

Hello. It looks like you're using an ad blocker that may prevent our website from working properly. To receive the best experience possible, please make sure any blockers are switched off and refresh the page.

If you have any questions or need help you can email us

businesses. As of 2016, there were over 3 billion internet users, so this number is quickly approaching half of the world's estimated population. Similarly, internet ...

Nov. 15, 2016

The growth of the internet has been a distinct boon to everyone — especially small businesses. As of 2016, there were over 3 billion internet users, so this number is quickly approaching half of the world's estimated population. Similarly, internet commerce is quickly becoming a key part most modern economies. In the U.S., e-commerce sales alone **topped \$340 billion** in 2015.

All of these sales must pass through secure, online servers, either hosted by the company or remote cloud servers hosted by one of many cloud hosting services. While all of these sales are beneficial to companies, it often requires the transfer of a significant amount of data. Much of that data includes customer account information, such as usernames, passwords, and identifying information such as addresses, phone numbers and, at times, even Social Security and credit card numbers.

Although there are federal regulations dictating how businesses of every size handle private information (HIPAA, SOXBY, PCI-DSS, GLBA, FERPA, et. al.), many small businesses assume that simply meeting these regulations is enough. However, small businesses are a unique target for hackers and data breaches do occur, with increasing regularity. While many big businesses make the news, it's small businesses that are often targets. According to the **First Data Corporation**, 90% of all data breaches that occur affect small businesses.

Data Breaches Are Costly

A 2015 Ponemon Institute **report** shows that the average cost of a data breach was \$154 per record overall, and \$170 per record for malicious cyberattacks. These numbers

include the costs associated with detecting and responding to a data breach. Data

Hello. It looks like you're using an ad blocker that may prevent our website from working properly. To receive the best experience possible, please make sure any blockers are switched off and refresh the page.

If you have any questions or need help you can email us

policies in place, most small businesses are at a high risk of seeing significant out-of-pocket expenses should a data breach occur.

Cyber Insurance is Misunderstood

In most cases, the reason why a business may lack the proper [cyber insurance protections](#) is a mixture of confusion as to which party is liable, and incomplete information regarding the restrictions of their own insurance policies. Most small businesses already have several forms of insurance, however few standard insurance policies, such as a General Liability or Professional Liability policy, will also cover liability for data breaches, or they'll only cover a restricted amount. At times, a cybersecurity or data breach endorsement can be added to a more common insurance policy, but this needs to be inquired about specifically.

The assumption that a policy extends to data breaches also lies in the fact that it's not necessarily intuitive to understand culpability in the event of a data breach. Many businesses believe that the fault or responsibility in a data breach lies not with them, but with the credit card company or data hosting service, if for example they keep sensitive data in the cloud. However, even if someone's account information is fraudulently used, the source of the breach can, and often will be, held at fault.

On a similar note, many businesses believe that software companies should bear some brunt when holes are found in their software that leads directly or indirectly to a breach. Even still, the business where the breach occurred will usually be found responsible. Faulty third-party software does not excuse a company from liability, even if the business was not fully responsible for the breach.

Additionally, First Data found that in 2011, 96% of businesses that suffered a data breach were not compliant with federal regulations meant to protect customer credit card data. One would hope more companies are conscious of the dangers 5 years later,

but for a new business owner these regulations may seem confusing and it may seem

Hello. It looks like you're using an ad blocker that may prevent our website from working properly. To receive the best experience possible, please make sure any blockers are switched off and refresh the page.

If you have any questions or need help you can email us

CoverWallet, a startup dedicated to simplifying insurance for small businesses. Previously, she launched the personal insurance team at NerdWallet, and helped create an innovative brokerage comparison product.

Firm Management

CPA Practice Advisor is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing professional education on the National Registry of CPE Sponsors.

© 2024 Firmworks, LLC. All rights reserved