Build Your Cybersecurity Breach Defenses Before It's Too Late

By Rachel Sams

Lead Consultant and Editor

Resource Type: Risk eNews

Topic: Data Privacy, Tech Risk, Cybersecurity

When a cybersecurity breach hits your organization, it's too late to build optimal defenses. Your best opportunity to protect your nonprofit's data exists now.

It's tough for any nonprofit to prepare for a crisis that hasn't happened yet. Staffs and budgets are stretched thin everywhere. But with a reasonable amount of time and effort, you can strengthen your nonprofit's ability to deal with a breach if it happens.

That's time well spent: Microsoft's 2021 Digital Defense Report found that non-government organizations and think tanks were the second-most-targeted sectors by cybercriminals. And the average organizational data breach in 2021 cost $4.24 million, according to IBM.

Matthew Eshleman, Chief Technology Officer at Community IT, which provides tech support to nonprofits, urges organizations to create policies that define requirements around passwords, mobile devices, multifactor authentication and more. Nonprofits should also ask their IT providers how they manage user access to systems; providers should have a set of security practices they can share with clients. And nonprofits should make a written outline of who would respond in a breach and how.

"Be able to articulate that beforehand so organizations aren't trying to build all of that on the fly whenever something happens," Eshleman said. "It's always a good idea to document that and make sure that your incident response plan is available in an offline place in case your systems are impacted."

October is National Cybersecurity Awareness Month. Below are some tips to build resilience in advance of a cybersecurity incident. If your organization begins work on these items in October, you could have at least a rough plan to handle a breach by year's end—and wouldn't that help you sleep better at night?

Identify who your nonprofit will call if a cybersecurity breach occurs.

Cyber insurance providers often have "breach coaches" who can lead an insurance response for nonprofits, Eshleman said. Put your legal counsel on the list of people to call, along with any cybersecurity law or forensic experts your counsel recommends. Your list might also include your information technology and security vendors, operations, human resources, communications, and management.

Know where sensitive data lives on your systems, and identify your first steps with hardware and software in a breach.

Identify what sensitive data your nonprofit collects and where it is stored. Train multiple people on your staff on how to bring any affected equipment offline right away in a breach. Create written protocols that inform staff not to turn off machines until forensic experts arrive, and not to delete or destroy anything that provides evidence of the breach. You'll also need to update credentials and passwords of authorized system users, and document your steps to preserve evidence for forensic investigations.

Make sure team members and/or vendors know how to remove improperly posted information from the Internet.

If personal information gets posted on your website in a breach, remove it immediately. You'll need to contact search engines to make sure they don't archive any personal information posted in a breach. There are some commercial services that can automate some of this discovery and removal. You'll also need to search for your organization's exposed data to ensure other websites haven't saved or published it. If they have, ask the company to remove it. If the disclosed information includes username and password data for your systems, you'll need to reset the accounts of the impacted systems.

Know how you will communicate information about a breach.

Determine your legal notification requirements. Every state has laws that require notification of security breaches that involve personal information. Other laws may apply as well. Outline a communications plan to inform those who will need to know about a breach: law enforcement, regulators, employees, service recipients, donors, vendors, and other close contacts of your nonprofit. Make sure your team knows not to say anything misleading about the breach or publicly share details that could put people's personal information at further risk.

Have a plan to bring systems back online safely when you can.

Let your team know that you'll need to wait for forensic experts to give you the OK before you bring affected systems back online. Take any additional steps the experts advise to ensure systems are secure against future attacks.

Of course, we hope your organization doesn't need to deploy any of these measures. But with the prevalence of cyberbreaches, at some point it probably will. Prepare now, and that day will be less unpleasant. In the meantime, you'll know that your organization has prepared for a cyberbreach as best it could. Make sure you let your staff know what steps you've taken, too. It will help build their confidence in your organization.

This article is the second in a series. Check out our previous Risk eNews on basic cyberhygiene for nonprofits.

Rachel Sams is a Consultant and Staff Writer at the Nonprofit Risk Management Center. She'd love to know how your organization prepares for cyberbreaches. Reach her at 703.777.3504 or rachel@nonprofitrisk.org.