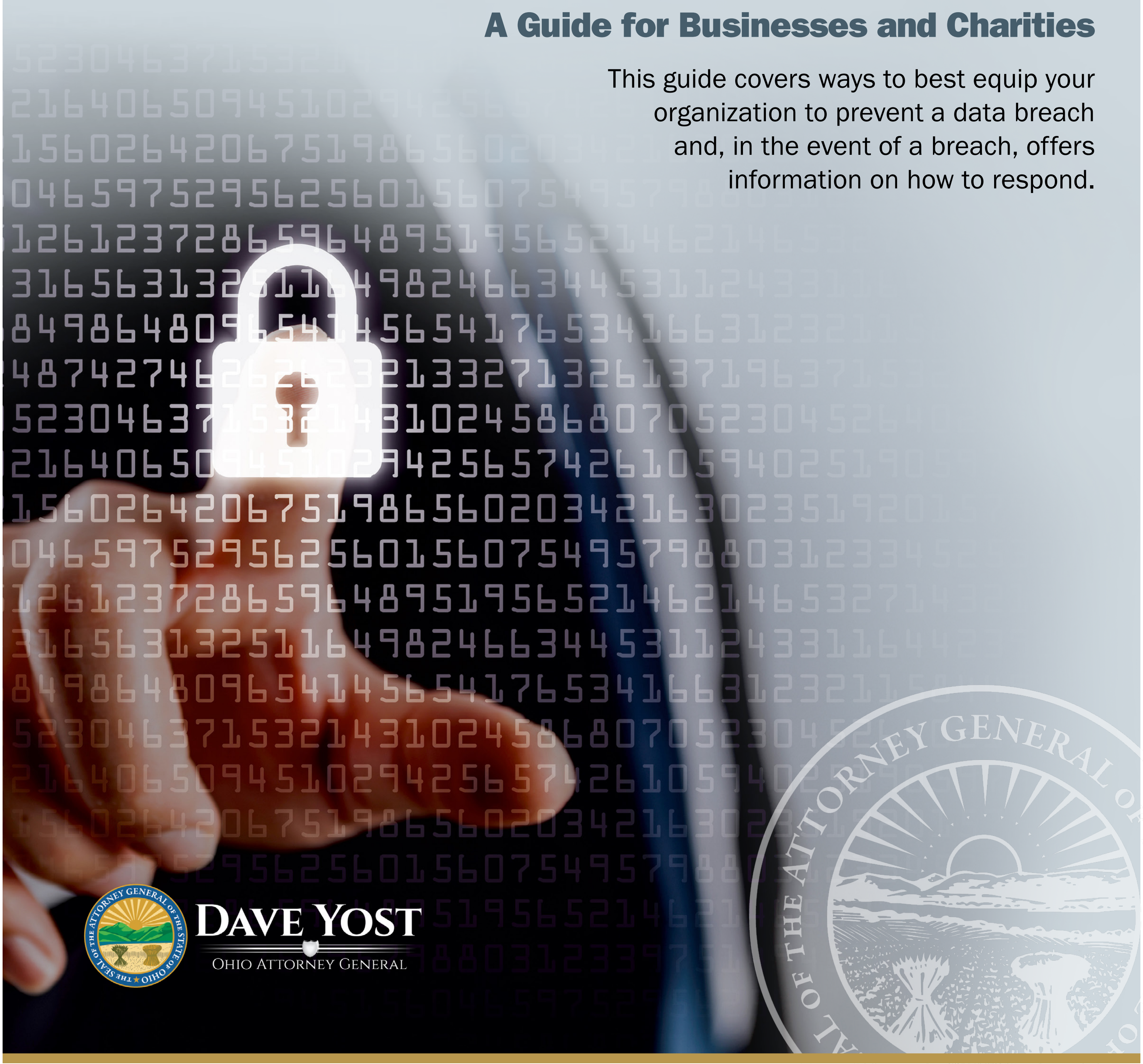
PROTECTING ★ THE ★ UNPROTECTED

Data Breach Prevention and Response

A Guide for Businesses and Charities

This guide covers ways to best equip your organization to prevent a data breach and, in the event of a breach, offers information on how to respond.



DAVE YOST
OHIO ATTORNEY GENERAL

DAVE YOST

OHIO ATTORNEY GENERAL

Dear Business Owners and Charitable Leaders,

The rise in data breaches poses a threat to all organizations, regardless of size or industry. Those that fail to address cybersecurity weaknesses risk major blows to their finances and reputation.

It is important to remember that your organization is both the first and last line of defense for the data in its cyber vault. But you are not alone. My office is committed to providing consumers, businesses and charitable groups with resources to help ward off bad actors. This publication is one such tool.

Inside this guide, you will find important information covering four main aspects of data security: how to create a strong data security plan, how to train employees about data security, what to do if a breach is discovered and how to notify consumers of a breach.

Please review this information and talk to your employees and volunteers about the importance of safeguarding consumer data. Prioritizing cybersecurity can save you time, money and frustration down the road.

Thank you for your valuable contributions to our state and for doing your part to protect Ohioans from data breaches. For more information about the Ohio Attorney General's Office, visit www.OhioAttorneyGeneral.gov or call our Help Center at 800-282-0515.

Yours,

Dave Yost

Dave Yost
Ohio Attorney General

Table of Contents

Data security basics

What is a breach?
A breach is an unauthorized access of information. The severity of a breach may depend on the type of information involved.

The five principles of sound data security:
1. Take stock.
2. Scale down.
3. Lock it.
4. Pitch it.
5. Plan ahead.

Source: Federal Trade Commission

The key to preventing a data breach is a strong focus on cybersecurity. Data breaches might seem inevitable, but, with the right training and tools, your organization can lower its risk of becoming a victim.

Take stock: To protect consumers' information, you need to know what information you have, where it's stored and who has access to it. Take time to understand what information is kept in both paper and electronic formats and how that information moves around your business or your charity.

- Inventory the office. Make sure you know what is stored on computers, laptops, mobile devices, flash drives and elsewhere. Also, take stock of what you have stored in paper form, and note where it is stored. For instance, do you have employment applications in an unlocked drawer that anyone can access?

  Remember that employees often use their personal devices for work purposes. It's important to know what information employees carry with them at any given time.

- Ask the major questions regarding information your business or charity keeps:
  - Who has access to information, and who is submitting information to your organization? Limit access to only those necessary. Beware of third-party vendors who may have

access, and make sure that they are practicing sound data security. Also, by understanding who is submitting information to your business or charity, you will have a better handle on the types of information in your system (say, consumers' credit card numbers and employees' Social Security numbers).

- What do those with access do with that information? You should know what your employees or vendors are doing with sensitive information. Are they storing it properly? Are they sending it to others, and, if so, are they using secure methods?

- When is information destroyed? Find out how long information is kept before it is destroyed. Evaluate whether that period is sufficient to meet both your needs and your customers' need for data security. Reducing the amount of sensitive information in accordance with a destruction schedule could decrease the volume of sensitive data on hand in case of a breach.

- Where is the information stored? Is information stored only on devices within your office, or do employees take information elsewhere? If they're taking information outside the office, it, too, should be secured.

- Why are you asking for the information you receive? Make sure you have a legitimate purpose for seeking customers' information so that you're not keeping data unnecessarily.

- How does your business or charity receive information? Does it receive it through a website, the mail and/or point-of-sale devices? Knowing how you receive information will help determine how to protect information repositories.

Scale down: Ask for, keep and retain only what you need. If you don't have a legitimate business need for the information, don't ask for it and certainly don't retain it. The more information you hold, the greater likelihood that personal information will be exposed in a breach.

Lock it: Whether in physical or electronic form, control access to information.

Firewall: software or hardware designed to block intruders from accessing your computer

Encryption: the process of coding a message so that only authorized parties can read it

- Make sure that offices, cabinets, desks and drawers remain locked when they hold equipment or files containing sensitive information.
- When storing sensitive information on a computer, use one without an internet connection, if possible.
- Encrypt information that you maintain or that is sent over the internet. You may need to hire professional help or consult outside resources. (See “Resources,” Page 8.)
- Do not put the free Wi-Fi offered to your customers on the same network as your business computers. Always have your computers on a secure network, behind an appropriate firewall and with up-to-date anti-virus and anti-malware protections.
- Require employees to use strong passwords — 12 characters or longer — and to change their passwords often. Do not allow them to keep their passwords in plain view. Additionally, each person in the company should have a different password, and any original passwords (for example, default passwords from an equipment or software manufacturer) should be changed.
- If you deal with payment cards, remember to review the Payment Card Industry Data Security Standards at www.pcisecuritystandards.org.
- Create a policy mandating that employees lock their computers whenever stepping away from their workstations, especially at the end of the workday. The policy should also require that mobile devices from which work-related information is accessed are locked when not in use.

Pitch it: If you don’t need it, get rid of it (securely, of course).

Once you take stock of your information, think about how long you need to retain the information. For instance, is it really necessary to retain credit card numbers for purchases made two years ago? Once information is no longer of use, dispose of it in a secure manner.

- Create a retention schedule that dictates when and how information should be destroyed. If you have the resources, invest in a system that electronically tracks and deletes information when it reaches its expiration date.
- Have appropriate disposal devices and services available to employees, including shredders and locked shred bins.
- Electronic devices also require special care during disposal. Simply clicking to “delete” sensitive files is not enough; devices such as computers, copiers and phones must be wiped clean so that restoration is not possible. Professional destruction companies can help remove data. Remember: If you can undelete an item, so can a hacker.

Plan ahead: Understand that even those with the best security measures may experience a data breach.

The time to put together a breach response plan is before one occurs. Make sure you know who you're going to contact, how to reach that contact and what the next steps will be.

- Create a policy and procedure regarding cybersecurity. Although running a business or charity is time-consuming, creating a cybersecurity policy is worth the effort. The policy should encompass the data and practices of employees in the office and the data and practices of those who travel or work from home.
- Learn about and invest in proper protections. At first, you might not know what certain technical features are or how they work, but take time to learn. Make sure that you have the proper anti-virus and anti-malware programs installed on your devices and that they are updated regularly, along with your other important software and operating systems. Consider hiring a cybersecurity expert to assist you with technical details.

Remember: It's important to protect your employees' personal information, too.

Employee training

Although many people would suspect that highly advanced hacking is responsible for most data breaches, human error more typically opens the door. It is vital to train employees on the proper precautions for preventing a breach. Here are some key practices to highlight:

- Secure a personal device. Many employers allow access to company servers, files or email from employees' own devices, such as personal cellphones. Security on those devices should mirror that of a business device. For example, your policy should dictate that employees not access their work email using public Wi-Fi. Also, employees should inventory what is on their personal devices in case the device is lost, stolen or hacked.
- Maintain a clean computer. Employees need to understand the importance of keeping a clean computer by not downloading attachments from unknown sources, clicking on unfamiliar links or plugging unknown devices into their computers.
- Guard against phishing. Phishing is a technique scammers use to trick employees into giving away information or access. The scammers pretend to be a trusted source, such as a bank, software provider or third-party vendor. Make sure that your employees know the scope of who would contact them, how to verify that the contact is legitimate and what information the contact would request. For example, your employees should know that no one would call requesting their password.

- Recognize suspicious activity. Would your employees know how to spot a skimming device? What about unusual activity on your website? Employees should be trained to recognize suspicious activity and to report it immediately.

- Understand what information exists. Employees need to know what personal information is retained by your business or charity, what rules and laws apply to it, and what should be treated with greater caution. Employees also need to know what to physically or electronically lock to prevent unauthorized access.

- Cultivate trust. Make sure employees know to inform management immediately if something goes wrong. If employees feel comfortable disclosing that they may have fallen victim to a phishing scheme or lost a device containing sensitive information, they will be more likely to alert management, thus allowing for quick implementation of a response plan.

- Terminate access. When an employee separates from your organization, you should immediately revoke physical access (making sure that all keys are returned) and electronic access (disabling login information).

Remember that third-party vendors who control information belonging to your business or charity should also be held to the same data-security standard. Relay your policy to those vendors and have them agree to follow your standards.

Reacting to a data breach

What happens when a dreaded breach occurs? You may notice the suspicious activity, or law enforcement officers may inform you that they think your system has been breached. Here are some immediate steps to take:

- Control the threat. Once you learn of the breach, consider taking your system offline if necessary. Create a “breach response team,” a group that understands your systems and can immediately neutralize an attack.

- Understand what information has been compromised. Has sensitive consumer information been breached, or did secondary security measures prevent access? The answers are especially important when deciding whether notice of the breach is necessary.

- Record all information available about the breach and maintain an ongoing, up-to-date log. Note when the breach was discovered, how it was discovered and whether any signs suggest how it occurred. The log should detail any steps taken or information discovered after the initial response. The log will come in handy later.

- Notify law enforcement. Contact local police, the FBI or the Secret Service to notify them of the incident.

- Consider hiring a forensic analyst to determine the extent of the breach. The forensic analyst can help discover how the breach occurred and what information was compromised.

- Decide whether you are required to give notice. Various federal and state laws dictate whether you are required to notify the public. The response usually depends on the type of information that was breached. Consult the relevant laws and/or your legal counsel to determine whether to issue a notice.

After a breach occurs is not the time to start thinking about the appropriate response. You might want to work with a breach-response company in advance to ensure that you have a proper plan in place.

Data breach laws and notification

Relevant laws:

- Fifty state data breach laws (plus Washington D.C., Guam, Puerto Rico, and the U.S. Virgin Islands)
- Federal Gramm-Leach-Bliley Act (financial institutions)
- Federal Health Insurance Portability and Accountability Act (health care)
- Federal Family Education Rights and Privacy Act (education)

This should not be considered an exclusive list.

Many states require that you give notice to consumers if their information is compromised. You should consult with legal counsel to determine the varying requirements for each state in which you operate.

In Ohio, the main data breach notification law is Ohio Revised Code Section 1349.19. The following are some frequently asked questions related to the law. You should consult with an attorney to make sure you are complying with this and all other state and federal laws:

- **Is the breach subject to disclosure?**

  In general, breaches must be disclosed when personal information has been, or is believed to have been, accessed and acquired by an unauthorized person if you believe that it will cause a material risk of identity theft or fraud.

- **What is personal information?**

  In Ohio, “personal information” generally means an individual’s name in combination with either a Social Security number, driver’s license number or state identification card number, or account number or credit or debit card number.

- **How should I disclose the breach?**

  You must disclose the breach in writing, electronically or by phone. If your business or charity does not have sufficient contact information, if the cost to provide notice would exceed $250,000, or if your organization would need to notify more than 500,000 people, you may be able to use email, postings on your website and notifications to major media outlets.

  If your business or charity has fewer than 10 employees and the cost of providing notice would exceed $10,000, you can use “substitute notice” by placing an advertisement in a local newspaper, posting on your website and notifying major media outlets in the area in which your business or charity is located.

- **Is there a certain time frame in which I must issue notice?**

  Breaches should be disclosed expediently but must be disclosed within 45 days of the discovery of the breach, unless law enforcement requires that you not notify within that time period.

- **What should be contained in the notice?**

  Ohio does not specify what must be included, but the notification should be meaningful and easy to understand.

- **Is my business or charity exempt from providing notification?**

  Your organization may be exempt if it is a financial institution, a business subject to the Health Insurance Portability and Accountability Act (HIPAA) or if all of the information taken was encrypted. But federal rules requiring notification may apply.

- **Do I need to contact the credit reporting agencies?**

  If the breach involved more than 1,000 residents of Ohio, all credit reporting agencies must be contacted.

- **Does the law address whether I can be sued as a result of a breach?**

  Ohio enacted the Data Protection Act, ORC 1354.01 et seq., to encourage businesses and other organizations to take appropriate steps to create, maintain and comply with a strong cybersecurity program. The law provides a “safe harbor” against certain claims for organizations that create cybersecurity programs that meet approved standards. Organizations can use the safe harbor as a defense to certain legal actions. Ohio R.C. 1354.02 identifies industry-recognized cybersecurity frameworks on which programs can be based. The law also takes into account the size and nature of the business or charity when determining the scope of an appropriate cybersecurity program.

Resources

Ohio Attorney General’s Office
800-282-0515
www.OhioAttorneyGeneral.gov

Federal Communications Commission
888-225-5322
www.fcc.gov

Federal Trade Commission
877-382-4357
www.ftc.gov www.OnguardOnline.gov

Department of Homeland Security
202-282-8000
www.dhs.gov

National Cyber Security Alliance
www.StaySafeOnline.org

Cybersecurity and Infrastructure Security Agency
888-282-0870
www.us-cert.gov

U.S. Small Business Administration
800-827-5722
www.sba.gov

DAVE YOST

OHIO ATTORNEY GENERAL

Data Breach Prevention and Response

A Guide for Businesses and Charities

For more information, to report a scam or to schedule a speaker on cybersecurity or consumer protection issues, contact:

Ohio Attorney General's
Consumer Protection Section
30 E. Broad St., 14th Floor
Columbus, OH 43215

Phone: 800-282-0515
TTY: Relay Ohio 800-750-0750

www.OhioAttorneyGeneral.gov