akerman

Practice Update

Online Resources Help Nonprofit Organizations Prepare for Cybersecurity Threats

November 7, 2018
By Elizabeth F. Hodge

Nonprofit organizations often collect personal information from a variety of sources such as donors, employees, volunteers, and the people who benefit from their services. This information is diverse and might include credit card and personal contact details of donors, financial and health information about the people served by the organization, and payroll and other employment information of its employees. The information collected and retained by nonprofit organizations is exactly the type of data cyber criminals pursue.

The effects of a data breach could be disastrous for a nonprofit organization, not only because of the harm to the affected individuals, including those served by the organization, but also the crippling impact it could have on day-to-day operations. A security incident can also damage the organization's reputation and ability to raise funds. Mitigating a data breach – which could include hiring network forensics investigators, retaining legal counsel, and sending breach notification letters to every person whose data may have been compromised – can get expensive quickly. Moreover, an organization's own unintentional release of sensitive information could have consequences as serious as a security breach caused by a scammer.

Related People

Elizabeth F. Hodge

Related Work

Tax-Exempt Organizations

Related Offices

Fort Lauderdale
West Palm Beach

Yet, often due to the nonprofit model, resources that could be used to proactively address cybersecurity threats may be allocated elsewhere. Even if resources are dedicated to cybersecurity, cyber criminals may perceive nonprofits as "soft targets." Unfortunately, an organization's nonprofit status does not shield it from enforcement actions by government regulators such as the Federal Trade Commission (FTC) and the U.S. Department of Health and Human Services Office for Civil Rights (OCR), when the organization fails to safeguard the privacy and security of personally identifiable information it maintains.

To help small organizations with their efforts to safeguard data, the FTC released an alert on October 25, 2018, with new cybersecurity resources specifically for nonprofits and small businesses. The FTC resources, available at FTC.gov/Cybersecurity, aim to help organizations protect the information they collect from people. The resources include to-the-point downloadable materials, online quizzes, and links to additional resources covering a number of topics, including:

- Implementing cybersecurity basics such as setting automatic updates for operating systems, web browsers, and apps; regularly making secure back-ups of important files; and ensuring routers are not using outdated encryption.
- How to identify, avoid, and address ransomware and phishing attacks.
- Monitoring vendors who have access to the organization's data to make sure that they are securing their own computers and networks.
- Implementing physical security to protect equipment, devices, and even paper files.
- Securing remote access so when employees or vendors need to connect to the organization's network remotely there are security measures in place as well as guidance for staff on using those measures.

- Understanding the National Institute for Standards and Technology (NIST) Cybersecurity Framework so nonprofits and small businesses can better manage and reduce the cybersecurity risks to their networks and data.

Related online materials provided by the FTC, "Protecting Personal Information: A Guide for Business," give guidance on developing a data security plan based on five key principles:

1. know what personal information is stored on the computers;
2. retain only the data that is necessary;
3. protect the information that is kept;
4. properly dispose of the data when it is no longer needed; and
5. create a plan to respond to security incidents before a breach occurs.

Additionally, with a focus on HIPAA, the U.S. Department of Health and Human Services has prepared on-line Cyber Security Guidance Material.

Due to the nature and volume of personal information nonprofit organizations routinely handle, it is critical that they focus on protecting against cybersecurity threats as they continue to serve their communities. The FTC resources offer organizations with limited data security budgets tools to understand and prepare for such threats. Nonprofit organizations should also seek guidance from an attorney in order to reduce their legal exposure from cybersecurity threats.

---

information contained in this Practice Update without seeking the advice of legal counsel. Prior results do not guarantee a similar outcome.