FPLG
FOR PURPOSE LAW GROUP
A Professional Law Corporation

GENERAL

Key Cybersecurity Threats for Nonprofits

11.22.17 | Linda J. Rosenthal, JD

A year ago, in November 2016, we issued a warning in *Nonprofits and Cybersecurity: Make it a Priority*: "Hacking is big news these days. There is a false belief that cyber threats are aimed at major businesses, governments, news organizations and other political targets."

But "[t]he reality is sobering: The risk is much more widespread, and has devastating consequences, financially and legally. 'Cyber threats are a factor for any organization with digital record-keeping. Hackers do not care what you do, only whether you have records they can harvest.'"

In that November 2016 post, we described the devastating experience of one small nonprofit, the Utah Food Bank. In a single cyber attack, "'hackers stole personal and financial data of over 10,000 donors: names, addresses, email addresses, and credit card numbers.' Even if you're not Harvard University, cybercriminals may be coming after you."

Cybersecurity Complexity

Unless you've been living under a rock, you know by now that the "hacking" threat is more pervasive than anyone previously thought.

A huge obstacle to taking precautions is the highly technical, complex nature of this 21st-century crime. Most people, including nonprofit board members and senior staff, know they should tackle cybersecurity right away, but whenever the issue is raised, all they hear is, "Blah, blah, blah, computer, blah, blah, back door, blah blah …."

One cybersecurity expert, Lisa Traina, CPA, breaks through this jargon barrier by explaining: "While cyber breaches can take many different forms, they typically occur when hackers target common technical weaknesses." She says the three most common threats for nonprofits are: phishing, vulnerabilities, and malware.

Phishing

Among the most high-profile commercial cyber attacks making big headlines recently are the security breaches at Target and Home Depot. They were examples of a technique known as "phishing." This method is used as well against nonprofits, large and small, including universities and churches.

"The word phishing was coined around 1996 by hackers stealing America Online accounts and passwords. By analogy with the sport of angling, these Internet scammers were using e-mail lures, setting out hooks to 'fish' for passwords and financial data from the 'sea' of Internet users."

These days, phishing is done by sending out "fraudulent emails designed to entice the recipient to click on an attachment or link or share sensitive information. This opens the door for cybercriminals to infect your computer systems with malware, steal sensitive data, or trick the recipient into an action such as wiring funds."

The phony emails look legitimate: They appear to be from "believable sources such as banks, credit card companies, package delivery services, or internal parties like your executive director or CFO." A more particularized form of this scam is "spear phishing": It focuses on specific people or businesses the target knows, sometimes using details gleaned from online posts and social media activity.

Periodic tests for phishing and consistent employee training may help reduce a target's risk, but even with a filtering system designed to stop these emails, some can "slip through even the best systems."

Vulnerabilities

Another method of cyber attack is benignly referred to as "vulnerabilities." These intrusions are the opposite of innocent activities: the huge Wannacry ransomware attack is an example.

In that case, it was "[j]ust days after President Trump signed a much-anticipated executive order on cybersecurity, a massive cyber attack — potentially the largest the world has ever seen, with more than 75,000 ransomware attacks in 153 countries — stole headlines." The 'WannaCry' ransomware program hit organizations around the world on Friday, May 12, encrypting computer files and demanding roughly the equivalent of $300 in Bitcoin (increasing over time) to restore user access.

Vulnerabilities are "holes in software code that hackers can use to gain access to a system. These holes can exist in all software, including operating systems and applications such as Java and Adobe Flash."

There are regularly issued updates and patches that can prevent these vulnerabilities, but an organization must be diligent in applying them as soon as they become available. However, a "staggering number of vulnerabilities are discovered every day."

"These are known as zero-day vulnerabilities because an update or patch isn't available at the time of discovery. That's why it's important to create and implement a plan for zero-day vulnerabilities."

Malware

“Malware” is computer-geek shorthand for “malicious software,” a catch-all term that includes “viruses, spyware, worms, and ransonware.”

A malware attack begins when someone – generally unknowingly – “visits an infected website or clicks on a link or attachment in a phishing email. It can wreak havoc on every device and system: desktops, laptops, networked printers, mobile devices – even ‘internet-connected “smart devices” such as thermostats and alarms.’”

Perhaps the most insidious aspect of a malware attack is that it can “lay dormant on a system for a long time before the hacker uses it to exploit a vulnerability or system weakness.” Worse still, it’s a “do-it-yourself” dream, available easily online for anyone aspiring to a career as a cybercriminal.

Conclusion

Because of the significant – and undeniable – threat, cybersecurity must be put at or near the top of the list of all nonprofits’ risk-management strategies.

— Linda J. Rosenthal, J.D., FPLG Information & Research Director