Cyber Liability: (How Well) Are You Covered – And Why Does it Matter? By Anthony E. Davis [1]

Let's begin with some questions:

- Has your firm's network ever been successfully hacked? (If you answered "no," how do you know?)
- Has anyone in your firm ever lost a laptop, a Blackberry, iPhone, Android (or any other PDA), or a flash drive?
- Did the lost device contain client specific and confidential information?
- Was the device password protected? Was all data contained therein encrypted?
- Has anyone in your firm accessed the firm's network or transferred sensitive data from an unsecured Wi-Fi connection?
- Does your firm have a "Bring Your Own Device" culture? If you answered "yes," how can you be sure each mobile user has adhered to practices within your IT department's control & security in every aspect of their use of the device?
- Does your firm use an open document or knowledge management system? If you answered "yes," how do you control access to confidential data? Do you track what has been accessed or removed?

Now let us explore the implications of your answers.

In an article on Bloomberg's website in January, 2012, *China-Based Hackers Target Law Firms to Get Secret Deal Data*, reporters Michael A. Riley and Sophia Pearson quoted Mary Galligan, head of the cyber division in the New York City office of the U.S. Federal Bureau of Investigation, as saying that "As financial institutions in New York City and the world become stronger, a hacker can hit a law firm and it's a much, much easier quarry." They reported that Galligan's unit convened a meeting with the top 200 law firms in New York City last November to deal with the rising number of law firm intrusions and issued a warning: Hackers see attorneys as a back door to the valuable data of their corporate clients. Mandiant, a consulting firm based in Alexandria, Virginia, estimated that 80 major U.S. law firms were hacked last year.

[1] Anthony E. Davis is a partner in the *Lawyers for the Profession®* practice group at Hinshaw & Culbertson LLP, practicing out of the New York office. Anthony and his colleagues regularly provide training and advice to law firms on the need for, and how to go about improving all aspects of technology management

As for losing devices, this is an inevitable – if not a frequent occurrence. And when they disappear, if the data they contain is not strongly protected – which in turn means properly encrypted or protected by a password (using 10 or more characters including upper and lower case letters, numbers and symbols) – it will be readily accessible to the finder. According to a report in 2011 on National Public Radio, it takes less than two minutes to break a four character password – and most of us know lawyers who carry around devices with no password protection at all.

Concerning the problem of "Bring your own device" (BYD) policies , firms are faced with a quandary. On the one hand, unless they agree to purchase any and all devices their employees wish to use (in order to register and thereby maintain the ability to wipe them all remotely, and to encrypt them), firms (and their clients) are at risk that confidential data will creep onto personal devices which are not in any way secured. We have heard of one firm that has instituted a policy that it will indeed purchase any and all devices and prohibited employees from owning any personal devices that have not been purchased by the firm. Failing that approach, it is evidently problematic for firms to manage and control the use of personal devices. Such devices also carry the additional risk that arises when owners, using social media, accepting an app or an infected personal email which can then in turn infect any PC it connects to, and then a virus or other malware can spread to the network.

The use of unsecure/Public Wi-fi has numerous risks, including if the device is being used other than through a secure remote connection that is behind the firm's firewalls, enabling hackers sitting within 300 feet of the user, to steal passwords, and access any and all data on the device, including emails, attachments and passwords.

Lawyers value ease and speed in their work environment, including the ability to conduct wide searches of the firm's (and its clients') data. They point to the savings to clients in allowing the efficiencies that an open document management system permits. But open document and knowledge management has significant risks. With an open document management system, once someone is in the network (either a hacker who got past the firewall or an employee) there is no barrier to prevent them from looking at confidential data? Equally troubling is the problem that if there has been an improper access to sensitive data, and the intruder has removed or altered the data, would the firm know it? On the other hand, how far should firms go to limit access rights to each client's (and the firm's own) files?

So what? This article will assist law firms to identify the principal ramifications that can result from data loss – including the scope of the potential financial losses; to understand the scope – and limitations – of lawyers professional liability (malpractice) insurance; the nature of additional coverages available under the general heading of "cyber" insurance – and why law firms may be well advised to consider acquiring this additional insurance protection.

The Potential Consequences of Data Loss And Security Breaches

It is critical to recognize at the outset that data losses and security breaches affect two distinct groups: the custodian (for our purposes, the law firm); and a wide array of possible third parties, who may include the client, the customers of the client, and others, such as the owners or managers of a network, or third parties alleging injury as a result of defamation or violation of intellectual property rights. The direct consequences of data loss and security breaches are likely to be very different, depending on who is affected.

Before examining the indirect consequences (i.e., liability to clients or other third parties) that face law firms when their clients' or third parties' data is lost, let us identify the direct consequences of data breaches to law firms themselves independent of liabilities to third parties.

When data is lost by a law firm, whether because its network is successfully hacked, or any device containing data is lost or breached, the implications internal to the firm may include:

- The obligation to report data loss to state regulatory authorities (almost all states now have some requirements). In turn this can have the additional consequence of having to respond to a regulatory investigation, from either of the state data protection regulators and/or the professional disciplinary authorities – or both;

- Disruption to the firm's operations while the cause of the loss is investigated, potentially involving the unavailability of the firm's network for some time. The consequential losses from such disruption in turn include the cost of the investigation and network restoration, as well as potentially significant business interruption;

- Responding to an extortion demand in connection with threats to the firm's website, network or confidential information; and

- Reputational injury resulting from the publication of the fact – and consequences – of data breaches and losses of the firm's and its clients' data.

When client or third parties' confidential information held by a law firm is lost as a result of any kind of breach or failure adequately to protect the data, the consequences for the firm may include:

- The obligation to notify clients and, potentially multiple individual third parties. And in order to meet those obligations, the firm is likely to incur significant costs in terms of computer forensic investigations in addition to the actual notification costs. Although law firms may not have the volume of third party information that clients have about their customers, it is worth noting that the notification to its customers of the loss of credit card information related to Playstation data reputedly cost Sony $170 million. But firms that handle HIPPA data of their medical industry clients, or customer information relating to regulated institutions in the banking and finance industries, may have significant exposure of this kind;

- Liability to the client where confidential or private information is disclosed and thereafter used to the client's disadvantage, privacy liability arising from a breach of personally identifiable or corporate confidential information, defense costs, fines and, potentially, indemnity liability in connection with proceedings brought by state regulators for violation of their privacy breach regulations; and

- Liability for defamation and copyright infringement arising from the dissemination of content (e.g. information on social media or the firm's website) as a result of breaches or other data protection failures.

The Insurance Implications

These consequences of data breaches and losses (which are not inclusive), in turn confronts law firms with two critical issues. First, law firms need to make realistic assessments of the risks in the context of their particular client base, practice areas and (because regulations differ among the states), their geographic footprint, based on the technology architecture they have in place. Second, firms need to assess what existing insurance coverage they have that would (or would not) respond to assist them if (or, more likely, when) they are confronted by a data breach or loss – and what additional coverage they should consider obtaining.

Risk Assessments: Very few firms have the internal resources to make such assessments, so that most firms turn to specialist consultants to undertake these evaluations. Conducted properly, these audits address the basics of physical security of firms' premises as well as looking at the firm's technology architecture (including computer hardware and software and digital footprint). By way of example, one law firm recently told the author that the first flaw in their security that their assessment had identified was that a well-dressed individual (an investigator employed by the consultant/auditor) had been able to walk into the firm's offices without being stopped, to find his way to an empty "visiting lawyers'" office, to turn on the computer on the desk, to access the firm's network, and to work undetected for *seven hours* before being discovered. For obvious reasons, therefore, such assessments are an essential part not only of understanding firms' vulnerabilities, but also of determining the options (and costs) in

addressing weaknesses that may be identified. Most firms of any substance are also finding that their larger clients are requiring responses to often lengthy questionnaires regarding the level of the firms' information security protocols. These questionnaires are frequently based on, or bear a striking resemblance to the standards set out in the comprehensive ISO 27001:270005 standards for technology security.[1] Some firms are also reporting actual audits being undertaken by, or at the insistence of clients to determine the actual (as opposed to reported) level of security in place.

Existing Insurance Coverage:

At best, Lawyers Professional Liability ("LPL") coverage provides only partial coverage for the kinds of consequences that flow from breaches of data security or other loss of confidential information described above. The basic limitations of LPL coverage in the context of these kinds of losses are that:

- LPL is negligence based. This is significant for two reasons. First, many of the acts giving rise to claims for data breaches and loss result from intentional acts of wrongdoing that are expressly excluded from LPL coverage. For instance, some of the causes of these losses are:

  Theft of data, e.g., by hacking or loss/theft of a laptop or PDA;

  Malicious, willful or intentional misuse of a computer system by third parties resulting in damage to or loss of data;

  Intentional employee acts (whether leaking confidential data, or issuing an extortion demand to do so).

Second, LPL Policies require a third party claimant, whereas, as described above, many of the potential consequences of data breach or loss arise where no liability to third party is involved. These include:

  System breach, including forensic expenses and digital asset restoration costs;

  Privacy breach notification costs;

  Data loss and business interruption losses;

  Reputation and crisis management costs.

[1] A description of these standards, as well as the standards themselves and other helpful reference material can be found at: http://www.27001.com/27001.aspx

Additional Coverage Afforded by "Cyber" Insurance:

First, appropriately worded "cyber" insurance should cover the kinds of losses described above, regardless of whether the injury resulted from negligence or intentional wrongdoing, and whether there is a third party claimant, or the injury is the result of a "first party" loss.

Second, cyber insurance enhances the scope of LPL coverage, even in instances where there is a third party claimant and the loss, as to that claimant arguably results from negligence. For instance, the cost of third party notification, which an LPL insurer might argue falls outside LPL coverage, can be provided as part of "cyber" insurance in the event an insured law firm's client has a regulatory requirement to notify individuals due to a breach of the law firm's network.

Third, "cyber" policies can sit both primary and in excess of other insurance. For example, coverage for losses arising from privacy liability, or for notification costs of response to regulatory requirements typically have a much smaller deductible, or self insured retention than an LPL policy. Similarly, the coverage for the failure to prevent unauthorized access or loss of confidential client data, including notification of client's customers, can be obtained with significantly higher excess coverage limits than many LPL policies.

Finally, these policies can provide coverage, often identified as "security liability" coverage, for losses that result when the law firm's network is instrumental in transmitting a virus or perpetrating a denial of service attack (when hackers organize a sustained massive and continuing barrage of attempted connections to a website, rendering it inoperable) on third parties, whether clients or others.

How Well Is Your Firm Covered?

Lawyers operate in an environment where technology can be used to inflict enormous economic damage on third parties, whether clients or not. In this environment, lawyers still owe clients ethical, fiduciary and tort standard of care obligations to preserve their confidences. Thus, in the digital universe in which lawyers and their clients function, however hard lawyers try, they can never offer their clients absolute certainty of protection of their confidences, or from other injuries of the kinds described above. Given these irreconcilable certainties, even after taking every care reasonable in the context of a law firm's clients and their needs, at least giving consideration to acquiring cyber insurance is a critical part of appropriate risk management in the modern world. Thus, an additional – and arguably essential – component of any technology centered risk assessment discussed above is determining what coverage the law firm already has, and what additional coverage is appropriate to protect the firm and its clients from the uncertainties and risks that pervade the digital universe in which we all operate.