Cybersecurity

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

Data Breach Prevention and Response Guide for Businesses and Charities

Mike DeWine
Ohio Attorney General
Dear Business Owner or Charitable Organization Leader:

As a strong supporter of Ohio businesses and charities, I understand the importance of implementing sound operational practices that treat consumers fairly and foster a solid reputation. Recently, data breaches have affected businesses and consumers throughout the country. Businesses and charities alike are being targeted by the costly, destructive intrusions.

My office wants to make sure that leaders of businesses and charities know where to start in terms of securing information and how to prevent data breaches. Additionally, because breaches do happen, we want businesses and charities to be prepared with a first-response plan. This publication focuses on 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.

I urge you to review this information, to speak with your employees about the importance of protecting consumers’ information, and to use this guide as a starting point in securing your data. By being proactive about cybersecurity, you will save time and money.

In today’s world, cybersecurity is an essential aspect of running any organization. Implementing strong cybersecurity procedures is important for businesses, nonprofits, consumers, and for the state of Ohio. For additional information about the Ohio Attorney General’s Office, visit www.OhioAttorneyGeneral.gov or call our Help Center at 800-282-0515.

Very respectfully yours,

Mike DeWine
Ohio Attorney General
<table>
<thead>
<tr>
<th>Table of Contents</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Data security basics</td>
<td>1</td>
</tr>
<tr>
<td>Employee training</td>
<td>4</td>
</tr>
<tr>
<td>Reacting to a data breach</td>
<td>5</td>
</tr>
<tr>
<td>Data breach laws and notification</td>
<td>6</td>
</tr>
<tr>
<td>Resources</td>
<td>8</td>
</tr>
</tbody>
</table>
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 key principles of sound data security:

1. Take stock
2. Scale down
3. Lock it
4. Pitch it
5. Plan ahead

Source: Federal Trade Commission

Remember! It’s important to protect your employees’ personal information, too.

The key to preventing a data breach is a strong focus on cybersecurity. It may seem as though data breaches are inevitable, but with the right training and tools, your business can lower its risk of becoming a victim.

Take stock: In order 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.

- Inventory your office: Make sure you know what is stored on your business’s 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 many times, employees may use their personal devices for work purposes; it’s important to know what information employees carry with them.

- Ask the major questions regarding information your business keeps:
  
  o Who has access to information, and who is submitting information to your business? Limit access to only those necessary. Beware of third-party vendors who may have access, and make sure they are practicing sound data security. Also, by understanding who is submitting information to your business, you will have a better understanding of what types of information you have in your system (for example, consumers’ credit card numbers and employees’ Social Security numbers).
  
  o What do they do with that information? You should know what your employees or vendors are doing with sensitive information. Are they keeping it stored properly? Are they sending it to others? If so, are they using secure methods to send it?
  
  o When is information destroyed? Find out how long information is kept before it is destroyed. Evaluate if that time period is appropriate to meet your business needs coupled with customers’ need for data security. Reducing the amount of sensitive information in accordance with a destruction schedule could decrease the amount of sensitive data on hand, in case of a breach.
  
  o Where is the information stored? Is information stored only on devices located within your office, or do employees take information elsewhere?
  
  o Why are you asking for the information you receive? Make sure that there is a legitimate purpose behind asking for your customers’ information. The less information you have, the less likely you are to suffer a breach in which sensitive information is exposed.
  
  o How does your business receive information? Do you receive information through a website, through the postal service, and/or through point-of-sale devices? Knowing how you receive information will help in determining 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 information may be breached.

**Lock it:** Whether in physical or electronic copy, 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 holding equipment or files containing sensitive information are kept locked.

- When storing sensitive information on a computer, use one that does not have an Internet connection, if possible.

- Encrypt information that you maintain or that is sent over the Internet. You may need to hire a professional 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 business computers on a secure network, behind an appropriate firewall, and with up-to-date anti-virus and anti-malware protections.

- Require your 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 initial 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](http://www.pcisecuritystandards.org).

- Create a policy mandating that employees lock their computers whenever stepping away from their workstations, especially at the end of the day. The policy must also address the locking of mobile devices from which work-related information is accessed.

**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, it should be disposed of in a secure manner.

- Create a retention schedule that dictates when information should be destroyed and how. If you have the resources, invest in a system that will electronically track and delete information when it reaches its expiration date.

- Have appropriate disposal devices and services available to your employees, including shredders and locked shred bins.
  - Electronic devices also require special care during disposal. Simply clicking to “delete” sensitive files is not enough; the devices such as computers, copiers, and phones must be wiped clean so that restoration is not possible. There are
professional destruction companies specialize in removing 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 them, and what the next steps will be.

- Create a policy and procedure regarding cybersecurity. While running a business is time-consuming, creating a policy regarding cybersecurity 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 how a firewall functions, but take time to learn about, and purchase, one. 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.

Employee training

While most people suspect highly advanced hacking to be the cause of the majority of data breaches, it is human error that is typically responsible. It is vital that employees are trained on the proper precautions to prevent a breach. Here are some key areas of concern:

- Using a personal device: Many employers allow access to company servers, files, or e-mail from employees’ personal devices, such as personal cellphones. Security on those devices should be equal to 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 have an inventory of what is on their personal devices in case their device is ever lost, stolen, or hacked.

- Maintaining 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.

- Being aware of phishing: Phishing is a technique used by scammers to trick employees into believing they are from 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 person is legitimate, and what information that person would request. For example, your employees should know that no one, aside from your internal information technology department, would call requesting their password.
Recognizing suspicious activity: Would your employee 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.

Understanding what information exists: Employees need to know what personal information is retained by the business, 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.

Cultivating trust: Make sure employees know that if something goes wrong, management should be informed immediately. If an employee feels comfortable disclosing that he or she may have fallen victim to a phishing scheme, or lost a device containing sensitive information, he or she will be more likely to alert management, which will allow for the quick implementation of a response plan.

Terminating access: When an employee separates from your business, you should immediately revoke physical access (making sure all keys are returned) and electronic access (disabling login information).

Remember that third-party vendors who control information belonging to your business 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 if that dreaded breach occurs? You may notice the suspicious activity, or law enforcement may inform you that they believe 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 were there secondary security measures that prevented access? The answer is 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 there are any signs of 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 your 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 may 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 business’ legal counsel to determine whether to issue a notice.

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

Data breach laws and notification

<table>
<thead>
<tr>
<th>Relevant laws:</th>
</tr>
</thead>
<tbody>
<tr>
<td>• 48 state data breach laws</td>
</tr>
<tr>
<td>• Gramm-Leach-Bliley Act (financial institutions)</td>
</tr>
<tr>
<td>• Health Insurance Portability and Accountability Act (health care)</td>
</tr>
<tr>
<td>• Family Education Rights and Privacy Act (education)</td>
</tr>
</tbody>
</table>

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 different requirements for each state.

In Ohio, the main data breach notification law is Ohio Revised Code (ORC) Section 1349.19. Following are some frequently asked questions related to ORC 1349.19; 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 it will cause a material risk of identity theft or fraud.

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

  You must disclose the breach in writing, electronically, or by phone.
If your business does not have sufficient contact information, if the cost to provide notice would exceed $250,000, or if your business 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 has fewer than 10 employees and the cost of providing notice would exceed $10,000, your business 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 is located.

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

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

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

  Ohio does not have specific requirements as to what must be included in the notice, but it should be meaningful and easy to understand.

• **Is my business exempt from providing notification?**

  Your business 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.

• **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.
Resources

Ohio Attorney General's Office
800-282-0515

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

U.S. Computer Emergency Readiness Team
888-282-0870
www.us-cert.gov

U.S. Small Business Administration
800-827-5722
www.sba.gov
Ohio Attorney General’s Office
Consumer Protection Section

Data Breach Prevention
and Response 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 Office
30 E. Broad St., 14th Floor
Columbus, OH 43215

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