Resources

Cybersecurity: Not Just for Home Depot Anymore

August 31, 2015
By: Craig Blackman and Jana Landon

Summary: Don't assume you're immune to a cyberattack just because you're not Target or Sony. Nonprofit organizations can be attractive, lower-profile targets for hackers. Associations should take steps to protect themselves and consider insurance options to cover losses if a breach occurs.
Rating: Rate This Item
0 Comments

We are bombarded every day with a new headline regarding another cyberattack that seems bigger than the previous one. The names alone—Sony, Target, Home Depot, Anthem, the Internal Revenue Service, the Office of Personnel Management—can send shudders down the most seasoned IT manager's spine. Last year was rightly named the "year of the data breach," and 2015 may outpace it: A recent study found that more than 40 percent of U.S. companies surveyed experienced a data breach of some sort in the past year.

While the media focuses on large hacking incidents that affect millions of consumer or patient records, other, less-publicized attacks have targeted not entertainment giants or major retailers but nonprofit organizations. A few recent examples:

- In September 2014, Goodwill Industries was hacked using the same software that struck Target and Home Depot. Goodwill franchises in 19 states and the District of Columbia were affected, totaling 330 stores. An estimated 868,000 credit and debit cards were compromised.
- In March 2015, the director of Colonial Williamsburg made an offer to help Iraq safeguard at-risk artifacts. Just days after the offer was announced, the Colonial Williamsburg website was hacked.
- In April 2015, the website of a small Alabama nonprofit, the Red Barn, which provides education and opportunities for people who work with horses, was attacked by an Islamic State sympathizer. The hacker posted pro-Islamic State messages, along with an image of a person holding an assault rifle. An expert noted that the Red Barn was simply unlucky; its site provided easy access for the hackers. It was not deemed to be a direct attack on the nonprofit or its mission.
- In July 2015, Planned Parenthood informed federal investigators that anti-abortion hackers had

accessed its website databases and the names and email addresses of employees. One of the hackers stated publicly that the attack was motivated by Planned Parenthood's politics. In a separate attack that same month, Planned Parenthood's website was hit by a so-called denial-of-service attack: The site went down after it was flooded with traffic to keep users from accessing it.

While all organizations have to be wary of data breaches, small and midsize nonprofit organizations in particular are likely to be easy targets for cybercriminals for a variety of reasons.

First, 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 of these organizations do not have internal controls or security in place. They also often have special relationships with their donors and rely on the goodwill they generate with that base. When a hack that compromises donor data happens, trust is shattered and may be difficult to regain.

Second, hackers may want to use a nonprofit's site to advance their own agenda, as in the Red Barn example. Some hackers are just looking for easy targets for "advertising," and organizations without robust security programs are a convenient landing place. A hacker may take over an organization's website to post its own content and make it difficult or impossible for the group to retrieve its original content.

Third, they may want to undermine the viability of the organization and its mission. As was the case in the Sony hack, releasing information, undermining confidence, and embarrassing organizations are all reasons that hackers may look to compromise data. 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.

Finally, the latest trend in data breaches is potentially the most troubling for nonprofits: In these cases, the organization's data or resources are not used, sold, or disclosed, but rather the entire IT infrastructure is held for "ransom." For example, in May 2015, a staff member at First Presbyterian Church of Birmingham, Michigan, opened an email from a supplier saying that a bill had not been paid and the account would be disabled. She clicked on an attachment purporting to be the invoice, but it actually launched a type of malware called ransomware, which locked the church's server and corrupted it. Although no payment was reported, the church had to rebuild its system from a backup copy of its server.

Similar situations have been on the rise across the nation. 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 have not seen themselves as targets of cyber threats and so have not 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

Nonprofits should make 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 do not do so already, consider regularly backing up critical information 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 is not limited to business- or client-related data. People use work email and their mobile devices to discuss personal matters or share observations that they would not 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 emails in the first place. Every organization, regardless of size, should have email best practices in place and should engage in top-down training for employees.

Consider Cybersecurity Insurance

In addition to planning and training, many organizations are also 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, property damage, and personal and advertising injury and have not been tailored to cover losses related to cyberattacks. Insureds have not 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 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 emails

Cyber insurance coverage is not standardized and is untested by most courts, leaving insureds with little assurance as to their level of protection. For example, in a recent case, 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 did not 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, which is still pending, 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, businesses and other 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.

Craig Blackman cochairs the insurance practice group at Stradley Ronon Stevens & Young, LLP, in Philadelphia. Jana Landon chairs the firm's e-discovery and cybersecurity group. Email: cblackman@stradley.com, jlandon@stradley.com.

☆☆☆☆☆
Simply click on a star to rate this item.
Comments:
Write A Comment

Top ^
To Articles Index
To ASAE home

ADVERTISEMENT

American Society of Association Executives™ (ASAE), 1575 I St. NW, Washington, DC 20005, P. 888.950.2723, F. 202.371.8315 or P. 202.371.0940 (in Washington, DC). © Copyright 2014 ASAE. All rights reserved.