Lawley

UNDERSTANDING WHY YOU NEED

CYBERSECURITY INSURANCE

As cyber incidents have become more frequent, insurers have added significantly more cybersecurity prevention requirements as part of their underwriting of this coverage. Here's what you need to know.

Why would someone target my small company? Only large companies are targeted by cyber criminals.

- Hackers do not care how large or small your business is. They will exploit any vulnerabilities discovered with your computer systems and look to lock down your data (encrypt) to demand payment (ransom/extortion) from you or your insurance company.
- There are no geographical limitations when it comes to breaches over the internet.

My data is in the cloud and my 3rd party vendor takes care of it, so I know it's secure.

- Take a good look at your contract with your IT provider. Most contracts limit their liability to the "annual cost of their services," which in many cases may be just a few thousand dollars of protection. In addition, you will need to file a claim with your provider and wait for the matter to be settled.
- Your 3rd party provider will likely not respond if the breach is caused by "human error" on your part, or that of your employees, which is the main way hackers gain access to your systems.
- Having your own policy will allow for immediate response from a breach coach to determine the best course of action following a breach.

As ransomware attacks continue to rise, these statistics are great examples of the damages hackers are inflicting on businesses all across the U.S.

The average ransom payment in Q3 2021 was

$139,739

83%
OF RANSOMWARE ATTACKS involved the threat to **leak exfiltrated data.**

22 DAYS
AVERAGE DOWNTIME stemming from ransomware

COMPANY SIZE OF RANSOMWARE TARGETS:

35%
11 TO 100 EMPLOYEES

44%
101 TO 1,000 EMPLOYEES

TOP INDUSTRIES TARGETED BY RANSOMWARE:

24%
PROFESSIONAL SERVICES

15%
PUBLIC SECTOR

13%
HEALTH CARE

Statistics from Evolve MGA and Coveware, a leading cryptocurrency exchange company, via their Q3, 2021 report.

Lawley

My IT team has me covered, and we already have security measures in place, including multi-factor authentication (MFA).

- Your IT team plays a key role in your first line of defense. Having multi-factor authentication in place is a great start for your security measures.
- While your IT team can help implement these safety measures, it is a challenge for them to control what employees may allow into your computer system, generally via emails that trick them into allowing malware to be launched in your system.

All of our information is backed up and our company can be up and running in a few days.

- Having back-ups (preferably multiple back-ups) in place is a good practice to have as part of your security protocols.
- Hackers have made their way into back-up systems as well, so having the proper "off-line" back-ups would be a critical part of your security.
- We have also seen where a hacker will contact the company to let them know how they got in, what information they have, as well as demand the ransom (extortion) by threatening to release your data on the dark web.

I don't hold any important information, so there is no need for it. Example: Protected Health Information (PHI) or Personally Identifiable Information (PII)

- A typical breach of your system may not provide much valuable information/data to the hacker, however, if you are unable to access any of your files (vendors, banks, clients, etc.) because your systems are down for over a week (which is fairly typical), you will likely suffer a business interruption loss that would not be covered by your property policy.
- Legal, forensics and possibly notification costs can add up as well.

Our average cyber policy premiums are under

$10,000

and that includes all sized businesses. A typical $1M limit, $5K deductible policy averages around $2,500-$3,000.

Premiums have and continue to rise as a result of the significant increase in cyber claims, however, so have the cost to a business from a cyber breach, which can be catastrophic.

Average claims we have seen in our agency for cyber losses are around

$285,000

That number continues to rise as hackers have become more embolden by the success they have seen and the ease of taking down a company's computer system.

Have questions about your identity theft protection coverage or personal insurance policies?

Don't hesitate to contact the team at Lawley
1.844.4LAWLEY or ***www.lawleyinsurance.com***

Statistics from Evolve MGA and Coveware, a leading cryptocurrency exchange company, via their Q3, 2021 report.