**BizBoost News**

**Volume 11, Issue 26**

**For distribution 6/13/22; publication 6/16/22**

**Should You Get Cybercrime Insurance?**

The short answer to this question is YES! Incidents of cybercrime have been problematic for a long time, but have soared exponentially since the start of the pandemic. If the reputation of your firm depends in part on your maintaining confidential client records secure and private, then this insurance is a must. It’s not a matter of “if,” but “when” your private business info will be breached.

**Finding the Right Insurance**

The best place to start is your current insurance agent or a general insurance broker that you trust. Cybercrime policies are separate policies that cover specific acts, and you will need to read the policy carefully to see exactly what you are protected from. You should also distinguish between personal and business policies; you may want both.

In a business policy, some of the items you want to consider being protected against include:

* Data breach
* Ransomware attack
* Spoofing and identity theft
* Wire fraud
* Civil fines
* Lawsuits
* Costs of notification, reputation repair, forensics and data restoration, credit monitoring, and other potential damages

A good policy will cover some or all of these costs:

* Business interruption costs
* Data breach costs
* Extortion costs
* Crisis management and public relations costs
* Data recovery costs
* Computer replacement costs
* The cost of reputational harm

Just like any other insurance, you will need to complete an application to obtain a quote. Some of the standard questions include:

* Type of products and services sold in the business
* Type of electronic data stored on its computer systems
* Whether laptops are password-protected
* Whether you have written network security and privacy policies in place
* Whether you have physical security procedures in place
* Whether you have the most current software and processes to keep it upgraded
* Whether you have backups
* Whether you monitor unauthorized attempts to access systems
* Whether you are in compliance with PCI DSS (Payment Card Industry Data Security Standard), HIPAA (Health Insurance Portability & Accountability Act), and GLBA (Gramm-Leach-Bliley Act)
* Whether you have a written document retention and destruction plan in place
* Whether you have encryption enabled
* Whether third parties are involved in data handling
* Whether you have a process to check copyrights of materials you use
* Whether you have a risk management education program for employees
* Your current insurance policies
* Whether you’ve had a breach in recent years
* Whether you’ve had any lawsuits or claims in this area
* Whether you use a firewall
* Whether you use anti-virus protection
* Whether you have an employee/third party off-boarding process that terminates access to computers and data

As you can see, the application process itself is an excellent way to “cross your Ts and dot your Is” when it comes to putting safeguards in place for your business. And of course, your premium will be less expensive when you have these items in place. It goes without saying that your premium will be less expensive if you get insurance *before* you are attacked, so that you have a clean application.

A key part of owning a business is managing enterprise risk effectively, and a cybercrime policy will go a long way toward protecting your hard-earned investment and giving you peace of mind so you can sleep better at night.

\*\*\*

Tweets

Insert a link to your newsletter, website or blog before you post these:

Our latest blog: “Should You Get Cybercrime Insurance?” is available now! Subscribe here: [link]

Incidents of cybercrime have been problematic for a long time, but have soared exponentially since the start of the pandemic. Learn about the importance of cybercrime insurance in our latest blog article: [link]

If the reputation of your firm depends in part on your maintaining confidential client records secure and private, then cybercrime insurance is a must. It’s not a matter of “if,” but “when” your private business info will be breached. Learn more in our latest blog article: [link]

#BusinessTip: Cybercrime insurance is more important now than ever before. Cybercrime policies are separate policies that cover specific acts, and you will need to read the policy carefully to see exactly what you are protected from. You should also distinguish between personal and business policies; you may want both. Learn more here: [link]

In a cybercrime business insurance policy, some of the items you want to consider being protected against include:

•Data breach

•Ransomware attack

•Spoofing and identity theft

•Wire fraud

•Civil fines

•Lawsuits

Learn more about this type of insurance here: [link]

A key part of owning a business is managing enterprise risk effectively. Cybercrime insurance can go a long way toward protecting your hard-earned investment and giving you peace of mind. Learn more about cybercrime insurance here: [link]

DID YOU KNOW… A good cybercrime insurance policy will cover some or all of these costs:

•Business interruption costs

•Data breach costs

•Extortion costs

•Crisis management and public relations costs

•Data recovery costs

•Computer replacement costs

•The cost of reputational harm

Learn more in our latest blog article: [link]

Do you know whether your business needs a cybercrime insurance policy? Sign up for our newsletter to learn more: [link]