Understanding Cyber Liability Insurance
INTRODUCTION

The internet was designed for the open and uninhibited exchange of information. It was intentional that there be no central authority or control. Anyone can use the internet and can do so anonymously and across borders. For law abiding citizens it gives instant access to a wealth of information. However, it also has created an environment for criminals, hackers and others access to information and systems that were never intended to have access.

Every business has an exposure and risk to becoming a victim of cyber crime. The breath and extent of that risk varies. For example, a retail operation that accepts credit card information has a different risk profile than a health system that stores confidential medical information. The risk may be considered low or high but it still exists

Most businesses are familiar with insuring for traditional risks to their business operations. However the internet has created a range of exposures that were never contemplated by the underwriters of traditional insurance. The insurance industry coined the term “cyber liability” and carriers developed policy forms and endorsements based on the risk that each was willing to assume.
As a result Cyber Liability Insurance is one of the most confusing coverages in the market. Not only are there a significant number of carriers offering stand alone policies but an equal number providing endorsements to other policies. They fall under general term “cyber” but the scope of coverage and service can be as different as night and day.

Any business considering purchasing cyber liability should take the time to understand the extent of the coverage that is being proposed. By working with an experienced insurance professional you will not only be able to assess your risks but also understand what risks are being insured, how the insurance company will or will not respond, what are your responsibilities in the event of a loss and what risk management services are available to you.

In this e book I will outline for you the major components of a cyber liability policy. Keep in mind that when reading these policies, not all companies offer all of these coverages, nor do they use the same terms and definitions. My goal is to provide you with a basic understanding of this coverage to assist you in making an informed decision that can have a great impact on your business.

At R&R Insurance we are the knowledge brokers. We have a team of professionals that can help you navigate this complex world of cyber liability. Thank you for downloading this ebook. We look forward to hearing from you.
BASIC COVERAGE

The main insuring agreements offered in most cyber policies are Network Security liability, Privacy Liability, Media Liability, and Business Income. As an insured you can choose which of these you which to purchase, although the network security and privacy are usually packaged together.

I. Network Security Liability: Intended to provide liability coverage when third parties suffer a loss due to the intentional and unauthorized access to the insured’s network. This usually includes the subsequent transmission of a virus, malicious code, targeted denial of service attack or disruption in service. It is important to understand what the policy defines as your network. For example, does it include mobile devices, hardware, software, firmware, virtual private networks, storage devices, etc.

II. Privacy Liability: The liability owed to third parties for the misappropriation or disclosure of personally identifiable information, a breach violation of Federal, State, or local laws associated with the control or use of personally identifiable information. The definition can also include the disclosure of business trade secrets and confidential information.

Note: Not all policies cover third party contractors, independent contractors, seasonal employees. Many of the major breaches, including Target, originated from third parties. Also be sure that the
policy covers the format in which you have this information. Does it only cover the breach of information stored electronically or does it extend to paper records, records stored on mobile devices, portable storage devices? Is encryption a requirement for coverage to be triggered?

III. Media Liability: Liability to third parties in connection with the Insured’s Advertising or electronic content. Coverage is typically included for defamation, slander or libel, disparagement, reputational harm, unfair competition deceptive trade practices, misappropriation or misdirection of messages or media of third parties, plagiarism, copyright infringement, etc. Many business office policies cover some of these exposures but not if electronic or on your website.

IV. Business Income: The net profit or loss that the insured would have earned or incurred had the network attack not occurred. Coverage may also include the costs to restore your system as it was prior to the event, and any extra expenses you may have incurred. If your systems are down due to a network attack how long will it be before you are operational? Will it take hours or days? Does your disaster management plan include contingency plans for this scenario?
**ADDITIONAL COVERAGE**

Policies may also include additional coverages that are frequently offered at various limits.

1. **Digital Assets**: Coverage to replace or restore the software or electronic data that was stored on your network.

2. **Network Extortion**: Coverage responds to a credible threat or series of threats to commit or continue to attack your network or to disclose personally identifiable information obtained by breaching your network for the purpose of obtaining payment from you.

3. **Extortion payments**: The reasonable and necessary payments you incur to respond to, mitigate and/or eliminate an extortion threat, including fees and expenses paid to third party security consultant to mitigate or eliminate an extortion threat.

4. **PCI (Payment Card Industry) fines and penalties assessed for non-compliance with security protocols**

5. **Regulatory fines and penalties, including HIPAA**

**RESPONDING TO A BREACH**

Many businesses are not prepared to handle the aftermath of a cyber attack or data breach themselves. Not only are there a myriad of laws governing notification to affected parties, but also the time, expense and expertise to investigate what happened, how it happened and how to shield your business from the potential fallout. A significant value in a cyber liability policy resides in the services and additional expenses that are provided. They are usually grouped into categories such as Breach management expenses, crisis management expenses or breach consultation services and include the following:

1. **Notification Expenses**: The costs associated with notifying affected individuals that their private information has been breached. Some policies only respond if the breach is large enough that the law requires notification. Other policies extend coverage for
voluntary notification. The notification requirements will also vary based on the residency of affected parties. These can also include the legal fees for preparing the notices and ensuring that the notices comply with each jurisdiction. Also frequently includes postage, paper, etc.

2. Credit Monitoring Expenses
3. Legal Expenses
4. Forensic IT Expenses
5. Identity Theft Repair expenses
6. Public Relations Expenses
7. Notice Fulfillment Services
8. Call Center Expenses

When it comes to paying these expenses, is the carrier going to reimburse you or are they going to pay these up front, subject to the retention or deductible? Are there certain vendors that the carrier requires you to engage? Is the retention applied based on a dollar amount or on the number of individuals affected?
RISK MANAGEMENT & RESOURCES

Risk management Resources can also be a valuable tool for a business. Carriers may provide:

1. Review of your policies and procedures
2. Breach Coach
3. Webinars
4. Self Help On-Line Portals
5. Awareness training for owners and staff
6. Software interfaces
7. On Site Risk Management visits
8. Table Top Breach exercises
9. News and alerts
10. On-call resources/Hot lines
CONCLUSION

Eventually every business will fall victim to a cyber loss in some form. The reality is that unless the entire internet is dismantled and redesigned there is no possible way to eliminate the security threats. Security is contradictory to basic design of the internet. However, businesses can be proactive and vigilant in protecting their network, employees, customers, vendors, and partners. Cyber Liability insurance is part of that equation.

Carla Borda
Professional Liability Specialist
R&R Insurance Services, Inc.
N80 W14824 Appleton Ave
Menomonee Falls, WI 53051
Ph: 262-502-3843
Fx: 262-953-1404
Carla.Borda@rrins.com
Follow Carla on Twitter: rri_formedical