Data Privacy and Cyber Liability: What You Don't Know Puts Your Mission at Risk

By Erin Gloeckner and Melanie Lockwood Herman

If you were a long-time donor to a nonprofit, and just learned that your credit card details provided to the nonprofit to make a donation are now in the hands of a hacker, would you ever trust that organization again? In an article about nonprofits and sensitive data published by the Nonprofit Technology Network (NTEN), the author points out that while data breaches occur at for-profits, government entities and nonprofits alike, consumers may be less willing to trust nonprofits after a data breach. This is because a consumer's relationship with a company or a government entity is largely based on the consumer's need, whereas his or her relationship with a nonprofit is not necessarily need-based. This suggests that nonprofits may be at greater risk for reputational and financial damage in the wake of data breaches.

Although data breaches seem to be increasingly common, most nonprofit leaders still know very little about the risks that arise from the collection and storage of personal information collected from employees, volunteers, clients and donors. Considering this dark and somewhat frightening landscape, what must you know to understand the exposure and fortify your nonprofit against the associated risks? This article explores:

- Data privacy risks and responsibilities
- What is personally identifiable information?
- Privacy and data breach law
- The importance of reaching out for help complying with legal requirements in the wake of a data breach
- Cyber liability insurance basics
- Data security strategies
- Tips for working with tech vendors

Data Privacy Risks and Responsibilities

Many leaders believe that the work of foreign hackers represents the greatest threat to the confidential information their organizations collect. Yet the truth is that many threats to data privacy lives much closer to home. The following common business activities can lead to a data breach and potential liability for a nonprofit:

- Conducting e-commerce on your website, especially collecting credit card data and processing payments online
- Storing and transferring personal employee, client or donor data—for both virtual data and paper records (e.g., sending sensitive data via email or storing sensitive data in the cloud; storing paper records in unprotected filing cabinets that anyone could access)
- Storing personal information on laptops or smartphones
- Allowing partners and/or vendors to access personal information without proper safeguards
- Storing personal information on cloud servers or systems

While it's true that cybercrimes such as hacking, insertion of malicious code into a data system, or the purposeful loss and destruction of data are a valid concern for nonprofit leaders, it's important to recognize that unintentional privacy breaches can be just as costly. A simple example is permitting personal information to be stored on a laptop or smartphone. The device—and all the vital data on it—could be damaged, lost forever, or it could even fall into the wrong hands. In some states, the mere loss of the device with personally identifiable information is a breach under the law and triggers reporting responsibility, such as the duty to notify the people whose data was lost.

What is Personally Identifiable Information or PII?

The starting point for understanding a nonprofit's duty to guard personal information is understanding *what constitutes personally identifiable information under the law*. Information found in a telephone book is not protected under the law. Which means that the loss of a paper or electronic file containing donor names and addresses probably doesn't constitute a breach or trigger state law notification requirements. In Illinois the definition of "personal information" contained in the Personal Information Protection Act (815 ILCS 530) is "Personal information means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted:

1. Social Security number.
2. Driver's license number or State identification card number.
3. Account number or credit or debit card number, or an account number or credit card number in combination with any required security code, access code, or password that would permit access to an individual's financial account.

Privacy and Data Breach Laws

Data management and security standards are becoming increasingly complex as data constantly moves between multiple devices and storage sites. So what should nonprofit leaders know about this changing regulatory landscape? Various federal and state privacy regulations require that for-profit and nonprofit businesses *protect personally identifiable information* (PII) no matter where it resides: on a network; on stand-alone systems such as billing, medical, and marketing databases; on remote devices such as laptops or employee-owned cell phones; and of course on paper. Additionally, there are data protection standards for specific industries or specific business practices, such as the PCI Security Standards Council's Payment Card Industry Data Security Standard. This standard requires organizations to enact information security best-practices if they handle major credit cards such as Visa and MasterCard. Failure to comply with these standards can result in enormous fines. Similarly, you might be familiar with federal data security regulations such as HIPAA if your nonprofit handles protected health information (PHI).

According to the National Conference of State Legislatures, 47 states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted laws that require organizations to notify individuals of security breaches of information involving personally identifiable information. Each of these laws generally has four key components:

1. who must comply
2. what constitutes "personal information"
3. what constitutes a breach (e.g., unauthorized acquisition of data); requirements for notice (e.g., timing or method of notice, who must be notified), and
4. whether there are exemptions. The most common exemption is for encrypted information.

Cyber Liability Insurance Basics

Your nonprofit's insurance agent or broker is the go-to resource for information about what's covered under the cyber liability policy you already purchase, or one you're considering. Each insurer offers different forms of coverage, but many policies address a few familiar coverage areas. Cyber liability policies may include third party coverages (items 1-5 below) and also first party coverages (items 6-7). Third party coverage protects the insured organization against claims that arise from losses suffered by third parties, such as donors or clients. First party coverage protects the insured for its own losses. The following is a list of some of the coverages that may be available through a cyber liability policy:

1. **Notification Expenses**: As discussed above, almost every state has notification requirements for both private and government entities. If a data breach occurred at your nonprofit, it is likely you will be required to notify parties affected by the breach. Spending weeks notifying affected clients, donors and employees could be costly. Coverage for notification expenses will protect your nonprofit from the strain on human and financial resources in the wake of a breach.
2. **Crisis Management**: After a data breach occurs and you've met your notification requirements, your nonprofit could still face harsh criticism and scrutiny from affected stakeholders or the media. These disenchanted former supporters may ask: How could this happen? Why didn't the organization do what was necessary to protect against a breach? Some cyber liability policies offer crisis management coverage to cover the cost of retaining PR help to minimize the damage to your reputation.
3. **Regulatory Investigation Expense**: Since data breach notification laws are subject to change, your commitment to comply may not be good enough. Which means there is always a chance you'll receive a call from a friendly civil servant. Both state and federal agencies can investigate and take action against a nonprofit that is negligent in guarding personally identifiable information. Some cyber liability policies exclude coverage for governmental or regulatory investigation costs, but other policies include it. And some policies will also cover fines and penalties, such as a fine levied for failing to notify the individuals whose data was compromised within the time limit required by law. These fines can be substantial, and are often on a per record basis.
4. **Data Breach Liability**: This coverage will defend your nonprofit against legal claims brought by a stakeholder who suffered a significant financial loss after their personal data was compromised. A typical suit will allege that your nonprofit was negligent in failing to protect the stakeholder's personal information, and that their loss was directly attributable to your nonprofit's negligence.

5. **Content Liability**: Some cyber liability policies offer financial protection related to the content of your website, blog or social media sites. This can range from copyright infringement and intellectual property claims to invasion of privacy or personal media injury (defamation, slander, libel) via electronic content. Some insurers refer to this coverage as "website liability." Keep in mind that many nonprofits that buy cyber liability coverage principally do so to finance the costs arising from the theft of personally identifiable information, and choose to cover content liability exposures under another policy, such as a media liability policy.

6. **Data Loss & System Damage (or Data Restoration Coverage)**: Your current property policy probably covers damage to computers you own, but **traditional property policies do not cover the data stored on computers**. Most cyber liability policies cover loss or theft of personally identifiable information (e.g., your clients' home addresses, your employees' Social Security Numbers, etc.). Some policies also include coverage for computer forensic analysis, the process used by an expert to assess the scope of the damage.

7. **Business Interruption**: Many cyber liability policies cover events related to the temporary or long-term shutdown of an insured entity's operations, such as: loss of revenue during the downtime after a hack; denial of service; damage to systems or data caused by a virus; etc. Some nonprofits may find this coverage beneficial, however it is unlikely that most nonprofits would be forced to close their doors while responding to a data breach incident. If your nonprofit would have to close in the event of a data breach, you'll place greater value on having this coverage in place.

Data Security Strategies

To reduce the likelihood and severity of a data breach, consider the following practical strategies.

- **Ensure Regular Software Updates**: Make certain that IT staff or contractors frequently install security patches and updates to your devices' operating software and other software. Oftentimes, data breaches occur when software is vulnerable due to age or other issues. Software updates typically include new security measures that will help protect your devices and data against harmful malware and viruses.

- **Encrypt Sensitive Data**: **Would the theft of a laptop or other mobile device constitute a data breach? Possibly, if those devices contain unencrypted personally identifiable information. Consider encrypting sensitive data so thieves who access to data can't use it.** If you work with protected health information and you are thereby required to comply with HIPAA, review this list of recommended protocols for securing mobile devices from www.HealthIT.gov. Consider the pros and cons of encryption. On the downside, encryption costs money and slows down response time. As a result, some experts suggest that organizations encrypt only data on mobile devices, or strictly prohibit the storage of personally identifiable information on mobile devices.

- **Schedule Data Security Training**: Some cyber liability policies offer proactive risk management resources, such as educational materials or access to helpful training on data security. Your data security efforts will be fruitless if your employees do not follow your protocols. Remember that human error is a major source of cyber liability exposure, an exposure you can mitigate by adopting clear policies and providing appropriate training. Topics you might want to cover in your training include: BYOD policies, network security protocols, encryption instructions, relationships with tech vendors, data breach notification laws, information on the nonprofit's cyber liability coverage, and your insurer's requirements for filing cyber liability claims. Ensure that your employees recognize how easily a data breach can occur, and how detrimental a breach could be to your nonprofit's mission.

- **Adopt a BYOD Policy**: Establish a Bring Your Own Device (BYOD) policy that clarifies whether employees may access PII on their personal devices (laptops, cell phones, etc.). Communicate the policy to employees, including instructions on what type of data may be accessed on personal devices, procedures for accessing data securely (e.g., through a secure network), and procedures for storing and transmitting data securely (e.g., using encryption). You might also decide to offer resources to employees such as AT&T Toggle, a BYOD solution that allows employees to switch from 'work mode' to 'personal mode' on a smartphone. Whatever your BYOD policy is, aim to strike a balance between protecting nonprofit's data and upholding the privacy rights of your employees.

To prepare your nonprofit for the breach you hope will never happen, consider the following important questions.

- *What constitutes a data breach?* State security breach laws generally define what constitutes sensitive information. But no two state laws are identical. In some cases, such as Florida, a data breach is an actual breach. Florida Title XIX, Chapter 282 defines "breach" as: "a confirmed event that compromises the confidentiality, integrity, or availability of information or data." In other states a data breach has occurred if there is reasonable belief that a data breach occurred, even without hard evidence of an actual breach.

- *Who must we notify?* Most states require organizations to notify all consumers affected by the data breach. Some states also require you to notify the state attorney general or consumer reporting agencies.

- *How should we contact our customers?* Some states require that specific communication methods are used to notify consumers of a data breach. For example, some states prohibit using pre-recorded phone calls, while other states only allow you to email consumers whom you have permission to contact via email.
- *How quickly must we contact our customers?* Every state notification law includes a timeframe for data breach notification. If you fail to notify your consumers within the appropriate timeframe, your nonprofit could face litigation and harsh fines.
- *What resources are available from our insurance providers?* As indicated previously, some insurers provide proactive risk management help, and have experts on call to either answer or help you determine the answers to the questions that follow. Keep cyber liability insurance information close at hand so that you're ready to make the call when you need to.
- *What changes should we consider?* Once you've addressed the crisis at hand and have complied with insurer and regulatory agency requirements, take time to consider lessons learned from the incident and the need for changes in policy, practice and training. Consider conducting a risk assessment focused on data privacy exposures, identifying training needs for staff, and updating internal policies that concerning the collection, storage and protection of personal information from clients, donors and employees.

Tips for Working with Tech Vendors

Aside from using the strategies above to mitigate potential data privacy exposures, remember to establish a process for vetting tech vendors if you outsource any IT processes or rely on a vendor for third-party "cloud" storage. Outsourcing IT support and/or data storage may be wise if your nonprofit lacks the personnel expertise or resources to manage data internally, but beware of placing too much trust in a tech vendor. Resolve to become a discerning consumer so you can distinguish dependable tech vendors from those unworthy of your trust. Take the time required to negotiate a contract with your tech vendor that ensures the support or services you need while adequately protecting your nonprofit against harm or loss caused by the vendor's negligence. For starters, consider asking these questions before you engage with a prospective tech vendor:

- **What warranties or protections does the vendor offer in the event of their negligence?** Require that your tech vendors carry errors and omissions coverage to protect your nonprofit against claims stemming from the vendor's negligence. Having this coverage won't insulate your nonprofit from a data breach claim, but you might be able to subrogate a claim against your vendor if turns out they were negligent, such as by failing to install an available patch when your contract indicated their responsibilities to do so. Never sign a tech contract absolving the company for its own negligence.
- **Do I understand my nonprofit's tech needs and existing IT infrastructure?** What must I do (or who must I consult with) to understand these things before I engage a tech vendor?
- **Can this particular vendor meet all of our technical requirements?** Can this vendor integrate its services seamlessly with our existing internal IT functions?
- **Does this vendor have a good reputation in the market and amongst its client base?**
- **Is this vendor willing to include a training and/or support package with our contract (e.g., if your nonprofit has limited IT personnel or resources)?**
- **What is the vendor's response time when its clients experience emergencies such as data breaches?**
- **Will my nonprofit still retain full ownership rights to any electronic documents and property that we store with the vendor (e.g., cloud storage vendors)? What are our rights and responsibilities as owners?**
- **What is the vendor's dispute resolution process?**
- **Are the vendor's payment terms reasonable and compatible with our accounts payable process?**

Erin Gloeckner is Project Manager and Melanie Lockwood Herman is Executive Director at the Nonprofit Risk Management Center. They welcome your questions about data privacy risks and cyber liability at 703.777.3504 and erin@nonprofitrisk.org or Melanie@nonprofitrisk.org.