Do You Know Where Your Data Is—And How To Protect It?

By Elyzabeth Joy Holford

Assistant Executive Director

Resource Type: Articles

Topic: Data Privacy, Tech Risk, Cybersecurity

All nonprofits—from local community organizations to international foundations—operate as data repositories. Every day, your team holds the keys to sensitive information, including data such as donor names, financial details, employee records, and beneficiary personal data. For cybercriminals, this information is not just data; it is currency.

We live in an era in which cyberattacks on nonprofits are not just possible, they are likely. Phishing threats and AI-driven scams have proliferated and working with third-party vendors grows ever more complex. To fulfill your mission, you must protect your organization, your team, and your constituents. A data breach can cost more than money; it can destroy the trust you've spent years building with constituents. This article focuses on the most important factor in your cybersecurity arsenal: your organizational culture. We've also included some additional, practical steps to securely maintain your data.

Establish and Maintain a Healthy Cyber Culture

Nonprofits often talk about cybersecurity as if it is only an IT challenge, best solved by deploying technology like firewalls and encryption. Yet human error is responsible for a staggering majority of data breaches. This means that our most valuable source of strength—our people—can also be a critical source of vulnerability. A robust, sustainable cybersecurity strategy must be grounded in a "no blame" attitude that fosters acceptance, curiosity, and transparency. This allows employees to help shape the cyber health of an organization through participation. Creating an open, responsive culture requires a deliberate, thoughtful approach. How?

- **Lead by Example and Foster a Speak Up Culture:** Leaders should explicitly state that honest mistakes will not be punished and encourage employees to report issues immediately. Leaders should model vulnerability by openly discussing security challenges and acknowledging their own near misses.
- **Implement Non-Punitive Reporting Mechanisms:** Create simple, anonymous, and accessible channels to report suspicious behavior or accidental clicks, such as a "Phish Alert" button.
- **Turn Mistakes into Learning Moments:** When incidents happen, conduct "post-mortem" or blameless post-incident reviews focused on identifying root causes of the system failure, not assigning blame. These incidents can be transformed into anonymous case studies to educate the whole organization.
- **Recruit Security Champions:** Enlist and empower individuals who are not in IT but can advocate for

good practices and act as liaisons.

Assess Where Your Data Lives (Data Inventory)

You cannot protect what you do not know you have. The first step is to conduct a data inventory, mapping out exactly what data you collect and where it is stored. This should cover:

- **Donor Databases:** Your constituent relationship management (CRM) system contains sensitive data about individuals including personal contact information, donation history, credit card data, and bank transfer information.
- **Email Platforms:** These systems often hold internal and external correspondence that may include sensitive conversations.
- **Third-Party Tools:** The event software, online donation portals, and cloud storage providers you contract with will likely have access to multiple data points in your cyber ecosystem.
- **Unstructured Data:** It is easy to forget that the spreadsheets and tables you have on laptops, USB drives, and as attachments in email inboxes often contain very sensitive data.
- **AI Tools:** Whether you have an AI policy or not, your staff may be using AI tools that are not secured.
- **Ghost Data:** There could be lingering copies of data in the backups, snapshots, and cloud storage logs that you use. This data consumes storage space, which costs money. It can also contain sensitive information which, if left unprotected, presents another target for gaining access to your systems.

Identify Your Vulnerabilities

Once you know where your data lives, assess how it could be compromised. The primary areas to investigate include:

- **Human Error:** Even in a risk-aware organization, it is important to keep your team vigilant to the fact that bad actors will try to promulgate scams. Phishing emails are becoming increasingly personalized, using AI to mimic the words and voices of donors, staff, board members, or executive directors.
- **Weak Authentication:** Using simple passwords or failing to use multi-factor authentication (MFA) for entry into databases makes it easier for cybercriminals to access your systems.
- **Third-Party Vendors:** If a vendor such as your online donation processor or your cloud service provider is compromised, your data is compromised**.**
- **Insecure AI Use:** One of the most common AI use errors is accidentally pasting information from employee and/or donor lists into unauthorized AI tools, which can expose confidential information.
- **Remote Work/Unsecured Networks:** Your data can be exposed to attack when staff access sensitive systems over public WiFi or from unpatched devices.

Take Steps to Protect Your Data

Protecting your organization from cyberattacks is not about perfection; instead, it’s about preparedness. Take these important steps:

- **Implement Multi-Factor Authentication (MFA):** MFA is the single most effective technology-based security measure. It requires users to verify their identity via two or more methods, blocking most automated attacks. Enable it for all email, financial, and donor databases.
- **Gamify and Personalize Training:** Replace long trainings with short, relevant learning modules that use storytelling to illustrate the real-world impact of a single click. Encourage attendees to ask questions. Reward proactive behaviors, such as reporting phishing attempts, rather than only punishing failures.
- **Utilize Penetration (Pen) Testing:** Pen tests are proactive, authorized cybersecurity exercises where security professionals simulate real-world attacks to identify, exploit, and remediate vulnerabilities in IT infrastructure, applications, and networks. Pen tests can simulate external attacks on internet-facing assets like websites and servers, or malicious insider or compromised employee activities.
- **Limit Access and User Roles:** Not every employee needs access to all donor data. Implement role-based access control, also known as the principle of least privilege. Ensure that staff only have access to

data needed for their positions.

- **Secure Your Payments:** If you accept any kind of payments online, it is your responsibility to protect those transactions.
- **Avoid the Storage of Sensitive Data:** Do not ask for credit card numbers via email and never store CVV numbers or full magnetic stripe data. The better practice is to use reputable payment processors or specialized donor platforms that are PCI-compliant, meaning they follow the strict data security requirements found in the Payment Card Industry Data Security Standard (PCI DSS).
- **Back Up Data:** Many organizations adopt the "3-2-1" rule: maintain 3 copies of data, on 2 different mediums, with 1 copy offsite/cloud. Some organizations rely on automated cloud-based backups and external hard drives. It is important to have a plan to back up data and make sure that plan is followed across the organization.
- **Purge and Archive:** If you don't need it, delete it. A data retention policy can set the cadence for safely destroying old records.
- **Encrypt Everything:** Ensure all laptops are encrypted and your website uses Hypertext Transfer Protocol Secure (HTTPS) to protect data in transit. Using HTTPS means encrypting the connection between a user's browser and your website using SSL/TLS protocols, protecting data in transit from eavesdroppers and cybercriminals.
- **Develop a Cyber Incident Response Plan:** If a breach occurs, you need a plan to act quickly. Your plan should document exactly who does what in the first 24–72 hours, including providing guidance on when and how to contact law enforcement, legal counsel, your insurance agent, your staff, affected donors, and other appropriate constituents.

Data as Mission Enabler

In the end, cybersecurity isn't just about protecting systems or preventing unflattering headlines. It's about encouraging your team to be more security-minded in an increasingly volatile digital world. By creating a supportive environment, taking inventory of your data, recognizing your vulnerabilities, and implementing robust, proactive security measures, you can protect your data from digital threats and clear the path to successfully achieve your mission.

Elyzabeth Joy Holford is Assistant Executive Director at the Nonprofit Risk Management Center. Reach her with thoughts or questions about this article at elyzabeth@nonprofitrisk.org or (703) 777-3504.