Cybersecurity for Nonprofits

If your nonprofit engages in any of the three activities below, it’s time to get serious about taking steps to address cybersecurity risks. Does your nonprofit:

1. Conduct e-commerce on its website, such as processing donations or event registrations?
2. Store and transfer (such as by sending to the cloud) “personally identifiable information,” about anyone, including donors? (Common examples of personally identifiable information include: clients’ medical information; employee records, including drivers’ licenses, addresses, and social security numbers.)
3. Collect information on preferences and habits of donors, patrons, newsletter subscribers, etc.

If so, there are real risks to your nonprofit's own data security as well as to its donors, and individuals it serves. Learn more about protecting the future of your nonprofit's data.

US nonprofits that raise money in the European Union, or provide services to citizens of the EU, AND collect data about those citizens, must follow the EU's General Data Protection Regulations.

- What is GDPR and why should you care? (Wired)

- The EU data-privacy law that may affect US nonprofits (For Purpose Law Group)
- Nonprofits can't afford to ignore the GDPR (BDO)

What are the risks? What should we do?

Data breaches that are both *likely to happen* and can *result in serious harm* fall in the “high priority” category. Many nonprofits collect and store sensitive personal information that is protected by law as confidential. When there is a breach of the confidentiality of those data, that poses a risk for the individuals whose data was disclosed, AND for the nonprofit that will now potentially be subject to liability for the breach. It makes sense for EVERY nonprofit to - at a minimum - assess the risks of a data security breach, and protect its data from unauthorized disclosure.

- Begin the Conversation: Understand the threat environment (US Dept. of Homeland Security)
- StopThinkConnect toolkit (US Dept. of Homeland Security)
- It's 2018: Do you know where your nonprofit's cybersecurity is? (Nonprofit Quarterly)

First Step | Risk assessment

The Nonprofit Technology Network (NTEN) suggests that the first step in assessing your nonprofit’s data risks is to take inventory of all the data your nonprofit collects and identify where it is stored. NTEN offers a template assessment tool. These inventory tools ask: *What data do we collect about people? What do we do with it? Where do we store it? Who is responsible for it*? Think about the cost/benefit of maintaining all that data. You may find that there is data your nonprofit is currently asking for and keeping that it *doesn’t really need*. If so, reducing or limiting the data that your nonprofit collects, and streamlining the storage process (as well as diligently destroying data in accordance with the nonprofit’s document retention policy) could be easy first steps towards mitigating risk.

Second Step | Are the data your nonprofit maintains "protected" or "confidential"?

Second, know whether the data your nonprofit collects and maintains is covered by federal or state regulations as "personally identifiable information." If so, forty-seven states' laws require nonprofits to inform persons whose "personally identifiable information" is disclosed in a security breach, and 31 states have laws that require disposal of such data in certain ways. Additionally, the Federal Trade Commission's Disposal Rule also requires proper disposal of information in consumer reports and records to protect against "unauthorized access to or use of the information." Protecting personally identifiable information is all about training staff how to collect/store/dispose of and generally protect this data.

Even if you are collecting data that doesn't rise to the level of "personally identifiable information," such as a community theatre collecting information on attendees' preferences for plays or musicals, a breach of that data can be harmful to the organization's reputation and ability to bring in contributions. All data reflecting personal preferences are important to keep secure.

Third Step | Drill down on the actual risks

Third, consider using the US National Institute of Standards and Technology (NIST) Cybersecurity Framework to help your nonprofit identify risks, and make management decisions to mitigate those risks. This framework is not intended to be a one-size-fits-all approach but to allow organizations to manage cybersecurity risks in a cost-effective way, based on their own environment and needs.

Take a look at the likelihood of some cybersecurity risks: What is the risk of a third party compromising your nonprofit's data security? Many nonprofits use outside assistance, such as an outsourced bookkeeper, IT consultant, payroll service, or even a cloud storage service. If any of these third-party vendors do not employ adequate data security protection, the nonprofit's data security will be at risk. Other types of third-party access might include a donation processing service or any outside professionals with authority to access the administrative side of your nonprofit's website or shared electronic files. Consequently, when hiring third-parties for any projects that involve data access by the vendor, make sure that you are satisfied with the firm's data security protocol. Here is a set of questions developed by Digital Impact.IO as a starting point for questions to ask the vendor about their approach to data security.

How likely is it that hackers will take over your nonprofit's website?

Hackers can access your nonprofit's site through a security breach, and transform it into something you would not recognize, like an online pharmacy. *How likely is this to happen*? That depends on the strength of the security of individual nonprofits' websites and how consistently users follow strong password protocols. *How serious are the risks*? Typically, the main website remains intact, but the hackers create additional content that can't be good for your nonprofit's reputation – or Google analytics. So, on balance, a site takeover does not create the same type of liability risks that other security breaches do, but cleaning up the mess can be time consuming *and costly*. Managing these risks is much like brushing your teeth. We all need to get in the habit of keeping software updated and being vigilant about usernames and passwords (example: Using "admin" as a user name creates vulnerabilities, say the experts.) Regular maintenance can go a long way towards reducing this and other data security risks.

What about cyber liability insurance? Is it needed?

Insurance policies are available to cover losses from breaches affecting a nonprofit's own information and losses affecting third parties' information (such as patients/clients, and donors). The types of losses/expenses that cyber insurance can cover range from the cost of notifying all the folks whose information may have been comprised; to the cost of content repair, such as repair to a hacked website; to the cost of hiring a PR whiz to help your nonprofit recover its reputation after a severe security breach. There are even some policies that address business interruption in the event a cybersecurity breach is so severe that it forces the nonprofit to temporarily suspend operations (an unlikely outcome, according to some experts.) Your state association of nonprofits may be able to help you identify an insurance professional with expertise in providing insurance for charitable nonprofits.

According to the Nonprofit Risk Management Center, there are three keys steps to take before deciding whether to purchase cyber-liability insurance: (1) Understand how a breach of privacy claim could affect your nonprofit; (2) Work with a

knowledgeable insurance agent or broker who not only understands how different cyber liability policies differ in their coverage, but also understands your nonprofit's operations and activities well enough that s/he can break down your nonprofit's exposures with you. Choosing insurance products should be a collaborative effort with your nonprofit's broker/agent; and (3) as with all insurance, take a hard look at the cost of the annual premium.

Yes, the idea of someone hacking your nonprofit's website or data storage is unnerving, but in today's world such incidents have become practically commonplace. Failing to assess and address cybersecurity risks is like failing to brush your teeth: Would you rather change a password or go to the dentist?

Remember that your state association of nonprofits may offer special workshops or educational programs on this topic and may have relationships with experts who can assist your nonprofit with cybersecurity maintenance and best practices.

Related Insights & Analysis

- Protect the future of your nonprofit's data (National Council of Nonprofits)
- New website security warnings raise the bar for nonprofits (National Council of Nonprofits)

Additional Resources

- Cybersecurity Strategies for Nonprofit Websites (NTEN)
- Data Privacy and Cyber Liability: What You Don't Know Puts Your Mission at Risk (Nonprofit Risk Management Center)
- Nonprofit Cybersecurity Insurance Checklist (TechImpact)
- Top Ten Cybersecurity Tips for Nonprofits: Managing your technical and legal risks (Venable, LLP)
- What nonprofits need to know about security: A practical guide to managing risk (TechImpact)