Vanguard

Cybersecurity for nonprofits: Improve your defenses

With so many bad actors today using increasingly sophisticated weapons, no one can confidently say that their organizations will not be hacked. That said, we believe *every* organization can improve its defenses and make itself a more difficult target.

Cybersecurity is not a one-and-done process. It should be an ongoing priority. A number of clients have asked what advice Vanguard can give nonprofits about remaining vigilant against cyberattacks. And while, as an asset manager, we're not provisioned to provide customized cybersecurity reviews, we'd like to share the following framework of measures and steps nonprofits can take to help reduce their risk, as well as additional resources for further guidance.

We've distinguished two types of cybersecurity measures: those focused on end users and those impacting nonprofit IT infrastructure. Each of these measures is separated into three categories: steps that should be taken immediately, longer-term efforts, and ongoing strategies.

Measures focused on end users

Immediate actions

Establish or revisit password policy best practices.

- Require passwords on all devices employees use, including desktops, laptops, tablets, and smartphones.
- Change passwords frequently and don't permit employees to reuse old passwords.
- Implement lockouts (a user is locked out of their account after a number of failed login attempts).
- Consider utilizing passphrases instead of passwords, but ensure they are not easily hackable.
- Never email, text, or write down passwords.

Password tips: There are two schools of thought on passwords. Some advocate complex passwords containing 15 or more characters, with a mix of upper- and lower-case letters, numbers, and symbols. Others favor combining phrases and numbers that an employee can easily remember but that are hard for a bad actor to guess. Keep in mind that if a password is both long and very complex, an employee may be tempted to write it down, which is not a good practice.

A recent study from the cybersecurity company Hive Systems found that a 6-character password with a mix of numbers and upper- and lower-case letters can be cracked instantly, whereas an 11-character password with the same mix takes three years to hack.

Implement multifactor authentication (MFA).

MFA requires the user to provide a combination of two or more authenticators to verify their identity before they gain access to a resource, such as an email account. There are three main types of authentication factors, based on things you *know* (such as a password or PIN), things you *have* (a badge or a smartphone), and things you *are* (biometric information like fingerprints or voice recognition).

Requiring only a password leaves an organization vulnerable to "brute force" attacks by hackers using a trial-and-error approach. But with MFA, even if the first factor (a password) is compromised, the chances of an unauthorized user bypassing the second factor are highly unlikely.

Longer-term efforts

Train end users to be careful about a variety of threats. Best practices include:

- Be suspicious of any email that asks the user to confirm their credentials.
- Check that a website is secure before visiting.
- Make sure that all sensitive information and authorizations (e.g., financial transactions) are transmitted in person or by a voice call.
- Never open anything other than a standard PDF or Office attachment, and open only those from recognized senders.
- **Combine awareness training with automated testing tools.** The aim is to train users to recognize phishing attempts and learn not to download malware.

Ongoing strategies

Create a cybersecurity mindset among end users.

Many employees are mission-oriented. If cybersecurity training is presented as a key element in preserving the nonprofit's ability to carry out its mission, rather than as a burden that employees must help shoulder, it's likely to be better received.

It is important for nonprofits to realize that cybercriminals will exploit whatever vulnerabilities they can find, regardless of the nature of the target. Hackers don't care if your nonprofit is rich or poor, nor do they care about the work you're performing. They just look for vulnerabilities.

Address necessary changes in cultural norms.

For instance, not every employee needs to have access to every aspect of the business. To the extent this represents a shift in your nonprofit's culture, emphasize to employees that it's a critical part of protecting the organization against attacks. That said, it's essential for all users to protect donor data, safeguard personal information, and take other steps to prevent bad actors from stealing money or compromising the mission.

Make it harder for bad actors to employ social engineering to target your nonprofit.

In part, this involves training users in detecting phishing attacks and avoiding opening emails or clicking on attachments from unknown senders. But it extends well beyond that, including having users check with other workers if they get a request that appears to come from a colleague but that feels "off" and taking care not to share too much information about themselves or their employer on social media.

Measures focused on nonprofit IT infrastructure

Immediate actions

Install additional protection, including:

- Firewalls.
- Spam filters.
- Next-generation antivirus/antimalware applications.
- Intrusion prevention and detection.
- Antispam and antiphishing software.

Update and patch all software.

This means *all* software, whether residing on a server, a desktop, a tablet, or a smartphone. It's particularly important to include equipment software (e.g., for networked printers) or software used for specific departments (general ledger software or human resources).

- Update operating system software as well as application software.
- Implement patches to fix all known security flaws.
- Update the software to the latest version according to the vendor's instructions.
- Upgrade software that is no longer supported.

Curtail poor cybersecurity practices.

- Replace end-of-life software products that no longer receive software updates.
- Replace any system or products that rely on known, default, or unchangeable passwords.
- Adopt MFA for remote or administrative access to important systems, resources, or databases.

Back up files.

- Offline.
- Using external hard drives.
- Back up to the cloud.

Encrypt devices.

- Anything used to access data: PCs, tablets, smartphones, and any other networked device, such as printers.
- Use full-disk encryption.
- Use at least WPA2 (wi-fi-protected access) encryption. WPA3 is better.
- Keep track of encryption keys.

Secure your router.

- Change the default name and password.
- Disable remote management.
- Log out as administrator after router setup.
- Use at least WPA2 (wi-fi-protected access 2) encryption.

Implement security tools.

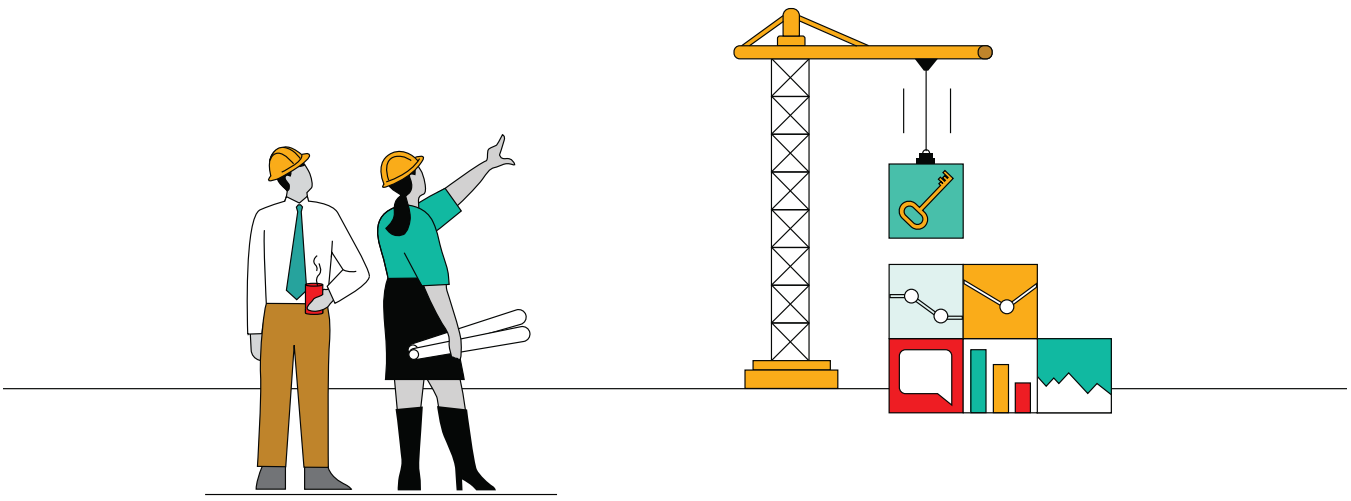
- Browser management.
- DNS filtering (blocks access to malicious websites).
- Network monitoring.
- Endpoint protection (EPP).

Longer-term efforts

- Review systems for paying vendors and receiving donor contributions.
- Review your general ledger system software.
- Plan a response to a cybersecurity breach, with a focus on:
  - —Limiting or preventing the likelihood of a damaging cyber incident.
  - —Detecting malicious activity quickly.
  - —Responding effectively to confirmed incidents.
  - —Maximizing resilience.
- Create a data backup plan.
- Create a user access management plan that limits access to physical and virtual assets (and associated facilities) to authorized users.
- Get rid of your servers and do everything on the cloud.
- Perform detailed mapping and inventories for:
  - —Software library.
  - —Hardware inventory.
  - —Network map.
  - —Configuration documentation.
  - —Archive list.
  - —Policies and procedures for how patches are implemented and how assets are managed.

Ongoing strategies

- Periodically review and reassess your defenses, particularly after a breach.
- Establish the following policies and review them regularly:
  - —Data classification.
  - —Password strength.
  - —Access control.
  - —Encryption.
  - —Data disposal.
  - —Patch management.
- Sign up for CISA's Cyber Hygiene Vulnerability Scanning and other free services from government sources.



The far-reaching consequences of cyberattacks on hospitals

There have been hundreds of cyberattacks on hospitals over the past few years, many of which involve ransomware (if you don't pay the bad guys, they disable your computers and even erase or hijack confidential patient data).[1]

The HITECH Act of 2009 incentivized investments in information technology and led to the explosion of electronic health record systems over the past decade. In a classic illustration of unintended consequences, today, there is an average of 10–15 networked medical devices per hospital bed across the U.S., any of which provides a point of cybersecurity vulnerability.[2]

The number of attacks climbed by the hundreds during the pandemic, in part because hospitals were in the news more often, but mostly as a result of a shift to staff working from home, to patients being monitored remotely, and to the greater use of telehealth.[3] These steps, while essential to providing health care services, introduced new points of vulnerability (in cyber jargon, "broad attack surfaces"). Employees working remotely proved more susceptible to phishing attacks. Telehealth consultations were not always encrypted and remote patients tend to be unsophisticated concerning cybersecurity measures. Moreover, researchers, both in academia and industry, identified vulnerabilities in patient monitoring, particularly in the protocols used to send data from devices hooked up to patients to central monitoring stations.

The increased number of cyberattacks has been linked to patient deaths and, in a report from the Ponemon Institute,[4] higher overall mortality rates, underscoring the need to improve hospital cybersecurity measures.

The Cybersecurity and Infrastructure Security Agency (CISA) is well aware of these problems and has developed a catalog of bad practices, with a particular focus on health care. It calls out the use of unsupported software, the use of known/fixed/default credentials (in everything from patient monitoring equipment to networked devices, such as copiers/printers), and the use of single-factor authentication.

1 "Half of Ransomware Attacks Have Disrupted Healthcare Delivery, Jama Report Finds," *Healthcare IT News*, January 10, 2023.

2 "Why Hospitals and Healthcare Organizations Need to Take Cybersecurity More Seriously," *Brookings*, August 9, 2021.

3 "Ransomware Attacks on Hospitals Put Patients at Risk," *Pew*, May 18, 2022.

4 "Cyber Insecurity in Healthcare: The Cost and Impact on Patient Safety and Care," *Proofpoint*, 2022.

Where can nonprofits turn for unconflicted guidance on improving cybersecurity?

There is a plethora of high-quality resources on cybersecurity available that don't come from companies trying to sell you products or persuade you that their solutions are the best. Here are just a few.

Government agencies

U.S. Department of Homeland Security Cybersecurity & Infrastructure Security Agency (CISA)

Federal Trade Commission, Cybersecurity for Small Business

National Institute of Standards and Technology (NIST) Small Business Cybersecurity Corner

Nonprofit organizations

Cyber Readiness Institute

Global Cyber Alliance

National Council of Nonprofits

Nonprofit Technology Enterprise Network (NTEN)

Groups associated with specific nonprofit verticals

A comprehensive list is beyond the scope of this brochure, but your nonprofit vertical (health care, education, etc.) undoubtedly has organizations, such as those noted below, that supply cyber information tailored for your unique needs.

- Healthcare Financial Management Association
- Higher Education Information Security Council
- Technology Affinity Group (foundations)

Follow the NIST cybersecurity framework

The National Institute of Standards and Technology (NIST), part of the U.S. Department of Commerce, developed this five-part best practices framework to help firms decide where to focus resources for cybersecurity protection.

1. Identify

—List all equipment, software, and data you use, including laptops, smartphones, tablets, and point-of-sale devices.

—Create and share a company cybersecurity policy that covers roles and responsibilities for employees, vendors, and anyone else with access to sensitive data as well as steps to take to protect against an attack and limit the damage if one occurs.

2. Protect

—Control who logs on to your network and uses your computers and other devices.

—Use security software to protect data.

—Encrypt sensitive data at rest and in transit.

—Conduct regular backups of data.

—Update security software regularly, automating those updates if possible.

—Have formal policies for safely disposing of electronic files and old devices.

—Train everyone who uses your computers, devices, and network on cybersecurity. You can help employees understand their personal risk in addition to their crucial role in the workplace.

3. Detect

—Monitor computers for unauthorized personnel access, devices (like USB drives), and software.

—Investigate any unusual activities on your network or by your staff.

—Check your network for unauthorized users or connections.

4. Respond

Have a plan for:

—Notifying customers, employees, and others whose data may be at risk.

—Keeping business operations up and running.

—Reporting the attack to law enforcement and other authorities.

—Investigating and containing an attack.

—Updating your cybersecurity policy and plan with lessons learned.

—Preparing for inadvertent events (like weather emergencies) that may put data at risk.

—Test your plan regularly.

5. Recover

After an attack:

—Repair and restore the equipment and parts of your network that were affected.

—Keep employees and customers informed of your response and recovery activities.

Stay up to date on the threat landscape

Know your cybersecurity threats

- Hackers/hacktivists (criminal groups, cyber criminals, script kiddies, government actors).
- Insiders.
- Environmental.
- Spyware/Malware.
- Phishing and spamming (malware and viruses).
- Ransomware.

Be aware of common hacking techniques

Denial of service attacks.

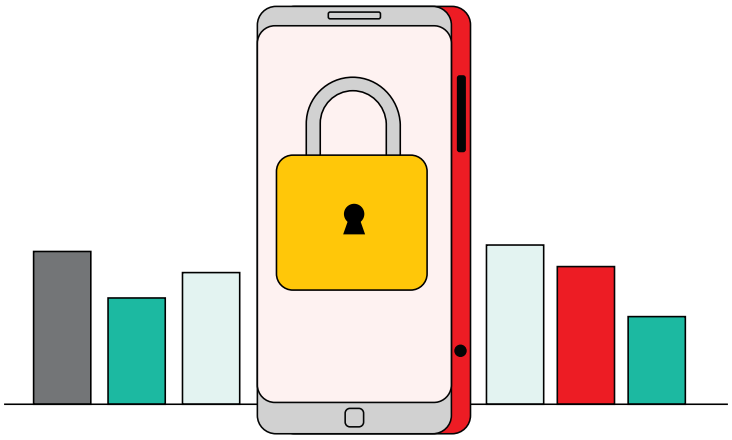
- Intends to shut down a server or network, keeping authorized users from accessing.
- Floods targets with traffic or sends information that triggers a crash.
- Can take significant time and money to fix.

Business email compromise.

- Targets all IT systems.
- Aims to enable wire fraud.
- Can result in significant financial loss.

Social engineering.

- Can be done in person.
- Sometimes accomplished via emails/electronically.
- Frequently done on the phone.



Can we help you?

Having worked with nonprofit organizations over the past two decades, we understand, and value, the essential contributions nonprofits make to our communities—from caring for our health, to educating our children, to supporting the arts, and more. You can count on our specialized expertise to develop smart investment strategies, helping you meet your goals as if they were our own.

Connect with Vanguard®
institutional.vanguard.com/nonprofit

Vanguard®

INPCSBRO 032023