WHAT NONPROFITS NEED TO KNOW ABOUT SECURITY: A PRACTICAL GUIDE TO MANAGING RISK

TECHIMPACT®

UPDATED FOR SEPTEMBER 2021

How to Share This Report

While Tech Impact makes our resources free to our audience, requiring registration to access them allows us to notify readers of updates, corrections, and other relevant changes, and to make the case to funders that our work is valuable by demonstrating our reach.

Please share a link to the download page rather than a PDF or print copy:

https://offers.techimpact.org/reports/practical_security2021/

Want more resources about nonprofit technology? Visit our Technology Learning Center (TLC) to browse our vast library of free publications, recorded training, and upcoming events:

www.techimpact.org/technology-learning-center

Reprinting and Quoting

For information about reprinting, quoting, or re-purposing this report, please read our policy online at https://techimpact.org/reprinting-and-quoting.

TABLE OF CONTENTS

INTRODUCTION ▶▶▶

There's a tendency to think about security in absolute terms—either you're secure or you're not. This mindset is dangerous for a number of reasons. It can make you complacent, lulling you into believing that you're more secure than you really are. The sheer number of threats lurking out there might overwhelm you, leading you to assume, wrongly, that you can't do enough to protect yourself.

But perhaps most importantly, it just isn't true.

Perfect security has never existed in the online age, and likely never will. Computers fail. Hackers seek targets. People click things they shouldn't. Phones get stolen. In a nutshell, there will always be risks to working with other people and transmitting data across networks.

When we talk about security, we mean the technology, settings, and policies put in place to minimize risk for your organization and its constituents and to ensure that your organization will be up and running with a minimal disruption if a security breach does occur.

Perfect security may not be possible. But practical security is well within your reach.

Nonprofit Pitfalls

Even if you are aware of all the risks you face online, you might think that security is something that small nonprofits don't need to worry much about. Why would someone attack your three-person office in Kissimmee, Kennewick, or Plattsburgh? The fact is, many hackers see small businesses and nonprofits as the perfect targets.

Ten years ago you might have been right that your nonprofit was too small for hackers to take notice, but today they don't even need to know about a target before they hit it. Sophisticated software allows them to trawl the internet and send out automated attacks to multiple organizations at once. If your organization is online in any form, it can be found and attacked.

> ***Perfect security may not be possible. But practical security is well within your reach.***

In fact, many hackers or threat actors have discovered that nonprofits make good targets. They are easier to penetrate than large companies with security teams and less likely to catch a hacker in the act. Today, most hackers are part of professional rings focused on the bottom line. If there is money to be made by hacking your nonprofit, they won't hesitate.

Getting Started

If your organization has taken few security measures, or none at all, getting started can seem a little daunting. It doesn't have to be. You can do a lot to protect yourself without spending a lot of money or needing much technical expertise.

In this report, we've tried to simplify security for nonprofits. We'll walk you through how you might assess your risks, and explain the basic protections that every organization should consider. We'll also discuss how to build a culture that values security, and how to develop policies to guide leadership and employees as they maintain their technology and make decisions about the future.

We’ve also included two case studies and a first-hand account of one nonprofit leader’s experience with a ransomware attack and the hard-earned lessons she took from it.

And to support the adoption of best practices across your organization, we’ve included a simple security checklist that you can print and distribute to your entire staff.

In the next section, we’ll take a look at some of the questions you should be asking yourself to understand what you need to protect and how it might be at risk.

90%

of data breaches could have been prevented.

Source: “Data Protection Best Practices and Risk Assessment Guide,” The Online Trust Alliance.

RISK ANALYSIS ▶▶▶

The list of potential security threats is long. You could try to address them all, but the game of security "whack-a-mole" can get expensive fast. A more commonsense approach is to first consider what risks your organization is most likely to face and to develop a plan to address them. This is called a *risk analysis*.

Your organization is unlikely to experience a wholesale attack on all of its systems. Instead, a security breach will most likely occur within one particular system—your website server, for example. The risk analysis process allows you to look at each system by itself, consider the value of the data it contains, and take specific action to deal with vulnerabilities in the systems that contain important data.

Assessing Your Data

The first step is to an inventory. Exactly what data do you have? Where is it located? List out all of the different types of data by location. For example, if you have a donor management system, list everything it collects and stores. Addresses? Donations given? Petitions signed? Then move on to your website and list everything stored on it.

Repeat this process for each location where your organization stores information, including Cloud-based storage. This will provide you with a comprehensive map of data that your organization collects.

Sticky notes are a helpful tool for this exercise if you're all together in one location. You could write each type of data onto a note that's color-coded by the system it's stored in. This will make it easier when you begin sorting. If you're collaborating remotely, a shared online document such as Powerpoint in Office 365, Google Slides, or an online whiteboard tool can work too.

> ***A security breach will most likely occur within one particular system—your website server, for example.***

Once you have inventoried all of your data, the next question is: How much do you care about it? What's essential to your organization's ability to function? What would risk your organization's reputation if it got out? What data are your constituents counting on you to protect?

One helpful approach is to divide up the data you've listed into three categories:

- Data you can't lose.
- Data that can't be exposed.
- Nonessential data.

We recommend focusing on the first two—data you can't lose, and data that can't be exposed. Examples of data you "can't lose" might include the final files for a major project, templates and brand standards, or employee handbooks and manuals. Examples of data you "can't expose" could be donor information, HR records, strategy documents, or payment information.[1] You might even feel that some things are both "can't expose" and "can't lose." That would indicate that those items are your highest priorities.

[1] For a discussion about whether certain kinds of information ought to be stored on your organization's servers at all, jump to our section on Cloud Security.

At the end of this sorting, you'll probably have a few sticky notes left over. Those are likely to fall in the "don't care about" bucket.

To be clear, the "nonessential data" category doesn't mean that you should be careless with that data, just that you're not going to place a high priority on securing it. For example, you may have put blog posts in the "nonessential" category because they don't contain any sensitive data or information your organization needs to keep itself running, but that doesn't mean you should not take steps to protect your website content from being lost or vandalized. The basic ways to protect your organization in the next section still apply. It's more that the priority on protecting that area of your website is low and you're confident that you could replace it fairly easily if a data breach occurred.

Considering the Risks

Once you've sorted out what you "can't lose" and what "can't be exposed," the next step is to identify the risks your organization faces. Ask yourself:

- What could happen to that data?
- How likely is the risk?
- How bad would it be if something happened to it?

"What could happen?" is about imagining the various scenarios that would put your data at risk. Is it at risk in a fire? Could it be held for ransom by ransomware—a malicious virus that encrypts your data until you pay a "ransom" fee for its release? Could it be picked up by a keystroke logger?

The number of security risk scenarios is potentially huge, but here are a few of the most common:

- Physical theft of equipment or printed files
- Natural disaster (flood, earthquake, fire, etc.)
- Improper disposal of equipment or printed files
- Inappropriate use of software (employees or others with access to software)
- Phishing (employees fooled into providing data)
- Insecure mobile devices
- Spying via software that tracks activity or keystrokes
- Spying via an unsecured WiFi connection
- Hacking through remote access to your network
- Vandalism through malicious viruses or adware
- Ransomware
- Denial of Service attacks (bots flooding your website with traffic and causing it to crash)
- Social engineering (someone without authorization convincing authorized personnel to hand over information or access to systems)

More generally, these scenarios describe various ways your data can be lost, changed, misappropriated, made unavailable, or exposed.

How likely any of these are to happen is a little less straightforward. In most cases, the likelihood of any of these events occurring depends on the behaviors of your organization and its employees. People who thoughtlessly click on links are going to significantly increase the risk of viruses and other malware. Other scenarios might depend on whether you're likely to be singled out as a target—organizations that work on politically charged issues or with populations in unstable regions where governments or terrorists target them are more likely to be vandalized or exposed. The outside perception that you handle a lot of money might also make you a target, and foundations may see more attacks than other organizations.

“How bad would it be if something happened?” is a trickier question, because the consequences can be both tangible and subjective. For example, a breach that causes your organization to lose money from its bank account is easy to count and to characterize within the context of the overall budget. But if that breach is publicly known, how will attitudes about your organization change? Will people still trust you to take their donations? Will they continue to invest in your programs? And this is one of the more straightforward scenarios. How would you weigh the exposure of emails that outline your advocacy strategy? How bad is it if your donors’ names and home addresses are exposed?

Also, don’t forget to consider the possibility that equipment and software could be physically lost or damaged. You might find that some of your infrastructure is rarely used and doesn’t contain much important information. This seems like an item for the “nonessential data” pile, right? It probably is, but that doesn’t mean you should ignore it. You may actually find that old and outdated technology poses a significant security risk. If old software or equipment is connected to your network, it can be a weak link that provides a way in for hackers. If losing a piece of technology is no great loss, you should consider getting rid of it.

> “*In most cases, the likelihood of any of these events occurring depends on the behaviors of your organization and its employees. People who thoughtlessly click on links are going to significantly increase the risk of viruses and other malware.*”

Ransomware

Ransomware is one of the most catastrophic and expensive forms of phishing. Ransomware attacks infiltrate your systems and lock them down, often by copying your data, erasing it from your computers or servers, and storing it on an encrypted server. Pay the ransom and you get the encryption key to unlock your data — at least in theory. If you don’t pay, you lose everything.

Local governments in multiple states have experienced increased ransomware attacks in recent months. While anyone can be a target, ransomware attackers often focus on governments and entities that provide essential services that hold a lot of sensitive data they can’t afford to lose, even for a few hours.

In our sidebar on page 18, one nonprofit leader shares her experience with a ransomware attack on her organization and what other organizations can learn from it.

After an Incident

A security incident can happen at any organization, not only because hackers are indiscriminate but also because human error is the most likely cause of data loss or exposure. It's not hard for someone to accidently delete a file. And since the pandemic, a lot of people have been working at home on networks not set up by their organization and might even be using personal devices for work.

The policies and culture of your organization are important factors in preventing an incident. We'll review these in a later section, but generally you'll want to write a guide that outlines the steps your organization will need to take when a data breach or other kind of security incident occurs.

In your guide, you'll need to think through:

- What mechanisms are in place to detect a security incident?
- Who will document the events leading up to and immediately following when the breach was discovered?
- Who will lead the response if a breach occurs?
- Who will be part of the response team?
- How will you respond to various scenarios?
- How will your response team communicate with the rest of the organization?
- How will your organization recover files or repair systems?
- How will your organization communicate with your constituents (if necessary)?

Some examples to help you think through how your organization should respond include the following schools, each of which has posted an incident response guide online:

- **University of California,** https://security.ucop.edu/files/documents/policies/incident-response-standard.pdf
- **University of Colorado,** https://www.cu.edu/security/system-wide-incident-response-procedure-data-breaches
- **Loyola University of Chicago,** https://www.luc.edu/its/aboutits/itspoliciesguidelines/incident_response_plan.shtml

Your own incident response guide could be as simple as a list of a few of the most likely scenarios and bullet points outlining roles and responsibilities. What's important is to have enough of a plan in place so that if something were to happen, you and your team aren't left wondering what to do.

It's wise to establish a relationship with an IT consultant that has some background in security. Many issues are stressful, complex, and will need to be dealt with quickly. Being able to draw on the expertise of a consultant (and gain the extra people power) in a time of crisis can save a lot of time, money, and hits to your reputation.

Staying Compliant

Your organization may need to address security to meet specific regulations. Each compliance standard will have its own specific guidelines, but generally you'll need to invest in systems that encrypt data and have in place additional layers of security to make it more difficult for an individual to access or move sensitive data. Cloud storage and Cloud-based software typically offer the level of security you will need to stay compliant, but research your options with security in mind before you choose on provider over another.

PII

All organizations are required to protect any Personally Identifiable Information (PII) they collect from employees and constituents. PII is defined as information about a person that contains some unique identifier, such as a social security number. More information on this topic can be found at: https://www.gsa.gov/directive/gsa-rules-of-behavior-for-handling-personally-identifiable-information-%28pii%29-

PCI

Any organization that handles payment card data is required to meet Payment Card Industry (PCI) Compliance regulations. Most organizations use third-party systems to handle credit card information, but if your organization collects and stores credit card numbers you should investigate further how to protect yourself and your constituents. For more on this topic visit: https://www.pcisecuritystandards.org/

HIPAA

Any organization dealing with patient health information, including health status, provision of health care, or payment for care, is required to follow the standards outlined in the Health Insurance Portability and Accountability Act (HIPAA). There are two rules to be aware of if your organization handles patient health information.

The HIPAA Privacy Rule specifies what information needs to be protected. For more visit: https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html

The HIPAA Security Rule establishes standards for protecting electronic health information. For more on this rule visit: https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html

BASIC WAYS TO PROTECT YOUR ORGANIZATION ▶▶▶

No tool or process can protect against all possible security breaches, but a number of inexpensive steps can reduce your organization's risk. Here are a few best practices you *can* find in place at many nonprofit organizations. (Note: See *Appendix A: Staff Security Checklist* for how your staff members can carry out many of these recommendations.)

Physical Security

Keeping your data safe starts with a secure office. What was true 100 years ago is still true today: Most security breaches are caused by natural disasters or improper activity by employees.

Here are a few ways you can make sure the physical office space is configured to keep your data secure.

Lock the Door

It seems both trivial and obvious, but there's a lot of peace of mind to be found in just locking the door, especially if you share a building with multiple tenants. Many organizations have installed door handles that require you to type in a code before they will unlock. Even if you choose to leave the door to your office unlocked, you should make sure someone is by the door and takes on the responsibility of greeting people who enter. This is a good deterrent and can stop people who are hoping to stumble into an opportunity.

Within your office, you still want to consider locking up sensitive information. Your HR staff members, for example, should be the only ones who can access employee records. Your HR Manager should probably have a lock on his or her door and should lock up at the end of the day. If this is not possible, make sure any sensitive paper records are kept in a locked cabinet.

88%

of security breaches are caused by employees.

Source: "Psychology of Human Error," Stanford University/Tessian.

Secure Equipment

If an intruder does enter your office, make it as difficult as possible to carry away valuable equipment. Use safety devices to lock laptops, computers, printers—any machine that contains organization data and that could easily be carried out of the office.

Log Off Machines

Every computer should be logged off at the end of the day. Consider installing automatic screen locks that kick in after a specific amount of time and require login information to unlock on every machine. This is especially important for workspaces that need to be in public areas.

Back Up Your Data Offsite

Sometimes keeping your data safe means insuring against accidental loss. You've likely heard many times how important it is to back up your data, but give some thought to *where* and *how* you back it up. An external hard drive will allow you to restore your data in the event your main drive fails, but what if a hurricane floods your office or a fire leaves nothing behind? Will your backup end up underwater alongside your server? To make sure your data will be there for you no matter what kind of disaster you encounter, choose a backup strategy that stores your data somewhere other than where your server is located. Cloud backups are a good solution, and many different vendors offer automated backups at a reasonable price.

Note that keeping a manual backup regimen is not likely to be your best option. Automated backups make it easy to secure your data and eliminate the risk that someone will forget or deprioritize this task. You'll want to work out how often to carry out a backup and how many iterations to store, but one expert recommends:

- Retain multiple daily backups for one day.
- Retain end-of-day backups for seven days.
- Retain one weekly backup for 12 weeks.
- Retain one monthly backup for 36 months.
- Retain one yearly backup for 10 years.

Online Security

The most complex and damaging security breaches are likely to occur online. Here are a few ways to protect your organization's data from spying, vandalism, and theft.

Update Your Software

You're not alone if you ignore the patch/update notifications from installed software, especially when installing them means restarting your computer. But those software updates are often intended to fix major vulnerabilities that hackers have already proven adept at exploiting.

This is why you cannot rely on staff members to do these updates themselves. Windows lets you automate many updates, or you can purchase third-party software that will automatically download and install them for you—even during the hours when the office is closed and staff members are not using their computers. It's often easiest just to contract an IT consultant to help you configure the automation of your software updates.

94%

of malware is delivered by email.

Source: "2021 Data Breach Investigations Report," Verizon.

Install Software to Detect Viruses, Spyware, and other Malicious Code

A number of free and low-cost antivirus and antispyware programs are available, but make sure to do your research on which ones are the most reliable and effective. Ideally, your software will check for malicious code at least once each day and update automatically.

Secure Your Internet Connection

Your organization is likely always connected to the internet, even when everyone has gone home for the day. A firewall set up between the internet and your internal network can add a critical layer of protection. What's a firewall? It's software that provides a first line of defense for screening out viruses and hacking attempts. Most routers come with software that includes firewall protection, but double check to make sure yours is installed.

If you're using a wireless router, you need to take additional steps to secure your connection. The first is to set a password. Many routers come with a default login and password—often "admin" and "password." Create a unique password that is made up of many characters and includes numbers and symbols. It's a good idea not to broadcast your Service Set Identifier (SSID), which is the name of your WiFi network, as it can act as a kind of password into your network—you can set this option in the router's administrative setup screen.

It's also a good idea to encrypt your wireless access point so that data cannot be easily intercepted as it is transmitted across the network or to other networks.

Make Sure Passwords are Complex

Staff members should be responsible for setting their own passwords, but you can set rules regarding those passwords. Generally, you want passwords to be at least eight characters long and include a mix of numbers and letters. Some IT managers require users to also use uppercase letters or incorporate symbols. Any rule that increases the number of possible passwords an automated hacker will have to enter before it can guess the right one will add an increment of safety.

Most Popular Passwords

1. 123456
2. 123456789
3. Qwerty
4. Password
5. 1111111

If possible, you should also set a lockout feature that limits the number of failed attempts to log in. Your password retrieval process should include a mechanism to "unlock" the user's access.

In the past, IT professionals had recommended that users change their passwords regularly. Today, more technology people recognize that users are inundated with passwords already and requiring them to change passwords frequently only encourages unsafe behavior such as posting passwords at a workstation, frequently reusing passwords, or setting passwords that are easy to guess such as "abc123."

Limited access means that less can go wrong—the fewer people who handle specific files, the less likely they are to be lost or damaged. You'll also reduce the temptation to break your organization's trust by opening files that are not meant to be seen by a large group.

Install Firewalls on Every Computer

Most computer Operating Systems have firewalls set by default. Check the settings on your systems to make sure they're enabled.

Require Individual Accounts and Limit Access

Every staff member should have his or her own login name and password, whether it's to gain access to a computer at your office or to log in to Cloud software shared by the entire organization. This simple step will help prevent many of the most common forms of loss due to the misuse of data by employees.

If your software allows you to differentiate between administrators and other employees, limit the number of staff members who have full admin status and carefully set the usage rights for each type of user. Often administrators have access to data and controls that can cause significant damage if they are misused.

Why are individual accounts and limited access so important? Individual accounts allow you to trace the source of strange activity on your network or within a specific software solution. They also mean you don't have to worry about employees accessing your systems after they've left your organization because you can simply deactivate their accounts without deactivating the whole system or changing login information for everyone.

Should You Be in the Cloud?

One of the big fears about putting data in the Cloud is the notion that the Cloud is inherently less secure than office computers and servers. In reality, the opposite is likely to be true.

Securing your data is a Cloud vendor's entire business model, so it has a strong incentive to make sure nothing goes wrong. Cloud data centers are often secured with barbed wire fences, surveillance cameras, and 24-hour security guards. They are also protected by network structures designed to make it difficult for hackers to reach stored data and are monitored by sophisticated online security tools that can detect attacks before they happen. And if hacks or physical failures cause a loss of data, Cloud vendors keep redundant backups in two or more data centers, making it simple to recover your organization's data.

How does your office's security stack up? Most nonprofits could not afford to maintain a fraction of the security that comes standard with a Cloud vendor.

Unless your organization is willing to invest in top-of-the-line security products, you should consider storing your most sensitive data—payment information and employee records that contain social security numbers and bank account numbers—with a Cloud vendor. Most payment, accounting, and HR software vendors now offer Cloud-based versions of their products.

THE NEXT LEVEL OF SECURITY ▶▶▶

For organizations that want to go beyond basic, there are a few additional measures you can take.

Information Rights Management

Word documents, PDFs, and even emails can be “locked.” This security feature usually requires that the user open the document only on a specific network or enter a password before viewing the content. Very few nonprofits are likely to need such protection, but if you’re working with information that you need to share but can’t let fall into the wrong hands, you might consider this measure, with the caveat that password discipline and secure communications about shared passwords are necessary and could significantly complicate the simple act of opening a document.

Multi-Factor Authentication

Many software applications—especially Cloud-based software—allow you to add a second layer of authorization. Multi-Factor Authentication, or MFA, is a stronger form of account verification designed to protect users by making it much harder for stolen passwords to be used to break into their accounts. MFA requires users to supply two different types of authentication information to log in — generally some combination of something a person knows (e.g., a password), something a person has (e.g., a phone or laptop), and/or something a person is (e.g., in a physical location). MFA often takes the form of a prompt or code that is sent to a user’s phone after they enter their username and password into an MFA-protected site. The protected site will not let the login process complete until the user enters a code or pushes a button to confirm that they have access to their phone.

56%

of nonprofits don’t require Multi-Factor Authentication for employees to log on.

Source: “State of Nonprofit Cybersecurity,” NTEN.

Network Security Monitoring

Larger organizations, especially those that feel they have a lot of sensitive data to protect and face a high risk of being targeted by hackers, might consider hiring a service to monitor traffic on their network and vigilantly defend in real time against cyber attacks. A number of different organizations offer these services, but they are expensive and are still no guarantee. Threats tend to move faster than any efforts to thwart them.

Password Management

Password services are emerging as a popular way to manage all the different passwords a person might need, as much out of convenience as for security reasons. These services typically require you to use one long, complex password to unlock all your other passwords. Many offer plug-ins that allow you to access your password and apply it without leaving your browser. While many services and features (such as automated password changing and the ability to handoff your password information to an emergency contact after your death) can make life more convenient and secure, there can be big consequences to a breach of this service. If a hacker—or even someone you know—gets their hands on your master password, then every online service you use could be compromised.

Single Sign-On

You can register all of your organization’s online services with a single sign-on (SSO) service such as OKTA, OneLogin, or Office 365. This allows staff members to log into a device once and then be automatically logged in to any other service. It also allows IT to control which services that staff member has access to. It’s a lot like a password manager, but with fewer steps for the user and no need for that user to actually create or know more than one password.

One Nonprofit Leader's Experience: Takeaways from a Ransomware Attack

Last year Delaware-based behavioral health provider Brandywine Counseling and Community Services fell victim to a ransomware attack. Speaking at our Tech Forward Conference, CEO Dr. Lynn Morrison shared a few hard-earned lessons from the incident in hopes of sparing other nonprofits the same aggravation.

Too Much Surface Area

BCCS began using electronic health records in 1994. As the organization grew and became more technologically advanced, the network surface area expanded. The bigger the surface area, the bigger the target.

"We had a multiple server environment instead of a secure business data center or a cloud based app," Morrison said. "Security can never be at its best with a large network surface area."

Don't Let Users Dictate Your Plan

Implementing security measures will almost always add inconvenience to users—for example, Multi-Factor Authentication takes more time than a simple password. But that's not a valid argument against such measures.

"Don't let the inconvenience to your users dictate whether you implement additional security measures," Morrison said. "We need to educate those users and explain why these changes are important and how they will protect them, the organization, and the people they serve."

Find a Trusted Partner

An ongoing relationship with a consultant or firm with security expertise can help you mitigate risk, prepare against attacks, and respond in the event it becomes necessary. But for such a relationship to work, you have to make sure that partner understands the barriers and concerns your organization faces so they can take them into consideration as they develop your risk assessment analysis and implement security measures.

"You pay for expert advice for a reason," Morrison said. "And while it's easy to push projects off or delay those suggestions, if you have a team or consultant you trust to guide you through your technological environment, listen to their advice."

Spend Smart and Trust Your Partners

Look for cost-affordable measures to help address any financial concerns you have around implementing security measures—it's better to get some in place than none at all. You can also plan to implement them on an ongoing basis so the cost is spread out over time. Make technology a budget line in operation budgets and include strategic tech planning and regular risk assessments every three to five years.

"The cost saving measures are really important, but it's also very important to think about the cost of a ransomware incident," Morrison said. "The money we had to spend to address this incident could have paid for at least four years of advanced security measures and saved the organization a lot of time and stress and heartache."

Don’t Think It Can’t Happen to You
Threat actors are always seeking vulnerabilities in systems across all industries and will attack the easiest to get into.

“Everyone gets attacked,” Morrison said. “If you think you’re immune, you’re not. Make sure your facility or organization is too much work for a threat actor to bother with. With the right security plan the threat actors will move on to someone else.”

One of the things that limited damage for BCCS was that it had backup data offsite, which mitigated the fallout from this ransomware attack.

Morrison said the attack made her realize that she needed to learn more about IT security so she could ask the right questions, identify the right security measures for the organization, and know what questions to ask trusted partners.

Her advice to other organizational leaders? Make sure you have an insurance policy that covers ransomware attacks. Get a security risk assessment. And make sure you have a recovery checklist or plan.

SECURITY AWARENESS ▶▶▶

Technology solutions can only offer so much protection. Your people are your best security measure. Organizations that take security seriously from top to bottom and that regularly promote security awareness are better equipped to prevent a major data breach.

It Starts with a Conversation

Do your staff members know what they need to do to keep your organization safe? Do they understand why, despite the inconvenience, certain security measures are in place? Would they recognize a threat if they saw it? Are they even aware of their responsibility to keep the organization secure? No organization is going to turn every staff member into a security expert, but there are many ways you can build awareness within your organization. Here are a few examples:

- At regular staff meetings, review a few security basics and remind everyone why they are important.
- Schedule “teach-ins” or “lunch and learn” sessions that provide basic information and promote discussion.
- Ask your staff about how they use your systems and what situations trip them up.
- When breaches are reported in the news, talk about them and look for opportunities to make connections with your organization.
- Include security as part of any discussion about new technology implementation projects.
- When new security features are being considered, include staff members in the process. Give them a chance to talk about the benefits they see for themselves and the organization. Also provide opportunities for staff members to express reservations about the inconvenience or talk through their confusion about these changes.

59%

of nonprofits do not provide staff cybersecurity training on a regular basis.

Source: “State of Nonprofit Cybersecurity,” NTEN.

Whatever approach you take to build awareness, your goal should be to help your staff members build good habits. Security measures are almost always inconvenient. How much easier would life be if you never had to lock a door or fasten your safety belt? Nonetheless, we all do these things automatically. In fact, we’re so accustomed to doing these things that they seem less like inconveniences and more like everyday routines.

Data security can also become a habit. A solid understanding of the risks your organization faces and repeated reminders about what each individual can do to protect your organization will go along way toward helping your staff members develop good data security habits.

DEVELOPING POLICIES AND PROCEDURES ▶▶▶

Most staff members want to keep your organization safe. Often, they simply don't know what is acceptable and what isn't. Clear policies and procedures are an important step toward building awareness and strengthening habits.

You'll want any policy to outline *dos* and *don'ts* in as much detail as possible while maintaining some flexibility to address new threats as they emerge. Different kinds of written policies to consider include the regulation of:

- Computers and online usage
- Information
- Mobile devices
- Devices used at home
- Social media usage
- What to do in the event of a data breach

Many universities have thorough policy documents that are publicly available. Consider reviewing those created by the University of Florida, Villanova University, Loyola University Chicago, or Arizona State University.

If you're starting a policy document from scratch, skim a few and use your favorite as a template to build your own policy. Just keep in mind that the process of creating a policy is as important as the policy itself. The time you take to think through your needs and the particular ways your organization works is important and shouldn't be cut short by simply repurposing an existing policy document.

20%

of nonprofits have a cybersecurity policy in place.

Source: "State of Nonprofit Cybersecurity," NTEN.

You can also download Tech Impact's free *Nonprofit Technology Policy Workbook*, which contains prompts to help you create and document policies for the acceptable use of technology and networks, personal devices for work, how to provide IT guidance to "accidental techies," how to respond to an IT incident, and how to recover your technology after a major disaster.

CONCLUSION ▶▶▶

Perfect security may not be possible, but practical security is well within your reach.

Even the largest corporations in the world cannot protect themselves from all threats at all times. That doesn't mean small organizations should consider their situations hopeless. A few low-cost measures can significantly reduce the risks your organization faces and protect it from a major data disaster.

Awareness of the risks and what they mean to your work as an organization that seeks to do good in the world is your first line of defense. Then it's important to put into place technology that can block the most common threats and the culture that can identify and act on threats as they emerge.

This is practical security. It's not a silver bullet or a magic wand that solves all your security problems, but it's a critical and common sense way to mitigate needless risk.

CASE STUDIES

NONPROFIT COORDINATING COMMITTEE OF NEW YORK ▶▶▶

Annual Budget: $1.6 million
Staff: 5

The Nonprofit Coordinating Committee of New York (NPCC) is a small nonprofit with a big mission. It seeks to be the voice and source of information for 1,400 member nonprofits in and around New York City.

NPCC provides workshops, vendor services such as liability insurance and payroll services, a monthly newsletter, and a website that's loaded with information for nonprofit leaders. If a member calls the office with a question, one of the five people on staff will answer the phone and track down an answer.

But a recent audit turned up one important blindspot: security.

"We were just going with the flow," said Melkis Alvarez-Baez, Director of Programs at NPCC. "We lacked awareness of the risks."

Audit

Like a lot of nonprofits, NPCC undergoes a comprehensive audit every year. Its last audit was pretty routine except for one important finding. The auditor pointed out that NPCC did not have any cyber-security policies in place. The organization hadn't evaluated its risks or considered what it could do to further protect itself. Moreover, NPCC had no plan to deal with a data breach if one occurred.

"It raised a red flag," said Alvarez-Baez. "We needed to do something."

The auditor recommended NPCC undergo a risk assessment to identify its most important data and outline the steps it would need to take to protect that data.

Assessing NPCC's Risk

Risk assessment requires organizations to take a close look at their data and sometimes to make tough decisions about how much risk they are willing to accept. It likely reaches every part of the organization and requires the expertise and judgment of a wide range of staff members.

NPCC asked its IT provider to perform a risk assessment, which it did under the scope of NPCC's existing managed services agreement. The process began with a questionnaire, which was developed by the IT firm and distributed to the majority of staff members. Based on the information uncovered by the questionnaire, the IT provider then followed up by leading a roundtable discussion where NPCC decision makers could discuss the risks, consider the potential mitigations, and prioritize action to address them.

At the end of the process, NPCC received a report that outlined the process, provided important definitions, summarized the organization's information, highlighted existing safeguards, identified vulnerabilities, and recommended mitigations.

"The process was seamless and helped our staff think about our information in a slightly different way," said Alvarez-Baez. "It was also heartening because the proposed fixes would not cost us anything—we were doing pretty well for a team our size."

Change is a Long Process

The risk assessment led to a few simple security provisions. NPCC now requires more complex passwords that need to be changed less frequently. This reflects a balance between security (more complex passwords) and access (less frequent changes). Emails for various online accounts, including NPCC's domain registration, were updated to ensure all communications would go to active accounts. Last, NPCC updated and, in some cases, created security policies to address various business areas.

These kinds of physical precautions are low-hanging fruit that can be implemented very quickly. Developing policies and building awareness is a much bigger process that requires the cooperation of the entire organization.

NPCC is still very much in the middle of developing its policies, in large part because it has new leadership. "We're on the cusp of change," said Alvarez-Baez. She speculates that new initiatives—especially those that involve online outreach or digital resources—might require additional security protections. The policies NPCC writes now will need to be flexible enough to inform both the present and the future.

Alvarez-Baez is confident that, thanks to its recent risk assessment and increased awareness of data security among staff members, that NPCC is up to the task of developing security policies that will evolve with the organization as it takes on new challenges.

"We have a good framework," said Alvarez-Baez, "but it's very much a work in progress."

PROSPECT PARK ALLIANCE ▶▶▶

Annual Budget: $10 million
Staff: 80

Central Park gets all the attention, but Prospect Park in Brooklyn is its equal as a marvel of urban landscape architecture and as a center of activity for its borough. Designed by Frederick Law Olmstead and Calvert Vaux 150 years ago, today Prospect Park receives more than 10 million visits per year.

One big reason the park is so loved is the Prospect Park Alliance. The Alliance partners with New York City to provide maintenance and programming over the park's 585 acres.

To manage all of work the Alliance does requires much of the same technology any other nonprofit would use. It maintains a database with more than 4,000 members and a separate database for volunteers. It also raises revenue through concessions, a tennis center, and programs, which requires taking payment information. Its staff of 80 also uses computers and mobile devices to schedule events, manage maintenance work, communicate with the community, and more.

So, when a recent audit pointed out that the organization faced risks from hackers and others who might try to steal information, James Snow, Chief Operating Officer and Chief Financial Officer, took the finding very seriously.

Insure or Secure?

The auditor recommended that the Alliance purchase hacker insurance for any lost or stolen data. On the one hand, the recommendation was prudent—it offered some financial protection in the event of a major data breach. However, it also felt like a misdirection of resources.

"The lifeblood of the organization is raising money," Snow said. "A lot of it is transacted by credit card. If it ever became known that giving your credit card to the Prospect Park Alliance is a risk, that would be a big problem for us."

To Snow, insurance didn't cover the biggest risk of a data breach—the hit to the Alliance's reputation.

With limited resources available for IT, Snow considered another option: What if, rather than buying insurance, the Alliance spent its money on reducing the risk of a data breach?

Assessing the Risks

Snow reached out to an IT consultant the Alliance relies on for strategic help and technical expertise. The consultant initiated a risk assessment that helped the Alliance inventory its data and evaluate how significant the loss would be if particular data sets were lost or exposed.

Together, the Alliance and its consultant identified a handful of ways the Alliance carried unnecessary risk and put together a plan for addressing those risks. Today, the Alliance has policies in place to protect its computers from opportunists who walk through the doors looking for an easy target. (Working in a public park means that its offices are in public buildings.) It also now requires more complex passwords and has stricter policies on handling credit card information, including making sure that card numbers that are stored by the Alliance are done so appropriately and in accordance with a defined policy.

In fact, the Alliance took the extra step of certifying that it is compliant with the Payment Card Industry Data Security Standard (PCI DSS). This is a voluntary certification program that allows you to self-evaluate whether your organization is sufficiently protecting payment information.

Policies and People Are the Best Protection

Snow estimates that the one-time cost of the risk assessment was roughly the same as its annual hacker insurance premium would have been. That means that by being proactive about data security, the Alliance will see cost savings starting next year and every year after that.

"You're never going to have enough money to keep the bad people out," Snow said. "Being safe comes down to policies."

Policies are ultimately about people—they are guides that can help people make the right choices and avoid major risks. For the Alliance, the next step is making sure everyone in the organization understands and internalizes the policies.

"It's important to educate employees of what the risks are," Snow said. "They need to be reminded that there's risk in what we do with our data."

APPENDIX A: STAFF SECURITY CHECKLIST ▶▶▶

Data security is everyone’s job. Here are a few ways you can protect yourself and your organization from spying, vandalism, theft, and accidental data loss.

Your Workspace

- Don’t leave sensitive documents out on your desk. Lock them away in a safe or a cabinet.
- When you dispose of documents that contain organization data, shred them.
- When you leave your workspace, take laptops and mobile devices with you or secure them.
- Log out of or lock your computer screen whenever you’re going to be away for more than a few minutes.

Passwords

- Set a strong password that is at least eight characters long and combines letters and numbers. Including uppercase characters and symbols will also strengthen your password.
- Do not write down your password and keep it near your workstation.
- Disable browser features that auto-fill your passwords.
- Do not share login information or passwords with others.

Email

- Do not click on email links unless you’re certain the email has come from a trusted source and that the content of the email is directly applicable to your work together.
- If your email program includes it, use the “preview” function to review attachments and determine whether they’re safe.
- Sign out of your email client when you are not using it.
- Pay attention to safe links and attachment checks built into your email provider. They can often catch unsafe content before you click.

On the Web

- If your organization does not automatically install antivirus software and software patches, install them yourself and check for updates daily.
- Do not click on links unless you’re certain they come from a trusted source. Look for slight changes to URLs that are intended to pass the site off as a legitimate source.
- Vigilantly watch out for spam on social media and messenger apps. Do not click ads that offer too-good-to-be-true deals.
- If a website asks you to transmit any data, make sure the URL says it is using “HTTPS,” a more secure protocol than “HTTP.”
- Avoid downloading new or untested browser plug-ins—they often contain vulnerabilities that could compromise your device.

Mobile Devices

- Download updates to your operating system and apps.
- Do not assume all apps are safe. Some apps are fake and are intended to compromise your device. Read reviews, seek out “editor’s choice” picks, and look up the developer’s profile to gauge your risk.
- Double check the source of any shared images, videos, or links.
- Download a device location app to help you find a lost or stolen device.

At Home/On the Road

- Make sure your home internet connect is password protected and has a built-in firewall.
- Install updates/patches on all devices you might use for work.
- Avoid sending sensitive data via public WiFi.
- Do not set your device to automatically roam for a WiFi signal—it may pick up an unsecure signal and compromise your device.
- If you use a remote desktop application, do not save login credentials and make sure it is updated every time you login.

APPENDIX B: ADDITIONAL RESOURCES ▶▶▶

For more information on security, check out these valuable resources.

Small Business Information Security: The Fundamentals

A thorough, straightforward guide created by the National Institute for Standards and Technology.

https://csrc.nist.gov/publications/detail/nistir/7621/rev-1/final

The SANS Institute

A computer security organization that provides training and certification for security professionals. Its website contains resources for experts and novices alike.

https://www.sans.org/security-resources/

Lecture 1: Introduction, Threat Models

An overview of a security methodology that attempts to map out the threats, your assets, and the points where you can protect yourself.

https://ocw.mit.edu/courses/electrical-engineering-and-computer-science/6-858-computer-systems-security-fall-2014/video-lectures/lecture-1-introduction-threat-models/

Graham Cluley

Computer security news, advice, and opinions from a widely-respected security expert.

https://grahamcluley.com/

Mind the Gap

A presentation from Roger Hagedorn, Information Security Analyst for the City of Minneapolis, on the current security climate and how nonprofits can close the gaps in their protection.

http://www.slideshare.net/techfrogger

2021 Cybersecurity Readiness for Nonprofits Playbook

Included in this playbook is an eight-step framework that provides a multi-layered approach to cybersecurity.

Krebs on Security

A blog by Brian Krebs, an investigative journalist who has a knack for making security issues relatable and interesting.

http://krebsonsecurity.com/

Cyber Degrees

This website was created to help aspiring security professionals figure out what level of education and certification they need. Included on its site is a massive list of online resources about security, many of them focused primarily on experts.

http://www.cyberdegrees.org/resources/the-big-list/

Techopedia

An IT news and best practices website with a section on security.

https://www.techopedia.com/topic/4/security

Tech Soup: Security

Security products offered at a discounted price by TechSoup

http://www.techsoup.org/security

APPENDIX C: ABOUT THIS REPORT ▶▶▶

Authors and Contributors

Dan Rivas, Managing Writer

Dan is a versatile writer and editor who specializes in translating complex information into compelling stories. Prior to Idealware, he was a copywriter and editor at a marketing agency that serves large technology and financial services companies. He also has experience as a freelance writer and journalist, a census enumerator, a bookseller, and a college instructor. He is a graduate of Willamette University and the University of Michigan, where he studied anthropology and creative writing.

Chris Bernard, Managing Editor

Chris is a career writer and journalist with two decades of experience in newspapers, magazines, advertising, corporate and nonprofit marketing and communications, and freelance writing. Prior to Idealware, he was managing editor of a newspaper and a senior copywriter at an ad agency. For the past seven years, he's overseen Idealware's editorial and communications efforts, driving the creation and publication of more than a hundred articles, reports, and other resources and managing the communications calendar. Outside of his work at Idealware, he's an award-winning author and a frequent speaker and lecturer at literary conferences and festivals around the country.

The following people contributed to the research of this report:

- Melkis Alvarez-Baez, Director of Programs, *Nonprofit Coordinating Committee of New York*
- Roger Hagedorn, Information Security Analyst, *City of Minneapolis*
- Joshua Peskay, Vice President, *RoundTable Technology*
- Gail K. Reynolds, *CISSP*
- James Snow, COO and CFO, *Prospect Park Alliance*
- Larry Velez, Founder and CTO, *SINU*

How Was This Report Funded?

This report is funded by the generosity of our sponsor Community IT; through the continuing contributions of our Leadership Circle sponsor Microsoft; and through the generosity of a grant from Fidelity Charitable. It was entirely researched and written by Tech Impact.

Maintaining editorial integrity and impartiality while funding reports in the technology sector demands rigor. We work hard to meet those demands as well as the expectations of our audience.

To maintain editorial integrity and impartiality, we take the following steps:

- Tech Impact is responsible for research and editorial content of this report.
- Ads are sold by fundraising staff without any collaboration or communication with those responsible for researching and writing the report.
- Neither vendors, advertisers, or sponsors see the report prior to publication and have no input over content.

Additionally, Tech Impact may work with promotional partners to help the report find as wide an audience as possible. Such partners agree to help us distribute the report to widen our reach in exchange for promotional considerations.

About Our Sponsor

Community IT

Community IT is a top-ranked Managed Services Provider (MSP) in the Washington, DC region and a recognized leader in the nonprofit technology community. A 100% employee owned company, Community IT focuses on helping nonprofit organizations achieve their missions through the effective use of technology. Services include IT security, cloud migration, help desk support and strategic IT planning. Learn more at communityit.com.

About Tech Impact

Tech Impact is a nonprofit on a mission to empower communities and nonprofits to use technology to better serve the world. The organization is a leading provider of technology education and solutions for nonprofits and operates award-winning IT and customer experience training programs designed to help young adults launch their careers. Tech Impact offers a comprehensive suite of technology services that includes managed IT support, data and strategy services, telecommunications, and cloud computing integration and support.

In 2018, it expanded its education and outreach capabilities by merging with Idealware, an authoritative source for independent, thoroughly researched technology resources for the social sector.

Tech Impact's ITWorks and CXWorks training programs have graduated hundreds of young adults with the knowledge, skills and confidence they need to start their careers in the technology and customer experience industries. The organization also operates Punchcode, a coding bootcamp based in Las Vegas, NV. Learn more at www.techimpact.org.

About the Technology Learning Center

Tech Impact's Technology Learning Center, or TLC, is an expansive collection of technology education materials—just like this guide—created exclusively for nonprofits. It includes hundreds of free publications and downloads, a free organizational tech assessment, and the most comprehensive curriculum of webinars, courses, and on-demand learning about nonprofit technology currently available. The vast majority of resources are free, and the remainder are priced within reach of even the smallest nonprofits. Give your tech knowledge a little TLC at https://techimpact.org/technology-learning-center.