Centreville Bank

Transcript for ID Theft For Business From Centreville Bank

Introduction

Most company's keep sensitive information in their files... whether it's names, Social Security numbers, credit cards, or other account data that identifies customers or employees. Businesses often need this information to fill orders, meet payroll, or perform other business functions. But if the information falls into the wrong hands... it can lead to fraud or identity theft. The cost of a security breach can be measured in the loss of your customer's trust and perhaps even a lawsuit... which makes safeguarding personal information just plain good business. I'm Pablo Zylberglait, an attorney at the Federal Trade Commission. The FTC thinks protecting personal data is important... we also think this tutorial has some great tips and tools to help you do just that. So let's get started. A sound data security plan is built on five key principles. Take Stock. Know what personal information you have in your files and on your computers. Scale Down. Keep only what you need for your business. Lock It. Protect the information that you keep. Pitch It. Properly dispose of files or data you don't need anymore. And Plan Ahead. Create a plan to respond to security incidents. Let's walk through those five principles so you can see how your company's practices measure up... and where you might want to make some changes. Ready?

Overview

Effective data security starts with an assessment. Taking stock of what information you have and who has access to it. Understanding how personal information moves into, through and out of your business... and who has or could have access to it... is essential to figuring out your security vulnerabilities. So where do I begin?

Where Do I Begin?

Start by taking an inventory... do an audit of what you got. Your file cabinets and computers are a good place to start but remember... most business get personal information in a lot of different ways... through websites, from contractors, from call centers. Inventory all computers, laptops, flash drives, disks, home computers, cell phones and other equipment... to find out where your company stores sensitive data. "But how can I keep track of all that personal information?" Talk to your sales department, your IT staff and your HR office. Don't forget your accounting staff and any outside service providers you use. Then ask a few questions. Who sends personal information to your business and how do you receive it? "We get personal information from customers..." "credit card companies, banks and credit bureaus." "Sometimes it's sent through websites." "Sometimes by email and sometimes the U.S. mail." What kind of information do you collect at each entry point and where do you keep it? "We get credit card information from clients." "Our accounting department keeps customer's checking account numbers..." "and the information can be stored, well, in a lot of places." "In our central computer databases..." "on individual laptops..." "on disk and tapes..." "in their file cabinets..." "in our branch offices..." "some employees might even have that information at home." Remember to ask who has access to the information? Which employees have permission to have it? Can anyone else get ahold of it? What about vendors who supply and update the software you use

to process credit card transactions? Or contractors who operate your call center. “That’s a lot to keep track of.” “But I can see that it’s worth it.” It’s a new way to think about information and security. But it’s not only doable, it’s essential. “Should I be handling all information in the same way?” Different types of information present different levels of risk. The fact is, some information is more valuable to thieves. You need to pay special attention to how you keep personally identifying information. Those Social Security numbers... that credit card or financial information... and other sensitive data. That’s what crooks usually use to commit fraud or identity theft.

Laws And Requirements

“Do any laws require my company to keep sensitive data secure?” Yes. Federal laws like the Gramm–Leach–Bliley Act... the Fair Credit Reporting Act... and the Federal Trade Commission Act... may require that businesses in your industry provide reasonable security for sensitive information... and you’ll want to check into state and local laws too.

Chapter Notes

Overview

“The question I keep asking myself is what kind of information should I keep?” “And of course, what kind of information shouldn’t I keep?” That’s the second principle, Scale Down. Keep only what you need for your business. If you don’t have a legitimate business need for sensitive information, don’t keep it... in fact, don’t even collect it in the first place. And if you do have a legitimate business need for the information... keep it only as long as necessary.

Storing Customer Information

“We usually create a permanent file about our customers.” “That’s where we keep information from the magnetic stripe on their credit cards.” “Are we putting their information at risk?” Yes you are. Keep sensitive data only as long as you have a business reason to have it. Once that business reason is over... dispose of the data properly. If it’s not in your system, it can’t be stolen. “Well that makes sense to me.” “But we also collect a lot of Social Security numbers.” “How do I handle those?” Use Social Security numbers, only for required and lawful purposes... like reporting employee taxes. In this day in age... don’t use Social Security numbers unnecessarily. For example as an employee or customer identification number... or just because you’ve always used them.

Storing Credit Card Numbers

“I think our software saves credit card numbers.” “What can I do about that?” Check the default settings. Sometimes they’re preset to keep information permanently. Change it, to make sure you’re not keeping anything you don’t need.

Written Retention Policies

“But what if I have to keep certain information?” If you must keep information for business reasons or to comply with the law... develop a written record retention policy. Identify what must be kept... how it should be secure... guidelines for how long to keep it, and ways to dispose of it securely when you don’t need it anymore.

Chapter Notes

Overview

“What’s the best way to protect information that you absolutely have to keep?” The answer really depends on the kind of information your dealing with and how it’s stored. The most effective data security plans deal with four important elements... Physical Security... Electronic Security... Employee Training... and the Security Practices of your Contractors and Service Providers. Many data compromises happen the old fashioned way... through lost or stolen paper documents. So much of the time, the best defense, is a locked door or an alert employee.

Control Access

Control who has access to your offices. Tell employees what to do, and who to call if they see somebody unfamiliar on the premises. If you have offsite storage facilities... limit access only to employees with a legitimate business need. Know if and when someone accesses the storage site.

Computer Security

“What about computer security?” Computer security is everyone’s business, not just the IT staff. Make sure you understand the vulnerabilities of your computer system... and follow the advice of experts in the field to make it safe.

What Is A Firewall?

“What is a firewall?” “And how do I know if ours is good enough?” A firewall, is software or hardware, designed to block hackers from getting into your computer. “I’ve heard of a border firewall, what’s that?” A border firewall, separates your network from the internet and can prevent an attacker from getting to where you store sensitive information. It’s important to allow only trusted employees with a legitimate business need to access the network. To do this, set the access control settings... to determine who gets through the firewall and what they will be allowed to see. The protection a firewall provides is only as effective as its access controls... so review them periodically.

Detecting A Security Breach

“How do we know our systems are working?” “How do we detect a breach?” Your best bet to detect a network breach, is to use an intrusion detection system. To be effective, you really have to update it often.

Sending Data Thru Email

“We encrypt the financial data customers submit on our website...” “but once we receive it, we decrypt it and then email it to our branch offices.” “Is there a safer way for us to do this?” Glad you asked... regular email is not a safe way to send sensitive data. Any email with information that could be used by fraudsters or ID thieves, should be encrypted. “Another question.” “Do you have any tips on what kinds of computer passwords are best for security’s sake?” Experts say the longer the password, the better, because simple passwords like common dictionary words can be guessed easily. Insist that employees choose passwords with a mix of letters, numbers and characters. Require that an employee’s username and password be different... and that your employees change their passwords often.

Passwords

“Our account staff needs access to our database of customer financial information.” “To make it easier for people to remember, we use our company name as the password...” “sounds like that could create a security problem.” Yes it could. Hackers try words like password, your company name... the softwares default password and other easy to guess choices. They also use programs that run through common words and dates.

Employee Training

Your data security plan may look great on paper... but it's only as good as the employees who implement it. Take time to explain the rules to your staff, and train them to spot security vulnerabilities. Periodic training emphasizes the importance your business places on data security. A well-trained workforce may be your best defense against ID theft and data breaches.

Third Party Outsourcing

Your company's security practices depend on the people who implement them... that included contractors and service providers in addition to your employees.

Chapter Notes

Overview

Trash can be a gold mine for an identity thief... leaving credit card receipts, credit reports, papers or cds with personal information in a dumpster... exposes your customers to the risk of identity theft and fraud. By properly disposing of sensitive information... your doing your part to insure that it can't be read or reconstructed. "So what's the safest way to get rid of documents or files we don't need anymore?" It depends on the sensitivity of the information, the costs and benefits of different disposal methods and changes in technology... as well as the nature and size of your business.

Data Stored On Computers

"What about computers?" When your getting rid of old computers and portable storage devices, use wipe utility programs... there inexpensive and can override the entire hard drive so the files can't be recovered. "Can't I just delete files using the delete key?" Deleting isn't good enough because the files can remain on the computer's hard drive which means they can be retrieved easily.

Home Based Employees

"What about employees who work from home?" Good point. Make sure employees who work from home follow the same procedures for disposing of sensitive documents... old computers and any portable storage devices.

Discarding Information

"My company collects credit applications from customers." "The forms I use ask for a lot of financial information." "Once were finished with the applications we're careful to throw them away." "Is that good enough?" It's not. At least not for smart, security minded companies. Ensure that sensitive paperwork is unreadable before you throw it away. Like I said... burn it... shred it... or pulverize it to make sure ID thieves can't steal it from your trash.

Paper Records

"So with paper?" Get rid of paper records by shredding... burning or pulverizing them before discarding. Put shredders throughout your office, including next to the photocopier.

Chapter Notes

Overview

"As a chef..." "I live by plans..." "but I never thought of making a plan to keep my data secure..." "let alone my customer's and supplier's data." Security is important to your business and your customers. Taking steps to protect the data you're holding can go along way toward preventing a security breach. Have a plan in place to respond to security incidents. Start by designating a senior member of your staff to implement it.

Working Within Your Budget

“I own this business.” “Will these precautions cost me a fortune?” I got good news for you... no, they’re not going to cost you a fortune and frankly a breach can be much more expensive than implementing a plan upfront. But there’s no one size fits all approach to data security. What’s right for you depends on the nature of your business and the kind of information you collect. Some of the most effective security measures... using passwords... locking up sensitive paperwork... training your staff... will cost you next to nothing. In fact you’ll find free or low cost security tools at nonprofit websites dedicated to data security. As I said, good security is just good business.

Chapter Notes

Summary

So when it comes to protecting personal information for your business, remember the following principle... Take Stock. Know what personal information you have in your files and on your computer. Scale Down. Keep only what you need for your business. Lock It. Protect the information that you keep. Pitch It. Properly dispose of what you no longer need. Plan Ahead. Create a plan to respond to security incidents. For more information check out the links in the Additional Resources section of this tutorial. And don’t forget to print your own note to self. On behalf of the FTC, I hope this tutorial has helped you understand how best to protect personal information. After all, it’s just plain good business.