Business Insurance

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, especially with the rapid acceleration in which artificial intelligence (AI) is being used in business operations, it is more critical than ever to protect your organization against cyber-related losses.

Previously, it was relatively 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.

$10.22 million

Average cost of a data breach in the U.S.

1 in 6

Number of breaches involving AI-driven attacks

97%

Share of organizations that reported an AI-related breach and lacked proper AI access controls

63%

Share of organizations that lack AI governance policies

241

The mean time to identify and contain a breach

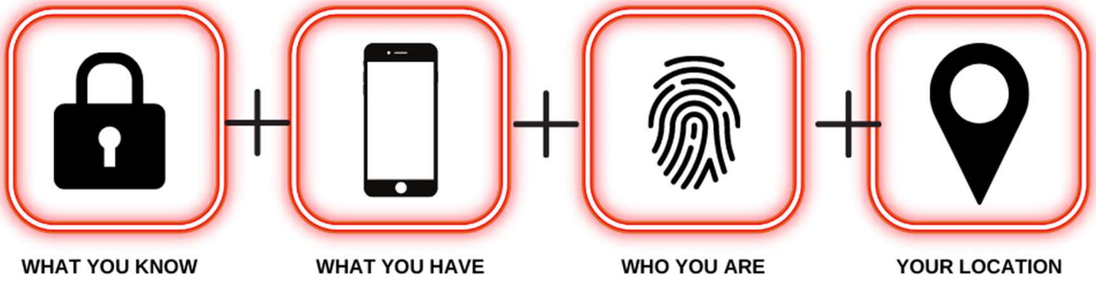
All statistics are from IBM's Cost of a Data Breach Report 2025

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 up to 80% of hacking-related breaches. Additionally, multi-factor authentication (MFA) should be in place, which assists with blocking various automated takeover accounts.

Multi-factor Authentication

a combination of criteria need to be met for a
user to gain access to resources



Why MFA?

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

Two or more authentication factors present a significant challenge for attackers, which can in turn substantially reduce the risk of compromise.

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

It’s now common practice to require that insureds have MFA in place before providing a quote for most accounts. Without MFA, clients risk non-renewal, a significant cost increase, and/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.