Managing Risks and Preparing for a Data Breach: Cyber Liability

Authors: Daniel P. Schrader and Nirali Patel

March 17, 2016

The digital revolution has changed the way business is conducted, how people communicate, and the way private information is stored and maintained. The advantages of this technology outweigh the risk, but rest assured the risk is present for all businesses that collect or maintain personally identifiable information (PII). Privacy and cybersecurity go hand in hand, in that one of cybersecurity's primary goals is to protect personal information.

Everyone is aware of news reports of hackers accessing retailers' computer systems (Target and Home Depot) and obtaining credit card and personal information about their customers. Equally troubling are the data breaches involving healthcare providers and insurers (Kaiser and Anthem BlueCross) and employers (Sony Pictures). Phishing and spear-phishing email attacks have become a significant threat facing U.S. companies. As incidents of data breaches have increased and become more sophisticated, so have the regulatory scheme and legal requirements for businesses to ensure that PII is protected.

PII includes, but is not limited to, personal information such as Social Security numbers, credit card accounts, healthcare treatment, telephone numbers, email addresses, or any other information that permits the identity of an individual across different websites or online services. (Cal, Civ, Code § 1798.80). In essence, almost all businesses on some level obtain and maintain PII of clients, customers, or employees. PII is information that hackers are seeking for the purposes of financial gain, disruption of business operations, and dissemination to the public. As a result, federal and state regulatory agencies and associated acts/laws (i.e., Section 4 of the Federal Trade Commission Act, SEC Regulation S-K Item 503(c), Sarbanes-Oxley Act of 2002, Health information Technology for Economic and Clinical Health Act (HITECH Act), Financial Services Modernization Act of 1999 – Regulation S-P) have enacted laws to protect PII (the definition of PII from Cal. Civ. Code § 1798.80 may differ from the definition used by federal agencies), and the failure of a business to take steps to comply with the myriad of such laws and enact viable methods of protection has potentially dire consequences. (Cal. Civ, Code §1798.80 et seq.)

Experts in the field of cyber technology have essentially conceded that there is no sure method to prevent data breaches, because as technology advances to protect against such breaches, cyber criminals find new ways to exploit the new technology. In order for a business to avoid potential regulatory liability, it must have in place a Security Protection Plan and a Data Breach Response Plan. Also, in addition to

regulatory penalties, there can be civil liability with the possibility of exposure to damages. It is also important for businesses to consider securing a cyber liability insurance policy to mitigate the losses from a data breach.

The Security Protection Plan will vary based on the type of business operations and the PII that is secured and maintained. At a minimum, the plan should include an effort to identify the PII stored or maintained; employ a viable cybersecurity system to prevent access to hard drives, software, email accounts, and cloud-based storage; have a stated protection policy; and implement a training program to ensure compliance with the policy. There are numerous, cyber vendors that provide framework for a Security Protection plan. Implementing such a plan helps to demonstrate that the company is exercising due care to protect PII.

The implementation of a Data Breach Response Plan is also paramount to avoiding regulatory fines and punishment. The Federal Trade Commission (FTC) is actively enforcing cybersecurity regulations. The FTC has far-reaching powers and authority to charge public companies fines and penalties for failing to adequately employ data security practices.

The Data Breach Response Plan should be in writing, identify a responsible individual in the company to enforce compliance, and identify a team of professionals (i.e., cyber technical specialists, legal counsel) to respond to a breach. The plan should identify the methods employed to access and identify possible data breaches. Additionally, the plan should address the means by which a potential data breach will be contained, remediated and eradicated. Finally, the plan must have stated means and methods to inform clients of the data breach after confirmation of its occurrence.

The insurance industry has responded to the increase in data breaches and placed on the market cyber liability insurance policies. The cyber policies typically provide coverage for customer notification expenses, credit and identity theft monitoring, liability protection from lawsuits, costs for regulatory defense, and business interruption damages. The nature and extent of insurance coverage will vary based on the nature of the business operations and the type of PII that is maintained and stored. The insurance coverage can also provide access to third-party resources to assist with efficiently and cost-effectively responding to a data breach incident.

In the ever-changing world of technology and the increasing likelihood of a data breach, it is imperative that businesses take proactive steps to implement a cyber data plan and secure the legal and insurance resources to protect its valuable commodity of client privacy and personal information.

About Walsworth

Walsworth was founded in 1989 with a commitment to establish a law firm focused on working collaboratively with clients to meet their unique objectives. Since then, the firm of over 80 attorneys, with offices in Orange, Los Angeles and San Francisco, is known for excellence in litigation and transactional matters. We are equally distinct in our longstanding commitment to diversity, which is recognized through our certification as a Women's Business Enterprise

(WBE) by the Women's Business Enterprise National Council (WBENC) and by the California Public Utilities Commission, and we are proud to be the largest certified WBE law firm in the United States. Walsworth is also a National Association of Minority and Women Owned Law Firms (NAMWOLF) member, the largest in California and third largest nationwide. For more information, visit www.wfbm.com.