Are You Prepared for a Cybersecurity Incident?

Here are keys to help you minimize your cyber risks.

By Meghan Tisinger

Exposing outsiders to sensitive and private information is one of the biggest fears organizations face when being hit with a cyberattack. There were 2,365 cyberattacks in 2023 – 27% of which were nonprofits. Sadly, due to sensitive donor information and outdated security procedures, nonprofits are especially vulnerable to devastating cyberattacks.

Those nonprofits that are most confident in their preparedness are often the ones failing to stay ahead of the reputational fallout. Ironically, those with the most exhaustive IT and readiness plans can be the least prepared to communicate with their stakeholders and protect their brand during and after the cyber incident.

Though cyberattacks are a nearly everyday occurrence, how the incident is managed – and how much damage to a brand's reputation occurs – has to do with how an organization engages with its stakeholders. Responses to a cyber incident can make or break donor trust in your organization. Here are tips for building a strong cybersecurity response in advance of an inevitable data breach.

Build a Culture of Awareness

One of the main challenges leaders face is ensuring that every employee understands cybersecurity risks. Many of us have been desensitized to data breaches over the years by receiving letters and e-mails alerting us to potential data exposure. Thus, few employees understand the implications to the entire organization if they fall for a phishing attack or share sensitive information.

Many times, it feels as if the IT personnel are speaking another language and the warnings are lost on those who don't consider themselves tech savvy. You can remedy this situation by holding security training sessions that speak to the employees at their level and address the unique needs of different roles within your organization.

In addition to training, you can build a stronger cybersecurity culture by creating a safe space for employees to work together, across departments, to understand, identify, and report security threats. The first step is helping all understand that they play an important role in maintaining cybersecurity. Send e-mails, hold team meetings, and talk

to each person about the protocols for reporting potential cybersecurity incidents.

Take Advantage of Peacetime to Solidify Your Team

If you have cybersecurity insurance, your coverage likely includes working with an outside law firm, forensic firm, and communications specialists during a cyber incident. What this means is that during a cyber breach, you'll receive a list of vendors that are covered by your insurance. As great as this is, valuable hours are wasted by interviewing law firms and communications firms when that time could be used to build your legal and communications response. Instead of waiting to interview the firms, reach out before you need them and schedule time to speak. This is a common practice so this request won't be seen as overstepping, and it's a free, introductory call. If you establish these relationships before a crisis occurs, then you can spend those precious initial hours doing the work instead of establishing the team.

Some of the most successful responses to data breaches occur when organizations work with cyber specialists *in advance* of a cybersecurity incident. This allows the cyber-security team to do a deep dive into the organization's culture, risks, key stakeholders, and tone of voice – allowing for seamless integration of their team amidst an active cyber matter. As a result, the response to the crisis is faster.

Assess Your Risks

What is the most dangerous, detrimental information that a threat actor could steal? What's the worst-case scenario? Is there a way to access information if the computer systems are locked down?

Answering those questions will help establish risks that you can address before an attack. Knowing the worst possibility can lessen the surprise and prepare you for what could happen.

Create a Strategic Cyber Plan

Knowing your risks and developing a strategy to address them are two very different things. The key to protecting a brand and reputation during a cybersecurity incident is to have a plan in place that can be adapted to reflect the realities of the situation. The plan should include who is on the response team, how information is escalated, who is leading the communications, and who will answer any media request. Having defined roles and responsibilities removes the guesswork and drama during an active incident.

Another side of cyber risk planning is to pinpoint critical stakeholders who you'll need to contact if the risks come to fruition. Knowing who these people are and how to communicate with them is crucial to ensure that no one is forgotten.

The planning phase is also the time to inform – or remind – your entire staff about media and social-media policies. During an active incident, media may contact employees for comment via e-mail or through their social accounts. It's vital that staff members know not to speak to the media but, rather, to refer all questions to one designated person.

Prep Communications Materials & Spokespeople in Advance

In the middle of a cybersecurity incident, there isn't a lot of time to sit and write the perfect media statement. That's why it's necessary to draft statements, talking points, and FAQs for various stakeholders that address many potential situations. Take your list of stakeholders and draft messaging

> "Nonprofits are especially vulnerable to cyberattacks."

> "Establish these relationships before a crisis occurs."

that will go to them. The messages should be similar between groups to ensure consistency, but the communications platform may differ. One audience might receive a phone call, which would require a script or talking points. Another audience might receive an e-mail. There should also be extensive communications drafted for employees because they're the first call that donors will make.

Think of these pre-written communications assets as Swiss-cheese materials. They'll have holes that need to be filled in but will serve as the foundation for all of the communications that are needed.

It's also critical that any communications materials be thoroughly vetted by legal and communication professionals. A cyber incident is different from other crises because the likelihood of litigation following the incident is higher. A statement that isn't approved by legal counsel is dangerous because those words could be used against the organization in a lawsuit.

Another great advantage of proactive planning is that leaders or any designated spokesperson can be media trained or coached before they're thrown into the lion's den. Addressing the press in a crisis situation is very different from everyday media relations. Conducting media coaching sessions during peacetime will equip the spokesperson to understand the media agenda, prepare for interviews, and frame and deliver the best messages.

Manage Social-Media & Website Content

During a cyber breach, external stakeholders turn to online content for information. To be sure they find helpful information, conduct regular audits of your website and social-media channels. If there is content bragging about internet safety or anything that can be misused by the media or critics, it should be taken down. Keeping a good handle on scheduled posts is also essential to make sure there aren't any posts that could affect your organization's reputation during or after an incident.

Another thing you can do before an active incident is to ensure that the right people have the right access to accounts. Too many people must reset accounts when they learn during a cyberattack that they don't have access to the administrative settings on their organization's accounts. Resetting an account could take days. As a result, your social platforms could experience harassment by the threat actor without a recourse from the organization.

Stay Safe

It's always better to take the time needed to prevent a crisis than to scurry to save your organization after disaster strikes, as these articles (NonprofitWorld.org) attest:

Mitigate Cyber Risks with the Right Security Controls (Vol. 36, No. 1)

Hacking People: Why Your Biggest Vulnerability Isn't in Your IT Department (Vol. 37, No. 1)

Don't Get Caught by Phishing Schemes (Vol. 35, No. 2)

Risks Get Riskier for Nonprofits: ERM Can Help (Vol. 38, No. 1)

The Purposeful Techie: Nonprofit IT with Intention (Vol. 30, No. 5)

Keep Your Online Identity Safe (Vol. 35, No. 4)

Planning for the Quiet Disasters: Technology Mishaps (Vol. 40, No. 3)

What to Do When an Employee Becomes a Cybercriminal (Vol. 39, No. 4)

Wire Transfer Fraud: It Could Happen to You (Vol. 35, No. 3)

When You're Forced to Say "No Comment" (Vol. 22, No. 4)

Avoid Internet Dangers: Practice Safe Surfing & Defensive E-Mail (Vol. 39, No. 3)

Dealing with Viruses & Other Disruptions (Vol. 38, No. 2)

Are You Prepared for a Cybersecurity Incident? (Vol. 38, No. 4)

Five Technology Pitfalls for Nonprofits: Finding Cost-Effective Solutions (Vol. 25, No. 1)

Get Help

If you're like most nonprofits, your budget doesn't allow for a full-time cyber communications professional. That's why you need to seek external expertise to ensure that messaging and communications won't break the trust donors have in you and your mission. Outside legal and communications support will also assure that the communications and legal strategy are kept current with the ever-evolving landscape of cybersecurity issues.

It's no longer "if" an organization will be attacked but "when." The only "if" is if your organization will survive the cybersecurity incident with your reputation intact. By planning ahead, you have the opportunity to focus on the important work instead of drowning in a crisis.

Meghan Tisinger (meghan.tisinger@leidar.com) is managing director of Leidar, an international communications firm specializing in crisis communications, media relations, and strategic communications.