THE NONPROFIT TIMES®
The Leading Business Publication For Nonprofit Management

REPRINT OF COLUMN FROM *June, 2022*
The NonProfit Times
TECHNOLOGY

# Cybersecurity Readiness

## *If it ain't broke, you might still want to fix it*

**BY JON DARTLEY, PH.D.**

The quote "if it ain't broke, don't fix it" is widely attributed to T. Bert Lance, the director of the federal Office of Management and Budget during the first eight months of President Jimmy Carter's administration. Lance's aim was to reduce spending by adopting a fiscal policy that focused on essential repairs.

Over time, this colloquialism has come to represent a pragmatic approach to "triage" issues. However, when it comes to implementing cybersecurity procedures, this approach is ill advised. Put another way, the fact that an organization has not yet experienced a security incident should not be a rationale for maintaining the status quo.

It is unfortunate that data breaches are the leading threat in today's digital world, with a new cyberattack occurring approximately every 39 seconds. The financial cost of managing a data breach is well documented. A recent study by the Ponemon Group (https://ibm.co/3KYuhdb) estimates the cost of a data breach in 2021 at $ 4.24 million, a 10% increase from the average cost in 2019.

Nonprofits regularly store personally identifiable information (PII) and confront the same cybersecurity risks as their for-profit counterparts. But recent studies reveal that nonprofits generally lag behind for-profit organizations when it comes to the implementation of the recommended cybersecurity policies and practices. Not only do these practices minimize the risk of a data breach, they also mitigate the effects should one occur.

It's also important to keep in mind that while the financial impact of a data breach is easily demonstrable, less tangible but arguably more significant in the long term, is the potential impact of reputational harm. An organization that suffers a breach will likely experience a loss of trust from its donors, volunteers and the community, with possible negative consequences on its fundraising activities and donor engagement for years to come.

The good news is that vigilance makes a difference, and several simple changes can generate a protective layer around the organization's mission and goals.

### First Step: Risk Assessment

Although cybersecurity is not as heavily regulated as data privacy, it is important for leaders to ensure nonprofits to comply with current legal and regulatory requirements. As recent as July 2019, New York enacted the Stop Hacks and Improve Electronic Data Security (SHIELD) Act, a law that amended the existing data breach notification law and imposes more data security requirements on companies, including nonprofits, who collect certain types of personal information on New York residents.

In addition, it has been suggested that directors and officers of nonprofits might soon

continued on page 2

# Cybersecurity Readiness

continued from page 1

face greater personal liability for breaches of security and their impact on a nonprofit.

For managers seeking to decrease an organization's cybersecurity vulnerability, the first step is to obtain a comprehensive understanding of their current risk environment. The most effective method is by conducting a data privacy audit. The goal of the audit is to ask and answer these questions:

- *What data do we collect about people?*
- *Why are we collecting this data?*
- *Where do we store it?*
- *Who has access to it?*
- *How is it protected?*

The information and insight this kind of audit provides will help managers better manage risks by focusing and prioritizing cybersecurity efforts consistent with the organization's risk management strategy and business needs.


**Second Step: Drill Down On The Actual Risks**

Depending upon the size of the organization and the scope of PII collected, there are a variety of frameworks helpful in conducting such assessments. *Cybersecurity Framework* (https://www.nist.gov/cyberframework), published by the U.S. Department of Commerce's National Institute of Standards and Technology, is commonly used to help identify risks, and make management decisions to mitigate those risks. For example, it can help managers determine whether the nonprofit collects PII, and if such PII is subject to federal or state regulations.

Most states require notification of an unauthorized disclosure, and the majority have requirements for how such PII is deleted. However, while the "Cybersecurity Framework" provides helpful guidance for standards, guidelines, and practices that organizational managers can undertake to better manage and reduce cybersecurity risk, it needs to be tailored for each organization's individual circumstances. Ideally, the results will assist in determining which activities are most important, with the goal of minimizing the risk of a data-security incident.

**Third Step: Address Key Cybersecurity Risks**

By conducting a data privacy audit and utilizing the NIST's "Cybersecurity Framework," managers should be able to develop a better understanding of the cybersecurity risks they confront. The ultimate goal is to focus and prioritize the cybersecurity and data privacy efforts consistent with the findings.

While specific takeaways will vary, there are a few key activities and focus areas that should be addressed. Below I briefly describe these activities and focus areas are briefly described and some guidance is provided regarding their implementation.

***1. Implement (Or Update) Organization-Wide Cybersecurity Policies***

An important step in an organization's data security posture is to adopt and implement a consistent, documented cybersecurity policy which all employees must follow. Employees tend to be the weakest link in an organization's security position, often inadvertently putting organizations at increased risk by their actions. For that reason, cybersecurity needs to be a priority and concern for each employee, not only for its information technology professionals.

An effective way to educate employees on the importance of security is to adopt and disseminate a cybersecurity policy and acceptable use policy. Such policies describe each employee's responsibilities for protecting systems and data within the organization, and what "is" and "is not" permitted in regard to the handling of the data. Implementing such policies is considered a best practice for promoting better cyber "hygiene."

Managers shouldn't stop there. Other policies are required to provide additional safeguards, and to provide a comprehensive framework for protecting the data stored. Those policies include:

• *Data Retention and Deletion Policy*

Most organizations collect more data than they need, and hold the data longer than necessary or practical. The more data the organization stores, the greater the liability if a breach occurs. It is imperative that organizations adopt a policy that dictates the types of data to be stored, and when/how that data is deleted when no longer relevant or useful.

• *Data Breach/ Incident Response Policy*

The goal of a data breach and incident response policy is to describe the process of handling an incident and remediating the impact on an organization's operations and donors. It can also help organizations to comply with applicable laws and regulations, and launch a rapid and coordinated response that will mitigate the damaging consequences of a data breach.

This policy typically defines staff roles and responsibilities in handling an incident, and provides guidance as to specific actions to take and resources to leverage. The SHIELD Act in New York, discussed above, requires organizations that collect certain types of information from New York residents to have both a Data Retention and Data Deletion policy, as well as an Incident Response plan in place, among other requirements.

• *Remote Access Policy*

According to an IBM study (https://ibm.co/3w5NiGr), remote work during COVID-19 increased data breach costs in the United States by $137,000. While many managers are focusing on getting employees back to the office, most will likely adopt a "hybrid" model where some remote work is more common. As such, it is wise to implement a remote access policy that outlines and defines procedures for remote access to the organization's internal networks, and provides additional guidance as to expectations regarding cyber practices for their home offices.

• *Privacy Policy*

A privacy policy is a statement that discloses all of the ways an organization gathers, uses, discloses, and manages donor's data. The exact contents of a privacy policy will depend upon your specific online and backend data-collection practices, and should take into account applicable laws.

***2. Third-Party Vendor Risks***

Every organization uses third-party vendors/SaaS providers to provide and source key needs. If any of these third-party vendors does not employ adequate data security protection, the organization's data security will be at risk.

The "default," provider contracts, are extremely one-sided. Consequently, the legal terms of all such agreements must be a focus, and managers should be certain there are appropriate terms and conditions to both comply with applicable laws and to protect the organization. While it is not feasible to cover all addressable provisions, any contract negotiations should address the following.

• *Adjust the Limitation of Liability Cap*

Vendors routinely attempt to limit any claims for losses or damages that might be incurred. They typically try to limit the recovery to six months of fees paid, or even less. The "cap" should be set at some multiple of the contract value, and not be tied to monies paid to date. This avoids having limited recompense for claims that occur early on.

Also, because certain damages pose a greater risk to the organization and its reputation, they should be excluded from these caps. As an example, damages that result from a data breach, indemnified claims and breaches of confidential information should not be capped.

• *Request Transition Services*

Not all vendor relationships last forever. When it's time to change a vendor, transition can be a lengthy and arduous process. When a vendor is reluctant to assist with the facilitation of the transition, the client gets stuck with the logjam. To mitigate this, you should insist on including a provision requiring the vendor to provide ongoing services and specific transition support at their then standard rates for a certain period of time.

• *Insist on Specific Representations and Warranties*

During the sales pitch, clients are presented with polished and detailed marketing materials that exhaustively detail the various aspects of the vendor's product, and are promised all sorts of things. If responding to an RFP, the vendor meticulously details the features and functionality of the system. It's odd that when the client finally gets the agreement, it's scant on the details of what is to be provided. To make matters worse, many vendor agreements actually disclaim or exclude statements or information that might have been made during the upsell. For this reason, make sure the client attaches all marketing materials, RFP responses or other descriptions to the agreement, and have the vendor attest to their accuracy and truthfulness. It ensures that the vendor will put their money where their mouth is when it comes to delivery.

• *Coverage for Breach Notification and Credit Monitoring Expenses*

Vendors are only legally responsible for notifying the client if a breach occurs. It is the organization that will be tasked, and will have to assume the costs, for notifying donors, and for paying for all required (and recommended) remediation costs and expenses. Any contract with vendors should have these costs covered as an indemnified claim, among other related terms.

The fact is that most organizations need to collect some types of PII -- and the definition of PII is getting broader with each passing year. For many organizations, this type of data is essential to their acquisition, outreach, marketing and donor cultivation efforts. This type of data certainly comes with rewards, as well as risks. Adopting and implementing more thoughtful data security and data privacy processes and practices will certainly help to minimize the likelihood of a security incident, and mitigate the damages should one occur. **NPT**

---

*Jon Dartley, Ph.D., is an attorney at Perlman & Perlman, LLP, in New York City. His email is jon@perlmanandperlman.com. The information provided above does not constitute legal advice and is not intended to substitute for legal counsel.*

*maria.gollayan@marcumllp.com*