONNECT ▸ LEARN ▸ CHANGE

NTEN envisions a just and engaged world where all nonprofits use technology skillfully and confidently to meet community needs and fulfill their missions. We support organizations by convening the nonprofit community, offering professional credentials and training, and facilitating community skill and resource sharing.

NTEN reports support the growth and development of the sector through benchmarking the technology goals and challenges of nonprofits, and identifying areas of need. For more, visit **nten.org/reports**.

Microsoft

Microsoft's Tech for Social Impact program empowers nonprofits and humanitarian organizations around the world with technology to advance their missions.

With recognition that many nonprofits have limited IT staff, the program provides solutions and resources that help nonprofits innovate new ways to tackle global issues. For more, visit **microsoft.com/nonprofits.**