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 a Cyber-Liability Claim and Related Insurance Issues

Mariah Quiroz

Author Contact Information:
Mariah Quiroz
Thompson, Coe, Cousins & Irons, LLP
Dallas, Texas

mquiroz@thompsoncoe.com
214.871.8258

TABLE OF CONTENTS

Overview

Mariah Quiroz is a partner in the Dallas office of Thompson, Coe, Cousins & Irons, LLP, where she devotes her practice to representing insurers in complex coverage matters and insurance-related litigation. Mariah is one of the few Texas attorneys with a focus on cyber insurance and coverage issues arising from cyber and data security risks. Mariah has vast experience representing international and domestic insurers in a variety of high-stakes commercial claims, including oil and gas industry claims, claims involving technology services or products, catastrophic bodily injury claims, pollution and environmental losses, residential and commercial construction defect, workplace accidents, professional liability, personal and advertising injury, and additional insured tenders and contractual indemnification.

Mariah also regularly advises and represents insurers in bad faith litigation across Texas and out of state, and is a frequent speaker on industry topics including cyber insurance, *Stowers* liability, bad faith and insurance claims handling.

Mariah is a member of the Dallas Bar Association, the Tort & Insurance Practice Section of the Dallas Bar Association, and the Insurance Section of the State Bar of Texas. She is a graduate of Baylor University and Baylor University School of law.

Contact Mariah:
Phone: (214) 871-8258
FAX: (214) 871-8209
Email: mquiroz@thompsoncoe.com
Mail: THOMPSON, COE, COUSINS & IRONS, LLP
700 N. Pearl Street, Suite 2500
Dallas, Texas 75201

I. INTRODUCTION – WHAT IS CYBER LIABILITY AND A CYBER-LIABILITY CLAIM?

As the internet becomes more integral to communication, information, and the conduct of business, the threat of insecurity to a company's proprietary information, computer network and livelihood increases. Businesses depend on the internet for their daily affairs, including soliciting customers, transacting money and reporting information. Yet, many are significantly unprepared for a data breach and resulting fallout. For instance, prudent businesses have a number of different insurance policies in place to address various risks. But, which policy or policies could help alleviate their financial burden in recovering from a cyber attack?

This paper and corresponding presentation identify the most common cyber risks, which types of policies are implicated by the risks, and how courts across the country are interpreting the relevant policy language in light of these developing legal issues.

II. THE ALARMING STATISTICS – COMING SOON TO A BUSINESS NEAR YOU

The USA Today has reported that 43% of all businesses experienced a data breach in 2014.[1] This number is no doubt higher now. In fact, when 60 Minutes interviewed FBI Director James Comey he said, "there are two kinds of big companies in the United States. There are those who've been hacked and those who don't know they've been hacked." Although there have been numerous recent high-profile cyber attacks, one of the first and largest breaches to capture the news was the Target breach after Thanksgiving 2013. Between November 27, 2013 and December 15, 2013, a Russian hacking heist installed Kaptoxa, a malware strain designed to siphon data from credit cards at point-of-sale ("POS") systems operated by Target. Although every cyber attack is different, the Target breach involves fascinating statistics revealing how vulnerable many businesses are and the breadth of the resulting damages. For example:

- 40 million credit card numbers were stolen from Target customers through Target's POS systems;[2]
- Of these numbers, 1-3 million (estimated) credit card numbers were sold successfully on the black market and used for fraud before being cancelled;
- The hackers resold the credit card numbers at Rescator[dot]cc, an underground cybercrime shop, for between $18 and $35.70 per card. It is estimated that the hackers generated as much as $53.7 million in income from the sale of the credit card numbers;
- In addition to customers' credit card numbers, hackers stole 70-110 million customer records, including names, addresses, email addresses and phone numbers;[3]
- Target experienced a 46% drop in profits in the 4th quarter of 2013 compared to the prior year;
- Credit unions and banks incurred approximately $200 million in reissuing 21.8 million credit cards (about half of those stolen in the breach);
- Target spent approximately $100 million upgrading its payment terminals to support chip and PIN-enabled cards, which are contained in all cards issued by Visa and MasterCard; and
- Target disclosed in its Form 10-Q for the quarterly period ending November 1, 2014 that it already had incurred $248 million in expenses as a result of the cyber attack.[4]

  When the breach occurred, Target reported $80 million in related costs and anticipated that insurance will cover $52 million, leaving at least $36 million uninsured—a phenomenal hit for any business.[5]

  Compared to the Target breach, most cyber attacks are not as widespread or high-profile, and many are unknown or unreported. Up to 35% of data breaches are caused internally by a careless employee or contractor.[6] Regardless of the cause,

---

1 Weise, Elizabeth, "43% of Companies Had a Data Breach in the Past Year," *USA Today*, available at http://www.usatoday.com/story/tech/2014/09/24/data-breach-companies-60/161061971.

2 For reference, the combined population of New York and Florida is about 40 million.

3 Seventy million is greater than the population of the United Kingdom, South Korea, France or Thailand.

4 Krebs, Brian, "The Target Breach, By the Numbers," available at http://krebsonsecurity.com/2014/05/the-target-breach-by-the-numbers.

5 Perlroth, Nicole and Elizabeth A. Harris, "Cyberattack Insurance., a Challenge for Business," *The New York Times*, found at http://www.nytimes.com/ 2014/06/09/business/ cyberattack-insurance-a-challenge-for-business.htm

6 Ponemon Institute, "2013 Cost of Data Breach Study: Global Analysis," p. 3 (May 2013), http://www.ponemon.org/local/upload/file/2013%20report%20GLOBAL%20CODB%20FINAL%205-2.pdf.

the resulting damages can be disastrous for a business.

III. Is There Insurance for That? – The Types of Damages Resulting from a Cyber Loss

Unlike many other types of claims, cyber-liability claims are unique in that are difficult to insure against. Given the relative novelty of cyber-crime, there is virtually no historical or actuarial data available to evaluate the risk of an attack. Many damages resulting from an attack are intangible and hard to quantify, such as lost sales or goodwill, further making underwriting a challenge. Moreover, such data is challenging to compile because many breaches go unreported and attacks have few commonalities as hackers become increasingly sophisticated. Therefore, the insurance market is continuing to adapt and respond to this type of risk, and there is no standardized policy or form commonly utilized to insure against cyber risks.

Cyber-liability claims also are unique because they give rise to both first-party and third-party claims. Some types of commercial policies, such as commercial general liability policies, only provide coverage for a certain type of claim and do not provide coverage for both first-party and third-party claims within the same policy. Generally, however, a business has a combination or package of different types of policies for the various risks it faces. For instance, a typical business may have a commercial general liability policy (for third-party claims), a professional liability policy (for third-party claims), and a commercial property policy (for first-party claims). Unless a business has specific cyber-liability coverage, discussed at the end of this paper, a cyber-liability claim typically impacts multiple different policies.

A. First-Party Claims

A first-party claim is a claim for which the insured is damaged and seeks recovery under its own policy. A common example of a first-party claim is where a homeowner suffers a damaged roof in a hailstorm and seeks insurance money to repair or replace the roof. In the context of a cyber-liability claim, therefore, the insured has sustained damage to its own business or operations and seeks recovery under its own policy. Examples of first-party damages an insured can sustain in a cyber attack include:

- Theft of proprietary or financial business data or information;
- Damaged software or hardware caused by a virus or other malware;
- Business interruption damages caused by the insured's inability to access or use its network or software, or loss of information;
- Regulatory fines and expenses to be paid in conjunction with a loss;
- Expenses in upgrading software and network security, and in monitoring;
- Costs incurred to restore or recollect corrupted or stolen data; and
- Damaged reputation or lost sales following a breach and the public's perception of the company having inadequate data security in place.

Whether insurance potentially covers these damages largely depends on the type of policy at issue and the jurisdiction of the insured.

B. Third-Party Claims

A third-party claim is a claim made by a third party against the insured. The policy at issue, subject to its terms, provides coverage to the insured for its own liability to the third party. For instance, if the insured causes an auto accident injuring a third party, the injured third party may make a claim against the insured. The insured's auto liability policy may provide coverage for the claim asserted by the third party against the insured, which may include a defense if the third party sues the insured. Examples of third-party damages an insured can sustain in a cyber attack include:

- Claims for invasion of privacy resulting from theft of a third party's confidential information;
- Claims for damaged credit by a third party;
- Costs to monitor a third party's credit against misuse after theft of an account number or other identifying information; and
- Claims by financial institutions for financial losses incurred with fraudulent charges on stolen credit cards and in issuing new cards.

Similar to first-party claims, whether insurance potentially covers these damages largely depends on the type of policy at issue and the jurisdiction of the insured.

A business also can expect to incur a substantial amount in attorneys' fees defending against lawsuits (including class action lawsuits) resulting from a data

Title search: Hacking Through a Cyber-Liability Claim and Related Insurance Issues

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"