WS&Co. Blog

June 19, 2014

CYBER LIABILITY

Cyber Insurance 101: The Basics of Cyber Coverage

By Lauri Floresca

What do American Express, Home Depot, VFW, Kmart and the North Dakota University System have in common? They are all part of the 342 data breaches exposing 9,015,970 personal records that have occurred this year through June 10, 2014, according to[1] the non-profit Identity Theft Resource Center (ITRC). This represented a 17.1-percent increase over the same time period in 2013.

Just in the last few months, we've seen massive breaches at major brands like Target[2] and eBay. But we also constantly have small ones in all sorts of industries including healthcare,[3] retail and even manufacturing—really any company that is consumer facing or heavily reliant on technology is vulnerable.

A robust cyber insurance policy can help businesses weather the storm more effectively when a data breach or network security failure has occurred. Unfortunately, many do not understand the scope of what a cyber insurance policy can provide in the event of a network security failure, and how that scope has expanded over the past few years.

In this cyber insurance 101 post, we'll dive into where cyber coverage came from, and what the components are, paying special attention to the network security and privacy components that cover the common cyber threats organizations face today.

The Evolution of Cyber Coverage

The roots of cyber coverage go back about 20 years. Back then, technology companies bought errors and omissions (E&O) insurance, which over time, was extended to include things like a software product bringing down another company's network, unauthorized access to a client system, destruction of data, or a virus impacting a customer. (For a while there, spreading a computer virus was the big concern – remember the Love Bug[4] Virus that swept the globe in 2000?)

[1] *http://www.idtheftcenter.org/images/breach/ITRC_Breach_Report_2014.pdf%20*

[2] *http://www.wsandco.com/about-us/news-and-events/cyber-blog/target-calculators*

[3] *http://www.wsandco.com/about-us/news-and-events/cyber-blog/record-hipaa-fine*

[4] *http://en.wikipedia.org/wiki/Love_bug_virus%20*

(continued on page 2)

The companies that bought this early cyber insurance were generally in the technology space and already buying E&O insurance. The technology coverage, often called "network security" or "Internet liability" was an add-on.

Five to 10 years ago, we saw these "network security" policies expand into the privacy space by providing clear coverage for breaches of confidential information. That got the attention of retailers and other companies holding considerable consumer data, but who weren't providing the type of technology services that would warrant buying E&O insurance.

Those companies wanted standalone cyber products that covered network security and privacy liability. That evolution has been important to where we are now because those exposures are so dominant today.

Cyber Coverage Today

Cyber coverage can mean different things to different people. Most commonly, cyber coverage is some combination of four components: Errors and omissions, media liability, network security and privacy. I'll touch on all four, but go into more detail about network security and privacy, where coverage has changed most significantly.

Errors and Omissions: E&O covers claims arising from errors in the performance of your services. This can include technology services, like software and consulting, or more traditional professional services like lawyers, doctors, architects and engineers.

Media Liability: These are advertising injury claims such as infringement of intellectual property, copyright/trademark infringement and libel and slander. Due to the Internet presence of businesses today, technology companies have seen this coverage migrate from their general liability policy to being bundled into a media component in a cyber policy (or a separate media liability policy). Coverage here can extend to offline content as well.

Network Security: A failure of network security can lead to many different exposures, including a consumer data breach, destruction of data, virus transmission and cyber extortion. The culprits might be looking to shut your network down so you can't conduct business, either for financial or political gain. Network security coverage can also apply if you're holding trade secrets or patent applications for a client, and that information is accessed due to a failure of your security.

Privacy: Privacy doesn't have to involve a network security failure. It can be a breach of physical records, such as files tossed in a dumpster, or human errors such as a lost laptop, or sending a file full of customer account information to the wrong email address. Companies have also faced liability from returning a photocopier with a hard drive that contained unwiped customer tax records. A privacy breach can also include an action like wrongful collection of information.

All insurers use different terminology for cyber coverage; some subdivide the four components above even further, which means that cyber policies can be very difficult to read and compare.

Network Security and Privacy Liability Coverage

What's unique about the privacy and network security coverages is that both first-party costs and third-party liabilities are covered: First-party coverage applies to direct costs for responding to a privacy breach or security failure, and third-party coverage applies when people sue or make claims against you, or regulators demand information from you.

Some common first-party costs when a security failure or data breach occurs include:

- Forensic investigation of the breach.
- Legal advice to determine your notification and regulatory obligations.
- Notification costs of communicating the breach.
- Offering credit monitoring to customers as a result.
- Public relations expenses.
- Loss of profits and extra expense during the time that your network is down (business interruption).

Common third-party costs include:

- Legal defense.
- Settlements, damages and judgments related to the breach.
- Liability to banks for re-issuing credit cards.
- Cost of responding to regulatory inquiries.
- Regulatory fines and penalties (including Payment Card Industry fines).

(continued on page 3)

Sublimits, Deductibles and Limits in Cyber Coverage

All of the first-party coverage elements, and the fines and penalties aspect of the third-party coverage, are typically offered as a sublimit of liability. As these coverage extensions were first introduced, the sublimits would be small – for example, a $5 million policy might have offered up to $100,000 for "breach costs" such as forensics and notification.

Another $100,000 sublimit might apply to regulatory fines and penalties. These sublimits have generally increased in recent years, and in most cases, you can get up to 50 percent of the total limit to apply to first-party costs. Some markets will offer blanket policies with no sublimits.

In addition to a dollar deductible (which ranges widely depending on the size of the policy and the company being insured), most policies include a time element deductible to trigger the business interruption coverage.

For example, a cyber policy might require that your network be impaired for more than 8 hours due to a security failure for the business interruption coverage to apply.

The total market capacity for cyber coverage currently exceeds $300 million, which is more than enough for most companies. Factors to consider in making limit decisions will be covered in a later post.

What's Not Covered?

There are a few key items that are currently not covered in network security and privacy liability policies. These include:

- Reputational harm.
- Loss of future revenue (for example, in the case of Target if sales were down due to customers staying away after data breach).
- Costs to improve internal technology systems.
- Lost value of your own intellectual property.

These topics are continually being discussed by cyber liability brokers and insurers, and policies may continue to evolve.

Conclusion

Data breaches and network security failures happen. In fact, IBM reports[5] more than 91 million security events per year. The likelihood that your business is next is not that far-fetched. Luckily, cyber coverage has evolved from its early days as an E&O component for technology companies into a robust offering that covers both first-party and third-party costs.

---

[5] http://www-935.ibm.com/services/us/en/it-services/security-services/data-breach/%20%5BJL7%5D

This content originally appeared as a blog post in "Cyber Liability" Woodruff-Sawyer & Co., June 19, 2014. https://wsandco.com/cyber-liability/cyber-basics/

Lauri Floresca can be reached at 415.402.6523 or lfloresca@wsandco.com.