CAPINTECH

5 Steps to Strengthen Your Organization's Cybersecurity Defenses

By Lisa Traina, Partner

Russia, China, the CIA, and the FBI. Hacking has been receiving a great deal of attention lately in the political arena, but many nonprofit leaders may not realize the severity and scope of the threat to their own organization.

The reality is that all nonprofits are at risk of a cyber breach, so it's critical that leaders devote adequate resources and take proactive steps to maintain a secure environment.

The five steps below will help you understand the key issues and risks and how your organization can strengthen its cybersecurity defenses.

1. Acknowledge the Risk

The first step in improving your organization's cybersecurity is acknowledging the risk and understanding what opens the door for hackers to target your nonprofit. In fact, several factors can make nonprofit organizations vulnerable, regardless of their size. These include:

- highly desirable data, including personally identifiable information (names, addresses, Social Security numbers, dates and places of birth, etc.) and user names and passwords
- an assumption by cybercriminals that nonprofits lack the staff and resources to implement strong cybersecurity defenses
- online bank accounts
- connections to other organizations' systems
- the growing threat of hacktivism, a form of hacking that occurs for politically or socially motivated purposes

2. Understand the Threat

Cyber breaches typically occur when hackers target common technical weaknesses. Here are three of the most prevalent threats, with considerations for addressing them:

- **Phishing:** Phishing emails can take many forms, including package shipment notifications and credit card fraud alerts from what look like legitimate sources as well as fraudulent leadership emails. The objective of these emails is to entice the recipient to click on a link or attachment that opens the door for hackers to steal data or infect systems with malware. Although your organization probably uses filtering to stop many of these emails, some slip through in even the best systems.

  It only takes one employee or volunteer to make one mistake that can compromise an entire network and cause a data breach. Repetitive testing and training for network users is the best way to minimize the chances of someone falling victim to a phishing email.

- **Malware:** All systems are vulnerable to malware, which is malicious software installed without a user's knowledge. This typically occurs when a user clicks on a link in a phishing email or visits an infected website.

  It's imperative to have appropriate controls in place to protect *all* your systems, including servers, workstations, networking equipment, networked printers, laptops, and mobile devices. This includes the growing number of Internet of Things (IoT) devices like thermostats, alarms, cameras, and appliances that can connect to the Internet.

- **Technical Vulnerabilities:** Vulnerabilities are holes in software code that can allow cyber criminals to gain unauthorized access to a system. These can exist in all software, including applications and operating systems. The holes can be closed by applying patches and updates.

  However, an astounding number of vulnerabilities are discovered every day. These are known as zero-day vulnerabilities because a patch or update is not available at the time of discovery. This is one reason why it's imperative to have multiple controls in place.

3. Establish a Culture of Security

It's crucial to create a culture where the importance of cybersecurity is recognized and appreciated. This includes ongoing training and communication to help staff

and volunteers understand the following doors to security breaches:

- The dangers of visiting unsafe websites
- How phishing emails work and how to detect them
- The latest cybersecurity threats
- Why they need to use, and regularly change, complex passwords and should not use the same password for multiple sites
- The risks of using public Wi-Fi networks

4. Implement Strong Information Systems Controls

Your organization's IT department should develop and maintain a comprehensive list of network and data security controls. Although this is the responsibility of the IT department, it's helpful for leaders to understand the issues enough to ask relevant questions and ensure the appropriate steps are being taken.

Here are some basics to be aware of:

- **Perimeter Security:** This includes firewall and intrusion detection systems, as well as intrusion prevention systems. These should be set with appropriate restrictions to filter and block any harmful incoming and outgoing Internet traffic.
- **Endpoint Security:** This protects servers and workstations by requiring each device on the network to comply with set standards before being granted network access. These measures include administrative access limitations and anti-virus protection.
- **Authentication Controls:** Authentication controls should require complex passwords that expire on a set frequency and restrictions (such as lock-out) after a set number of invalid login attempts. Ideally, systems will also have multifactor authentication requiring an identifying factor, such as device authentication, in addition to the password. These controls should be applied to the network and all critical systems, especially cloud-based systems that can be accessed from anywhere.
- **Administration Controls:** User administration also requires strong controls ensuring that only appropriate individuals have login credentials.
- **Updates and Patches:** Your IT department should establish an inventory reconciliation, which will help ensure that all systems are protected. There should be a procedure in place for keeping all operating systems and applications up to date at all times. In addition, anti-virus protection is needed for desktops, laptops, IoT devices, and mobile devices, including devices that employees own but use to connect to your network.
- **Network Security:** Frequent, ongoing monitoring for all IT systems, including network traffic and system resource monitoring.
- **Incident Response Plans:** Your organization should have appropriate plans that include detailed response procedures for responding to a cyberattack.

5. Identify Existing Risks and Test Your Controls

The steps above are essential to maintaining cybersecurity, but it's also important to periodically identify and address any existing risks through independent testing.

There are two components to this testing:

- **Vulnerability testing,** in which various systems are automatically scanned to identity whether any known weaknesses exist. The results are then analyzed to determine critical gaps in security.
- **Information security controls testing**, which helps to determine whether you have the appropriate protection, processes, and procedures in place; and if so, whether they are functioning properly.

Don't be misled into thinking that any single "magic" control exists that will protect your organization. The key to adequate protection is to implement several controls in a layered fashion so that if a control fails, one or more secondary controls exist to protect the asset.

CapinTech offers a comprehensive Cybersecurity Assessment to help nonprofit organizations assess their information security controls and identify and address any risks and vulnerabilities. More information is available at capintech.com.

About the Author

Lisa Traina, Partner
CapinTech
ltraina@capincrouse.com
o 505.50.CAPIN ext. 2000

Lisa uses her more than 30 years of experience to assist organizations in implementing measures to secure data and manage risks efficiently and effectively. She is a nationally recognized speaker and author, and serves on the AICPA Cybersecurity Task Force. Lisa founded Traina & Associates in 1999 to provide IS security services to a broad range of industries. Traina & Associates joined CapinCrouse in January 2017 and is now CapinTech.

About CapinTech

CapinTech, a CapinCrouse company, provides information security services, including cybersecurity assessments, consulting, and training services, to nonprofit organizations, financial institutions, medical entities, professional services firms, and other organizations. Each year the firm performs hundreds of assessments, consulting, and speaking engagements with a team of experienced professionals retaining numerous certifications, including CPA, CISSP, CISM, CISA, CITP, CGMA, and CTGA. Each engagement is tailored to fit the unique needs of the organization, and information and reports are presented in a clear, concise manner intended for an audience with varying information systems (IS) knowledge. More information is available at capintech.com.

About CapinCrouse

As a national full-service CPA and consulting firm devoted to serving nonprofit organizations, CapinCrouse provides professional solutions to organizations whose outcomes are measured in lives changed. Since 1972, the firm has served domestic and international outreach organizations, universities and seminaries, foundations, media ministries, rescue missions, relief and development organizations, churches and denominations, and many others by providing support in the key areas of financial integrity and security. With a network of offices across the nation, CapinCrouse has the resources of a large firm and the personal touch of a local firm. Learn more at capincrouse.com.

CapinCrouse is an independent member of the BDO Alliance USA.