Nonprofits and Cyberattacks "A Constant Challenge"

Speaking with several nonprofit leaders and boards a few years ago, conversations around the likelihood of being hit with a cyberattack appeared to be remote. With limited resources, those leaders often found it difficult to put money into protecting against something that seemed unlikely to happen. Fast forward into 2024, that same group's conversation regarding the peril of cyber breaches and Artificial Intelligence (AI) is everywhere. The persistent and targeted cyberattacks seem to be constant in the news today.

When you consider the type of people who trust nonprofits with their information, e.g., donors, members, wealthy families, students, and employees, it's clear that cybersecurity must be more of a priority – if for no other reason than to limit potential reputational damage should an attack occur.

Not only are there reputational risks, but there are legal risks that can arise if a nonprofit fails to reasonably secure its data. Federal and state laws allow those impacted by a cyberattack to pursue civil liability against companies that have been hacked. This fact, coupled with the reality that many states require companies who've been hacked to notify those affected and provide protection against financial damages or identity theft, means the cost of not having a cybersecurity plan is very real – with exposure coming not just from the hackers.

As such, nonprofit leaders should be working with their cybersecurity firm to ensure their data is protected. The following recommendations include some helpful and cost effective protections to implement. In the end, these steps should be joined with more vigorous cybersecurity defenses supplied by a cybersecurity firm.

Nevertheless, starting small can still help ensure your nonprofit is acting prudently with its electronic information.

1. Regularly update your computer software and operating system. By so doing, the most common cyber threats can be defeated as your software and operating system already know about them and have ways to stop them in place.
2. Require regular password updates and multi-factor authentication for system access. Implementing password policies that require a mix of characters, numbers and symbols, and requiring one extra step before someone signs in to your system will ensure users verify who they are and why they are there. This adds an extra layer of security, making it more difficult to gain access.
3. Backup information regularly to minimize the impact of cyberattacks. The more often the system is backed up to a server in a secure location (onsite or in the cloud), the less of an impact any cyberattack will have. Naturally, ransomware and virus attacks will be neutralized if the information the hackers hope to damage is secured elsewhere.
4. Encrypt Personal Identifiable Information (PII) and other sensitive information. Login passwords, for sensitive information, should be encrypted any time it is transmitted from your system, and even when it is not being transmitted. While this does require purchasing encryption software, such software doesn't have to break the bank for good protection.
5. Train your team on cybersecurity. Not every employee knows what an email phishing scheme is or that third-party vendors can provide a back door to your system for hackers. But, if you take the time to educate them, they can be your nonprofit's eyes and ears, and stop threats before damage occurs because they're aware enough to question suspicious activity.
6. One of the more important factors to not only protecting the data is to establish a plan if the organization is impacted by a cyber issue. An "Action Plan" or a "cyber incident response plan" is a document that outlines the organization's protocols on how to respond to a cyber security incident (i.e. locked out of system by cyber-attack, ransomware data breach, or data leak etc.).
7. Lastly, making sure the organization is properly insured. Bill Dalton, vice president and national practice leader of Assured Partners, recommends working with an industry expert when seeking a cyber insurance policy. The policy should cover a wide set of incident types and provide high sub-limits for funds transfer fraud, ransomware, social engineering, third-party business interruption and more. Also, it's so important to verify that the carrier has proven success in handling cyber incidents - with 24/7 experts available to respond quickly and if needed access to the appropriate remediation team.

Cyber security is a critical aspect of maintaining the integrity and reputation of organizations. Understanding the threats, implementing security measures, and promoting a culture of awareness is critical. Nonprofit leaders must do their part to protect the organization's data. In this day and age, there's no doubt we are all vulnerable to cyberattacks. Unfortunately, the biggest targets are not always the ones with the most to lose. Instead, it is those who don't take cybersecurity seriously – don't let your nonprofit fall into that trap….

Article contributors

Matthew O'Dell, CPA, Partner at COMD

Kim McDonough, Director of Operations at COMD

Brad D. Steele, J.D., is Founder of PCC – and a longtime collaborator with COMD.