Safeguarding Customer Data and Privacy

Protecting your customers' personal information requires diligence and continual issue spotting. It only takes one data breach and you may face expensive legal battles and severe fines. But, the worst thing that can happen is losing trust with your customers. All of this can be prevented by safeguarding your customer data through proven strategies and a solid plan.

Maintaining your customers' trust is a priority. You may need to update aging technology and have the right privacy policies in place to reassure them that you are doing everything in your power to keep their information safe and private.

Privacy and Security Audit

According to the Federal Trade Commission Act (FTC), you are obligated to safeguard personal information for your customers and employees. Unfortunately, you will need to maintain similar data security standards as a large corporation. However, as a small business, you have the advantage because there are fewer employees and points of access to your data. Those points of access pose the greatest threat for any business.

The best way to protect your business is to start is a privacy and security audit. This will give you a general overview of all your policies and the technology in place that protects personal information.

To understand what you need to do to be compliant with the FTC, you should perform an annual audit of your privacy policies and information systems. The following questions are designed to help you perform a general audit.

- **Do you have a privacy officer or someone in charge of privacy and security?**
  This important position keeps your company compliant while ensuring customers that their data is safe.
- **How is customer/employee data collected?**
  Cloud-based applications offer higher levels of protection from cyberattacks.
- **How is customer/employee data used?**
  You may still be responsible if data is sent to a third party vendor and they experience a breach.
- **Where is your customer/employee data stored?**
  Digital and physical forms need to be stored properly and with restricted access.
- **Are your privacy policies up-to-date?**
  Typically, your privacy officer will review these with legal counsel or a privacy expert.

Answers to these questions can be easily kept in a manual or used to update your current privacy policies. They can also guide you through the necessary technology updates or changes in procedures.

It's important to communicate these policies with your customers and employees every year. They will also need to be notified when changes are made.

Your Data Security Plan

The FTC does offer some advice on how to create a plan that will limit your exposure to risks and prepare you for any future events. Here are their 5 key principles:

1. **Take Stock –** You can start your plan by identifying all of the assets used to hold and access data. This is a more specific audit of every device and system that resides within your company. It includes printers, laptops, tablets, and cellphones. From this, you can create a master list of all the technology you have by type, location, and user. You will also need to include physical files, their locations, and who has access to them. Remember, personal information may also contained on websites, email, or third party software.
2. **Scale Down –** Your business plan should guide your decisions on which types of sensitive personal information you need to collect. Because of this, you should not collect information that you will never use. The rule of thumb here is to keep what is necessary and skip the rest. This will reduce your amount of risk exposure.
3. **Lock It –** Security software and surveillance, combined with employee training, are the best ways to protect sensitive data. The FTC requires that you provide reasonable security.
4. **Pitch It –** Keeping files and sensitive information for too long becomes a hazard. Information disposal is important, so ensure that all customer information is properly thrown out. Just to be safe, remember to shred, delete, or destroy it.
5. **Plan Ahead –** You need to know how to respond to a data breach. This will go a long way in protecting your company from further damage.

Securing Customer Data and Privacy

Over the years, threats to your data have evolved into malicious attacks, but how you can protect yourself has remained the same. It's important to take some time to assess your options and make reasonable choices about data security and privacy.

Related

Focus on Your Core Business Strengths

Opportunities for Middle Market Retailers During a Labor Shortage

6 Tips to Get People Through the Door

Latest Articles

Inland Ports May Increase Efficiency for International Shipping

Reverse Logistics: Balancing Retail and Resale

Overcome Challenges with Omnichannel Inventory Management

Furniture Shopping Has Changed

Meeting the Needs of Convenience-Centric Customers

Keeping Your Brand Front-Of-Mind When Customers Are Away

8 Important Tips to Improve Shipping and Delivery

Advanced Inventory Management for Specialty Retailers

CONTACT
Call 800-237-5913 x101
or email us.

4625 East Bay Drive Suite 201
Clearwater, FL
33764