Business Insurance

The Uhl Agency

Cyber Insurance

What is cyber insurance?

Cyber insurance protects against damages caused by electronic threats to your computer systems or data. The threats can lead to damage or misuse of sensitive information and can result in downtime and lofty recovery costs. Any business that stores or processes sensitive information like names, addresses, social security numbers, medical records or credit card information should consider the purchase of cyber insurance.

Cyber insurance covers risks that are divided into two parts. First-party coverage covers damages you and your business suffer because of a data breach, including extortion and ransomware attacks. Third-party coverage covers damages if your customers or partners are affected by a cyber-attack on your business.

Why cyber insurance?

It is important to protect your business from these types of threats. If you were to experience a claim, cyber insurance can help reduce the effects of a claim by covering costs for data restoration, legal liability and customer notification.

In our technology driven world, many recent events have been deemed by many to be sufficient cause to re-evaluate their priorities. Over the last 18-24 months the rate of ransomware attacks has skyrocketed in both frequency and severity, driving significant changes in the cyber insurance marketplace. In years prior, it was easy to obtain bindable quotes from multiple markets. Now, underwriters across the board are asking for more information related to ransomware loss controls and IT risk management.

Fast Facts:

- FBI Internet Crime Complaint Center received 467,361 complaints in 2019 (1,300 every day) and recorded $3.5 billion in losses.[1]
- 46% of respondents said the Chief Information Security Officer (CISO/CSO) would be held responsible for a data breach, but only 27% said the CISO/CSO was most responsible for cybersecurity policy and technology and decision-making. [1]
- $1.12 million was the average cost savings of containing a breach in less than 200 days.[1]

$3.86 million

Average cost of a data breach[1]

19%

Of malicious breaches were caused by compromised credentials and cloud misconfiguration

280

Days was the average time to detect and contain a data breach[1]

What can I do?

Besides the cyber practices you may already have implemented, you should also consult an outside firm to take a look at your information security systems to ensure that you are using the best practices. The major weakness is often passwords, which are accountable for 80% of hacking-related breaches. Additionally, 94% of ransomware victims did not have multi-factor authentication in place. Multi-factor authentication (MFA) can be an effective method to offer a second line of defense against email account hijacking. This one requirement could block 99.9% of all compromises.

Why MFA?

Since remote workforce is becoming the new norm, it is critical that businesses today consider MFA as part of their cyber security health.

2 or more authentication factors presents a significant challenge for attackers which can significantly reduce the risk of compromise.

As the cyber insurance market hardens, insurers are scrutinizing their portfolios and looking for clients with security controls that more closely align to a higher standard. Insurers view MFA as a best practice and are starting to ask more questions around MFA when placing or renewing cyber insurance.

It's now common practice to require that insureds have Multi-Factor Authentication (MFA) in place (especially when it comes to email access) before providing a quote for most accounts. Without MFA, clients risk non-renewal or a retention hike of 100% or more. MFA will benefit your insurance program by reducing your claims activity, which over the long term can significantly improve your insurance pricing. MFA also qualifies your company for cyber insurance quotes from multiple carriers, ensuring competition for your business that will produce favorable terms.

1. IBM, *Cost of a Data Breach*