This article presents general guidelines for Georgia nonprofit organizations as of the date written and should not be construed as legal advice. Always consult an attorney to address your particular situation.

Data Security Is Important for All Organizations, including Nonprofits: 10 Security Steps to Consider

By Kevin Coy, CIPP/US[1]

Data security and data breaches seem to be in the news constantly. While most of the press tends to go to mega data breaches involving millions or tens of millions of potentially affected individuals (Target, Anthem, Ashley Madison, and the federal Office of Personnel Management to name just a few), data breaches can—and do—occur at organizations of all types and sizes. Nonprofits, including small nonprofits, also almost certainly have personal information that needs to be secured.

Personal information held by even a small nonprofit could include information (including credit card or other payment information) from contributors or from individuals who purchase publications or merchandise or services from the organization. A nonprofit also likely has sensitive information about its employees or others (such as payroll and tax information including Social Security numbers). All of this personal information needs to be secured from potential internal and external risks in order to protect the privacy of the individuals the organization interacts with, as well as to help protect against a host of potential risks in terms of staff resources, the organization's reputation, and legal liability that could arise from a breach.

This article identifies ten steps that a nonprofit can take to help protect the personal information it holds.

1. **Conduct an inventory and risk assessment.** It is difficult to effectively protect personal information if you do not know that you have it or where it is. Take an inventory of what types of personal information your organization collects, as well as information such as, why it is collected, where it is stored, and who has access to and day-to-day control over it. Also, conduct a risk assessment regarding the sensitivity of the information (are there, for example, Social Security numbers, payment card numbers? Government identification numbers? health or medical

[1] Kevin Coy is a Partner in the Washington DC office of Arnall Golden Gregory LLP. Kevin is a member of the firm's privacy and consumer regulatory practice group and advises clients on a range of privacy and data security matters, including the handling of data breaches, the development of internal and external privacy and data security policies, and developing incident response plans. He also has represented clients before federal and state regulators in connection with data breaches and other consumer protection matters.

information?), how it could be misused, and the potential risks to the individual if it were compromised. Are there gaps between your safeguards and the risks you identified? If so, look for ways to close the gaps or mitigate the risks posed.

2. **Collect only what is needed and limit access to those who need it.** Once you know what types of personal information your organization collects, consider whether all of that information is needed by the organization. Just because a particular form, for example, has "always" asked for particular information, does not mean that the organization needs it today. If you do not need it, do not collect it. The less information the organization collects, the less information can potentially be exposed during a breach. This analysis also is helpful as the organization creates new forms, new offerings, and new systems. While the project is being designed, consider if all of the information being sought is necessary (as well as other privacy and security implications of the new form or offering). Addressing privacy and security on the front end—"privacy and security by design" can produce long term benefits and minimize the chances that it will be necessary to rework things later to address security issues. Limiting access to information to those who need it to do their job is another important means of safeguarding the data.

3. **Keep personal information only as long as necessary and securely dispose of it.** Deciding how long to keep information is a difficult decision for many organizations. However, just as not collecting information in the first place lowers your risk of a data breach, so too does only retaining the information only as long as you need to have it. Sometimes it is necessary to keep information, whether it is for legal, operational, or other purposes. Other times, however, it is just inertia that results in boxes or paper records or an increasing volume of email and other electronic records accumulate. If you can dispose of it, that is less information that could be compromised in a breach later.

4. **Secure paper records and destroy them (as well as electronic media) securely.** The largest data breaches have been of electronic records, but do not forget about sensitive information that your organization may maintain in paper files or that your employees or volunteers may maintain in their "desk" files. Organizations often strive to be "paperless" but in practice many organizations frequently have a host of paper records with sensitive personal information. Files on applicants and employees; case files; medical records; payroll reports; contributor or membership lists all potentially can include sensitive information that could be harmful if breached. Does your organization keep these files in locked drawers, cabinets, or storage rooms when it is not being used? Does your organization have a "clean desk" policy so that employees or volunteers do not leave paper records containing sensitive records "lying around"? Is the policy enforced?

   Once you've decided to dispose of paper or electronic devices or media, make sure that you do so in a secure manner, such as cross-cut shredding, either in-house or through use of a document destruction service. Tossing the records in the regular

trash or in the dumpster in the parking lot is not appropriate. Many states have laws requiring secure destruction of data and regulators have brought actions against organizations for failing to dispose of information in a secure manner. This applies to computers, photocopiers, mobile devices, back-up tapes, thumb drives and other electronic media that the organization is disposing of that may contain personal information.

5. **Payment card processing/PCI.** Payment card processing is a common activity for many nonprofits. Contributors may want to use their payment card to make a donation. Users of the nonprofit's services may want to use payment cards to pay for the services. Supporters or other members of the public may want to purchase books, reports, or merchandize that the nonprofit sells to increase awareness of the organization and the issues that it supports. This information needs to be secured in accordance with the Payment Card Industry Data Security Standards (PCI DSS or often just referred to as the PCI standards). See https://www.pcisecuritystandards.org/merchants/ for more information. Failure to meet your organizations PCI obligations can increase your organization's potential liability in the event of a breach, as financial institutions increasingly seek to shift the losses associated with compromised payment cards to organizations where the information has been compromised. Use of a third-party processor, such as PayPal, may allow your nonprofit to outsource some of the technical PCI compliance work, but processing arrangements vary and your organization could still have PCI-related obligations.

6. **Control and encrypt laptops and mobile devices.** Laptops, mobile phones, USB drives and other portable devices are a frequent source of data breaches. A well-meaning employee may take a laptop or thumb drive containing sensitive information out of the office to work remotely and then the device is lost or stolen. Depending upon what is on the device and how the device was secured, this could result in a significant data breach. First, consider whether any employees (or volunteers) should be taking personal information out of the office. Is it necessary? If so, which employees have a need to do so? Does your staff know what is and is not allowed? What about the security of the devices? Encryption is a very important. If the data is encrypted the lost device or drive may not produce a breach. This assumes, of course, that the encryption key is not lost or stolen too. Make sure that employees/volunteers know not to tape their user id/password or encryption keys to their laptop or do anything else to expose this information because it can defeat all of your efforts to use encryption to protect the data in the first place. Also consider whether it is feasible for your organization to equip your laptops and other devices with other safeguards, such as software which would allow you to "wipe" the devices clean in the event that they are lost or stolen.

7. **Secure your network and website.** Security for your computer network and your organization's website(s) is an ongoing and essential part of any information security program. In the case of many nonprofits, particularly smaller nonprofits, this is an

area that the organization may outsource to a hosting company or other service provider rather than having an in-house resource. Regardless of which approach your nonprofit takes to staffing your information security needs, work with information security professionals to make sure that firewalls are in place and tested; that anti-virus and other software your organization uses is up-to-date (on all relevant systems and devices); that you have rigorous password or other user authentication processes (including requirements to change passwords periodically); that you encrypt sensitive information in transit and, if appropriate, also at "rest"; that you have audit trails and other controls to protect against a potential internal bad actor; and that steps are being taken to monitor and protect against emerging threats.

8. **Remember your service providers.** Outsourcing is a common occurrence, including for many nonprofits, and "out of sight" can too often also mean "out of mind." To the extent service providers handle personal information for your nonprofit (for example, payroll services, payment card services, or information security services) your organization can be responsible if your service provider (or their service provider) experiences a data breach involving your data. Work with your organization's lawyers to include language in your agreements with your service providers to require appropriate information security safeguards for your organization's information, address what will happen in the event of a data breach, and other issues such as whether your service provider will pay your costs if they have a breach involving your organization's information.

9. **Develop an incident response plan.** Hopefully, your organization never has a data security incident or an actual data breach, but it is well worth planning ahead. A potential breach can trigger a host of potential action items. Did a breach actually occur? Is the breach still ongoing and how do we stop it? Is there a need to notify law enforcement? Do we need to notify potentially affected individuals? What do the notices have to include? How quickly do they have to be sent? Do we need to notify any federal or state regulators of the breach? What about our insurer? Do we have a communications plan in case there are media inquiries? Who needs to be involved from various parts of the organization to help deal with the incident and any related issues? These are just a few of the questions that can be triggered by a data security incident. The nature of the specific incident often will shape your organization's response, but organizations that have developed incident response plans have found them to be helpful in organizing themselves to deal with incidents when they actually occur.

10. **Training.** Policies are great, but your organization's employees or volunteers need to follow them if they are going to be effective. Training on the importance of privacy and security and the steps they need to take to help the organization protect its information is essential and is an ongoing need. Even the most well-intentioned employee or volunteer can make mistakes or fall prey to a social engineering or phishing scam. Frequent training and reminders can help protect against these types of threats.