CYBER STORM

HOW TO PROTECT YOUR BUSINESS FROM A DATA BREACH AND THE RESULTING CYBER STORM OF FINES, LAWSUITS & CUSTOMER LOSS

SCOTT KREISBERG

INSURE YOUR COMPANY'S SAFETY AND WELL-BEING


CYBER
STORM

CHAPTER 11

INSURE YOUR COMPANY'S SAFETY AND WELL-BEING

BY SCOTT KREISBERG
Founder and Owner – One Step Secure IT Services

In the past couple of years, the number and frequency of cyber-attacks have skyrocketed. It is now no longer a question of whether your company will suffer an attack but rather when it will happen. Just as we protect our homes and health with insurance for when an issue will arise, it is essential to protect the security of our businesses. The time has passed that cyber liability insurance (CLI) is an extra bit of coverage to have, just in case. It has become an essential part of a functional business, and very often is the only thing that stands in the way of a breach decimating a business.

Without CLI, business owners are fully responsible for the entirety of a security event, as well as any consequences that follow. These consequences could include fines and penalties, forensic audits, public relations consultations, data restoration, reputation and client trust loss, lawsuits, and credit monitoring services for anyone whose information the breach compromised – all of this in addition to the company's own downtime and loss of income. In total, the cost of a data breach for a small business can easily shoot past several hundred thousand dollars. The deeper damage is almost incalculable, as successful cyber-attacks demolish your business's reputation and client trust, which inevitably results in

additional business loss. In fact, 60% of small businesses close up shop within six months of a breach.

This is a universal danger that does not discriminate – but it does hunt for prey strategically. Although every business needs cyber liability insurance, criminals target small businesses more often simply because they tend to be easier hits. The year 2020 alone saw a 400% increase in cybercrime, with 43% of all cyber-attacks targeting small businesses and almost a third (28%) of data breaches involving small businesses. Cybercriminals know that small businesses have fewer resources. Because of this, the best way to minimize risk is to use those resources in the most effective and efficient areas and to contract with professionals who will provide the highest value security.

It is important to note that time is not anybody's friend in this field. Our company recently brought on a client that spent many months deliberating with us due to slow-moving bureaucracy. While initial conversations continued, they suffered a large breach that left them with a huge mess. The fact that they could have prevented the attack was the true heartbreak. They were so close to a full team for their protection. Thankfully, we were on hand to assist with the cleanup. However, they learned the hard way: the criminals search and hope for the opportunity to find a company that will put off security, take their time with that decision and assume that a bit more time won't make a difference.

Cyber liability insurance is a crucial layer of protection, and your business needs it now more than ever. Cyber liability insurance is designed to cover many of the business expenses, losses, interruption, fines, and penalties that result from a data breach, ransomware attack, or other cyber security issues. Every business that uses any technology that connects to the Internet needs to have a policy with adequate coverage and to understand that policy fully.

Unfortunately, many business people tend to operate under the impression that their general liability insurance will cover them in

the case of a cyber security issue. The truth is that most general liability insurance will not take on this huge responsibility. So, in the case of a devastating loss, these businesspeople are left with no protection because they did not verify that they were covered and take the necessary steps.

There are many possible types of losses that a business could experience as a result of a successful cyber-attack. While CLI covers many of these types of losses, just as many of them are not covered and therefore require additional endorsements. Some of the types of losses that CLI covers are:

1. ***Data breaches from employee theft:***
   Disgruntled or unsavory employees are a large liability since they generally have the most direct access to your systems. This becomes more common when the employee who leaves the company harbors resentment toward their former employer.
2. ***Denial-of-service attacks:***

   A denial-of-service (DoS) attack is meant to shut down a machine or network and make it inaccessible to its intended users. DoS attacks flood the targeted machine or network with traffic, such as a flood of robocalls, or sends it information that triggers a crash. In both instances, the DoS attack deprives legitimate users (i.e., employees, members, or account holders) of the intended service or resource.
3. ***Cyber business interruption:***

   If your company's product or service is distributed, accessed, or managed online, a business interruption due to a cyber-attack could cause a devastating loss of sales or production.
4. ***Data breaches from hacks:***
   This is another loss that is a rather broad category, as it can happen in a large number of ways and can have many outcomes and consequences. A data breach often requires a forensic audit and cleanup when the data is posted on the dark web. It takes many skillful professionals to handle a breach of this type.

It is important to remember that just because it is titled "cyber liability insurance," these policies do not magically adopt all cyber liability once you purchase. There are also many things that CLI does not cover or will only cover in particular circumstances. Many of these CLI claim denials occur because policyholders do not know or understand the exclusions and stipulations on their policy. Some of the most common reasons for denial are:

(i). *Negligence, or "failure to follow or maintain."* This is a claim denial that cites the policyholder's failure to meet and/or maintain the security standards stipulated within the policy.

(ii). *Payment card industry (PCI) fines and assessments.* Some policies contain exclusions of coverage that depend on the way the criminal(s) accessed the compromised card information, e.g., via virus or self-propagated code.

(iii). *Cyber-extortion*. It can be difficult to understand the policy clauses on extortion and ransomware. While a policy may help cover a ransom, it might not provide the coverage you need to recover from lost income.

(iv). *Social engineering.* This includes phishing and any other attack based on manipulating a user on the targeted system. Coverage for this type of loss is often not included in the main policy and will likely require an additional endorsement.

In addition to the list above, CLI also typically will not cover potential future loss of profits, loss of value due to theft of intellectual property, as well as costs to improve cyber security systems. Ensure that you thoroughly understand your policy coverages and requirements – this is the best way to easily avoid the shock of coverage denial in any of these situations.

The challenge to even qualify for a new CLI, or renew a current policy, increases every year. Businesses must follow increasingly strict security measures to be considered for coverage, whether or not a policy is already held. In the past, a business owner could simply say they implemented the correct security – now, they need

to prove it. Business owners are unable to simply fill out an affidavit that they adopted and use the appropriate security measures. Many insurance providers even turn companies down and will not write the policies if the company is not up to compliance guidelines.

This is the unfortunate reality built from an increase in breaches. As companies fail to put in the preventative work, the number of breaches increases, which drives up the liability for insurance companies. This, in turn, inflates the security measures that insurance companies are forced to require to mitigate their risk. As some companies are unable to meet these strict requirements, they fall out of compliance and are left with insufficient coverage in their policies, which leaves them vulnerable. It's a cycle that continues to get more dangerous for everyone involved, and early prevention is the key to safety.

The best and most efficient way to ensure that the security standards – as well as the CLI policy itself – are understood, met, and maintained is to partner with a third-party cyber security firm. A cyber security team takes two important roles: keeping your company compliant with the CLI policy and all other relevant guidelines and conducting proactive management to minimize your risk of a breach. They will also provide validation documentation management on a continual basis to prove compliance and ensure you are eligible for coverage. It is important to note that a lot of insurance companies also have preferred vendors they use for remediation. You can have anyone you want as your cyber security team, but you may have to use someone else for the cleanup after a breach.

It takes two professional teams to ensure the safety and well-being of your company. The third-party cyber security firm is the safety – the proactive prevention specialists who will keep the risk and damage of a breach to a minimum. The cyber liability insurance is the well-being. It creates a safety net so your company can retain its health in the case that an event does happen. You must maintain both of these in order to remain fully covered.

Although it is possible for much larger companies to have an internal security officer, if you don't have a third party validate the steps you've taken to protect yourself, the insurance policy is much less likely to pay out in the case of an event. When your company experiences a breach, it is much harder to prove that it did all the right things when your security is handled internally. When a third party validates your precautions, it is much more credible. Even if the insurance policy does pay out a portion of the damages when due diligence cannot be fully proven, the premium on the policy will skyrocket.

Our firm has a client company that came on board to get assistance with compliance for their current cyber liability insurance policy, valued at $1 million. They soon accomplished this. The next year, when the policy came up for annual renewal, we were shocked to find it had more than doubled in length. In just that one year, the insurance company's security requirements, particularly for e-mail, rose to a level beyond what the client company could implement. The company could not meet the new guidelines. Consequently, the insurance company could only offer half the coverage of the previous year's policy. In our work as IT security professionals, we see this dangerous cycle continue, and we urgently tell these stories to bring to light that early preventative compliance is a team effort that can increase everyone's safety.

If you have not yet obtained crucial cyber liability insurance, here is a list of recommended steps to take:

1. Find a trusted third-party security contractor. As with many other areas in business, keep in mind that you get what you pay for. This is not an area to take shortcuts and go with the cheapest option. Remember that the key is to use your limited resources efficiently, and this is an efficient investment.
2. Have your security contractor run a full audit of your cyber security. Whether the results are good or bad, this will show you exactly where you are currently and help inform the next steps and priorities for resource allocation and timing. This

will also help the contractor learn what types of coverage you need, how much and where.
3. Receive a 'findings' report and a personalized plan of recommendations from your contracted advisors. They will advise you on what needs to be done and when.
4. Put the plan into action and stick with it. Remember that security and coverage can only work together to keep you protected if they are both maintained.

Cyber technology has created a whole new world of business. Unfortunately, as with the rest of the world, criminals will always invade and use every space available. As cybercrime rises, security regulations must follow. This is not a ploy to scam business owners into unnecessary precautions – the precautions exist because people are already being scammed every second. As long as businesses continue to operate on the web, cyber liability insurance will be absolutely essential to having a business at all.

About Scott

Scott Kreisberg founded One Step in 1985, providing technology solutions to retail businesses and helping retailers harness technology to run their businesses more efficiently. Fascinated by computers as a child, he has dedicated his entire 36-year career to the implementation and security of technology. Scott saw the role that cyber security would play in the future of retail and the critical need for improved security throughout retail businesses. His response was to form One Step Secure IT Services, a division of One Step that is designed to provide IT services and support with an emphasis on cyber security and compliance.

Knowing that a proactive and multilayered approach to cyber security was the only way businesses could truly lower their risk of a cyber-incident, Scott ensured that One Step's expertise encompassed knowledge of numerous state and industry compliance regulations. This allowed his business to provide protection not only to retail businesses but also to any business that needed to protect sensitive data and customer information. One Step Secure IT has branched out since, taking on clients in aerospace, engineering, architecture, and many other fields.

In 2004, payment card industry (PCI) compliance became a requirement for businesses, and Scott and the One Step team were quick to step in. They helped businesses navigate the requirements and ultimately worked with their clients to prevent cardholder data theft and breaches.

Businesses continue to be a prime target for cybercriminals, particularly as these businesses store increasingly massive amounts of customer data and are continually processing transactions through online networks. In more recent years, as businesses build their online presence to engage customers, the cyber security risk has skyrocketed. To mitigate this risk, Scott and the One Step team began developing partnerships with insurance companies. Scott soon realized it would now take both industries – IT security and insurance – to provide adequate protection to businesses. Now, cyber liability insurance is a critical layer of protection for any business that uses technology and stores sensitive data.

Today, One Step Secure IT – headquartered in Phoenix, Arizona, with offices in New York, Boston, and Los Angeles – is a recognized expert for many regional insurance companies to help guide businesses through policy application and recommending the correct security measures to qualify and maintain compliance for cyber liability insurance coverage. They provide education through their online blog for anyone looking to learn more about cyber security and cyber liability insurance.

You can reach Scott at:

- E-mail: SKreisberg@OneStepSecureIT.com
- LinkedIn: Scott Kreisberg (https://www.linkedin.com/in/scott-k-7463b42/)
- Website: www.OneStepSecureIT.com
- Phone: 623-227-1997

CYBER STORM

FEATURING

SCOTT KREISBERG

Scott Kreisberg founded One Step in 1985, providing technology solutions to retail businesses and helping retailers harness technology to run their businesses more efficiently. Fascinated by computers as a child, he has dedicated his entire 36-year career to the implementation and security of technology. Scott saw the role that cyber security would play in the future of retail and the critical need for improved security throughout retail businesses. His response was to form One Step Secure IT Services, a division of One Step that is designed to provide IT services and support with an emphasis on cyber security and compliance.

Knowing that a proactive and multilayered approach to cyber security was the only way businesses could truly lower their risk of a cyber-incident, Scott ensured that One Step's expertise encompassed knowledge of numerous state and industry compliance regulations. This allowed his business to provide protection not only to retail businesses but also to any business that needed to protect sensitive data and customer information. One Step Secure IT has branched out since, taking on clients in aerospace, engineering, architecture, and many other fields.

In 2004, payment card industry (PCI) compliance became a requirement for businesses, and Scott and the One Step team were quick to step in. They helped businesses navigate the requirements and ultimately worked with their clients to prevent cardholder data theft and breaches.

Businesses continue to be a prime target for cybercriminals, particularly as these businesses store increasingly massive amounts of customer data and are continually processing transactions through online networks. In more recent years, as businesses build their online presence to engage customers, the cyber security risk has skyrocketed. To mitigate this risk, Scott and the One Step team began developing partnerships with insurance companies. Scott soon realized it would now take both industries – IT security and insurance – to provide adequate protection to businesses. Now, cyber liability insurance is a critical layer of protection for any business that uses technology and stores sensitive data.

Today, One Step Secure IT – headquartered in Phoenix, Arizona, with offices in New York, Boston, and Los Angeles – is a recognized expert for many regional insurance companies to help guide businesses through policy application and recommending the correct security measures to qualify and maintain compliance for cyber liability insurance coverage. They provide education through their online blog for anyone looking to learn more about cyber security and cyber liability insurance.

You can reach Scott at:

- E-mail: SKreisberg@OneStepSecureIT.com
- LinkedIn: Scott Kreisberg (https://www.linkedin.com/in/scott-k-7463b42/)
- Website: www.OneStepSecureIT.com
- Phone: 623-227-1997

The Authors of this book have donated all royalties to St. Jude Children's Hospital.
For more information please visit **www.stjude.org**

DESIGNED AND PRODUCED BY TECHNOLOGYPRESS™
Printed in the USA

$19.95
ISBN 978-1-7369881-5-2
51995>
9 781736 988152