Cybersecurity: Not Just for Home Depot Anymore

Nonprofits are increasingly being targeted by hackers. Here's why, and what you need to do.

By Craig Blackman & Jana Landon

We're bombarded every day with a new headline regarding another cyberattack that seems bigger than the previous one. While the focus is on large hacking incidents that affect millions of consumer or patient records, other, less-publicized violations have involved nonprofit organizations, and these attacks are increasing.

While all organizations have to be wary of data breaches, small and midsized nonprofit organizations in particular are likely to be easy targets for cybercriminals. There are four main reasons:

1. **The hackers may be looking for "quick hits" of data** to sell. Nonprofit organizations often have high-value donor, client, and employee data, and many nonprofits don't have internal controls or security in place.
2. **Hackers may want to use a nonprofit's site to advance** their own agenda. Some hackers are looking for easy targets for "advertising," and organizations without robust security programs are a convenient landing place. A hacker may take over a group's website to post its own content and make it difficult or impossible for the organization to retrieve its original website content.
3. **Hackers may want to undermine the viability of the organization** and its mission. They may want to release the organization's information, embarrass the organization, and cripple the public's confidence in the organization. (This was the case when Planned Parenthood was attacked by anti-abortion hackers and when Colonial Williamsburg was hacked days after the director offered to help Iraq safeguard at-risk artifacts.) Even if a hack is simply a website takeover, the targeted nonprofit is suddenly forced to expend resources to remedy the attack — resources that could be going to support the organization's mission.

> "Small and midsized nonprofits are likely to be easy targets for cybercriminals."

> “Nonprofits often have high-value donor, client, and employee data.”

4. **The latest trend in data breaches is potentially the most troubling** for nonprofits: In these cases, the organization’s data or resources aren’t used, sold, or disclosed, but rather the entire IT infrastructure is held for “ransom.” Often, a hacker will contact a victim and demand payment, sometimes substantial, to restore the hacked information. And there’s no guarantee the information will be restored after payment.

Many nonprofits haven’t seen themselves as targets of cyber threats and therefore haven’t invested in robust security software and protocols. In fact, banks, retailers, and other obvious handlers of consumer data may be harder to hack than nonprofits, precisely because they know they are targets. Fortunately, once you appreciate the seriousness of the risk, you can take steps to minimize it.

Have a Plan in Place

Create and regularly update a robust cyber incident response plan, which should include a public relations and notification component. The plan should address who needs to be notified of a data breach (for example, certain states require that individuals be notified within a certain time frame) and lay out who will be responsible for delivering the message to the public and which channels will be used to convey it. Your organization should also consider engaging an attorney early in the process to guide you through any legal or regulatory obligations and spearhead any internal investigation that you may undertake.

Manage the Risk before an Attack

If you don’t do so already, back up critical information regularly (at least once a day) on a server (or even a drive) that is separate from your day-to-day work environment. If your system goes down, you should have ready access to critical files to minimize work disruption.

Recognize that cyber risk isn’t limited to business- or client-related data. People use work e-mail and their mobile devices to discuss personal matters or share observations that they wouldn’t want made public. While it’s helpful to have strong detection and technological intervention when a hack occurs, it would be even better not to have the embarrassing e-mails in the first place. Every organization, regardless of size, should have e-mail best practices in place and should engage in top-down training for employees.

An organization should pay close attention to how employees use e-mail, the Internet, and social media. Employees should be cautioned not to click on suspicious links, enter unknown websites, download unfamiliar software, or watch videos on the organization’s computers.

In the end, the organization must weigh the obvious benefits of utilizing technology to further connections, reach donors, and otherwise fulfill the organization’s mission against the possibility that such utilization may give hackers additional doors into IT infrastructure. Some organizations, especially those that deal with personal health information or personally identifying information, such as financial information, may decide that a complete ban on certain technology (such as social media) is appropriate. Others may want to limit sites to only some members of their organization, or to have their IT group maintain strict controls to monitor for viruses on the sites that are visited.

Consider Cybersecurity Insurance

Many organizations are looking to insurance to cover costs associated with a data breach. There are two options available to most organizations: attempting to find coverage under a standard commercial general liability (CGL) policy or procuring a specific cyber insurance policy.

Claiming coverage under a CGL policy for a data breach is difficult. CGL policies were originally designed to protect for bodily injury and property damage and haven’t been tailored to cover losses related to cyberattacks.

Insureds haven’t found much sympathy with courts when bringing cybersecurity claims under CGL policies: Many courts have required claimants to show physical harm or damage to a “tangible object,” which is often difficult in cyberattack circumstances.

Further, many CGL policies now include an exclusion that expressly bars coverage for damages related to any access or disclosure of, among other things, “patents, trade secrets, processing methods, customer lists, financial information, credit card information, health information, or any other type of nonpublic information.” In other words, these policies exclude coverage for damages related to most of the information that is compromised in data breaches. This exclusion is likely to become a more common feature of all CGL policies, and while this may take some time, this move by insurers demonstrates that in the future policyholders will have an almost impossible task if they try to claim cyberattack coverage under CGL policies.

With CGL exclusions limiting coverage and insurers fighting data breach claims under CGL policies, it is no surprise that the use of specific cyber insurance policies is on the rise. These policies have been available in some form for almost 20 years, but they are only now gaining prominence.

These policies fill the gaps in traditional coverage and often offer first-party coverage for direct costs associated with a data breach, such as a forensic investigation, business interruption, and computer and data loss. They also cover certain risks from third parties:

- damages allegedly related to privacy liability — for example, claims from individuals whose health or financial information was exposed
- network liability, such as claims regarding inadvertent transmission of viruses to third parties if your network was infected
- Internet media liability — for example, costs associated with lawsuits involving claims that your organization committed defamation, libel, or slander, which may arise in cases allegedly resulting from the release of questionable internal e-mails.

Cyber insurance coverage is not standardized and is untested by most courts, leaving insureds with little assurance as to their level of protection. In one case, for example, Cottage Healthcare Systems suffered a data breach and requested coverage from its insurance company, Columbia Casualty, under a cyber insurance policy. Columbia, however, alleged that Cottage did not maintain its security controls as required under the insurance policy, leaving the company vulnerable to the cyberattack. Columbia argued that its policy language didn't require it to pay for losses resulting from the attack because of Cottage's failure "to continuously implement the procedures and risk controls identified in the Insured's application for this insurance."

This case demonstrates the need for a nonprofit to understand fully the terms of any cyber insurance policy it procures. Nonprofits should consider having an attorney familiar with such policies review any potential policy before signing.

In the future, organizations of all sizes are likely to obtain cyber insurance policies to fill much-needed coverage gaps, even if these policies are still new to the insurance market. Until then, a nonprofit's best defense is risk management before any data breach occurs. All organizations should assume that it is only a matter of time before they will be the target of a cyberattack and should take steps to identify key assets and take sufficient precautions to protect them.

> "Sometimes the entire infrastructure is held for "ransom.""

Craig R. Blackman (cblackman@stradley.com) is co-chair of Stradley Ronon Stevens & Young's insurance practice group and a member of the firm's nonprofit & religious organizations' practice group. Jana Landon (jlandon@stradley.com) is counsel in Stradley Ronon Stevens & Young's Philadelphia office and founder and chair of the firm's e-discovery team.

Control Your Risks

For more ways to mitigate risks, see these articles at NonprofitWorld.org:

Setting Up a Control System for Your Organization (Vol. 16, No. 3.)

Can Your Organization Afford to Lose $100,000? Safeguards Every Nonprofit Needs to Implement (Vol. 30, No. 3)

Avoid Catastrophe by Addressing Cyber Risk (Vol. 33, No. 3)

How to Prevent an Information Disaster (Vol. 23, No. 1)

New Internal Control Guidance: What You Need to Know (Vol. 28, No. 1)