How to Reduce Your Cybersecurity Risk

By Lisa Traina, Partner

Malware. Ransomware. Identity and data theft. Phishing. Corporate account takeovers. Denial of service attacks. As recent headlines illustrate, cyberattacks are a real and growing risk for all organizations. It's no longer a question of *if* an attack will occur, but rather *when*.

That's the bad news. The good news is that there are steps you can take to strengthen your organization's defenses and respond quickly and effectively when an attack occurs.

If cybersecurity is still on your organization's to-do list, the following steps and considerations will help you tighten up your controls and reduce your risk. If you already have controls and processes in place, this article can serve as a useful review to help you identify any areas that may need to be assessed or addressed.

Build a Strong Foundation

Good cybersecurity defense starts with a strong foundation. The steps below must be taken to ensure the success of the cybersecurity controls and processes you put into place.

- **Understand and accept the threat** – Cybersecurity is no longer just an "IT issue" — it's a critical business issue. It's vital for nonprofit leaders to understand the scope and nature of the threat, and then ensure that adequate resources are dedicated to creating and maintaining a secure environment.

  Many nonprofits believe that they are not large enough to be at risk. But the reality is that all organizations are at risk, regardless of size. Many cyber breaches are random, which means that small organizations are just as vulnerable as large ones. And in targeted attacks, cyber criminals often focus on small to medium-sized organizations because they assume these organizations do not have the staff or resources to maintain strong information security controls.

  Other nonprofits feel they don't have data a cybercriminal would want, but any personally identifiable information is valuable to hackers. This includes an individual's name, address, date and place of birth, Social Security number, and mother's maiden name. User names and passwords are also extremely valuable, because many people use the same password across multiple systems. Cybercriminals can then use these login credentials to attempt to gain access to other cloud-based systems.

  And let's not forget that every organization has a bank account, and most access accounts online these days. That is certainly an attractive target, and corporate account takeover schemes are prevalent. In addition, most organizations have connections to other organizations' systems. Hackers can get into one system and use it to access others.

  It's also important to understand that having strong IT support, whether through an internal department or outside vendor, does not guarantee security. That's because IT teams are often busy moving from one issue to the next, leaving little time for maintaining security. It's vital for nonprofit leaders to understand their organization's current cybersecurity defenses and risks, determine what resources need to be dedicated exclusively to cybersecurity, and then ensure that the focus is continually maintained despite whatever other IT issues crop up.

- **Appoint an Information Security Officer with the appropriate skills and authority** – Whatever title you give them, it's important to have an individual within the organization who is responsible and accountable for ensuring the security of your systems and data. This will likely be someone outside your IT department who has the authority to ensure the appropriate resources are devoted to information systems security.

- **Provide comprehensive and ongoing training** – It only takes one employee clicking one link in one fraudulent email to create a major cybersecurity breach. Provide ongoing training and communication to help all employees, board members, and volunteers understand the latest cybersecurity threats and why security measures are important and must be followed. This includes topics such as phishing emails, complex passwords, and why the same password should not be used for multiple sites. Keep the information simple and direct.

- **Create an inventory of all systems** – The saying "You can't manage what you can't measure" is very applicable here. Before you can ensure that you've protected all your systems, you need to create and maintain a complete record of all servers, laptops, desktops, mobile devices, routers, switches, firewalls, and peripherals owned by your organization. This includes items that are no longer used but might contain confidential information. It also includes the Internet of Things (IoT) — the growing number of devices like thermostats, alarms, and appliances that can connect to the Internet and act like computers.

- **Ensure someone is monitoring your systems** – Implement ongoing monitoring for areas such as virus protection, patching of operating systems and applications (e.g., Java and Adobe Flash), systems and data backups, confidential information in email, firewall and event logs, and rogue applications. You should also monitor the removal of data from your internal network through methods such as email, cloud services, mobile devices, and USB drives. These tasks are often overlooked due to resource constraints.

- **Implement 24 x 7 perimeter monitoring** – Many organizations use intrusion detection systems that provide around-the-clock monitoring for intrusions. Consider who will be notified, and how. If the process is that an email is sent to someone in the IT department, an email in the middle of the night will probably go unseen. If the process is to provide an alert via a phone call, who will be on call? Some systems can be set to automatically react to and terminate certain levels of suspicious activity.

Address Current Risks

Cyber breaches typically occur when criminals target common technical weaknesses. Let's look at the most common threats and how to address them.

- **Malware** – Malware is malicious software that installs without a user's knowledge, often after visiting an infected website or clicking a link in a phishing email. It can lay dormant for a long period before the hacker exploits a vulnerability or system weakness.

  Malware is available for purchase online, which means that anyone can become a cybercriminal, not just tech-savvy hackers. All systems are at risk, so you need to have controls in place to protect *all* the systems in your inventory.

- **Ransomware** – Ransomware is a type of malware that prevents or limits users from accessing operating systems or files. The hacker demands payment (ransom) via wire transfer, at which point the files may — or may not — be unlocked.

  The malware can be in an email, website, or even bundled with software. The best defense is to maintain strong controls on all your systems, and educate employees on the potential impact of this breach and how it can occur.

- **Phishing** – Some phishing emails are easy to spot because they are full of misspellings and poor grammar. However, many look like legitimate communications from internal parties like the CEO or CFO, or external parties such as banks, credit card companies, and other believable sources. Although your organization may use filtering, some fraudulent emails can slip through even the best systems. The best way to minimize the risk is to provide repetitive phishing testing and education for all network users.

- **Vulnerabilities** – These weaknesses or holes in software code can allow hackers to gain access to a system. They can exist in all software, including operating systems (e.g., Microsoft Windows, Apple, iOS) and applications (e.g., Java, Adobe Flash), and are closed by applying patches and updates.

- **Risks posed by mobile devices** – This area has become increasingly important as more people use their own mobile devices at and for work. You should have an accurate inventory of all devices in use on your network, regardless of who owns them. Additional controls should include acceptable usage policies, virus protection, updating and patching, data storage, and encryption. You also should develop procedures for lost, stolen, or traded devices that include device tracking and remote wipe capabilities. If there are more than just a few mobile devices in use at your organization, you need Mobile Device Management (MDM) software.

Plan Your Response

While the steps above will help you reduce your cybersecurity risk, it's also crucial to plan how you will respond if and when a breach occurs. This will enable you to act quickly and take all the necessary steps.

- **Zero-day vulnerabilities** – Many times, there isn't an update or patch available at the time a vulnerability is discovered. These are known as zero-day vulnerabilities, and it's important to plan for how you will respond. This plan should outline:
  - The sources you will use to stay informed on new vulnerability discoveries
  - Who will be responsible for assessing whether each new vulnerability exposes your organization
  - If your organization is exposed, the process for obtaining the necessary patches and updates, including a process for following up to obtain patches or updates that aren't yet available
  - A process for documenting the steps taken

- **Incident Response Plan** – Determine which current cybersecurity crimes pose a risk for your organization, and what specific risks and outcomes could occur from each. Then, plan for:
  - Forensics
  - The retention of audit and activity logs
  - The steps you will take to return to normal operations
  - Notification of affected parties
  - Notification of law enforcement and regulatory agencies

Monitor and Test Continually

Once you have strong defenses in place, it's important to continually monitor and test for any issues. Many organizations overlook the following considerations.

- **Develop and implement a vendor review process** – Don't underestimate the risk your vendors can pose. Vendors are focused on providing services, not security. The Target cybersecurity breach started when an employee at a small HVAC contactor with connections to Target's systems opened a phishing email. Vendor security issues also led to major data breaches at Goodwill, Home Depot, and Lowe's.

  It's important to conduct a formal review process for all vendors that provide critical functions, or that host or have access to your data. You should perform this review before signing a contract with a new vendor, and review all existing vendors annually. This should include an assessment of the vendor's:
  - Financial condition
  - Data security, including confirmation of vulnerability testing
  - IT security controls
  - Incident response
  - Business continuity and disaster planning
  - Insurance coverage
  - Performance standards
  - Service-level agreements (SLAs)

  You also should ask whether the vendor undergoes independent information security assessments, and whether it reviews the security of its own vendors. In addition, you should periodically evaluate the authentication controls each vendor offers, such as password parameters, account lockout settings, and multifactor authentication. Multifactor authentication is critical for cloud systems. These typically improve over the lifetime of a service.

- **Complete periodic cybersecurity assessments** – An independent cybersecurity assessment tests for any existing risks in your organization. It should include two components:
  - Information security controls testing, which examines whether you have the appropriate controls in place and if so, whether they are functioning as intended. This might include network authentication, user administration, virus protection, updating and patching, and backup procedures. When performing this testing, our firm often uncovers numerous significant issues such as missing virus and malware protection, inadequate updating of systems, failed backups, confidential information sent in emails, unfiltered Internet access, and failed phishing testing.
  - Vulnerability testing, which uses software to scan your organization's internal network and external Internet-facing systems against a database of known vulnerabilities. The report is then analyzed to determine what systems need to be updated.

  Your organization should perform cybersecurity assessments annually, with vulnerability testing done more frequently, such as monthly or quarterly. This is particularly important because vulnerability testing uncovers any holes or weaknesses that can be seen from the public Internet.

  It's also important to address all of the issues identified in an assessment in a timely manner. Because this is such a key issue, it's important for someone outside the IT department to follow up and ensure this takes place.

- **View cybersecurity as an evolving process –** Cybersecurity is never done. Once you have the appropriate controls and processes in place, it's vital to ensure they are maintained consistently and are functioning as intended, and that new risks are being identified and assessed. Cyber risks are always changing, and cyber security should be an evolving process at your organization.

As this article illustrates, there are many ways a cyber breach can occur and there is no one single control or fix that will fully protect your organization. It’s important to implement controls in the layered fashion outlined above so that if one control fails, one or more secondary controls are available to protect your organization against attack.

Cybersecurity is no longer just an issue for the IT department. Nonprofit leaders need to understand the risks and issues to ensure their organizations have sufficient defenses in place.

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.

AN INDEPENDENT MEMBER OF BDO ALLIANCE USA