insureon

Data Breaches & Retail

A Guide for Small-Business Owners

TABLE OF CONTENTS

© 2015 insureon, a BIN Insurance Holding Agengy

Introduction:

Cyber Risks and Data Breaches at Your Store

Cyber Risks and Data Breaches at Your Store

During the busy holiday shopping season of 2013, the retail world received a shock when Target's stores were hacked – credit card data for millions of customers was stolen in what was than the biggest data breach of all time. By now, that story is old news. But the risk isn't.

Mom-and-pop shops and major retailers alike are being hit with data breaches. In fact, Verizon's 2014 Data Breach Investigation Report found that **31 percent** of all data breaches attack point-of-sale systems like the one in your store. Whether you have a credit card terminal or an iPad with a point-of-sale (POS) app, your store could be a target (pardon the pun) for hackers looking to steal credit card data.

But that's only part of the story: data breaches are expensive. Even if your retail business is small, a data breach could leave you with exorbitant cleanup costs. That's why we've written this eBook.

In the following pages, we'll dive into data breaches, providing an overview of what retailers can do to:

- Minimize their risks.
- Improve their technology.
- Prevent breaches.
- Prepare for the cost of a data breach.

data · breach

noun

unauthorized access of a business's protected information

WHAT A DATA BREACH MEANS FOR A RETAILER

Unless you're a tech expert, you might be uncertain about what exactly a data breach is. No worries. Data breaches occur when an unauthorized person gains access to your data. We'll explain how this can occur in the section "What Are Data Breaches?" For now, you should know that criminals can break into your data through many channels, ranging from sophisticated cyber attacks to dumb tricks like guessing your password.

In addition, your employees can access sensitive data when it’s not adequately protected. Employee-led breaches may be accidental or malicious; either way, they have the potential to hurt your business.

For retailers, data breaches are costly. After a breach, you'll have to pay for all kinds of services, upgrades, and other costs that come with cleaning up 21st-century theft and fraud. These costs include...

- Credit monitoring services for your customers (to prevent identity theft).
- IT professionals to investigate the incident and find where the breach occurred.
- Crisis management.
- The cost to notify customers whose data may have been stolen.

© 2016 insureon, a BIN Insurance Holding Agengy

And there's more. A store might have thousands of customers. Imagine having to deal with all those complaints and questions. The amount of time you'll spend responding to a breach will be a huge drain on your business. In fact, according to a report by Experian [PDF], **60 percent** of hacked small businesses close up shop within six months.

It should be no surprise to learn that data breaches can be devastating for a retailer's reputation. That's especially true for small businesses. You're working to attract new customers to your business, but a breach could be enough to convince even your most loyal customers to shop elsewhere.

90

90% of breaches in 2014 were preventable.

IS THERE ANY GOOD NEWS ABOUT DATA BREACHES?

Yes, there is. Many data breaches are preventable. For those that aren't, the costs (while huge) can be managed with proper financial planning and investment in Cyber Liability Insurance.

Small-business owners have the power to prevent many of the data breaches that could destroy their business. As ZDnet reports, more than **90 percent** of the data breaches that occurred in the first half of 2014 were preventable. In this eBook, we'll go into detail about what you can do at your store to prevent data breaches. These strategies will be both technical (e.g., investing in certain technologies) and practical (e.g., improving the ways you handle data).

And then there's the cost of breaches. Insurance carriers have responded to the spree of data breaches, and now many offer Cyber Liability Insurance (also called Data Breach Insurance) to cover the costs we listed in the section above. Just as a fire could wipe out your store, a data breach could overwhelm your business with IT costs, repairs, and other expenses. Data Breach Insurance offers financial security to protect you from these costs.

By the time you finish this eBook, even if you're not tech-savvy, you'll understand...

- Which cyber risks are most threatening to your retail business.
- How you can prevent data breaches.
- How to prepare for the cost of a data breach.

While nobody can prevent all data breaches, this eBook should help you better understand your risks and how to mitigate them.

© 2016 insureon, a BIN Insurance Holding Agengy

Chapter 1:

Which Retailers Are Most Vulnerable to Data Breaches?

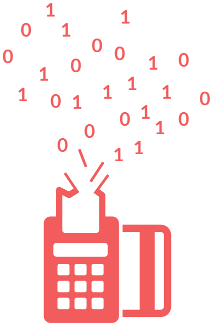
Which Retailers Are Most Vulnerable to Data Breaches?

Nearly all retailers are vulnerable to data breaches. From billion-dollar companies to small seasonal shops, almost any retailer can be hacked and face the extraordinary cost that comes with a data breach.

Why are retailers so vulnerable? If you accept credit cards or online payments, your business has a POS system or other electronic system to process the payment. Your customers' financial information passes through that system. That means that cyber criminals and employees can attack this spot to potentially steal customer data and use it to commit identity theft.

Unless your business only accepts cash, you're at risk of a data breach (and even then, a thief could walk off with record books). In this section, we'll go into more detail about why you have this risk. Read on to learn...

- What data breaches are.
- How they happen.
- Where retailers are most exposed.



WHAT ARE DATA BREACHES?

A data breach is an incident in which confidential information – credit card numbers, Social Security numbers, addresses, etc. – falls into the hands of people who are not authorized to have it.

Often, this happens when criminals breach your network by hacking your software or POS system, but that's not the only way a data breach happens. In fact, the following scenarios are all considered data breaches:

- Theft of laptops, computers, and mobile phones that contain customer data.
- Theft of POS devices (iPads or cash registers).
- Network hacks carried out by cyber criminals.
- Theft by POS skimmers (devices attached to your card readers used to steal data as your customers swipe their cards).
- Hacks into email, cloud, or online sales accounts that store business records.
- Improper employee access of sensitive customer information.

We'll go over these threats in more detail in the section "How Do Data Breaches Happen to Retailers?" For now, let's just take one as an example: laptop theft.

Many small-business owners don't realize that a stolen laptop could actually count as a data breach. Remember that as a storeowner you have to protect all your customers' data, not just their credit card info. Your laptop's hard drive might contain customer records, mailing lists, and other protected data.

© 2016 insureon, a BIN Insurance Holding Agengy

If that's the case, you may be legally obligated to inform customers their data has been compromised. You weren't "hacked," and the thief may have no intention of committing fraud, but your customers' data is now in someone else's hands and you may have to report the breach.

For more information on your obligations following a breach, take a look at this state-by-state guide to data breach laws.

WHY DATA BREACHES ARE MORE THAN JUST STOLEN DATA

When we talk about data breaches, we're really talking about fraud. Criminals steal data in order to commit fraud against your customers. By stealing addresses, credit card info, or other data, criminals can…

- Commit identity theft against your customers.
- Make purchases under a customer's name.
- Apply for loans.
- Steal money directly from your customers' bank accounts.

Say your company is hacked and you lose credit card records for 100 customers. Compared with the mega-breaches you read about in the news, this breach is tiny. Cyber criminals may end up only using a few of those customers' credit cards illegally. But even for a small attack with minimal financial loss to your customers, your store will rack up data breach expenses. You might have to pay for…

- **IT experts** to look over your payment system, find out how it got hacked, and fix it.
- **A year of credit monitoring** for all 100 customers (even if only one or two were victims of identity theft – after all, some damage could happen down the road).
- **Notification of all affected customers** and resources for handling their complaints.

In addition to the time, expense, and headache that come with a data breach, you'll also have to deal with the reality that your business just suffered a devastating blow to its reputation.

When you look at a data breach this way, it's easy to see why it has little to do with data – it's the cost that comes along with breaches that make them so harmful to retailers.

fraud

noun

a deliberate deception, perpetrated for unlawful profit or gain.

© 2016 insureon, a BIN Insurance Holding Agengy

WHAT IS A HACKER?

Before we go any further, we should take a second to talk about hackers and cyber criminals. You've probably read about "hackers" in news stories about data breaches. The word may conjure the image of a cyber punk with green hair. The word "hacker" implies that there is someone out there who is specifically going after your company. But this stereotype isn't accurate at all.

Instead of "hacker," you should really be thinking about this person as a criminal or thief. Hackers are cyber thugs who use technology to break open your network and steal data that they can sell or use to commit fraud.

Having trouble believing that a hacker would target you? Then here's a wakeup call: many cyber criminals are merely committing "crimes of opportunity." Just as burglars might pass an unmanned delivery truck and grab some goods, cyber criminals strike businesses if the opportunity presents itself. For example, it might happen like this:

- They use automated software to scan your business.
- They test whether you're vulnerable to certain attacks.
- They smash open your network to see if there's anything valuable inside.
- They might not steal much of anything, but you'll have to deal with the cleanup costs.

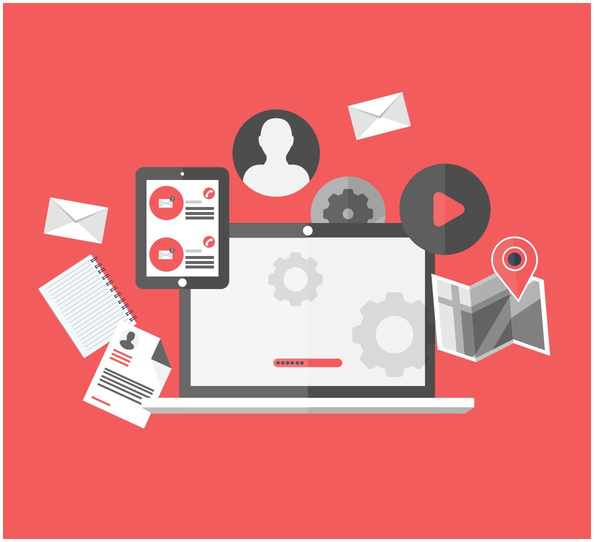
While Hollywood portrays hackers as computer wizards with funny hair, the reality is that, like other criminals, they're just looking to cause damage, steal valuable property, and commit fraud. They're looking to get quick money by robbing your store's data.

WHY DO DATA BREACHES HAPPEN TO RETAILERS?

The simple answer is cyber criminals break into retailers' computers because they process lots of customer information, including credit card numbers, names, addresses, email addresses, phone numbers, and other information that's highly valuable to thieves.

Why do they want this data? As we've mentioned, cyber criminals can use it to commit fraud. By taking your customers' personal information, a criminal could sign up for a loan in their names or make bogus purchases by using their credit card information.

Cyber criminals know that retailers are sitting on stockpiles of data and so they attack, targeting your store's network, POS system, or e-commerce site.

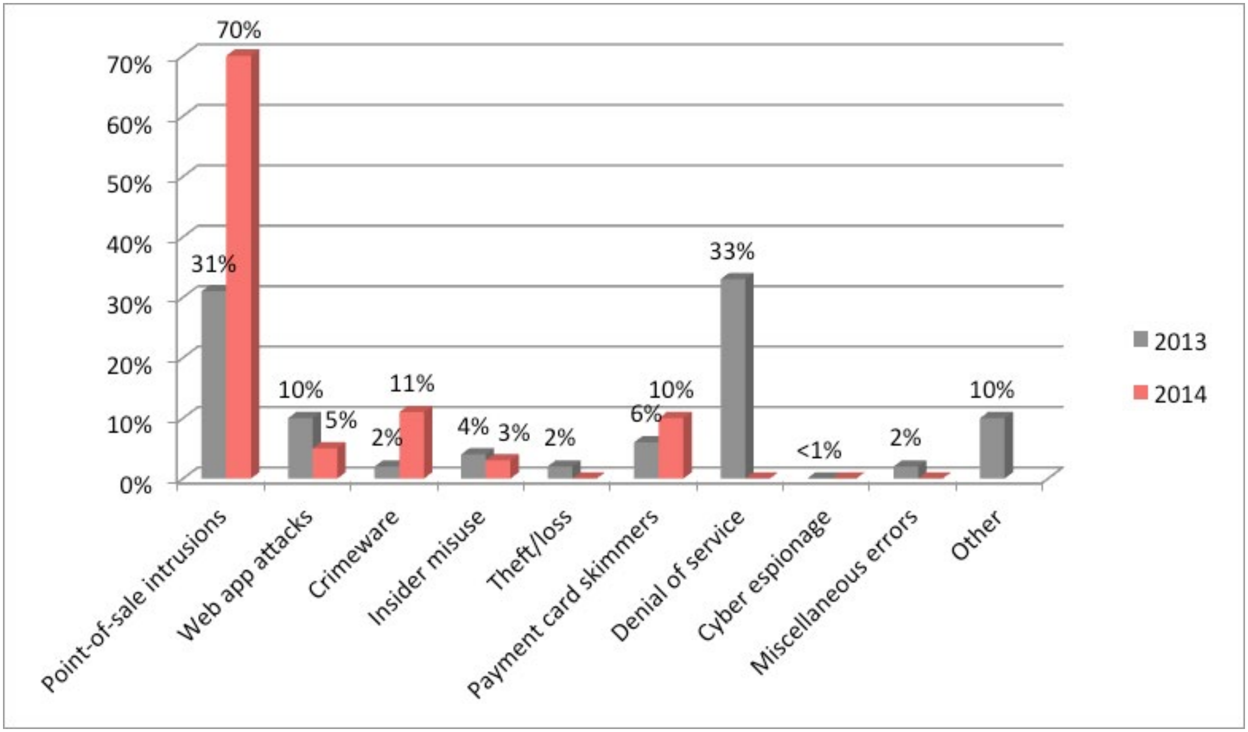


© 2016 insureon, a BIN Insurance Holding Agengy

LURKING IN THE SHADOWS OF RETAIL

Each year, Verizon publishes a Data Breach Investigation Report that tracks how cyber criminals attack various industries. We won't overwhelm you with the technical details, but a quick look at the techniques cyber criminals use will help us see where your store is vulnerable and year-over-year changes between 2013 and 2014.

CAUSES OF RETAIL DATA BREACHES



Source: Verizon 2013 and 2014 DBIR

© 2016 insureon, a BIN Insurance Holding Agengy

Here's a breakdown of the most common causes of retail data breaches:

- **Point-of-sale intrusions**. By breaking into your POS system, hackers can directly harvest your customers' private information and illegally download it.
- **Crimeware**. Crimeware is a name for the specific malware that has been designed to help criminals break into a network, find personal information, and steal it.
- **Payment card skimmers**. A skimmer is a physical device that's attached to your payment card terminal. These devices are sometimes laid over the card reader, so that your customers unknowingly swipe cards through them.
- **Web app attacks**. If your store has an online or mobile presence, cybercriminals can bully their way inside by breaking into your web apps.
- **Insider misuse**. Your own employees or contractors could install malicious software or download customer data in order to use it for fraud.

Interestingly, the attacks we saw in 2014 were a little different than in the previous year.

Cyber criminals regularly change their methods to take advantage of vulnerabilities.

In 2013, **33 percent** of breaches resulted from DDoS attacks, where criminals overload your servers with traffic in order to break in. The next year, criminals changed their targets and focused more on point-of-sale systems. What does this tell us? Every year, cyber criminals adapt their strategies when they find better techniques or changes in technology make certain targets more vulnerable.

The Point-of-Sale System: A Frequent Target for Cyber Criminals

While hackers adapt their strategies, they will always target your point-of-sale system because that's where your transactions occur. Small retailers might be especially susceptible to these attacks because they have less tech knowhow and smaller IT budgets than their larger counterparts.

The Verizon report explains that cyber criminals actually attack small and large retailers differently. Here's how:

- **Large retailers**: Sophisticated attacks are used to break into computer systems, then malware worms its way onto their POS system.
- **Small retailers**: Cyber criminals usually don't have to work that hard. They can often guess the passwords on POS systems because small retailers sometimes keep the factory default settings or forget to update their software.

In other words, small retailers can shoot themselves in the foot by not taking basic precautions with their POS system. Remember: **90 percent of data breaches in the first half of 2014 were preventable**. That's because a lot of us (retailers and others) are skipping simple steps that could keep hackers out.

© 2016 insureon, a BIN Insurance Holding Agengy

Chapter 2:

What Happens When Your Store is the Victim of a Data Breach?

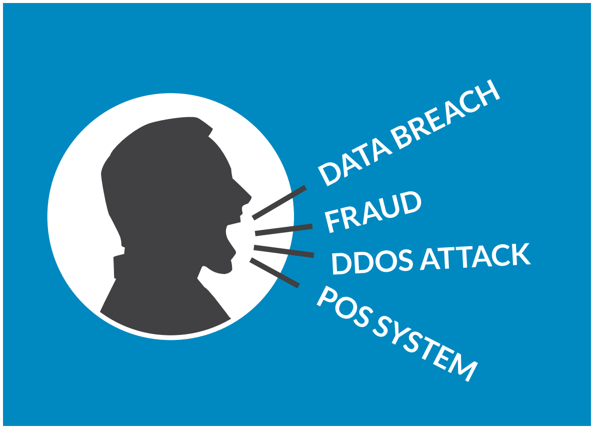
What Happens When Your Store Is the Victim of a Data Breach?

When discussing data breaches, it's easy to get lost in the technical jargon. So let's look at it from another angle: what does a data breach mean for your store?

By taking this perspective, we won't be looking at the technology side of things. You won't have to know anything about software, hardware, or hacks. Instead, we'll focus on what you have to do after a breach and what impact a data breach might have on your store's bottom line.

In this section, we'll explore the impact of data breaches, looking at...

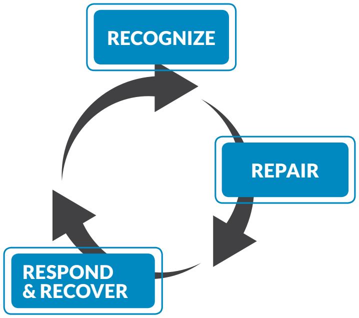
- The lifecycle of a data breach for small retailers.
- The business side of things.



LIFECYCLE OF A DATA BREACH FOR SMALL RETAILERS

A data breach isn't a one-and-done occurrence. Breaches are really the beginning of a series of headaches, legal expenses, and unplanned costs that can overwhelm storeowners.

If you've never had a breach at your store, you're probably unfamiliar with everything involved. So let's start with the basics. You can typically divide a breach into three phases:



1. **Recognize:** discovering the data breach.
2. **Repair**: fixing the data breach.
3. **Respond & Recover**: handling inquiries, notifying authorities, and helping customers avoid identity theft.

But even these three phases don't really paint a clear picture of what you'll have to do during a breach. Let's start with day one, when you've just discovered the breach.

© 2016 insureon, a BIN Insurance Holding Agengy

DAY ONE OF A RETAILER DATA BREACH: HERE'S WHAT HAPPENS

The moment you learn about a data breach, it's already too late. Cyber criminals have already broken into your store, stolen its data, and may have already committed identity theft against some of your customers.

Verizon's data breach study shows that, **60 percent** of the time, criminals are able to compromise an organization within minutes – yet it can take weeks or months for an organization to notice it's been breached.

You read that right: a data breach only takes minutes. By the time you finish reading this section, a hacker could have broken into your network. And you probably wouldn't have noticed.

So how do you find out you've been hacked?

- Often, law enforcement officials contact you to tell you that there's been a pattern of identity theft among your customers.
- Law enforcement officials, banks, and security professionals track reports of identity theft.
- When a pattern emerges – i.e., the victims all shopped at your store in the last six months – it's safe to assume that there's a breach.

Remember that famous data breach at Target? Well, Target discovered and stopped the breach on December 15, but criminals had been stealing data since November 27. Despite all the security professionals Target employs, it took weeks for the company to realize what had happened.

DATA BREACH TIMELINE: INS AND OUTS

After discovering a data breach, you'll have to fix the issue that led to the breach and try to control its damage. These two steps are interrelated. After law enforcement officials, banks, or security professionals notify you that your store's been hacked, you'll want to take these steps:

1. Contact your insurance provider if you have Cyber Liability Insurance.
2. Hire a security professional and contact your POS service provider to figure out where the breach is occurring.
3. Patch your system, upgrade, or take other measures to stop the leak.
4. Review your legal obligations and state data breach laws.
5. Contact the state attorney general or consumer protection agencies, and contact customers affected by the breach (if required by state law).
6. Offer free credit monitoring to customers (not always required by law).
7. Handle customer complaints and respond to ongoing inquiries.

© 2016 insureon, a BIN Insurance Holding Agengy

Depending on the size of your breach, it could take months or even up to a year to fulfill these obligations. States often require you to notify customers within 30 or 45 days of discovering the attack. So you'll have to work quickly to get your IT repaired and make sure you're ready to handle the influx of complaints.

THE HIDDEN BENEFIT OF CYBER LIABILITY INSURANCE FOR STORES

Cyber Liability Insurance can not only pay for many of these costs, but also help ensure you're meeting your legal obligations. Your insurance agent can put you in touch with crisis management teams, IT experts, and other data breach professionals who've been there before.

As we saw above, there will be plenty to worry about once you get the news your store has been hacked. Between offering credit monitoring to customers and finding the source of your data leak, it's easy to get overwhelmed. Data Breach Insurance helps make sure you don't miss anything in your data breach response plan.

WHAT HAPPENS ON THE BUSINESS SIDE OF THINGS?

A data breach is many things – it's a loss of trust, a PR nightmare, and a huge, unplanned expense. For retailers, a breach means that you have legal and professional obligations to repair your technology and protect your customers' data. This can have a huge impact on your budget.

Breaches can affect your bottom line in two ways:

- **Direct costs** for repairs, response, and other expenses that come with the breach
- **Indirect costs** and lost revenue as a result of damage to your business's reputation

How Much Will a Data Breach Cost a Retailer?

In the previous section, we looked at the Lifecycle of a Data Breach for Small Retailers, but we didn't actually talk about costs. In addition to the direct costs we discussed in the previous section, your business may be affected in other, indirect ways, including:

- Lost customer trust
- Lost revenue from slow sales
- Increased advertising and PR costs as you seek to rebuild your reputation
- Profit loss from discountsand free services offer to your customers.

© 2016 insureon, a BIN Insurance Holding Agengy

In other words, data breaches hurt your ability to make money by damaging your reputation, while also presenting new bills for IT repairs, crisis management advice, and upgrades.

The Ponemon Institute's Cost of a Data Breach Study estimates that retailers should expect to pay $105 for each customer record compromised in a data breach. If you breach involves data for 100 customers, it might cost $10,000. For 1,000 customers, you could be looking at a six-figure bill.

Financial Security for Retailers

Cyber Liability Insurance offers two main benefits for retailers: cost certainty and guidance. Was your head spinning while we went over your legal obligations after a data breach? Would you have any idea how to find a data leak if you're hacked? Cyber Liability Insurance policies can help fund the IT forensic investigation, data monitoring, and customer notification often required after a breach.

Cyber Liability Insurance typically covers…

- Crisis management teams.
- Credit monitoring for your customers.
- Data breach notification costs.
- IT investigations.
- PR assistance.

By paying for the cost of hiring security and PR professionals, Data Breach Insurance can help ensure you don't botch your data breach response. Given how quickly data breach costs add up, having insurance in place may offer you some protection for the financial risk that comes with cyber crime.

$105 = cost of each customer record compromised in a data breach

© 2016 insureon, a BIN Insurance Holding Agengy

Chapter 3:

Data Breach Prevention for Small Retailers

Data Breach Prevention for Small Retailers

In this eBook, we've seen how costly data breaches can be – even small data breaches can cost tens of thousands of dollars – so let's talk about what you can do to prevent them.

Below, we'll go into detail about building a data breach prevention plan that will…

- Train your employees about common security threats.
- Help you maintain Payment Card Industry (PCI) compliance.
- Encourage data security best practices at your store.
- Keep your technology up to date and take advantage of the latest security measures.

HOW TO PREVENT DATA BREACHES AS A SMALL RETAILER

Instead of data breaches, let's pretend we're talking about preventing theft at your store. What would you do to curb theft?

- Develop a plan.
- Train employees about their role.
- Implement a system to monitor inventory.
- Adopt best practices and invest in technology and other resources to help you.

The same overall strategy holds true for data breaches. Sounds simple, right? You'll develop a plan, train your employees, and make sure your store has the right technology and resources. Of course, nothing is ever quite that easy. Below we'll go into more detail about industry-standard data breach prevention strategies and what you can do to avoid bumps in the road.

> Data breach prevention works on the same principles as shoplifting prevention.

© 2016 insureon, a BIN Insurance Holding Agengy

PLANNING FOR DATA BREACHES IS KEY TO PREVENTING THEM

Let's talk about why planning is a smart move. Like shoplifting, some data breaches can be averted simply by establishing a workplace that takes these threats seriously.

If your employees are on the lookout for theft and you regularly check inventory, you may prevent it through diligence. That's what you want to do with breaches. If you're conscientious, you may nip problems in the bud or minimize the damage caused by any breaches that do happen.

To establish this kind of workplace, your data breach plan should include...

- ☑ Employee training
- ☑ A strict password policy
- ☑ Limits on how store computers are used

In addition, your plan should outline responsibilities and actions to take in the event you store is hacked. To do so, make sure to include...

- ☑ Contact information for IT experts and other professionals who work with your cyber security
- ☑ Information about state data breach laws and customer notification guidelines
- ☑ Your small business insurance policy coverage details and your insurer's contact info

> It takes a village to prevent a breach. For best results, involve employees, an IT consultant, and your insurance agent.

© 2016 insureon, a BIN Insurance Holding Agengy

PREVENTING DATA BREACHES THROUGH EMPLOYEE TRAINING

You'll need to tailor your data breach training so that it makes sense for the type of retail business you run. E-commerce stores have different risks than brick-and-mortar retailers. Here are some of the general strategies you should use when training employees:

BREACH PREVENTION BEST PRACTICE	DO	DON'T
Require all employees to use unique and complex passwords.	Use a random mix of numbers, letters, symbols, and capitalization for all work passwords.	Use passwords like "123456" and "password." That's just asking for trouble.
Train your employees about common schemes and online threats.	Encourage employees to report to your IT specialist any suspicious emails or computer pop-ups urging them to click a link or open an attachment.	Ignore suspicious messages or behavior. The longer a breach goes undetected, the more damage it can do.
Teach all employees to report claims of fraud to you.	Train employees to pass all customer complaints to you. Sometimes customers are the first to see signs of fraud on their accounts.	Put off dealing with suspected fraud. The sooner you contact your IT consultant (and possibly insurance agent), the better.

Aside from in-house training and preparation, it's a smart idea to hire a security professional to look at your network, POS system, and store computers. But these security professionals can also help you institute policies and procedures that will help your store prevent data breaches.

Talk with your IT consultant or technology expert about tailoring a data breach prevention plan and training your employees to avoid common mistakes that make it easier for cyber criminals looking to break into your network. (Tip: even working with an IT consultant now and then can help give you an idea of where your weaknesses lie so you can bolster your system.)

© 2016 insureon, a BIN Insurance Holding Agengy

ACTIONS TO KEEP YOUR STORE'S TECHNOLOGY SECURE

You'll want to make sure your technology is up to date, but it's not always as simple as having this or that software. Secure technology is also about how you use it and how you store your data.

As we saw in "Why Do Data Breaches Happen to Retailers?" cyber criminals are often able to break into POS systems. Small retailers often don't change the factory settings on their technology and sometimes use the default password, making it easy for hackers to sneak in. Here are tips to help you improve your security and avoid common mistakes:

- **Limit the amount of data you have**. If possible, don't keep a backlog of customer records unless you actually use this data. The more data you have, the more data can be stolen , and the more expensive a breach can be.
- **Replace old technology**. If you're still using the same POS system you got in the 90s, you could be exposing your store to unnecessary risk. Newer technology generally has better encryption standards and may be easier to upgrade in the future.
- **Use PCI-compliant payment technology**. PCI compliance is the industry standard for businesses that accept credit and debit cards and other electronic payments. Having PCI-compliant technology is a must. In addition, storeowners can have their technology scanned to ensure it is secure (see ControlScan's PCI Compliance Guide for more information).
- **Secure your network**. Because your technology is all interconnected, you want to make sure that everything from your wireless router to your POS system is secure. Use firewalls and anti-malware software to do so.
- **Make sure data is encrypted**. "Encryption" refers to the way files can be scrambled so that outsiders can't read them. Even if criminals break into your network and download your data, they won't be able to read it. Changing the settings on your computers can encrypt your data when you're logged out. If necessary, hire an IT expert to make sure your technology is secure.

Don't hesitate to hire outside help if these strategies seem confusing. Many small retailers are used to doing things on their own, but remember that working with security experts can save you money in the long run if it helps you avoid a costly data breach.

© 2016 insureon, a BIN Insurance Holding Agengy

Conclusion:

Preventing Retail Data Breaches: A Final Word for Small-Business Owners

Preventing Retail Data Breaches: A Final Word for Small-Business Owners

We began this eBook with a startling statistic: **31 percent** of all data breaches attack point-of-sale systems. This high volume of attacks explains why we've seen so many retailer data breaches. Criminals are going after retail payment systems every day. Even stores with million-dollar IT budgets can be victims.

Cyber Liability Insurance may offer you cost certainty by paying for the cost to clean up a breach and take measures to prevent identity theft among your customers.

But as we saw in this eBook, even with insurance your business should be proactive about limiting risk and preventing breaches by...

- Training your employees.
- Keeping your POS system up to date.
- Working with IT professionals and payment processor experts.
- Having a plan that outlines the steps you need to take after a breach.

As a small-business owner, you don't have money to throw away, so it's important to have a strategy that minimizes your chances of being hit by a breach and sets you up for a fast recovery if one should occur.

© 2016 insureon, a BIN Insurance Holding Agengy