Fortifying the Law Firm

Understanding and Protecting Against Cyber Risk

By Seth L. Laver

With law firms increasingly serving as relatively easy stepping stones between clients and cyber thieves, taking precautionary measures will doubtlessly benefit lawyers and clients alike.

The paradox of technology is that while it makes our lives infinitely easier in certain respects, it opens the door to vast, new worlds of potential risk and liability. Whether a mom-and-pop shop or a Fortune 500 company, anyone maintaining a website or storing information electronically faces certain exposure to cyber risk and associated liability.

This is especially true and especially scary for law firms, both small and large, which rely on 24/7 accessibility through smart phones and tablets to meet the demands of their clients. Attorneys publish online immense amounts of scholarly and promotional materials and house their clients most closely guarded secrets on data servers or remotely in the information "cloud." Frighteningly, current statistics suggest that while instances of intentional data breach are on the rise, those responsible for protecting that information do not take appropriate steps to defend against it.

Attorneys across the country face a troubling trend in that cyber criminals now target law firms more than ever. Modern corporate America has paid better attention to protecting information as it increases its dependence on mobile devices and electronic data. Accordingly, these businesses have become more difficult cyber crime targets. In response, cyber criminals now focus on corporations' law firms because they frequently have unlimited access to the prized data yet less frequently use the best or any cyber protection making law firms "softer targets."

Cyber Risk—On the Rise

Cyber risk can imperil both first and third parties. Third parties can suffer Internet domain name or trademark infringement, copyright or patent violations, defamation, unauthorized network security breaches by hackers or infection by a computer virus, and, privacy liability arising from theft of personal data stored in electronic format.

On the other hand, first parties can suffer the often substantial expenses associated with disclosure costs resulting from private data or confidential information theft. Costs to first parties may include defense coverage for negotiating with any number of regulatory agencies for claims involving personal or confidential information theft as well as payment of the associated fines and penalties that the government may impose. Damage caused by a virus or hacker and business interruption during any system down time may lead to additional expenses. Notably, of course,

■ Seth L. Laver is a partner of Goldberg Segalla LLP in Philadelphia, where he concentrates his practice in employment and labor law and professional liability defense, including the representation of non-medical professionals. He is an active member of the DRI Professional Liability Committee and serves as its program vice chair and webcast co-chair.

first-party losses also include direct damages when a successful hack results in lost dollars.

The nature of the legal profession makes lawyers and law firms particularly vulnerable to these risks because two of their most important ideals—confidentiality and dedicated client service—mean that they possess valuable data and electronically stored information to address client needs anytime, anywhere, which criminals can find tempting to steal.

The number of reported incidents of identity theft and data security breaches in the United States continues to grow at an alarming rate. According to the 2012 Data Breach Investigation Report, the number of compromised records rose to 174 million in 2011 and 855 reported incidents. Verizon Risk Team & U.S. Secret Service, the 2012 Data Breach Investigations Report. It is entirely possible that hundreds of additional breaches were not reported. The estimated cost of responding to a breach is anywhere from $5 to $204 *per record* with an average cost of $2.4 million per breach, and legal services account for the majority of that expense. Larry Ponemon, *Five Countries: Cost of Data Breach*, Ponemon Inst. & PGP Corporation, Apr. 19, 2010; Mark Greisiger, *Cyber Liability & Data Breach Insurance Claims*, NetDiligence, June 2011. The average cost of defending a cyber liability claim is $500,000, and the average settlement is $1 million. Every quarter second someone steals an electronic file containing information that could compromise an individual's identity. Paul W. Burkett, *What Are the Cyber Risk Liability Exposures?*

Since cyber crime is a relatively new and evolving source of risk, many organizations have not kept up with managing cyber risks compared to other risk areas. A telling statistic is that the victim of a breach in over 85 percent of the reported data breaches in 2011 did not discover the breach; external parties such as law enforcement personnel discovered them. *Risk Intelligent Governance in the Age of Cyber Threats*, Deloitte Development LLC, 2012. It appears that most organizations are not even equipped to detect cyber crime, let alone defend against it.

Cyber criminals also are efficient. Seventy-two percent of cyber attacks last year reached pay dirt within minutes, if not sooner. Moreover, experts viewed the great majority of all reported cyber attacks—97 percent—as avoidable even without difficult or expensive counteracting controls. What this means is that cyber attacks are frequent, easy, and quick to pull off yet relatively defensible with the right tools.

Cyber Risk in the Courts

With respect to case law affecting cyber liability, the landscape continues to develop as the judiciary attempts to define the limits of exposure. Victims of data breach have filed many cyber-related lawsuits, but few survived the initial pleadings. The early cyber law decisions demonstrate the difficulty that plaintiffs must overcome to litigate a negligence action based on a data breach successfully. The problem that the plaintiffs encountered was that they lacked standing or failed to establish a recognized injury. Without theft and misuse of personnel data resulting in an actual injury, the courts almost universally dismissed the plaintiffs' claims since "allegations of hypothetical, future injury are insufficient to establish standing." *Reilly v. Ceridian Corp.*, 664 F.3d 38, 42 (3d Cir. N.J. 2011).

Recently, however, the tide has shifted somewhat in favor of the victims of data breaches in some circuits. For example, in *Krottner v. Starbucks Corp.*, 628 F.3d 1139 (9th Cir. 2010), the Ninth Circuit Court of Appeals joined the Seventh Circuit and perhaps others in holding that data breach victims had sustained a "credible threat of harm" sufficient to establish standing. *See also*, *Pisciotta v. Old National Bancorp*, 499 F.3d 629 (7th Cir. 2007). Although the court in *Krottner* eventually dismissed the claims on the merits, this decision may represent vulnerability upon which creative plaintiffs' attorneys can capitalize. The increase in legislation and in regulation related to data breaches at the state and federal level may also have contributed to the plaintiffs' recent success. Rodd Zolkos, *Data Breach Plaintiffs Increasingly Successful*, Business Insurance (June 9, 2011), http://www.businessinsurance.com/article/20110609/NEWS/110609911 (last visited May 29, 2012). The new class of attorneys representing cyber liability plaintiffs is more adept at moving claims beyond the pleadings and into discovery, which significantly affects defense costs.

The current cyber-related litigation pending before the state and federal courts should provide a clearer picture of the future of cyber liability. Given the split among the circuits, however, lawyers have many unknowns to contend with. Accordingly, all professionals with access to sensitive customer information must remain vigilant in their data security efforts.

Since cyber crime is a relatively new and evolving source of risk, many organizations have not kept up with managing cyber risks compared to other risk areas.

Anatomy of a Cyber Attack

Understanding how lawyers and law firms may be exposed to cyber crime is the first step toward prevention. Cyber crimes may range from the technologically advanced to the elementary. Rather than engaging in hacking, criminals may obtain financial information or sensitive client data from a stolen laptop, a smart phone, or another electronic device. Moreover, the very same cyber risk may result from a smart phone accidentally left in a taxi, a missing briefcase, or another innocent mistakes common in our increasingly mobile business world. The consequences of theft of an inexpensive piece of equipment may exceed a victim's expectations: the victim may need to engage in expensive data retrieval, to meet regulatory responsibilities and to deal with the potential disclosure of sensitive client data, not to mention explaining this loss to the client.

The electronic hack is the highest profile and most complex means of data theft. Generally, a hacker targets weaknesses in a computer network and develops methods to exploit them motivated by profit, protest, or the challenge. Those with criminal intent use remote devices to steal infor-

mation and may search for electronic data or passwords, often exploiting default or "guessable" credentials. Others may use stolen log-in credentials to access electronic data. Some hackers may use a friendly e-mail or other electronic communication in the hope that an unsuspecting attorney will open his or her door to the enemy and allow the criminal to gain access, review information, or plant a virus. Hacking is an advantageous attack method because the hacker conducts it remotely, which allows anonymity. If someone doesn't have the appropriate security measures in place, a criminal can achieve hacking fairly easily, and it permits the criminal to cast a wide net toward many potential victims.

The reason that cyber risks are real and increasing for law firms is because one of the fundamental elements of the attorney-client relationship is trust.

The "Easier Quarry"—Law Firms in the Crosshairs

The reason that cyber risks are real and increasing for law firms is because one of the fundamental elements of the attorney-client relationship is trust. Attorneys stress to clients the importance of an open dialogue resulting in the disclosure of personal, confidential, and otherwise privileged information, whether social security numbers, trade secrets, inventions, corporate strategy, or marital assets. As a result, law firms maintain a goldmine of data that unintentionally could allow an unforeseen recipient to engage in identity theft, insider trading, extortion, copyright infringement, and other crimes.

It should come as no surprise then that law firms have become favorite targets of hackers and other cyber criminals. Over a several month period beginning in September 2010, for instance, hackers based in China attempted to unravel a $40 billion acquisition of the world's largest mined salts or "potash" producer by hacking into the parties' Canada-based law firms. The hackers attempted to pilfer one secure network after another, eventually striking seven law firms and Canada's Finance Ministry before someone uncovered the threat. The stolen data, reportedly valued at tens of millions of dollars, could have provided a negotiation advantage to the cyber thieves. Although the parties eventually uncovered the scam, this event began to raise the collective awareness of the vulnerability of law firms to cyber exposure.

According to the head of the cyber division of the FBI, Mary Gilligan, cyber criminals consider law firms "much, much easier quarry" than some other targets. Michael Riley & Sophia Person, *China-Based Hackers Target Law Firms to Get Secret Deal Data*, Bloomberg (Jan. 31, 2012), http://www.bloomberg.com/news/2012-01-31/china-based-hackers-target-law-firms.html. During a recent meeting with some of the country's largest law firms, Gilligan warned the law firms' decision makers to be wary of the apparent shift in hackers' focus from businesses to the businesses' law firms. According to one estimation, 80 U.S. law firms were hacked in 2011. *Id.*; David G. Ries, *Cybersecurity for Attorneys: Understanding the Ethical Obligations*, Law Practice Today, Mar. 2012, http://www.americanbar.org/newsletter/publications/law_practice_today_home/law_practice_today_archive/march12/cyber-security-for-attorneys-understanding-the-ethical-obligations.html (last visited May 29, 2012). Unless the legal industry acknowledges and reacts to this growing risk, the number of law firms falling victim to cyber crime will continue to grow in 2012 and beyond.

The consequences of a breach of a law firm's electronic data may become especially dire. In addition to unintentionally disclosing confidential materials, a firm could face civil proceedings including causes of action sounding in breach of contract, professional malpractice, breach of fiduciary duty, or other torts. Likewise, a law firm may face regulatory issues pertaining to disclosure of protected health information or financial data. Depending on a law firm's professional errors and omissions policy, the firm's malpractice carrier may cover some of these claims. However, without independent cyber liability protection, it is entirely possible that the costs of defending and responding to a cyber loss will fall squarely on the lawyers themselves.

Precautions for Law Firms

By most accounts law firms are not ready to combat or to react to cyber crime. The time is now to heed the warnings and set safeguards to prevent or at least to help defend against cyber crime. The International Organization for Standardization and the International Electrotechnical Commission aligned to form a set of security techniques to combat electronic data breach known as "ISO/IEC 27002." This guide provides best practice recommendations for those responsible for maintaining information-security management systems. Although the time and the expense necessary to achieve full ISO/IEC certification may seem daunting to most law firms, the security methods identified provide a workable outline for law firms to consider. *See*, Anthony Davis & Michael Downey, *Protecting Client Information*.

The ISO/IEC has identified the following 12 things that an information security manager needs to address to achieve security certification:

1. Risk assessment;
2. Security policy (management direction);
3. Organization of information security (governance of information security);
4. Asset management (inventory and classification of information assets);
5. Human resources security (security aspects for employees joining, moving and leaving an organization);
6. Physical and environmental security (protection of the computer facilities);
7. Communications and operations management (management of technical security controls in systems and networks);
8. Access controls (restriction of access rights to networks, systems, applications, functions and data);
9. Information systems acquisition, development and maintenance (building security into applications);
10. Information security incident management (anticipating and responding

appropriately to information security breaches);
11. Business continuity management (protecting, maintaining and recovering business-critical processes and systems); and
12. Compliance (ensuring conformance with information security policies, standards, laws and regulations).

Again, many law firms may find seeking complete certification impractical, but the ISO/IEC warnings are helpful for the modern law firm. Consider undertaking the following.

Implement Data Management Safeguards

Most law firms maintain computer-use policies requiring employees to use and routinely to update passwords for e-mail, document management systems, and electronically stored materials. Presumably, law firms use anti-virus protection as well. Other safeguards include limiting who may access particular materials electronically and when they may share, print, or alter data. The ISO/IEC also suggests that law firms monitor electronic usage with an eye toward unusual activity, particularly if information is being pulled off of a firm's network. As one risk-awareness publication aptly put it, "when Jane from Kansas logs in from Uzbekistan, worry." *Risk Intelligent Governance in the age of Cyber Threats*, Deloitte Development LLC, 2012.

Become Familiar with the Risks

Law firms should make an effort to educate attorneys and support staff that the very materials that they access at the click of a button may become the target of unknown cyber criminals. This will communicate the full implications of confidentiality and everyone must take it seriously. Moreover, in the event of a potential data breach, a firm must educate attorneys and staff on the practice for reporting a suspected disclosure. A firm's computer-use policy should explain this procedure.

Address Data Retention Policies

The modern law firm stores incredible amounts of data electronically. Many law firms have joined the "green" push toward a paperless practice, which certainly means that they have converted even more materials into electronic form. But where and how is the data stored? A law firm must maintain clear policies regarding electronic storage and who can access that information permissibly. Consider how long a law firm will maintain data electronically and whether that material is secure. A firm should eliminate unnecessary data and keep tabs on the data that it does store. So too should a law firm maintain up-to-date and accessible computer and social networking policies geared toward combating inadvertently and innocently disclosing client information.

Respecting destruction of electronic and hard copy data, law firms need to heed the danger of theft of discarded electronic or hard copy materials. Just as a firm should shred and dispose of sensitive hard copy materials, the firm likewise must completely remove and destroy electronic data from a firmwide database. Finally, consider carefully the method of destroying unwanted, out-of-date computers and equipment that may also contain client data.

Examine Insurance Coverage

Today's law firm cannot assume that its professional errors and omissions policy will cover all cyber liability losses, including those associated with unintentionally disclosing client data. In all likelihood a law firm's professional errors and omissions policy would cover some of the third-party professional malpractice claims arising from a disclosure, but many of the first-party-related losses, including those associated with regulatory issues, reporting costs, and data retention, may fall outside of the standard policy.

For its part, the insurance industry is adapting to the seemingly ever-changing landscape of cyber liability and working toward creating products specifically tailored to help law firms meet these new challenges. As technology develops and case law continues to emerge regarding cyber liability, the policies available evolve to protect the needs of the industry. Some cyber liability insurance policies offer coverage options to assess the range of third-party and first-party risks. A law firm often has the option to customize particular types of cyber liability coverage to meet the firm's specific needs depending on its size, location, client base, technological sophistication, and other factors. Policies that address the following are worth considering:

- Data privacy and security breach coverage including coverage for violations of data privacy laws, unauthorized access or unauthorized use of computer systems, and identify theft claims
- Copyright and trademark infringement and libel, slander, and defamation claims
- Notification and credit monitoring coverage to comply with reporting requirements
- Crisis management coverage including coverage for costs associated with public relations and law firms to mitigate reputational harm
- Regulatory proceedings coverage, including coverage for fines associated with Health Insurance Portability and Accountability Act (HIPAA), Fair and Accurate Credit Transactions Act (FACTA), and other regulatory violations
- Information asset recovery and business interruption expenses coverage.

Conclusion

With law firms increasingly serving as relatively easy stepping stones between clients and cyber thieves, taking precautionary measures without doubt will benefit lawyers and clients alike. FD