The Importance of the PCI DSS: Why You Should Get Compliant

Learn why getting PCI compliant should be important to you, your business, and your customers.

With the rise in data breaches comes the rise in changes and rules to the PCI DSS. For many businesses, getting PCI compliant is considered an unnecessary chore, and the fines breached businesses are given for not being compliant seems to increase that resentment.

So what's the point of the PCI DSS? Why should businesses be so concerned about getting PCI compliant? And is there any benefit to being compliant with the PCI DSS? We believe so.

Here are a few reasons why the PCI DSS is and should be important to your business.

Secures your business data

It's important to protect the data of your business and your employees. While you may be paying attention to physical security in your business, are you dedicating enough time to protect your information digitally? Between malware threats, remote-access attacks, and social engineering, it's important to take the proper precautions to keep your computers, networks, and servers secure.

The whole purpose of the PCI DSS is to protect card data from hackers and thieves. By following this standard, you can keep your data secure, avoiding costly data breaches and protecting your employees and your customers.

Boosts patient confidence

Would you go to a business if you knew it was likely your credit card information could get stolen? Probably not.

Customer confidence can really affect whether your fiscal year is profitable or not. People are less likely to take your business if they don't feel confident in you keeping their data safe. Two-thirds of US adults wouldn't return to a business after a data breach. Should you get breached, or if your customers aren't confident in your security, you could lose business.

Getting PCI compliant and promoting that to your customers shows your clients that you are serious about security and you're taking every precaution to keep their payment data safe. It gives them (and you) some peace of mind.

Protects your clients

Your clients trust you with their card data as they make transactions in your business. Should you get breached, you're not the only one that suffers. Your clients card data needs to be protected by your business. You are responsible for keeping their data safe while it's in your possession.

Remember that if you do fail to protect your customer's data, you are liable to lawsuits and fines, especially if you falsely told them your business was secure.

Provides a security standard

The PCI DSS provides a baseline of security requirements that help businesses know what to do and where to start on their security program.

Many organizations we speak to simply don't know where to begin with information security. Some may think simply locking the doors to their business is enough, others may not even see the need to secure their data. The goal is to reduce data breaches and following the 12 requirements provides a strong foundation.

The PCI DSS provides a standard that every business can and should follow. What's helpful is the standard does have specific rules for different businesses, depending on size, type, methods of storing card data, etc.

Helps you avoid fines and lawsuits

Should you get breached, not only will you deal with the loss of data, but you may deal with fines and lawsuits from customers and other organizations.

A good example is the Wyndham Hotel breach. After they were breached three times, Wyndham Hotel was sued by the Federal Trade Commission because they had falsely said they were secure after each breach. This lawsuit ended in a settlement, but it shows what repercussions you could get in the event of a data breach.

Other fines can include customer lawsuits, third-party lawsuits, government fines, card brand fines, and more.

If you're PCI compliant, you can reduce these fines and reduce the amount of lawsuits and liability your company may incur.

Reduces the cost of a data breach

Data breaches can cost you a lot in both money and customer confidence. There's the cost of replacing credit cards, paying fines, and paying compensations for what the customers have lost, not to mention investigation costs and audits. It all adds up pretty quickly.

Remember the Target breach? What you may not remember is how much it cost the business, which was over $162 million in 2013 and 2014. That's a pretty heavy price to pay for not being secure.

Here's a list of average costs your business could sustain in a data breach

- Merchant processor compromise fine: **$5,000 – $50,000**
- Card brand compromise fees: **$5,000 – $500,000**
- Forensic investigation: **$12,000 – $100,000**

- Onsite QSA assessments following the breach: **$20,000 – $100,000**
- Free credit monitoring for affected individuals: **$10 – 30/card**
- Card re-issuance penalties: **$3 – $10 per card**
- Security updates: **$15,000+**
- Lawyer fees: **$5,000+**
- Breach notification costs: **$1,000+**
- Technology repairs: **$2,000+**
- Loss of customer confidence: businesses often lose 40% of customers after a breach.
- Forensic investigation cost: **$10,000-$100,000**

So the total cost of a data breach could range between **$77,000 and $875,000**.

For many businesses, a data breach could easily shut them down for good. Target was fortunate to have enough capital and income to cover the costs, but most businesses aren't that lucky.

Getting compliant with the PCI DSS will help reduce cost by helping to prevent data breaches in the first place, but to also help prevent fines. If you can prove you were compliant, the fines won't be as bad if you weren't making the effort.

Get PCI compliant with StrongBox!

While many businesses may not see the PCI DSS is necessary, it is important to both businesses and their customers that they follow the requirements. After all, they're handling valuable information about their clients, and should that information get stolen, it has repercussions beyond just a simple theft.

Also keep in mind that the PCI DSS is the bare minimum you should do to safeguard against breaches that have occurred. You should be compliant with PCI DSS and build from there to address issues that could be specific to your industry or environment.

Every PCI DSS requirement is there because a breach could have been prevented by having that control in place.

Take the extra time and money to make sure your business is complying with the PCI DSS standard. By doing so, you're protecting your business, your employees, your clients, and your brand.

StrongBox eSolutions LLC