Cyber Liability: Understanding Technology Losses in an Age of E-Commerce

By: Suzanne C. Midlige, William J. Hoffman

October 11, 2007

In today's digital world, where electronic transactions are processed with lightning speed and where companies both large and small typically maintain confidential or proprietary data in electronic format, both the inadvertent loss of data and the theft of data by a new breed of thief —the cyber-criminal—pose an ever-increasing risk for unwary businesses.

Just ask one of America's largest retail conglomerates, The TJX Companies, Inc. ("TJX"), parent company of TJ Maxx, Marshalls and several other discount retailers operating in the United States and abroad. Over an 18-month period between July 2005 and December 2006, sophisticated computer hackers stole approximately 46 million credit and debit card numbers belonging to TJX customers in the United States, Canada and Puerto Rico. *See* Joseph Pereira, *Breaking the Code: How Credit Card Data Went Out Wireless Door,* The Wall Street Journal (May 4, 2007). Other estimates have put the number as high as 200 million card numbers stolen from four years' worth of electronic data. *Id.* To make matters even worse, the hackers also stole the social security numbers, military identification numbers and driver's license numbers of approximately 450,000 TJX customers —the type of information that is a veritable goldmine for identity thieves. *Id.*

TJX has been hit with several consumer class action lawsuits as a result of the breach of its computer network, as well as various investigations from state attorneys' general and a Congressional inquiry. As part of a proposed class action settlement recently announced in late September, TJX has agreed to, among other things, pay the cost of three years' worth of credit monitoring and identity theft insurance to the 450,000 or so customers whose personal information is believed to have been stolen. See TJX Settlement Filing (September 22, 2007). While the specific cost of credit monitoring is not set forth in the proposed agreement, the ultimate cost to TJX could be quite significant. Assuming, for example, that the cost of three years of credit monitoring amounts to $300 per person, the cost to TJX would be $67,500,000 if only *half* of the 450,000 individual consumers had their credit reports monitored for fraudulent activity.

That cost is in addition to the $6.5 million in legal fees TJX has agreed to pay to plaintiffs' class counsel, the $30 store vouchers it has agreed to provide to customers who made non-cash purchases during the relevant period, as well as other significant costs the company will incur under the terms of the proposed settlement. *Id.* In its earnings report for the second quarter of 2007, TJX took a $118 million after-tax charge for the quarter to cover current and potential costs arising from the theft, and may record an additional $21 million in non-cash charges in the future. *See* Walaika Haskins, *TJX Asked Too Much, Protected Too Little, Say Canadian Officials,* CRMBuyer (September 26, 2007) available online at http://www.ectnews.com. In addition, estimates are that TJX will spend an estimated total of $125 million on network security improvements as a result of the breach. *Id.*

TJX's experience is not unique, however. Choice Point, Inc. ("Choice Point"), a consumer data broker, experienced a security breach in 2005 that affected more than 140,000 people in all fifty states. Mary J.

Hildebrand and Jacqueline Klosek, *Recent Security Breaches Highlight the Important Role of Data Security in Privacy Compliance Programs,* 17 NO. 5 Intell. Prop. & Tech. L.J. 20 (2005). In order to resolve a suit brought by the Federal Trade Commission, Choice Point agreed to pay $10 million in civil penalties and another $5 million in consumer redress. *See* Warren Agin, *Information Security Law,* 26-3 ABIJ 54 (April 2007). Other corporate victims of lost or stolen data include Bank of America, which lost the personal information, including names and social security numbers, of approximately 1.2 million federal employees; DSW Shoe Warehouse, a retailer from whom 1.4 million credit card numbers were stolen; and TD Ameritrade, an online brokerage from whom cyber-criminals stole the personal information of approximately 6.3 million customers. These are but a few examples of the many companies that have experienced significant cyber-risk losses in recent years, whether as a result of theft, accident or their own inadvertence or carelessness.

In another noteworthy matter, Fidelity Federal Bank and Trust ("Fidelity"), a West Palm Beach-based bank, settled a class action lawsuit brought by Florida motorists for an estimated $50 million, including $10 million in attorneys' fees to plaintiffs' counsel. *See* Jeff Ostrowski, *Tens of Thousands of South Florida Drivers to Get $160 Checks,* Palm Beach Post (December 8, 2006). Fidelity allegedly violated federal anti-stalking legislation, which prohibits companies from buying driver records from state governments, when it purchased the records of approximately 565,000 Florida drivers between 2000 and 2003. *Id*. Fidelity reportedly purchased the information for a penny a name from the Florida Department of Highway Safety and Motor Vehicles, and then used the information to mail out brochures advertising its auto loans. *Id.* The plaintiffs involved in the settlement will each receive $160. *Id.*

It is evident that the recent advances in technology that have driven the growth of e-commerce have also resulted in unforeseen potential liabilities for businesses. Whether through a lack of foresight, a failure to understand and appreciate the potential perils of new technology or, perhaps, an underestimation of the determination of cyber-criminals to gain access to confidential data, many companies have left themselves uninsured against potential losses arising out of the storage of electronic data. Recognizing and acknowledging the presence of those perils will enable a company to protect itself from losses that may arise out of new technologies.

Insurance is one of the most common devices utilized by businesses to safeguard against catastrophic losses. Traditional insurance policies, however, were not designed to protect against the cyber-risks. As a result, many businesses that have, until now, relied solely or primarily on their comprehensive general liability ("CGL") policies will likely find themselves unprotected against the risks presented by many new technologies.

This paper will present an overview of certain technological advancements and the risks those advancements pose to businesses. We will also address the insurance coverage issues presented by so-called "cyber-risks" under a CGL policy and why businesses facing cyber-risk liabilities may find themselves without insurance protection. Moreover, we will discuss cyber-risks from an underwriting and risk management perspective, providing an overview of what may be done to protect against such risks.

While the trials and tribulations of companies such as TJX and other businesses that have fallen victim to lost or stolen data are noteworthy and have been the subject of significant media attention, they do not represent the only examples of cyber-risks that may befall a business in the digital age. For example, a business might inadvertently post copyrighted content on its website, leading to claims of copyright infringement, or host a chatroom or bulletin board on which, if not monitored vigilantly, potentially defamatory or private information may be posted, resulting in claims for defamation or invasion of

privacy. In another scenario, an internet worm or computer virus might shutdown or paralyze a company’s computer network or website, resulting in lost sales or a shut-down in operations until the problem is corrected. Moreover, a ripple effect may be felt by other businesses that, for example, may rely on another company’s network or website for the placement of orders.

For purposes of the present discussion, we will focus on two potential cyber-risks faced by any business that has a computer network or engages in e-commerce over the internet: lost or stolen data.

Read More