HOW TO BE SECURE IN AN UNSECURE WORLD

Karen Painter Randall and Steven A. Kroll Connell Foley LLP

Whether you are a Fortune 500 company or a law firm, no organization today is immune from the threat of a costly data security breach. Between 2011 and 2012, security breaches were seen across various industries from retailers such as Amazon's Zappos to marketing firms such as Epsilon, to defense contractors such as Lockheed Martin. Perhaps the most publicized breach took place in 2013, when hackers stole data from up to 40 million credit and debit cards of Target shoppers who visited its stores during the first three weeks of the holiday season. It was reported as the second-largest such breach involving a U.S. retailer. These security thefts have led to the filing of numerous lawsuits, including class actions, across the country.

The threat posed by criminal hackers who use networks of secretly hijacked computers has substantially increased over the past several years, and hackers are now creating networks known as "botnets." It has taken an international effort to stop one botnet in particular called "Gameover Zeus." Specifically, once a computer is infected by Gameover Zeus, often after its user clicked on a malicious link or email attachment, it becomes a "bot" and started communicating with other infected computers, creating a network of similarly afflicted machines. While communicating with each other, the bots also pass along stolen banking information to servers that relayed that data to the hackers. The hackers commit their cyber burglary by exploiting the security hole bored by Gameover Zeus.

In the electronic age of convenience, a hacker requires very little information to steal personal identification and health information, obtain credit cards in another's name, or do a host of other damage. Breaches are caused not only by hackers but rogue employees and loss/theft of equipment. Because organizations have become increasingly reliant on digital technology in their operations, the potential for damages from a cyber-attack continues to rise.

TYPES OF EXPOSURE

In the wake of data breaches across the country that have seen hackers obtain the personal information of individuals, businesses and law firms alike have been making significant investments in network hardware and software to protect confidential data. The financial exposure associated with a data breach can be quite substantial as studies show that the average cost of a breach is well over five million dollars. The amount of damages can also be quite significant. By way of example, the U.S. Court of Appeals for the Sixth Circuit recently held in *Retail Ventures, Inc. v. National Union Fire Insurance Company of Pittsburgh, PA*, 691 F. 3d 821 (6th Cir. 2012), that DSW, Inc., DSW Shoe Warehouse, Inc., and Retail Ventures, Inc. were entitled to coverage under a commercial crime policy for a $6.8 million loss resulting from a data breach. Moreover, in *Zurich American Insurance Co. v. Sony Corp. of American, et al.*, Index No. 651982/11 (N.Y. Sup. Ct.) while granting summary judgment in favor of Zurich in a coverage dispute, Sony alleged in its Court papers that a data breach stemming from the hacking of their PlayStation online services had exposed personal information of tens of millions of users, and Sony's losses were reportedly estimated to be as high as $2 billion. Furthermore, the stopping of the botnet Gameover Zeus did not occur until after infecting between 500,000 and 1 million computers worldwide and inflicting more than $100 million in losses. As a result, the potential for damages in the event of a data breach can be astronomical, and, in some cases, cause a company to go out of business.

A cyber breach can also cause substantial and long term damage in other ways such as loss of productivity, loss of data and intellectual property, business interruption, and, perhaps, most importantly, injury to reputation and loss of client goodwill. Furthermore, now more than ever, regulators such as the Federal Trade Commission and state Attorney General offices are getting involved and imposing fines and penalties on businesses for failing to protect data or provide timely notice of a breach. Moreover, even non-government entities, such as the Payment Card Industry Security Standards Council, have established Best Practice standards.

DIRECTOR AND OFFICER LIABILITY FOR DATA BREACHES

Besides the corporation itself being at risk for litigation, individual directors and officers can also be exposed to liability for breach of a fiduciary duty in failing to properly oversee cyber security. With so much at stake in protecting personal identifiable information, it is not enough for a director and officer of a company to simply delegate responsibility for protecting such confidential information to their IT staff.

The Division of Corporation Finance of the SEC recently issued a 'Disclosure Guidance', which recommends that material information regarding cyber-security risks and cyber incidents should be disclosed in order to make other required disclosures, in light of the circumstances under which they are made, not misleading. Moreover, information is considered material if there is a substantial likelihood that a reasonable investor would consider it important in making an investment decision or if the information would significantly alter the total mix of information made available. While this is merely a recommendation by the SEC, not a rule or regulation, non-compliance is risky. Furthermore, although these recommendations are only directed at public companies under the SEC's jurisdictions, other businesses would be prudent to heed the same advice. As a result, directors and officers must be attuned to new regulations to protect themselves against the impact of cyber risks and costs in the larger context of their company's disclosure obligations to investors.

Shareholder lawsuits have already begun to be filed across the country against companies like Target and Wyndham Worldwide Corp. that have fallen prey to data breaches. In addition to these lawsuits,

directors and officers face other concerns. For example, a proxy adviser, Institutional Shareholders Inc., recommended that Target stockholders vote against seven of ten directors because they failed to manage cyber risks. This is the first time that there has been an effort to unseat board members because of a cyber breach. In the Wyndham case, director and officer litigation followed an enforcement action by the Federal Trade Commission sending a clear message that regulators are going to be more active in these claims. Today, some regulatory settlements require that the business agree to a Comprehensive Written Information Security Program, which mandates periodic audits over a period of years and includes fines and penalties along with the cost of implementing the program. Thus, given the increased prevalence and effectiveness of cyber-attacks and breaches, and in light of the Disclosure Guidance, it would be difficult to justify why proper protective measures, including sufficient cyber insurance, were not implemented, and why the risks were not disclosed to the investing public.

DATA BREACHES INVOLVING LAW FIRMS

In a profession based upon tradition and precedent, the practice of law is also not immune from data breaches as many law firms today rely upon digital technology including the use of mobile devices, laptops and email to be in constant communication with their clients. Moreover, as law firms are "going green" confidential documents containing a client's personal information are often scanned into and maintained on a computer network or a company's Cloud susceptible to hackers.

Pursuant to American Bar Association Model Rules of Professional Conduct 1.6(a), a lawyer shall not reveal confidential information. Thus, attorneys have a duty to take reasonable steps in communicating with their client in a manner that protects the confidential information received. As a result, law firms, like many other businesses, are making significant investments in network hardware and software to protect sensitive and confidential client data. However, the question becomes what exactly should a law firm, or any other business for that matter, do to protect against a data breach?

MITIGATION STRATEGY

First and foremost, preparation is vital to preventing any sort of data breach. Thus, consider creating a committee, which includes members of its IT department, to develop and implement a risk management plan for preventing a data breach. Once a committee has been established, there should be policies in place regarding the privacy and security of business data, which includes the use of encryption, remote access, mobile devices, laptops, email accounts, and social networking sites. In addition, conduct an inventory of the software systems and data, and assign ownership and categorization of risk; the higher the sensitivity of the information, the stronger the security protections and access control must be. Furthermore, the IT department should conduct third-party vulnerability scans, penetration tests, and malware scans to protect against potential data breaches. Most importantly train employees so that they are aware of the company's security protocol in place, and protected against the potential for accidentally exposing a client's personal, confidential information with the click of a button.

Unfortunately, in the evolving technological world even the best security can be penetrated by skilled hackers from around the world. Thus, besides having policies and procedures in place to prevent a data breach, it is critical that a company also implements a Rapid Response Plan to react quickly to a cyber-attack. Once a potential data breach has been identified, a company should determine what type of information was exposed, as well as consider reporting the incident to the law enforcement authorities for investigation. It should be noted that each state has its own notification laws regarding reporting a data breach, thus, one should be familiar with same.

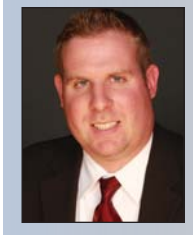
A corporation also has an obligation to inform its clients of any potential compromise of personally identifiable and confidential information. Thus, it is imperative that either a timely letter or personal telephone call be made to each client advising of the data breach so that the client can take reasonable steps to protect themselves from any vulnerabilities that could potentially result in having their personal information out in the open. Many companies also include in the letters to affected customers a telephone number to a call center that will provide information about the extent of the breach, the company's response, or next steps. Moreover, many times as a courtesy to the client, and in order to gain back their trust, a company pays for credit and identity monitoring. Furthermore, many companies are engaging an external public relations firm that specializes in damage control to help mitigate harm to its reputation caused by a data breach.

Lastly, due to the potential for significant damages, companies should consider purchasing cyber insurance to cover the costs of a breach and claim against them. Although companies may have a CGL or professional liability insurance policy, they should retain a specialized insurance broker to make sure that any policy in place covers the type of loss associated with a cyber breach. As referenced earlier in the *Zurich* matter, the Court held that action taken by a third party hacker was not covered under Sony's CGL policy. Conversely, in *Hartford Casualty Insurance Co. v. Corcino & Associates, et al.*, the U.S. District Court for the Central District of California ruled that there was coverage under a CGL policy for a data breach involving hospital records. Thus, in order to avoid a potential coverage dispute, a company should contact an insurance broker well-versed in cyber coverage to ensure that they have the necessary coverages in place in the event of a cyber breach.

CONCLUSION

Overall, companies, including law firms, are becoming increasingly dependent upon technology to run their business. As a result, all organizations need to become familiar with the risks associated with a data breach, and have policies and procedures in place to not only prevent such attacks, but provide a quick response plan in the event of a breach. Being prepared for a potential cyber-attack will protect a business from significant financial exposure.

Karen Painter Randall is a Complex Litigation Partner with Connell Foley LLP in Roseland, NJ, and Chair of the firm's Professional Liability and Director and Officer Practice Groups. She provides representation and advocacy services to professionals and businesses in a wide variety of complex litigation matters and is a veteran trial attorney in state and federal courts. Ms. Randall, a former Chair of USLAW's Professional Liability Group, is designated a Certified Civil Trial Attorney by the Supreme Court of New Jersey.



Steven A. Kroll is an Associate with Connell Foley LLP in Roseland, NJ. In addition to representing professionals in various areas, Mr. Kroll concentrates his practice in the areas of professional liability, general insurance litigation and employment law handling matters in both New Jersey and New York. Mr. Kroll received his J.D. from Rutgers-Newark School of Law in 2009, cum laude, and received the distinguished award of Order of the Coif.