RESOURCE CENTER

Qualifying for cyber insurance with secure password management

Get the full interactive view at https://bitwarden.com/resources/qualifying-for-cyber-insurance-with-secure-password-management/

bitwarden

The Security Challenges

For businesses, an ever-increasing online footprint means a non-stop treasure trove of data for cyber-criminals and a steady reminder of unfortunate data breaches. According to the Identity Theft Resource Center's 2021 Annual Data Breach Report, the overall number of data compromises (1,862) was up more than 68% compared to 2020.

Companies contending with data breaches face a host of post-breach challenges. Often, they have to contend with reputational damage and angry customers, reduced revenue, and in some cases, legal investigations.

Precarious security practices also put businesses in a uniquely vulnerable position. The second annual Bitwarden 2022 Password Decisions Survey revealed 92% of IT decision makers reuse passwords across multiple sites. Compared to last year, the number of respondents sharing passwords via email skyrocketed from 39% to 53% due in part to the sudden adjustment to remote work and increased rate of employee turnover. And, 30% find themselves resorting to shadow IT - even though the long-term security impact is potentially ruinous.

The Security Solutions

With breaches such as Solar Winds and Colonial Pipeline top of mind, there is a continuous emphasis on the steps businesses can take to protect themselves against the fallout of a data breach. One option, that may have been considered a 'nice to have' just a few years ago but is increasingly viewed as a necessity, is cyber insurance.

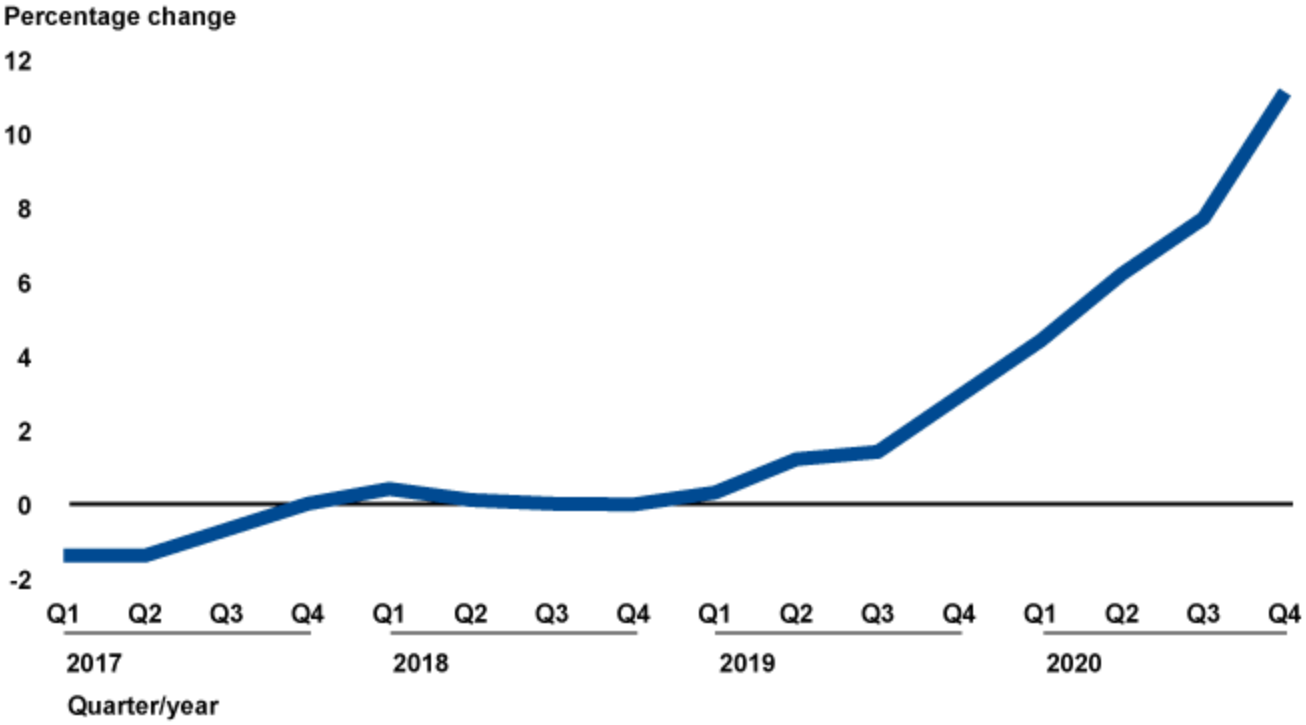
In its 2021 cyber insurance report the Government Accountability Office (GAO) found that data from a global insurance broker showed the proportion of existing clients electing coverage for cyber insurance rose from 26% in 2016 to 47% in 2020.

According to the Federal Trade Commission, businesses who are at risk of cyberattacks should first decide whether they want to deploy first-party coverage (protects your data, including employee and customer information), third-party coverage (protects you from liability

if a third-party brings claims against you), or both. For example, first party coverage typically includes (among other things) a business's costs related to legal counsel, recovery and replacement of lost or stolen data, lost income due to business interruption, and fees, fines, and penalties related to the breach. Meanwhile, third-party coverage might include payments to consumers, claims and settlements expenses, and accounting costs.

All this sounds ideal, and it is, in a security climate of this nature. But, finding a cyber insurer who will cover you isn't a guarantee. In most cases, businesses will need to show they are making a good faith effort to protect their critical data. This is quite understandable. As Marsh notes in its State of the US Cyber Insurance Market Report:

> "Cyberattacks, including ransomware, have soared over the past year, contributing to an increasingly difficult cyber insurance market characterized by climbing rates, reduced insurer appetite, tighter underwriting, and an increased focus on systemic risks report."



Source: GAO presentation of data from Council of Insurance Agents & Brokers. | GAO-21-477

Minimizing Cyber Risk with Bitwarden

One surefire strategy for reducing systemic risks and demonstrating to a cyber insurer that you're taking security seriously? Deploy a password manager. Password managers are one of the most straightforward, commonsensical technologies businesses can utilize to protect their data.

Here are some reasons why you should take a closer look at Bitwarden if you don't utilize a password manager but are looking to qualify for cyber insurance:

- Bitwarden allows users to generate strong and unique passwords

- Bitwarden allows users to access passwords from any device - a must-have in remote and hybrid workplaces
- Bitwarden quickly enable teams to share passwords among colleagues easily and securely
- Bitwarden establishes a first line of defense against data breaches by enforcing strong password policies for employees
- Bitwarden is built on open source security, utilizes end-to-end encryption, and is audited by third-parties providing official security assessments and penetration testing
- Many brokers and providers offer favorable rates to companies that have deployed password managers to all of their employees

Using a business password management solution like Bitwarden will help meet cyber insurance requirements and reduce cyber insurance premiums. Level up your cybersecurity today with a free enterprise trial or a free individual account.