UT LAW CLE THE UNIVERSITY OF TEXAS SCHOOL OF LAW

PRESENTED AT

20th Annual Insurance Law Institute

November 12-13, 2015
Dallas, Texas

Hacking Through Cyber Insurance

Jes Alexander
Dickey's Barbecue Restaurant, Inc.
8150 N. Central Expressway, Suite 215
Dallas, Texas 75206
972-248-9899
jalexander@dickeys.com

Table of Contents

Hacking Through Cyber Insurance[1]

In the early eighties, Hollywood depicted hackers as benevolent characters that allowed curiosity to get the better of them. For example, in WarGames, a curious teenager played by a young Matthew Broderick unwittingly stumbled into a military supercomputer, and almost triggered a nuclear war with the former U.S.S.R. At the time, the notion of a hacker doing that much harm was laughable to security experts and hackers alike.

Nobody laughs anymore about the exploits of these cyber black hats intending to steal information and to disrupt a company's operations. Upon opening a newspaper on virtually any day of the week, you will be bombarded with horror stories of yet another company falling victim to a cyber security data breach. Most often, these stories are accompanied by a headline of "largest and most costly data breach ever." As the former director of the FBI succinctly stated, "there are only two types of companies: those that have been hacked and those that will be. And even they are converging into one category: companies that have been hacked and will be hacked again."[1]

What is responsible for this trend? The 21st century is not known as the information age for nothing. Combined with exponentially falling costs to store and process data, businesses of all stripes realize that information is an invaluable resource. Now, more digital information is collected and stored by companies than ever before. As a result, strict information control is vital to companies' ability to protect trade secrets, store confidential customer information, and payment information.

However, properly securing a company is like trying to keep a dam plugged that has thousands of holes. As the many potential vulnerabilities range from the hardware, the software, and human error, perfection is a nearly impossible goal even for the largest and most sophisticated companies. As recent data breaches illustrate, attackers need only a small vulnerability to infiltrate a company's system and wreak havoc.

Therefore, digital pirates possess great power to terrorize a company on many different fronts - blackmail a small business by holding its computer system hostage, post employees' confidential information on websites, steal payment information, and espionage. Unfortunately, these digital thieves turned away from Spider Man's sage advice that, "with great power, comes great responsibility."

Given these transcendent risks, a new market has arisen - cyber liability insurance. At its core, cyber liability insurance is an amalgam of first party and third party insurance expressly designed to cover typical losses faced by a company after a data breach. These covered losses include costs related to regulatory compliance, which are a major component of any cyber loss.

As data breaches affect businesses with greater cost and consequences, the need for cyber liability insurance is more crucial than ever. In fact, insurers are currently attempting to scrub away any arguable coverage from standard liability, property, or professional liability policies. For example, the drafter of the standard commercial general liability ("CGL") policy introduced restrictive data liability endorsements gutting coverage for almost any cyber-related claim.[2] Moreover, recent court decisions involving coverage for cyber risks under standard policies have not ended well for policy holders. Thus, those companies that solely rely upon standard policies do so at great peril.[3]

Unfortunately, the procurement of cyber insurance runs into two significant problems:

---

[1] The author of this paper, Jes Alexander, is deputy general counsel at Dickey's Barbecue Restaurants, Inc. Prior to joining Dickey's, Mr. Alexander spent nearly a decade successfully handling high profile insurance coverage cases and civil appeals. The views reflected in this article are not necessarily the views of the author's company.

1. Massive data breaches are a relatively new phenomena. As a result, case law is scarce and courts are currently struggling to define the parameters of liability faced by a breached company. Currently, the trend is to allow increasingly creative claims to be filed against a company after a data breach; and

2. The cyber insurance market is relatively new, and no standard policy form exists. Thus, the risks covered under cyber liability policies often vary amongst insurers. Moreover, like D&O and E&O polices, cyber policies vary by the particular insured's industry.

Thus, the coverage afforded under a manuscript cyber policy must be compared to the individual risks faced by a particular company.

Although the risks faced from company to company will vary, recent data breaches involving Sony, Target, and Anthem health insurance illustrate many of the unintuitive risks shared by all companies, regardless of size. Likewise, these three digital canaries in a coal mine highlight some of the major areas that should be addressed in a cyber policy.

I. Like Father, Not Like Sony

In the past, making a satirical movie lampooning a dictator came with little risk. Perhaps a strongly worded denunciation by the offended country, which comes with the side-benefit of free advertising for the movie. For example, the film "Team America: World Police" depicted the then-leader of North Korea, Kim Jong Il, as an outlandish and petulant villain. Eventually, he is impaled on a spiked German helmet (although he did not die, he morphs into an alien cockroach). The North Korean leader's only response was to ask the Czech Republic to ban the film – a request that was swiftly rejected.

So when Sony Pictures Entertainment ("Sony") decided to greenlight a comedy involving a similar plot-line involving the assassination of current North Korean dictator, Kim Jong-un, it is doubtful that Sony's risk managers even batted an eyelash. Unfortunately for Sony, the axiom "like father, like son" did not hold true with regard to the movie "The Interview."

In the most destructive data breach in history (for now), this electronic Pearl Harbor has left Sony debilitated. The aim of the data breach was not only to steal data, but to send a clear message to Sony. And, send a message they did.

First, Sony's crown jewels – unreleased films – were uploaded online by the perpetrators of the breach to be downloaded freely by all. Next came the release of confidential and highly embarrassing emails from executives and employees, including an email exchange calling Angelina Jolie a "spoiled brat."[4] In addition, confidential information was released of over 47,000 former employees, including some social security numbers and medical information. As a result of this breach, Sony has been forced to suspend its current film projects.

Unlike the simplistic data breaches involving Target or The Home Depot, security experts describe the Sony attack as "unprecedented in nature."[5] The techniques used were "undetectable by industry standard antivirus software."[6] Before analyzing the legal pain that is just beginning for Sony, it is significant to understand how this slow-moving disaster began.

A. "I'm Gonna Make Him An Offer He Can't Refuse"– Coverage For Digital Extortions

Three days prior to the initial wave of destruction that has gripped Sony, two Sony executives received the following cryptic and hilariously translated ransom demand:

> We've got great damage by Sony Pictures. **The compensation for it, monetary compensation we want.**

Title search: Hacking through Cyber Insurance

Also available as part of the eCourse
Industry-Specific Insurance Trends 2015

First appeared as part of the conference materials for the
20th Annual Insurance Law Institute session
"Hacking through Cyber Insurance"