Alternative Balance
Professional Group

# Cyber Liability Insurance: A guide to protecting your online business

It’s a new decade, and our lives are more steeped in technology and the Internet than ever before. Almost everything we do depends on being connected instantly via wireless transmissions, satellites, fiber optics, and more. From smartphones to tablets and ever-thinner laptops, our information is available to us within moments right from our fingertips. Unfortunately, that means other people have instant access to our private information as well—and not always with good intentions.

By learning about the risks of cyber attacks and how to prevent and manage their effects, you can get ahead of hackers and those who wish to sell your clients’ information to the highest bidder.

## Most Prevalent Cyber Attacks are on Small Businesses

In 2018, a whopping 43% of cyber security breaches involved small business victims (Verizon, 2019). Luckily, that’s down from 58% in 2017 (Verizon, 2018). This is proof that knowledge is power and can protect small businesses and their clients.

Another significant aspect of cyber attacks is how long it takes to discover the attack. With small businesses, the chance for an attack to go unnoticed is significantly higher than with a large company that has the resources to monitor their systems 24/7. With fewer employees, unnatural patterns in website usage or social media logins can remain hidden for months. According to the Verizon (2019) report, 56% of breaches took months or longer to discover. When that amount of time passes, user information can be bought and sold multiple times to people looking to steal identities, engage in credit theft, and illegally access users' bank accounts.

Further, while 39% of breaches were committed by organized criminal groups, 23% of breaches came from "internal actors" (Verizon, 2019), including people like negligent system admins, customers (end-users), and other insiders who already had some kind of access to the systems. Data security breaches don't have to be malicious in nature—they may simply be the result of careless work.

The three largest types of attacks between 2017–2018 were phishing/social engineering, web-based attack, and general malware (Ponemon Institute, 2018). Compromised/stolen devices came in a close fourth.

## Preparation Pays Off

As you can see, there is quite a bit of risk involved when it comes to protecting your and your customers' online data. Being prepared might take a bit more work upfront, but it's well worth it to reduce your risk of a hack or data breach.

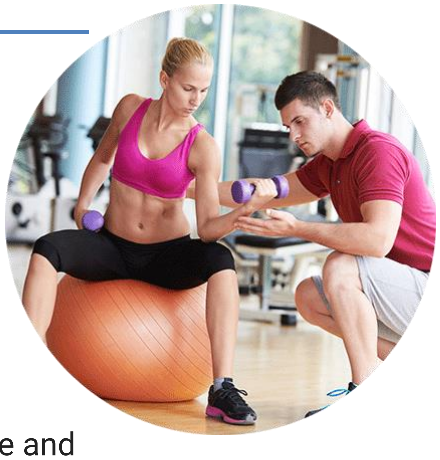
One of the biggest issues leading to the risk is businessowners' denial of the issue. According to Keeper Security's 2019 SMB Cyberthreat Study (Lurey, 2019), "(66%) believe a cyberattack is unlikely (even though in reality 67% of SMBs experienced a cyberattack in the last year)." Preventing data breaches takes effort and a realization that the risk will only increase the more society relies on digital technologies. Luckily, there are some simple and key solutions to help protect your customer data.

- **Acknowledge the Risk**: The first step in solving a problem is acknowledging that there is one in the first place. Be prepared to research and implement solutions that fit your business size and structure.
- **Cyber Liability Insurance**: Cyber liability insurance coverage is more than just another policy to purchase for your business. This coverage kicks in to help with your state-required filings and notices to those affected by the breach, your

business reputation, and getting your business back up. Read more on this in the next section.

- **Security Protocols**: To manage the internal risks mentioned above, be sure you have a solid plan in place for secure access to your website's administrative areas/functions, social media accounts, and any paper documents you may keep in an office or storage area. Carefully tracking who has access to those things can greatly reduce the risk of data breaches caused by negligence.
- **Protective Software**: Search for software that is designed to protect against malware, phishing, DoS, and other types of attacks. Most companies have plans designed for small businesses so that you can keep your data safe without breaking the bank. Once you have a system in place, be sure to educate any employees on how to use the system, for example keeping the virus definitions up to date, looking for the software's phishing identification in emails, and more.

## What is Included in Cyber Liability Coverage?



You are probably used to your business insurance coverage being described in terms of defense costs, aggregates, and deductibles. While there are some similarities with cyber coverage, there are some pretty distinct benefits to having this specific cyber liability benefit.

Cyber liability insurance policies have their own aggregate and deductible amounts, along with sublimits for specific coverages. Policies should also include the following key elements:

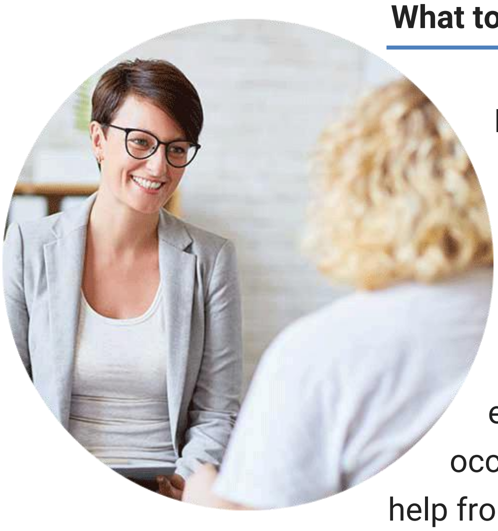
- **Privacy Notification Costs**: Issues notifications to individuals who are required to be notified under a state or federal Breach Security Law.
- **Computer Expert Services**
- **Legal Services**
- **Call Center Services**
- **Public Relations Consultant**: This service is used to address actual or possible material damage to your reputation as a result of the breach. This coverage part often has its own sublimit.

- **Credit or Identity Monitoring Product**
- **Payment of Claims Expenses, Penalties, and Fines**: These would be those obligations arising out of the breach.
- **Defense Costs**

We recommend that anyone who accepts payments online or who hosts classes online maintain cyber liability insurance coverage for their business, including:

- Yoga instructors
- Life coaches & wellness coaches
- Online personal trainers

## What to Do if You Have a Data Breach or Cyber Attack



In the unfortunate event your business experiences an attack, there are some first steps you should take to stop the attack and prevent further data loss.

- **Secure the Affected Area**: If the breach involved hardware located at a specific location, then ensure no one has access to that equipment. If it is occurring on your website, then lock down the site and get help from your website host (like GoDaddy or Wix) to remove the server from online remote access, if possible. Do not turn the computer or servers off, however, until someone has examined it for evidence. If the breach involved private information exposed on your website, then take steps to remove the information from public viewing (Federal Trade Commission, 2019).
- **Notify Your Insurance Company**: If you have cyber liability coverage, pull up your policy and contact the insurer using the contact information on your declarations page. Generally, you will want to provide your name (and business name, if applicable), phone number, email address, mailing address, and policy number. Explain the nature of the claim and the date and method by which you were first notified. The insurer will respond with any additional information they need to determine coverage. Once they determine coverage, they will provide the available tools to help you comply with laws and prevent future breaches.

## Conclusion

The digital world is here to stay, and keeping up on digital security is as important as our physical security. With some simple preparations, you will be able to protect your business from catastrophic monetary losses resulting from hacking and other types of data breaches. Start planning today by adding cyber liability to your business insurance policy.

For more information on cyber liability insurance coverage as a practitioner in the health, beauty, and wellness industries, visit AlternativeBalance.com.

## References

Alternative Balance Professional Group. (2019). *Cyber liability*. Retrieved from https://alternativebalance.net/cyber-liability-insurance

Federal Trade Commission. (2019, April). *Data breach response: A guide for business*. Retrieved from https://www.ftc.gov/tips-advice/business-center/guidance/data-breach-response-guide-business

Lurey, C. (2019, July 24). 2019 SMB cyberthreat study. Retrieved from https://www.keepersecurity.com/blog/2019/07/24/cyber-mindset-exposed-keeper-unveils-its-2019-smb-cyberthreat-study/

Ponemon Institute. (2018). *2018 State of cybersecurity in small & medium size businesses*. Retrieved from https://www.keepersecurity.com/assets/pdf/Keeper-2018-Ponemon-Report.pdf

Verizon. (2018). *2018 Data breach investigations report*. Retrieved from https://enterprise.verizon.com/resources/reports/DBIR_2018_Report.pdf

Verizon. (2019). *2019 Data breach investigations report*. Retrieved from https://enterprise.verizon.com/resources/reports/dbir/2019/summary-of-findings/

Media Inquiries:
Alternative Balance, LLC
41 Liberty Hill, Bldg. 2
Henniker, NH 03242
1-800-87-3848
contact@alternativebalance.org