PRESENTED AT

ESSENTIAL CYBERSECURITY LAW
July 28, 2017
Dallas, Texas

Cybersecurity Insurance

Larry Hansard
Noah Nadler

Author Contact Information:
Noah Nadler
Wick Phillips
Dallas, Texas
noah.nadler@wickphillips.com
214-740-4044

Larry Hansard
Arthur J. Gallagher & Co.
Dallas, Texas
larry_hansard@ajg.com
(972) 663-6114

I.
Introduction

Technology and the internet have helped companies and organizations accomplish unprecedented growth over the past 30 years, but costly problems in the form of data-breaches continue to threaten most businesses, government entities, and non-profit organizations of all types and sizes. Reportedly, healthcare and financial services are the two most affected industries at the moment, but any business that stores private information electronically is at risk.

The quantity, size, and financial impact of cyber-attacks have continued to increase since the attacks started occurring more frequently in the early 2000's. In 2004, the largest data breach affected 92 million AOL accounts. In stark contrast, approximately 1.5 billion Yahoo! accounts were breached between 2012 and 2014.[1] Because of the highly-publicized data-breaches of numerous large companies who have had their customer data stolen (such as Yahoo, Home Depot, AOL, and British Airways), the disclosure of internal Democratic National Party emails during the 2016 election, and the very recent ransomware cyberattack on companies throughout the US and Europe, the public and corporate world are intimately aware of cyber risk.

Although the cyber-breaches that make the headlines are the attacks on large, international companies, the breaches on small to mid-size companies and non-profit organizations are far greater in number. 62% of cyber-breach victims are small to mid-size businesses, which are at the greatest risk for an attack because their level of preparation is often low.[2] The impact that cyber-attacks have on small companies is often severe, with the majority of these companies going out of business within the next year.[3]

The reality now facing many companies and non-profit organizations is not *if* they will have to deal with a data-breach, but *when*, how big, and how costly the breach will be. Businesses, non-profit organizations, and governmental entities therefore not only must have a contingency plan in place to handle such a breach, but also should consider whether they have the necessary insurance in place that will cover losses arising from the breach. This determination should be made before an attack occurs, which requires a review of the risks facing the company and a clear understanding of what coverage the company has in place. The cost of conducting this analysis and purchasing additional coverage, if necessary, will be miniscule compared to the uninsured losses stemming from a cyber-attack.

Most large and small companies will have commercial general liability policies ("CGL") in place, but these policies often have exclusions precluding coverage for losses arising out of a data breach or they may not provide coverage for the losses because there is no property damage or advertising injury. Additionally, there may be certain losses sustained by the company or

[1] https://www.wired.com/2016/12/yahoo-hack-billion-users/.

[2] http://www.propertycasualty360.com/2015/05/27/small-mid-sized-businesses-hit-by-62-of-all-cyber.

[3] http://www.denverpost.com/2016/10/23/small-companies-cyber-attack-out-of-business/.

organization in responding to the data-breach (outside of payments to third-parties) that are not covered under a CGL policy.

As a result, most companies and organizations must consider purchasing specific "cyber" insurance. It is important to understand what losses and liabilities may be covered under this insurance and what losses may still be uncovered—while also understanding that the coverage provided may differ significantly depending on the specific cyber policy purchased. Executives, in-house counsel, insurance brokers, and risk managers therefore must educate themselves on the coverage granted by the specific policy purchased and not simply assume that all losses associated with a cyber-attack are covered because they have procured such insurance. This way, they are not left unprepared and surprised when an attack occurs.

This article will provide a summary of the recent uptick in the severity and frequency of cyber-attacks and the related liability/costs companies have incurred as a result. The article will also discuss the insurance issues arising out of an attack and the types of coverages under cyber policies that may mitigate the risks of an attack.

II.
The Significant Increase in Cyber Attacks

Over the past ten years, the frequency, size, and financial impact of cyber-attacks have grown with each passing year. The reason for this is that hackers have developed more efficient tools and methods to infiltrate their targets. The simple reality today is that no industry or organization is free from the threat of hacks. Everyone has likely heard of some of the larger and more publicized attacks. Examples of these cyber-attacks include the following:

- One of the first and largest cyber-attacks of its time occurred in 2005. An AOL employee, Jason Smathers, stole 92 million screen names and email addresses.[4] AOL experienced significant difficulties in estimating the costs of the attack. It was estimated that the attack cost AOL at least $400,000.00 and possibly millions of dollars.[5]

- In 2006, the Veterans Affairs Department ("VA") misplaced a laptop containing records of private information of approximately 26.5 million veterans and active personnel.[6] Once the breach was reported, the affected individuals filed a class action lawsuit seeking $1,000.00 for each person whose data was exposed—a demand of up to $26.5 billion.[7]

[4] http://www.nbcnews.com/id/8985989/#.WVz-49UrLRZ.

[5] *Id.*

[6] https://gcn.com/Articles/2009/02/02/VA-data-breach-suit-settlement.aspx.

[7] Eventually, the case settled for $20 million, and a new paradigm emerged. Companies were no longer risking merely their reputations and good-will by playing fast and loose with their customers' data; rather, a single class action lawsuit (and its astronomical demand for relief) could create an existential threat to the most solvent company.

Title search: Cybersecurity Insurance

Also available as part of the eCourse
2017 Essential Cybersecurity Law eConference

First appeared as part of the conference materials for the
2017 Essential Cybersecurity Law session
"Cybersecurity Insurance"