SHIELD
INSURANCE SOLUTIONS

BE SHIELDED!

4th Edition, 07/19/2021

How Cyber Insurance Can Protect Your Business from Cyberattacks?

Written By: Brendalisse Rivera-Casanova, ESQ., CISR, CIC, CRM

Recent statistics show that in January 2020 alone, nearly 1.8 billion user records were leaked due to cyberattacks, representing personal information and passwords for approximately 772 million people. Additionally, a recent study from the University of Maryland shows that hackers attack every 39 seconds, averaging 2,244 attacks per day.

It sounds scary, right?

It's even scarier that these statistics were released prior to COVID-19. Unfortunately, cybercriminals have taken advantage of the pandemic, so the number of companies and individuals affected by cyberattacks continues to rise. As a matter of fact, the FBI recently reported that since the start of the coronavirus, cyberattacks have increased by 300%.

There is no doubt that digital technology has transformed the way we do business today. Every business uses its own computer network, in addition to portable media devices, to send, receive and store sales projections, business strategies and any other information owned by the business. The hard reality is that if any of this data is lost, damaged or stolen due to a cyberattack, it could cost thousands of dollars just to restore or replace. On top of that, your computer network might also store sensitive data of others, such as your vendors, clients, customers and employees. If there is a cyber breach and such info is leaked or accessed by a hacker, you could be held liable for their damages, in addition to all the expenses your firm will incur to notify those impacted by your data breach as required by law. Additionally, you will need to hire legal, public relations and computer forensics firms to help you investigate, handle and mitigate the loss and the possible impact to your business and brand.

So, how can cyber insurance protect you?

Cyber insurance can protect your business against costs associated with a data breach, as it will cover legal defense, settlements, crisis management response expenses including notification costs and credit monitoring, and business interruption and related expenses, among other coverages.

Here are some of the first-party, third-party and crime coverages you could find in a cyber policy:

First-Party Coverages

- **Cyber Breach Costs:** Notification and credit monitoring costs arising from the theft of personal identifiable information of customers arising out of a cyber breach. It will also provide for reimbursement of fees and expenses for forensics consultants and public relation firms.

- **Cyber Extortion Costs**: Coverage for the investigation and settlement of a cyber-extortion threat.
- **Data Restoration:** Coverage for costs to replace, restore or recover digital information from written or electronic records due to their corruption, theft, or destruction caused by a cyberattack.
- **Business Interruption and Extra Expense:** Covers income losses that might be sustained by your business and additional expenses you might incur to restore the operations following an interruption caused by a failure of security. Coverage is also available for business interruption from cyber events affecting your vendors (IT, cloud providers, etc.)

Third Party Coverages

- **Privacy or Network Security Liability:** Costs incurred in the investigation and defense of the Insured, including monetary amounts the Insured is legally obligated to pay to others.
- **Media Liability:** Online copyright infringement, libel, slander, plagiarism, and invasion of privacy as a result from your publication of electronic data on the internet (either on your webpage or social media).
- **Regulatory Defense and Penalties**: Protection for the Insured in the event they are fined or penalized by a governing body (HIPAA).
- **Payment Card Loss:** Coverage in the event your business is fined or penalized by the Payment Card Industry.

Crime Coverages

- **Social Engineering:** Coverage when the Insured suffers a loss of money because of a spear phishing scam, which dupes an employee of the insured into wiring money to a third party.
- **Telephone Fraud:** Coverage for telephone service charges and fees incurred by the Insured in the event of their telephone system being hacked by a third party.

Steve Durbin is the Management Director for the Information Security Forum, an organization with over 30 years of expertise on information security and risk management. Steve recently said the following about the future of cyber security:

"By 2022, organizations will be plunged into crisis as merciless attackers exploit weaknesses in immature technologies and take advantage of an unprepared workforce. At the same time, natural forces will wreak havoc on infrastructure. Invasive technologies will be embraced across both industry and consumer markets, creating an increasingly tumultuous and unpredictable security environment.

Organizations will have to adapt quickly to survive when digital and physical worlds collide. Those that don't will find themselves exposed to threats that will outpace and overwhelm them."

As I was reflecting on his thoughts, one of my favorites quotes by Sun Tzu came to my mind: "In the midst of chaos, there is also opportunity." The COVID pandemic has taught us that our biggest line of defense against cyberattacks should be a combination of equipment, software and education. Consistency and prevention work far better than reaction and improvisation. Therefore, it is the perfect timing to:

1) Have a cyber discussion with your team;
2) Review your security parameters in order to detect any vulnerabilities in your network;
3) Establish, implement, and review your cyber-incident response and business continuity strategies;
4) Provide regular employee training and testing; and
5) Start thinking about buying cyber insurance (or if you already do, chat with your broker or agent about limits and coverages).

As the technology continues to evolve, the sophistication and ever-changing nature of cyber will continually challenge us in terms of cyber mitigation and prevention. However, there is no doubt that cyber insurance can give all of us some peace of mind.

SHIELD
INSURANCE SOLUTIONS

Triple S Plaza Building
Suite 704
1510 Ave. Franklin D. Roosevelt
Guaynabo, PR 00969

Our mission is to understand your business and risk exposures and to lead the process of formulating and implementing cost effective insurance solutions to Risk.

Our dedicated cyber professionals will design a comprehensive and tailor-made policy for your needs.

For further information, please contact our offices,

(787)498-0222
Service@shieldpr.com

Be Shielded, Your Best Protection!!!