4 Steps for Next Level Cybersecurity

By Lisa Traina, Partner, Traina & Associates

As recent headlines illustrate, cybersecurity should be a top priority for all organizations. Many nonprofit leaders believe that they have adequate cybersecurity in place, but might not know the specifics. Given the high stakes, it's vital to ensure that your organization has sufficient protection.

The four steps below go beyond the basic cybersecurity practices you should follow to help you further strengthen your organization's cybersecurity defenses.

1. Create and implement a plan for zero-day vulnerabilities.

Zero-day vulnerabilities are security holes without an update or patch available at the time of discovery. According to the Trustwave Global Security Report, vulnerabilities exist for an average of 100 days before being made public. That gives hackers an average of 100 days to exploit them.

Although an astounding number of vulnerabilities are discovered every day, this is a relatively new threat and many organizations don't have a plan in place. An effective zero-day vulnerability plan should detail:

- The sources you will use to stay abreast of new vulnerability discoveries
- Who will be responsible for determining whether your organization is exposed each time a major vulnerability is discovered
- A process for obtaining and applying the necessary patches or updates, if available
- If patches and updates aren't available, a process for following up to obtain them once they are released
- A process for documenting all efforts made to address each identified vulnerability

This can be time-consuming, but a comprehensive plan will help ensure your organization takes the necessary steps every time.

2. Create and implement an Incident Response Plan.

It's no longer a question of if a cyber breach will occur, but rather when. While it's crucial to invest in preventative security measures, it's also critical to plan for how your organization will react and respond to a breach. Start by determining which cybersecurity crimes are potential risks for your organization, and which specific risks could follow from each crime. The plan should then address:

- Forensics: Research and identify a forensic firm now, rather than waiting until a breach happens.
- Timelines for retaining audit and activity logs: Retain at least six months of logs for critical systems so forensic investigations can be conducted. The investigation in at least one recent major breach was hampered because of log retention periods of only 30 days.
- A return to normal operations: Investigations can take time, but your organization must continue to operate. Plan for the fact that normal operations can only resume after you've received assurances that the risk of additional intrusion or data loss has been mitigated.
- Notification of appropriate parties: Identify who you will need to notify, and how you will do so. This includes members, donors, and law enforcement and insurance agencies. Many states have regulations requiring entities to notify individuals of breaches of personally identify information.

3. Undergo routine Information Systems (IS) assessments.

Effective risk mitigation can only occur after you have a list of issues to target. All organizations should undergo a periodic independent IS security assessment that includes:

- Vulnerability testing, in which software is used to scan your internal network and external Internet-facing systems against a database of known vulnerabilities. A known vulnerability is a huge opening for an intruder. The report is then analyzed to determine which systems require updating.
- Information security controls testing, which helps to determine whether the appropriate controls are in place and operating effectively. This might include a test of network authentication, user administration, virus protection, updating and patching, and backup procedures. Such assessments often turn up issues such as missing virus protection, failed backups, confidential information sent via email, and

inadequate password security. Many times organizations believe controls are in place, but testing determines that they are not operating as planned. Frequent examples include web filtering issues and USB drives not blocked according to policy settings.

IS assessments should be performed annually. The external vulnerability assessment is particularly critical, as it exposes any holes that can be seen from the public Internet. Ideally, that assessment should be performed quarterly or even monthly.

4. Develop a formal vendor review process.

With the growing reliance on vendors, it's crucial to recognize the significant cybersecurity risk they can represent. Major data breaches at Goodwill, Target, Home Depot, and Lowe's all started with vendor security issues.

Vendors focus on providing services, not security, so it's important for your organization to have a formal process for evaluating all vendors that provide critical functions or have access to critical data. This should include any third parties that host your data and any vendors with regular access to it.

You should perform an annual review for all current vendors and review all new vendors before you sign a contract. These reviews should assess the vendor's:

- Financial situation (vendors in financial difficulty are more likely to take shortcuts or discontinue services or security measures)
- Data security, including confirmation of vulnerability testing
- Business continuity and disaster planning to assure the availability of your data
- Incident response (include provisions for timely notification of incidents in the contract)
- Information Technology (IT) security controls, including:
  - Strong password parameters requiring complex passwords that expire periodically and strong controls that limit administrative privileges for vendors
  - Multifactor authentication to prevent logins from unidentified devices and new systems
  - Account lockout settings
  - Encryption of data during transmission as well as at rest, which is sometimes treated as an optional feature
  - Limits on which resources vendors have authorization to access
    - An audit trail to identify (by name) individuals who access the systems and what data they could see or change
- Independent IS assessment to provide assurance of adequate security
- Frequency of employee training
- Insurance coverage
- Performance standards
- Service-level agreements (SLAs)
- Compliance reporting

It's also important to ask whether your vendor reviews the security of the vendors it uses and conducts periodic vulnerability testing. You should also ask where your data is stored, as you need to know if it is stored in foreign countries. Vendors often have multiple data centers and backup locations.

Cybersecurity is like cake — the more layers, the better. The steps outlined above will help your nonprofit add strong controls in a layered fashion so if one control fails, secondary controls exist to defend your organization.

About the Author

Lisa Traina, Partner
Traina & Associates, a CapinCrouse Company
ltraina@capincrouse.com
o 225.308.1825

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.

About Traina & Associates*

Traina & Associates, a CapinCrouse company, has been providing information security services, including cybersecurity assessments, consulting, and training services, to financial institutions, nonprofit organizations, medical entities, professional services firms, and other organizations since 1999. Each year the firm performs hundreds of assessment, 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 trainacpa.com.

*Traina & Associates is an authorized trade name of Capin Technology LLC, a subsidiary of Capin Crouse LLP.

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.