The Metropolitan
Corporate Counsel®
National Edition www.metrocorpcounsel.com
Volume 23, No.1 January 2015

The Challenge and Responsibility of Protecting Client Data

Steven L. Henning

Marks Paneth LLP

Data Security Concern

According to an October 2014 Gallup Poll, 69 percent of Americans frequently or occasionally worry about theft of their credit card information. Other than having a computer or smartphone hacked, the majority of Americans worry about this crime more than any other crime they were asked about.

These worries are driven by the growing wave of hackers that hit major retailers throughout 2014. Target revealed that credit and debit card information for 40 million of its customers was compromised. Neiman Marcus reported the theft of 1.1 million credit and debit cards by hackers who invaded its system. Sony, Morgan Stanley, eBay, AOL and others similarly reported that client or customer information was compromised.

The April 2014 discovery of the Heartbleed security flaw further demonstrated the vulnerabilities of digital data. The bug affected a widely used encryption technology intended to protect online transactions and accounts and went undetected for more than two years. It is unclear whether or not hackers have been exploiting the problem, but the malware is estimated to have affected up to 66 percent of active sites on the Internet.

Opportunity and Responsibility

The onslaught comes as businesses are moving to collect more and more information about their customers. The theory is that using data on a person's interactions with a business, along with other commercially available information, helps companies better understand consumers and better target their marketing. This means corporations keep increasingly sophisticated and detailed stores of data that provide a growing target for hackers. Yet, in spite of the concern over the theft of this data, few Americans are taking actions to protect themselves.

Steven L. Henning

For example, few people pay with cash for purchases rather than pay with plastic in response to data thefts. Consumers fail to check credit reports, change online passwords at retailers' websites, request new credit or debit card numbers from their bank or sign up for a credit-monitoring service.

This apparent failure to act reflects, in part, an acceptance of a new reality by consumers in the current economy. According to an Associated Press survey, it also reflects a belief by 88 percent of consumers that the burden of protecting data falls to the retailers who are collecting it. In addition, nearly two-thirds of consumers say the banks that provide credit or debit cards or the credit bureaus should bear most of the responsibility for protecting their data.

The expectations of consumers may be misplaced. A 2014 U.S. State of Cybercrime Survey reveals that most companies don't fully understand or address their security risks. Furthermore, only 38 percent of U.S. businesses prioritize security spending based on risk and the impact on their businesses. Even as the number of cyberattacks increases, most U.S. organizations' cybersecurity capabilities do not rival the persistence and technological skills of their cyber adversaries.

Repeat Offenders

Reports claim that Target did not react after two warnings from its own computer security system before cyber thieves stole the information. Sony has been the victim of multiple hack attempts over the past two years. The list of repeat victims is long even though security software is plentiful. Businesses seem to have ample incentives to protect themselves, but they routinely ignore such threats for a variety of reasons.

Among those reasons is that corporate executives often won't spend sufficient money on security because they see it as a pure cost that doesn't offer a financial benefit. This thinking ignores the very real cost of litigation and the loss of business from those affected by the theft of personal data.

Executives and managers often dismiss possible problems until one happens to them, and high corporate turnover means corporate leaders tend to forget the lessons they just learned. Keeping systems safe is an arduous task, requiring some companies to tend to thousands of computer servers and the ever-changing software they run. A constant stream of new vulnerabilities and attacks makes it difficult to keep abreast of everything. Changes in systems and software mean ever newer security flaws that hackers can exploit.

Litigation Risk

One of the fastest-growing sources of litigation in the U.S. is in the area of "privacy" litigation. This can be a drain on company resources and carries with it the possibility of significant financial loss. Privacy litigation arises in two primary ways: (1) as the result of a data breach arising from the unauthorized disclosure of personal information found in an organization's records, or (2) from the alleged invasion of an individual's privacy as the result of the collection, use and disclosure of personal information by companies with whom the affected individual has had contact.

Whether plaintiffs can establish injury to themselves and, if so, whether they can also establish damages has been a challenge. The cost of implementing greater levels of security, however, may be less costly than defending and losing a "privacy" lawsuit.

***Steven L. Henning**, Ph.D., CPA, is the Partner-in-Charge of the Litigation and Corporate Financial Advisory Services Group at Marks Paneth LLP.*

Please email the author at shenning@markspaneth.com with questions about this article.