BARNES & THORNBURG LLP

The Other Cyber Shoe Has Dropped – What Does That Mean For Your Insurance Program?

December 9, 2014 | | Cyber Insurance, Data Breach, Policyholder Protection

Scott N. Godes
Partner
Data Security and Privacy Co-Chair, Insurance Recovery and Counseling Group Co-Chair

PolicyholdercybersecurityimageJust when you thought that it could not get worse for companies in the context of cybersecurity and privacy issues…it does. The end of 2014 has been brutal. Perhaps most significant, a court allowed banks to proceed against a retailer to pursue damages allegedly flowing from a cyberattack and data privacy incident involving payment card numbers. That same retailer disclosed hundreds of millions of dollars in losses as a result of the cyberattack a data privacy incident. Another retailer fell victim to a cyberattack and data privacy incident involving payment card numbers. Major entertainment businesses suffered cyberattacks, with one allegedly involving information about celebrities, corporate IP, and user names and passwords for social media accounts of the company. Distributed denial of service attacks (DDoS) are also on the rise. Below, we provide the sobering news about cyberattacks and some tips when considering insurance for cyber risk in 2015. **First, the decision involving banks and retailers is significant.** In *In re Target Corp. Customer Data Breach Security Litigation*, MDL No. 14-2522, the court refused to dismiss a complaint in the "Financial Institution Cases." *In re Target Corp. Customer Data Breach Security Litigation*, MDL No. 14-2522, slip op. [Dkt. 261] (D. Minn. Dec. 2, 2014). The refusal to dismiss a putative class action complaint against a corporate defendant in connection with a data privacy incident is not the eye opening part. Rather, it's the identity of the plaintiffs.

> "Plaintiffs here are a putative class of issuer banks whose customers' data was stolen in the Target data breach."

Id. at 2. Those banks have sued Target Corporation, alleging that Target was negligent in failing to secure payment card numbers, that Target violated Minnesota's Plastic Security Card Act, that there was negligence *per se* (because of the alleged statutory violation), and that the failure to tell the banks of Target's allegedly insufficient security practices was a negligent misrepresentation by omission. *Id.* There is little case law on this point, as the law is nascent and continues to be developed. Even less case law exists on the exact question of whether banks can pursue retailers for alleged losses resulting from a cyberattack and data privacy incident involving payment card numbers. Unfortunately for Target, however, the court ruled that the banks

RELATED PRACTICE AREAS

Data Security and Privacy
Insurance Recovery and Counseling

RELATED TOPICS

Cyberattack
cyber insurance
cybersecurity
Data Privacy
Privacy

could proceed with their action. There can be little doubt that Target's defense costs will continue to mount. **Second, the losses that Target has suffered already are noteworthy.** Target recently disclosed in its Form 10-Q for the quarterly period ended November 1, 2014 that it already had "incurred $248 million of cumulative expenses" as a result of the cyberattack and data privacy incident. Target, Form 10-Q, at 9 (Nov. 26, 2014). **Third, Target is just one example in a continuing stream of news regarding retailers that have had payment card information stolen.** In early December, Brian Krebs reported that international retailer Bebe Stores Inc. was another victim of a criminal cyberattack. Krebs wrote that Bebe had confirmed " [t]hat hackers had stolen customer card data from stores across the country in a breach that persisted for several weeks last month." Brian Krebs, "Bebe Stores Confirms Credit Card Breach," *Krebs On Security* (Dec. 5, 2014). **Fourth, retailers are not the only victims in the news.** A major movie studio also reportedly fell victim to a criminal cyberattack in late 2014. The cyberattack reportedly " brought down the Hollywood studio's corporate email, and leaked five films and a slew of sensitive personnel data, including a spreadsheet allegedly containing salaries of some 6,000 employees and top executives," according to the *Wall Street Journal.* Rachel Emma Silverman & Ben Fritz, "Data Breach Sets Off Upheaval at Sony Pictures," *The Wall Street Journal* (Dec. 4, 2014). **Fifth, distributed denial of service attacks (DDoS) are on the rise.** Large-scale DDoS attacks reportedly grew by nearly 40 compared to 2013. Jeff Goldman, "Verisign Warns of Surge in Large-Scale DDoS Attacks," *eSecurity Planet* (Nov. 24, 2014). What's that cost? One analyst explains that a company with " $1 billion in annual revenue amounts to $114,155 per hour"; a 24 hour outage, under that analysis, would be over $2.7 million. Adam Greenberg, "DDoS Attacks Cost Organizations $40,000 Per Hour, Survey Finds," *SC Magazine* (Nov. 13, 2014). **Is there any silver lining to offset this sky full of gray clouds?** Yes. One positive piece of information for Target, for example, is that Target's losses were

> "partially offset by expected insurance recoveries of $90 million, for net cumulative expenses of $158 million."

Id. Target's cyber insurance program also reportedly has

> "a $50 million sublimit for settlements with the payment card networks."

Id. Coverage for those losses is crucial for retailers, as we have written previously. What does this all mean for corporate insureds considering their cyber risks and insurance programs for 2015? Ultimately, it means that insureds should take a hard look at their insurance programs to evaluate what coverage they have for these risks. We've been saying for years that cyber insurance has long been described as "the Wild West of insurance." That means companies would be well-advised to analyze cyber insurance policies closely. **What should companies look for? Here are three tips for evaluating an insurance program in connection with cyber risks.**

1. Developments in the law suggest that companies should reevaluate whether they are carrying sufficient limits. Keep in mind that defense costs usually erode the limits of a cyber insurance policy. When lawyers are called upon to defend against claims in developing areas of law, legal bills add up quickly. After the company pays defense costs, will there be money left for settlements with plaintiffs, regulators, or anyone else?
2. Think about business interruption coverage. If your company

suffered a computer shut down, how much revenue would your company lose? Would your insurance cover the losses?

3. Retailers should pay close attention to what losses they would suffer after a cyberattack involving payment card numbers. Would your company's insurance cover tort claims by banks made in court? And all losses to payment card brands and payment card processors?