CAPINTECH

Top Cybersecurity Myths and How to Overcome Them

By Lisa Traina, Partner

Cybersecurity is a big buzzword today, and the topic is getting much more attention from CEOs and board members of all types of organizations, including nonprofits. The number of breaches and incidents is skyrocketing, and that pattern will continue. So what should nonprofits be doing? How should you address the risk?

The first step lies in understanding the problem. To do so, let's look at two prevalent cybersecurity myths and the steps you can take to help protect your organization.

Myth: My organization is too small or doesn't have data a hacker would want.

Many nonprofit organizations feel they are too small to be a victim of a breach. When you consider that the Target breach began with a phishing email sent to an employee at a small HVAC contractor with connections to Target's systems, however, it's easy to see that the size of an organization does not make it immune. Most nonprofits have electronic connections to others, not to mention that most access bank accounts online.

Many nonprofits also believe they don't have data a hacker would be interested in, but hackers value more than just credit card info. Any record that includes personal information can be sold for identity theft purposes. Usernames and passwords are also extremely valuable, since they can be used to access other systems.

Myth: My organization is well protected.

Many organizations feel that they are fairly well protected, but in reality most are not. Typically, CEOs asked how their organization is dealing with cyber risks will say that the IT department has controls in place to prevent breaches. While this is usually accurate, in our information systems (IS) assessment work across many industries we've seen that having a "good IT department" does not necessarily equate to having appropriate security. We frequently issue reports flagging more than 40 issues to organizations with large divisions of capable IT personnel. That's because IT departments tend to act as firefighters, moving from one issue to the next as they flare up. This leaves little time for maintaining appropriate security. Therefore, one of the most important steps a nonprofit leader can take is to determine which resources are dedicated solely to IS security versus support and implementation, and then ensure a continual dedication to security that is not interrupted by the daily "fires" that arise.

Understanding the Threat

Breaches tend to occur when hackers target a few common technical weaknesses, including phishing, malware, and vulnerabilities. In many cases, a phishing email tricks an employee into clicking on a link or attachment that causes malware, a type of virus, to install on the employee's computer. The malware may lay dormant for quite some time before the hacker exploits a vulnerability or system weakness. These vulnerabilities (holes that hackers can use to get into systems) can be present in laptops, desktop computers, servers, mobile devices, routers, firewalls, and more. This includes the increasing number of devices like vehicles, refrigerators, and coffeemakers that can now connect to the Internet and operate like mini computers. The holes must be filled by patching or updating.

Critical Steps for the IT Department

There are several critical steps nonprofits should take to prevent cyber breaches. Steps for the IT department include:

- Blocking spam so phishing emails don't reach the end user
- Keeping anti-virus and anti-malware software running 24/7 on *every* system
- Continually patching and updating all systems

This may sound simple, but the task of updating systems can be quite time-consuming and daunting. The effort is worth it, though, because these critical steps, combined with traditional controls, can go a long way toward protecting an organization.

Creating a Culture of Security

The necessary steps extend beyond the IT department, however. First, your organization should implement a culture of security so that every individual understands and respects security measures. This means that even the CEO's password must be complex and expire periodically, and many Internet sites must be blocked.
As part of that culture of security, provide frequent training for all employees and stakeholders, including board members. You may be surprised how many people do not understand that clicking on one fraudulent email can result in a major breach. Once employees receive basic explanations, they are generally more careful. We've seen proof of this in the phishing testing we conduct: organizations that provide training have lower click rates on phishing emails than those that do not.

It's also important to consider who should provide the training. It may seem natural to have the IT department do it, but since that group typically does not have the time to devote to security, consider whether the training should be assigned to someone else.

Identifying Existing Risks

Culture, training, and dedicated resources for minimizing malware risks and vulnerabilities are vital to maintaining security. But it's also important to identify any existing risks through periodic independent testing.

This independent testing should involve two main components:

1. Vulnerability scanning to identify any potential weaknesses in various systems
2. An assessment to help determine whether you have the appropriate IS security controls in place and whether existing controls are functioning as designed

True risk mitigation can take place only after a list of issues has been developed, so that you can target your remediation efforts appropriately. The saying "you can't manage what you can't measure" is quite applicable to the cyber risk problem.

Leadership's Role

It's vital for nonprofit leaders to become more involved in understanding cybersecurity issues and risks, so that they can make the right resources available. Cybersecurity should be a major business issue rather than just an "IT issue."

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.