MARSH & McLENNAN AGENCY

WORLD CLASS. LOCAL TOUCH.

WHAT YOU SHOULD KNOW ABOUT CYBER LIABILITY INSURANCE POLICIES

A Q&A WITH DAN HANSON, DIRECTOR OF MANAGEMENT LIABILITY

FEBRUARY 2013

Introduction

"Cyber attack": two words that strike fear in the hearts of business owners, regardless of their company size, industry or method of operation.

While entry alarms, reinforced access points and security personnel can go a long way to protecting a business facility from a physical intrusion, the intangible nature of a hacker's method of attack is far more difficult to circumvent.

But it can be done — as long as businesses are aware, on guard and up to date with their defenses. In this interview with Dan Hanson, director of management liability for RJF, a Marsh & McLennan Agency LLC company, he explains what types of coverage are provided by cyber liability policies, and how companies can analyze their actual risks from these "virtual attacks."

CYBER LIABILITY BY THE NUMBERS
HIGHLIGHTS FROM THE VERIZON 2012 DATA BREACH INVESTIGATIONS REPORT

WHO IS BEHIND DATA BREACHES?
- 98% stemmed from external agents
- 4% implicated internal employees
- <1% committed by business partners

HOW DO BREACHES OCCUR?
- 81% utilized some form of hacking
- 69% incorporated malware
- 10% involved physical attacks
- 7% employed social tactics
- 5% resulted from privilege misuse

WHAT COMMONALITIES EXIST?
- 96% of attacks weren't highly difficult
- 94% of all data compromised involved servers
- 85% took weeks or more to discover
- 92% of incident were discovered by third party

(From a study conducted by the Verizon RISK Team with cooperation from the Australian Federal Police, Dutch National High Tech Crime Unit, Irish Reporting and Information Security Service, Police Central e-Crime Unit, and United States Secret Service.)

What does a cyber liability policy cover?

A cyber liability policy — also known as network security coverage, privacy liability or data protection coverage — provides support if there are suits against an organization for failing to protect the confidential information of others.

In general, companies have an obligation to protect the confidential information of others, and if that information is compromised or they have it stolen from them, they would be liable. A cyber policy is designed specifically to protect against that liability, although the extent and amount of the coverage can vary.

What are some examples of information that could be targeted by cyber thieves?

This can vary depending on the type of business or industry. For example, a cyber thief can go after a retail store's records of customer credit card numbers or their employees' Social Security numbers, while in the case of a health care organization, the focus would be on medical records and related confidential information. For banks and other financial institutions, the goal is to access financial records of their customers.

The bottom line is that everyone is fair game for a cyber attack. Unless you are a pure cash business with no employees, you have exposure.

What are the types of coverage?

Cyber policies can provide both first party coverage and third party coverage.

First party coverage is for costs a business would incur as a result of the cyber breach, such as:

- Notifying those affected that confidential information was potentially compromised. As of August 2012, 46 states, the District of Columbia, Guam, Puerto Rico and the Virgin Islands have enacted legislation requiring notification of security breaches involving personal information, according to the National Conference of State Legislatures. (Alabama, Kentucky, New Mexico, and South Dakota currently have no security breach law requirement.)
- Hiring a crisis management firm to ensure that these notifications are handled and documented in accordance with state-specific requirements. Otherwise, the company could face fines for not handling the process correctly and in a timely manner.
- Covering any potential fines and penalties assessed by regulators.
- Providing free credit monitoring to those whose information was affected — a service companies often offer as a goodwill gesture so as not to lose those customers.
- Covering the business interruption costs that resulted from a cyber attack. If a company's Website was hacked, for example, it may not be able to transact business via the Internet for a period of time, which could represent a huge business interruption loss.

What may be the most important feature of a policy is the support it provides to hire a forensic specialist to 1.) determine if there was in fact a breach, 2.) help determine the scope of the breach, and 3.) identify who must receive notification.

Third-party coverage is much simpler to understand. If it is alleged that a company did not protect confidential information, the affected person(s) could bring a suit attempting to recover damages. A cyber liability policy would provide protection to the company against those lawsuits, as well as the defense costs it incurs in responding to such claims. Since multiple records are often compromised, class action suits are commonplace and can be costly for an organization to defend on its own.

Also, many policies provide defense dollars for actions brought by both federal and state regulatory bodies.

Do all cyber liability policies carry first and third party coverage?

No, they don't, and often carriers will mix and match coverage, which results in a lot of variances in terms of what is included. And there is also a lot of variance in pricing too. That's where relying on insurance agents or brokers is essential. It's their job to explain the nuances of the policies to their clients.

Are businesses taking cyber liability more seriously now than five or 10 years ago?

Even though we at RJF have been talking about cyber liability with our customers for at least five years, it's only in the past few years that they are taking it more seriously. Unfortunately, given the issues with the economy, most companies are also looking for more ways to cut costs, and adding another insurance policy is often the last thing they want to do.

And, unlike D&O (Directors and Officers) or property insurance policies or workers' compensation, which companies are familiar with, cyber liability isn't as easily understood. One change that has occurred is with the tech people's attitude. In the past, they might try to dissuade company owners from purchasing cyber liability by pointing out that they have encryption and firewalls in place.

But now, because they know not only how much smarter these cyber thieves have become, and also because they realize their security is only as strong as the salesperson or executive who mislaid the smart phone or laptop, IT people are realizing the benefits of the policy. The challenge is in justifying to management the added cost of an additional insurance policy. Yet, when you compare the policy cost to the average loss amount per record — which in 2011 were estimated at $194 between direct and indirect costs — you can see that, regardless of the cost of the policy, it is worth it from a financial and reputational standpoint to the company.

What services does RJF provide with regards to cyber liability?

We start by meeting with our clients to find out what types of information they have and how vulnerable that data is to breaches. Our goal is to help them assess the risk and exposure, and then show them how we can protect that.

We also evaluate contracts they have with outside vendors such as cloud providers so they are contractually protected in case the vendor is hacked. We want to make sure that, if their vendors are doing the work, their vendors are picking up the liability.

And if a breach occurs, we make sure they are contacted immediately, and that a claim is started with the insurance company. We then work with our client to review the reservation of rights letter to make sure they are utilizing that policy as properly as they can. And through the whole process, we do our best to reassure our clients that everything will be handled in the best possible manner so they will be able to return to operations with peace of mind.

How do I get more information?

- Dan Hanson, Director of Management Liability Group, at hansond@rjfagencies.com or 763 548 8599
- Ask your RJF/MMA representative
- Find other Cyber Liability content at www.rjfagencies.com/CyberLiability

Marsh & McLennan Agency LLC
7225 Northland Drive North, Suite 300
Minneapolis, MN 55428
+1 763 746 8000
+1 800 444 3033
www.rjfagencies.com