

WS&Co. Blog

December 18, 2014

CYBER LIABILITY

# Cyber 101: Obtaining Cyber Insurance – The Process

By Lauri Floresca

Hopefully, by now you've come to the realization that your general liability insurance is not sufficient[1] to cover the very real and growing risk of cyber breaches. You may know a bit about cyber insurance[2] as a solution – and you might even be ready to buy it. So, where to begin? What's involved in the process?

In this post, as part of our "Cyber 101" series, we'll review the cyber insurance application process, what to expect, and what to prepare for when obtaining cyber insurance.

## The Cyber Insurance Application

For companies that haven't purchased cyber insurance yet, it requires providing information that you may not have needed in other insurance renewals. Here, an experienced broker can guide you through what you need.

Start by selecting an application that's industry-friendly and thorough. While it may be enticing to default to the simplest, easiest application, doing so can hamper your ability to get a good variety of quotes.

The application is going to ask a lot of technical questions around what kind of technology you use, how you encrypt data, what your audit processes are, security procedures, use of encryption, password management and employee training — and that's just for starters.

**The Information-Gathering Phase**

Completing applications will require gathering information from many parts of your organization:

- **IT and Network Security** teams are, of course, going to be necessary. You will need information about the types of technology your organization uses, the outside vendors and cloud providers that touch your networks, and details on your monitoring capabilities and third-party audits.
- **Finance** will need to provide information on your revenues, customers, demographics and other organizational issues. They will also need to provide input into your desired program

*(continued on page 2)*

[1] *http://www.wsandco.com/about-us/news-and-events/cyber-blog/cyber-roulette*

[2] *http://www.wsandco.com/about-us/news-and-events/cyber-blog/cyber-basics%20*

structure as you evaluate the different levels of risk transfer (premium, limits, deductibles and scope of coverage).

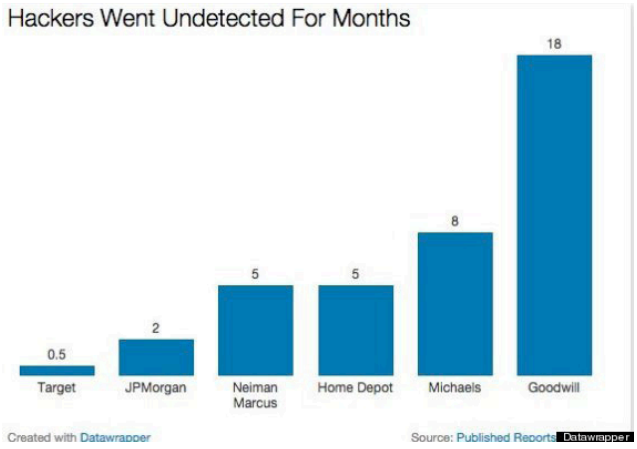
- **Legal** will be asked for information on your contractual protections, such as what your customers are demanding from you, and what you are demanding of your vendors in your contracts. Underwriters are very focused on how successful companies are in limiting their liability, and how aggressively they are seeking indemnity from vendors. Legal also can provide information on your privacy policies, relationships with privacy counsel, and any breach response planning that has happened to this point.

## What Insurance Companies Are Looking at Today: People and Process

In many recent high profile breach examples, the targeted companies had technology to monitor their systems, but didn't have the people in place to review the alarms when they sounded.

Reports state that hackers had access to JPMorgan[3] for at least two months before anyone was the wiser. That's actually a fairly short timeframe: hackers reportedly were inside Neiman Marcus for five months, in Michaels for eight, and in Goodwill for 18 months before they were detected!

From Huffington Post:




[3] *http://www.huffingtonpost.com/2014/10/23/jpmorgan-hackers_n_6029266.html*

Insurance carriers may also look at how you would handle a "Zero Day" vulnerability. These are software bugs or holes that are unknown to the vendor or creator of the software. Once discovered, it is imperative that organizations assess their technology and apply patches to close the hole before hackers are able to exploit the flaw.

The "Heartbleed Bug" was one such vulnerability discovered in early 2014.[4] It's estimated this has impacted about two-thirds of websites. And it's not a hack; it's a mistake written into OpenSSL that makes standard security encryption open to hackers.

When Heartbleed was discovered, companies ranging from Google to Amazon to Apple worked feverishly over a short timeframe to patch servers. Those companies have massive IT and network security resources, but still had to respond to the news when everyone else did. The question insurers are asking is, are you prepared to respond to the next Zero Day event?

## Cyber Response Plans: Incidents and Breaches

Insurers know that all businesses face cyber risk, so a key part of the underwriting is your ability to *detect* and *respond* to a breach or network security failure. The level to which companies formalize their incident response plans vary, but underwriters will want to see that you have done a level of planning commensurate with your exposures.

For businesses that rely heavily on technology to generate revenue or process transactions:

- How quickly are you able to resume operations following a network security failure or outage?
- What are your back-up plans and redundancies? (Read more about how cyber insurance can respond to technology-related business interruption in a previous blog post, here).[5]

[4] *http://www.zdnet.com/article/heartbleed-serious-openssl-zero-day-vulnerability-revealed/*

[5] *http://www.wsandco.com/about-us/news-and-events/cyber-blog/cyber-business-interruption*

*(continued on page 3)*

Companies that are consumer facing need a plan that specifically responds to a data breach of consumer information. These plans should include vendors you would call on for help, including:

- Law firms to advise on your legal obligations based on the nature of the breach.
- Forensic IT specialists to identify the source of the breach and its scope.
- Vendors to provide notification to customers and potentially offer credit-monitoring services.

Those expenses, because they are potentially covered by a cyber insurance policy, need to come from *approved* vendors. Some insurers offer more flexibility in vendor choice, while other carriers will insist that you use their preselected vendors.

**Providing Follow-Up Information**

Once you've gathered all the information, that's the point where your broker will make a formal submission to insurers and eventually narrow down the list of underwriters that are interested in providing coverage.

Those insurers will often have additional questions, which may be handled via conference calls or in-person meetings. Be sure to prep all departments that may not be used to having these types of conversations – IT could very well be one of those departments.

Ask for samples, in advance, of the types of questions they'll be asked, and the types of answers that should be provided. This is not a deposition, so "yes" and "no" answers without context are not very helpful. On the other hand, extremely technical responses with lots of jargon may be too much detail.

## Evaluating Cyber Insurance Quotes

Once you've satisfied the insurer questions, hopefully you'll have several quotes to choose from. Deciding between different insurers is a complicated analysis, and your broker will need to break the quotes down in detail. Don't just look at the pricing. Pay attention to key differences, including:

- Extra coverage grants (first party, business interruption, data restoration, cyber extortion)
- Sublimits
- Deductibles (retentions)
- Vendor selection
- Exclusions
- Prior acts

We've talked about many of the above items in prior posts, but it's worth taking a moment to focus on the importance of prior acts coverage.

**Prior Acts**

Cyber liability is almost always written on "claims-made" insurance contracts. This means that it will respond to "claims" that are "made" during that policy period. A particular feature of claims-made policies is that they usually contain a retroactive date, which limits coverage to claims arising out of events or acts that occurred after a certain date.

The first time you purchase coverage, that date is typically set at the policy inception date. In future years, you can hopefully keep that "prior acts" date, so the retroactive period gets longer and longer.

The challenge with prior acts and cyber coverage is clear from the above example about how long hackers might be inside a system before being detected.

Let's say you first buy a cyber policy in January 2015. In March 2015, the FBI contacts you with a warning: they believe your systems have been breached. Upon further investigation, you learn that the breach was kicked off in July 2014 when your CEO unknowingly fell victim to a phishing attack, and gave his password to a hacker posing as a member of your IT group.

Without prior acts coverage, the insurer can argue that the entire breach is based on an "act" that occurred before you first purchased coverage. Some insurers are willing to offer a year or two of backdated prior acts coverage on a new policy, but always for an additional premium.

If you can get that option – take it. The policy will be infinitely more valuable as a result. Many insurers have stopped offering this option, however, particularly for retail and hospitality risks, given the frequency and severity of recent attacks in those sectors.

*(continued on page 4)*

## Binding Cyber Coverage

In all cases, before binding coverage, you will have to sign a statement affirming that you are not aware of any circumstances that are likely to give rise to a claim under the policy.

This may be obvious – you can't insure against a breach that you already know about. But make sure that you understand the scope of that warranty statement, and how widely you are obligated to "poll" to answer the question.

In sum, buying cyber insurance for the first time is probably more complex and time consuming than other insurance procurement. Many companies find, however, that the process can lead to improved communication amongst your legal, IT, finance, and risk management teams in this critical risk area, and to a better overall understanding of the cyber risks faced by your organization.

*This content originally appeared as a blog post in "Cyber Liability" Woodruff-Sawyer & Co., December 18, 2014. https://wsandco.com/cyber-liability/obtaining-cyber/*

*The views expressed in this briefing are solely those of the author. This briefing should not be taken as insurance or legal advice for your particular situation.*

---



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