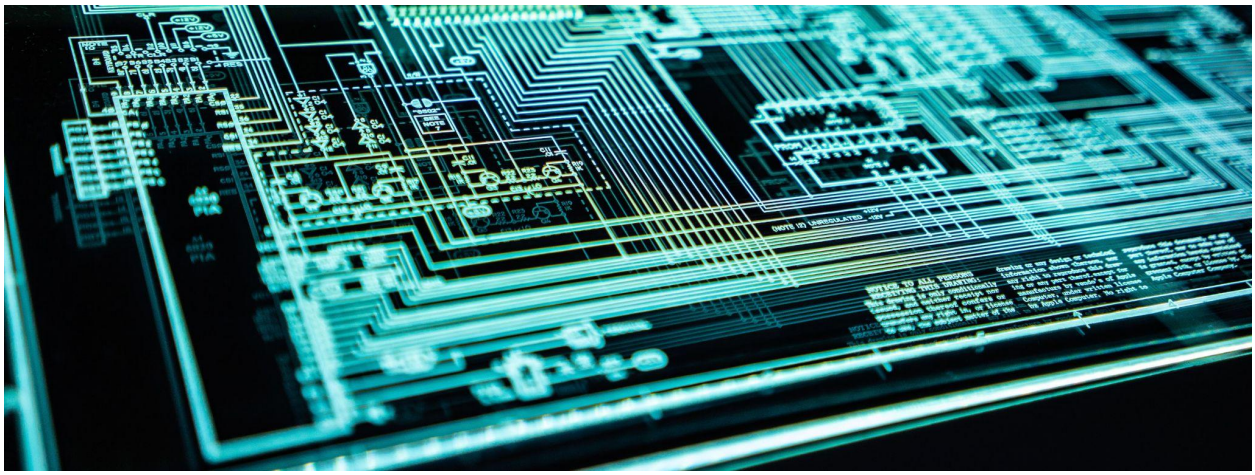
Roadmap to Data Security for the Nonprofit CEO



Introduction

You know it is important to keep the personal data of your donors, members, and clients secure. There are laws regulating how we collect, store, and use data. We feel an ethical obligation to protect the people who share data with us. And our organization's reputation is at stake. No one wants a data breach, and no one wants to deal with its aftermath.

This document gives you what you need to know and the key steps for ensuring the security of your organization's data. With some intentional focus, you will lay the foundation to protect your data, and with it your organization.

1. Make Data Security a Board-Level Priority

A CEO needs to think of data security in the same way he/she thinks of a financial or tax audit — It needs to be part of the regular duties a CEO addresses every year. It is the CEO's job to put data security on the Board of Directors' agenda, and it is the Board's responsibility to ensure that the CEO performs their managerial oversight duties appropriately. Together the CEO and Board roles are to ensure understanding and accountability for how an organization secures its data, and set in place appropriate controls to avoid complacency on the part of the staff.

The CEO and the Board should ensure that their liability insurance coverage is up to date and meets the needs of the organization. They should also consider carrying cybersecurity insurance.

2. Regular Audits of Data Security

One of the most important things a CEO can do internally is ensure that the organization has regular audits of its data security practices. This regular annual data security audit should be signed off by the CEO and presented to the Board for its approval. In other words, it's simply not good enough for the CEO to say to the board that "the team is on it in terms of data security." It has to be a formal, regularized process. Ideally, just as an outside CPA each year will review the organization's books, so too should an outside data security expert or team review data security processes each year.

This audit should look for several things:

- **Regular Software and Patch Updates**

The auditors must check to ensure that all systems — laptops, servers, and network devices — are both current in their patches, and have a process to ensure that they stay current throughout the year. The hybrid work environment makes this all the more difficult, and CEOs should press their team to identify how they plan to secure data that is resident on staff's personal computers and home internet.

- **Employee training program**

The auditor must also check to ensure that the staff is regularly trained on cybersecurity best practices. According to a study cited by a CNBC report, employee negligence is the main cause of data breaches. Nearly half (47%) of businesses pointed to human error, such as accidental loss of a device by an employee, as the reason behind a data breach at their organization. To meet this challenge, the organization should require data security training annually and data

security awareness has to be part of the on-boarding process of all new employees, including those working remotely. For the CEO, be intentional about the importance you place on completing cybersecurity training and make it a KPI for your department leads during their goal setting and annual review process.

- **Single Sign-on, Multi-Factor Authentication and Strong Passwords**

Logging in should be easy for your staff and hard for anyone else to do. Modern tools such as password managers, single sign-on solutions and multi-factor authentication are effective in the fight against cyber-threats and accessible to organizations of all sizes. All of these will make it easier for your staff to utilize strong passwords seamlessly.

- **Routine Data Back-ups**

Files need to be routinely backed up, with a frequency and location appropriate to the type of data. The CEO should ensure the organization practices restoring data on a regular interval.

3. Regular Data Destruction

When it comes to data retention, it's all about knowing what data has value and where it resides. A simple metaphor helps, "One should frequently clean out their clothes closet, since most of what is kept over time is never worn." Similarly, data ages quickly and loses value as it loses recency. When faced with a cybersecurity incident, the more data you have exposed, the greater your liability.

4. Practicing Incident Response

Once the Board and CEO have data security on their radar, and a process for conducting annual assessments, the CEO should next turn to practicing an incident response. The CEO must have the mindset that it is not *if* an incident will happen but *when*, and it is their job to look at maintaining strong data security as an important facet of the organization's reputation.

One helpful strategy in meeting the cybersecurity challenge is for the organization to include its cloud storage provider or other outside partners to help them perform an incident response exercise.

The bottom line: Data security is a team sport requiring the focus of the whole organization and its trusted partners and only the CEO can bring all of the players together.