Data Security and the Legal Profession: Risks, Unique Challenges and Practical Considerations

Anurag Bana and David Hertzberg*

Introduction

Data security is the area of information security that deals with the protection of digital assets.[1] It is an increasingly prominent and important area of risk for the global legal profession. This is due to the speed with which technology has developed, and is continuing to develop. The explosion of electronic communications and electronic storage and indexing of information, and new and easier ways to access that information, has ushered in a new suite of data security issues. Compared to other businesses, law firms are perceived to have particular data security vulnerabilities. In-house counsel are also considered to be critically lacking in data security expertise. Lawyers in all jurisdictions and practice settings need greater engagement with the issue of data security to protect the interests of their clients, their firm and the general public, and to discharge their professional ethical obligations.

There is evidence that the scale of the data security challenge is being recognised in the legal profession. In one survey of top UK law firms, the percentage of respondent law firms citing information security as their top concern doubled from 23 per cent in 2012 to 46 per cent in 2014.[2] For management in the surveyed law firms, information security was the most frequently mentioned risk management priority.

---

* Anurag Bana is a Senior Legal Adviser and David Hertzberg is an Intern at the International Bar Association

1 Jill D Rhodes and Vincent I Polley (eds), *The ABA Cybersecurity Handbook: A Resource for Attorneys, Law Firms, and Business Professionals* (ABA Publishing 2013), 27.

2 Law Firm Risk Roundtable, *2014 Law Firm Risk Survey: UK Edition.*

There is also evidence that the wider legal profession has less awareness of the data security issue. Respondents to a recent online Bloomberg BNA poll ranked 'hackers and data breaches' fourth out of five enumerated threats to law firms, with only 11 per cent of the vote.[3]

It is crucial that the legal profession understands and addresses data security risk. This means that data security cannot be written off as an IT issue.[4] Rather, it is a risk that requires attention and engagement at every level of a law firm's business. It should be seen as a senior management responsibility: data security is an area where firms need to be proactive, and that requires leadership from management. A proactive approach is equally important for in-house counsel and lawyers in small firms.

The second part of this article gives an overview of the data security risk for law firms and in-house counsel. The nature and scale of the data security risk mean that it must be a top priority for the legal profession. The next section examines the unique considerations and challenges that apply to lawyers as professionals. The intersection between data security and legal professional ethics necessitates a sector-orientated approach to data security risk. The fourth section elaborates on the practical considerations associated with particular technologies and initial steps to address the data security issue. It concludes that the global legal profession needs to act collectively to raise awareness and provide education, training and other resources to address data security risk.

Data security: a key area of risk for all members of the global legal profession

The nature of the risk

Assessing the scope of the data security challenge is inherently difficult. It is unclear how many data security breaches have occurred, who has orchestrated or benefited from these breaches, what information was stolen, how valuable that information was, how to quantify reputational damage and operational disruption, and so on.[5] The estimates of data security consultants and other stakeholders may need to be taken with a pinch of salt.[6]

However, there can be no doubt that data security is a pressing issue that will increasingly be a priority for law firms and businesses generally. A report

---

3 Ryan Schlunz, 'It's Time to Get Serious About Law Firm Cybersecurity' *Bloomberg BNA* (7 April 2015) https://bol.bna.com/its-time-to-get-serious-about-law-firm-cybersecurity/.

4 Solicitors Regulation Authority, *Spiders in the web: The risks of online crime to legal business* (March 2014), 3.

5 Michael McNerney and Emilian Papadopoulos, 'Hacker's Delight: Law Firm Risk and Liability in the Cyber Age' (2012) 62 American University Law Review 1243, 1248, 1260.

6 Peter Maass and Megha Rajagopalan, 'Does Cybercrime Really Cost $1 Trillion?' *ProPublica* (1 August 2012) www.propublica.org/article/does-cybercrime-really-cost-1-trillion.

released in May 2015 by market analyst firm Juniper Research predicts that the global cost of data breaches will reach $2.1tn in 2019.[7] By way of comparison, that is roughly the 2015 GDP of India. The same report predicts that the average cost of a single data breach will exceed US$150m by 2020, as businesses increase their connectivity.[8]

The consequences of a law firm data security breach may be severe. Risks include:

- financial loss to the firm's clients, third parties and the firm;
- reputational damage to the firm's clients, third parties and the firm;
- damage to the reputation and standing of the legal profession;
- in some cases, damage to economic infrastructure or threats to national security;
- possible questions of professional misconduct or failure to meet the minimum statutory standards for data protection.

The law firm risk profile

Law firms are perceived to be particularly vulnerable. In March 2015, a leaked memo from Citigroup's cyberintelligence centre warned that law firms are at 'high risk for cyberintrusions' and that bank employees should be aware that digital security at law firms generally remains below the standards for other industries.[9] A 2013 survey found that 80 per cent of partners and IT directors in surveyed law firms believed they were likely to be the subject of a cyberattack, while only 36 per cent believed that their systems could withstand an attack.[10] The survey also found that only 31 per cent of people working in law firms believe that management fully understands the issues around cybersecurity.[11] In the 2015 Cisco Annual Security Report, Cisco ranked law firms as the seventh most vulnerable industry to 'malware encounters'. This is the first time the legal sector has appeared in the top ten.

7 Juniper Research, *The Future of Cybercrime & Security: Financial and Corporate Threats & Mitigation*, cited at 'Cybercrime Will Cost Businesses Over $2 Trillion by 2019' (Juniper Research, 12 May 2015) www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion?utm_source=gorkanapr&utm_medium=email&utm_campaign=cybercrime15pr1.

8 Samantha Woodhill, 'GCs struggling to mitigate cyber risks' *Australasian Lawyer* (20 May 2015) www.australasianlawyer.com.au/news/gcs-struggling-to-mitigate-cyber-risks-200525.aspx.

9 Matthew Goldstein, 'Citigroup Report Chides Law Firms for Silence on Hackings' *The New York Times* (26 March 2015) www.nytimes.com/2015/03/27/business/dealbook/citigroup-report-chides-law-firms-for-silence-on-hackings.html?_r=0.

10 Anna Reynolds, 'Fears of Cyber Crime Rise As Nearly 80% Believe Their Firm Could Be Hit By Web Hack' *Legal Week* (3 May 2013) www.legalweek.com/legal-week/news/2265292/fear-of-cyber-crime-on-the-rise-as-nearly-80-believe-their-firm-is-likely-to-be-hit-by-web-hackers#.

11 *Ibid.*

Law firms are attractive targets for those who would steal digital assets for two main reasons. First, they hold a high concentration of sensitive and valuable information.[12] Law firms tend to store the most important and valuable client files. It is faster to find these files in a law firm than by searching through all of the information on the client's server.[13] Law firms also offer the potential to access the valuable information of numerous clients at once. Law firms electronically store:

- intellectual property, such as trade secrets or draft patent applications;
- business strategies;
- financial account details;
- inventories of assets;
- litigation strategies;
- IPO or M&A details;
- a wide variety of personally identifiable information and protected health information relating to employees of the law firm, clients, employees of clients or third parties.

In addition, law firms often hold large sums of money in their trust accounts.[14]

The second reason that law firms are attractive targets is that they are considered easier targets. Law firms often have weaker data security than their clients or third parties such as banks. Clients tend to be larger companies with more resources to devote to information security.[15] Economies of scale can assist larger businesses to implement data security measures. Smaller businesses are often more vulnerable. The client might store data on a private cloud, have a larger and better-resourced IT department and hire expensive external data security consultants. For example, in the US the perception is that compared to the Patent and Trademark Office and the businesses that own the intellectual property, the law firms that work with businesses to draft patent applications are an easy target for those who would seek to steal valuable IP.[16] Indeed, law firms have variously been described as the 'low hanging fruit', the 'soft underbelly', the 'Achilles heel' or the 'weakest

12 Rhodes and Polley (eds), see n 1 above, 127.

13 Ed Finkel, 'Cyberspace Under Siege' *ABA Journal* (1 November 2010) www.abajournal.com/magazine/article/cyberspace_under_siege.

14 Dan Pinnington, 'Cybercrime and law firms: The risks and dangers are real' (2013) 12(4) *LawPRO Magazine* http://practicepro.ca/LawPROmag/Cybercrime_and_Law_Firms_Risk_Real.pdf.

15 McNerney and Papadopoulos, see n 5 above, 1250.

16 Ellen Blanchard and Rodney Blake, 'Black Hats Look for Low Hanging Fruit: Law firms are the new target for IP theft' *IPWatchdog* (3 May 2015) www.ipwatchdog.com/2015/05/03/black-hats-look-for-low-hanging-fruit-law-firms-are-the-new-target-for-ip-theft/id=57329.

link' for hackers.[17] Whatever the metaphor, the message is clear: law firms are prime targets, and their information security is generally weaker than that of their clients or other stakeholders.

The relevance of data security in different practice settings

In some ways, the data security issue is particularly pressing for large firms, which hold the most valuable information pertaining to the largest clients, and which have large, dispersed networks (often across multiple jurisdictions) with multiple potential weak spots. On the other hand, the issue is a big challenge for small or medium-sized firms, or specialist firms servicing top-tier clients. These firms deal with sensitive and valuable information and property, but because of the economies of scale of implementing a thorough data security framework, they might be particularly stretched in terms of resources.[18]

Lawyers working in small firms may be particularly under-resourced and may never have received any training on data security risk. These lawyers are highly vulnerable. For example, a recent conveyance of a London apartment for £340,000 was the object of a targeted operation.[19] The vendor's email account was hacked, and a new set of bank account details were sent to the law firm. The lawyers did not suspect that the email was a fake, and transferred the £340,000 into the other bank account. The implications, even for small firms, can be very serious.

In-house lawyers also need to be aware of data security issues affecting their legal team and their employer's business. A survey of CEOs, board chairs and directors of publicly traded companies in the New York Stock Exchange Governance Services database, released in May 2015, showed the importance of cybersecurity to in-house counsel. In response to the question: 'For which

17 *Ibid*; J Ames, 'Cyber security: Lawyers are the weakest link' *The Lawyer* (28 October 2013) www.thelawyer.com/analysis/cyber-security-lawyers-are-the-weakest-link/3011315.article; Anupreet Singh Amole and Jane Jenkins, Freshfields Bruckhaus Deringer, 'Cyber-Security: The Risks and Opportunities' *Private Equity News* (30 March 2015); David Ruiz, 'Data Security's Achilles Heel: Some experts are saying it's not hacker or insiders, it's law firms' (2015) 22(4) Corporate Counsel; Jessica Silver-Greenberg and Matthew Goldstein, 'After JPMorgan Chase Breach, Push to Close Wall St. Security Gaps' *The New York Times* (21 October 2014) http://dealbook.nytimes.com/2014/10/21/after-jpmorgan-cyberattack-a-push-to-fortify-wall-street-banks/.

18 Nell Gluckman, 'To Satisfy Clients, Law Firms Submit to Cybersecurity Scrutiny' *The American Lawyer* (12 March 2015).

19 Nicole Blackmore, 'Fraudsters hacked emails to my solicitor and stole £340,000 from my property sale' *The Telegraph* (16 May 2015) www.telegraph.co.uk/finance/personalfinance/borrowing/mortgages/11605010/Fraudsters-hacked-emails-to-my-solicitor-and-stole-340000-from-my-property-sale.html.

of the following do you believe your general counsel/legal department would most benefit from additional expertise to add more value to your company and board in 2015?', 67 per cent of respondents named 'cybersecurity risk' as one of their choices.[20] This was the most commonly chosen risk area. The second most commonly chosen risk area, at 39 per cent, was another new frontier of risk for the legal profession: social media risk.[21]

In response to the question: 'How would you rate your general counsel with regard to his/her working knowledge of the following corporate issues/areas?', cybersecurity risk was the only area where less than half of respondents gave their general counsel a rating better than 'fair', with only five per cent giving a rating of 'excellent'. It is not only lawyers in firms that need to improve their data security competence.

The unique data security challenges facing the legal profession

The legal profession needs a sector-orientated approach to understanding and addressing data security risk. The professional ethical obligations for lawyers to maintain client confidentiality, carry out their work competently and protect property that comes into their trust set minimum data security standards for the legal profession. These obligations apply, in various forms, to lawyers in all jurisdictions. Further, professional ethics may have a bearing on how the legal profession approaches collaboration and information sharing, and create conflicts with breach notification requirements.

Confidentiality

Lawyers have a professional obligation to maintain confidentiality regarding the affairs of present or former clients, unless otherwise allowed or required by law or applicable rules of professional conduct.[22] The loss or theft of digitally stored information is a threat to confidentiality. To discharge the ethical obligation of confidentiality, lawyers must implement adequate administrative, technical and physical safeguards to protect client information.[23] They are also expected to have a reasonable awareness and

---

20 BarkerGilmore, *GCs: Adding Value to the C-Suite* (2015) www.barkergilmore.com/gcs-adding-value-in-c-suite.

21 See International Bar Association, *IBA International Principles on Social Media Conduct for the Legal Profession* (2014) www.ibanet.org/committees/divisions/legal_practice/impact_of_osn_on_legalpractice/Impact_of_osn_home.aspx.

22 See, for example, International Bar Association, *IBA International Principles on Conduct for the Legal Profession* (2011) www.ibanet.org/barassociations/BIC_resources.aspx, Principle 4.

23 Rhodes and Polley (eds), see n 1 above, 64.

engagement with technology.[24] What is reasonable will vary over time and across practice settings and jurisdictions, but clearly this requires more than passive reliance on the technology that lawyers use in their everyday practice. The professional obligation of confidentiality requires lawyers to be active in promoting and protecting data security.

Competence

The duty of competence is also relevant to the adequate protection of a client's electronically stored information.[25] The ABA has stated that the duty of competence includes keeping abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology.[26] In a modern practice, carrying out work in a 'competent and timely manner'[27] usually involves the use of technology (such as email, portable devices and cloud computing) that results in the electronic storage of sensitive information and creates data security risk.[28] Competent lawyers should be able to evaluate this risk and implement appropriate practices and technology to protect those files from loss or destruction, or retain an expert consultant who has the competence to do so.[29]

In some circumstances, the professional obligations of confidentiality and competence may impose a duty on lawyers to initiate a conversation with a

24 The State Bar of California Standing Committee on Professional Responsibility and Conduct, *Formal Opinion No. 2010-179: Confidentiality and Technology* (2010) http://ethics.calbar.ca.gov/LinkClick.aspx?fileticket=wmqECiHp7h4%3d&tabid=836; Canadian Bar Association, 'Guidelines for Practicing Ethically with New Information Technology', a supplement to its *Code of Professional Conduct* (2014) www.cba.org/cba/activities/pdf/guidelines-eng.pdf.

25 See, for example, the State Bar of California, n 24 above; Canadian Bar Association, n 24 above; E-Law Committee of the Law Society of South Africa, *LSSA Guidelines on the Use of Internet-Based Technologies in Legal Practice* (2014) www.lssa.org.za/index.php?q=con,363,LSSA_publishes_guidelines_on_the_use_of_Internetbased_technologies_in_legal_practice.

26 Comment [8] to American Bar Association, *Model Rules of Professional Conduct*, Model Rule 1.1, cited in James Podgers, 'The fundamentals: lawyers struggle to reconcile new technology with traditional ethics rules' (November 2014) *ABA Journal* published online at *LegalTrac* (19 May 2015) http://go.galegroup.com/ps/i.do?id=GALE%7CA389509922&v=2.1&u=usyd&it=r&p=LT&sw=w&asid=50c969003c88ab3889ab55f97eabc90b.

27 International Bar Association, *IBA International Principles on Conduct for the Legal Profession* (2011) www.ibanet.org/barassociations/BIC_resources.aspx, Principle 9.

28 Canadian Bar Association, n 24 above.

29 State Bar of Arizona, *Ethics Opinion No. 05-04* (July 2005) cited in Rhodes and Polley (eds), n 1 above, 65.

client about data security.[30] For example, at the beginning of the lawyer-client relationship, it may be prudent to discuss the data security expectations of both parties and the regulatory obligations for clients and law firms.[31] As with other areas of professional practice, lawyers must have the understanding to have frank and informative discussions with their clients about the client's interests and how their work will be handled.

Protection of client and third party property

Lawyers also have ethical obligations relating to the prudent treatment of trust funds and the preservation of client property that comes into a lawyer's trust.[32] Lawyers must implement appropriate practices and technology to safeguard client and third party property. Law firm trust funds have been the target of cyberattacks in the past, such as the theft of a 'large six-figure' amount from the trust fund of a Toronto law firm. This was a sophisticated attack involving targeted emails to the firm's bookkeeper purporting to be from a large Canadian bank, malware that mimicked the login page of the bank and direct calls to the bookkeeper purporting to be from the bank.[33]

Law firms may receive sensitive information without the informed consent of the owner of the information, or the person to whom it pertains.[34] This might occur through discovery in the course of litigation, or in the firm's capacity as legal counsel during an investigatory process. There are ethical concerns where information that is stored in a highly secure environment is compulsorily transferred, possibly without the knowledge of a third party to which it pertains, to a law firm that may have a lower level of data security.[35]

---

30 Rhodes and Polley (eds), n 1 above, 82. See, for example, Solicitors Regulation Authority, *Code of Conduct* (2011) www.sra.org.uk/solicitors/handbook/code/content.page, Outcome 1.12, which requires clients to be in a position to make informed decisions about the services they need, how their matter will be handled and the options available to them, and Outcome 4.2, which requires the fee earner to disclose to the client all information that is material to the client's retainer of which the fee earner is aware.

31 Rhodes and Polley (eds), n 1 above, 99.

32 International Bar Association, *IBA International Principles on Conduct for the Legal Profession* (2011) www.ibanet.org/barassociations/BIC_resources.aspx, Principle 8; Canadian Bar Association, n 24 above, 7; New Zealand Law Society, *Practice Briefing: Cloud Computing Guidelines for Lawyers* (2014) www.lawsociety.org.nz/epractice-resources/practice-briefings/Cloud-Computing-2014-07-21-v2.pdf.

33 Yamri Taddese, 'Law firm's trust account hacked, "large six figure" taken' *Law Times* (7 January 2013) www.lawtimesnews.com/201301072127/headline-news/law-firms-trust-account-hacked-large-six-figure-taken.

34 Rhodes and Polley (eds), n 1 above, 8.

35 *Ibid*.

Collaboration and information sharing

Legal professional obligations bear on the collective response of the legal sector to the data security threat. Governments and private sector commentators have called for greater collaboration and information sharing among businesses to promote best practices in data security, protect against similar threats and improve the general standard of information protection. Indeed, some law firms are working towards the formation of informal alliances that would allow them to share information about data security threats and vulnerability. In the US, major law firms including Sullivan & Cromwell, Debevoise & Plimpton, Paul Weiss Rifkind Wharton & Garrison, Allen & Overy and Linklaters have moved towards the formation of such an alliance.[36]

Lawyers face inherent difficulties in collaboration and information sharing. Boris Segalis, the US co-chairman of Norton Rose Fulbright's data protection and privacy practice, stated that 'I'm not sure the potential benefit is worth the potential risk to confidentiality and privilege'.[37] In addition to these concerns about confidentiality, law firms may justifiably be reticent to share information that might damage the firm's reputation and jeopardise existing and future client relationships.[38] In some cases, by admitting a breach a law firm may face questions about the adequacy with which it undertook its obligation to make reasonable efforts to prevent unauthorised access to client information.[39] An informed, sector-orientated approach is needed to resolve the tensions between collaborating to provide a collective defence to the growing threat of data security breaches, and concerns about confidentiality, reputation and raising issues of a lawyer's professional competence.

Breach notification

An increasing number of jurisdictions have enacted laws requiring entities that hold personal information to notify enforcement authorities and the persons to whom the information pertains in the event of a data security

36 Gluckman, n 18 above.

37 *Ibid.*

38 Emily Mermell, 'Tension between Client Confidentiality, Public Disclosure Stifling Law Firm Cyber-breach Reporting' *ACEDS* (16 April 2015) www.aceds.org/why-arent-law-firms-disclosing-data-breaches/.

39 *Ibid.*

breach.[40] Law firms often hold personal information pertaining to their clients (such as personal injury claimants) or third parties. In 2014, the UK Information Commissioner's Office (ICO) investigated 173 UK law firms for reported breaches of the Data Protection Act.[41]

Law-makers need to understand the unique position of legal professionals and how breach notification laws will interact with the framework of legal professional ethics. For lawyers, particularly those involved in cross-border work, there may be different and conflicting obligations in different jurisdictions concerning confidentiality and reporting obligations. These concerns must be balanced with the interests of business, government and all of society in reducing cybercrime. A further consideration is the need to protect privacy, particularly where information is being provided to government departments.

As with collaboration and information sharing, breach notification raises concerns about confidentiality and reputational damage. The New York City Bar has issued an ethics opinion that individuals attempting to conduct a trust fund scam are not prospective or actual clients and so lawyers do not violate their ethical obligations by reporting the scam to enforcement authorities.[42] The situation will be more complex where a duty of confidentiality does exist. For example, if a law firm holds client files that contain the personal information of the client's customers, notifying those customers of a breach that affects their personal information, and thereby disclosing that the firm was in possession of those files, would have implications for client

40 For example, EU Data Protection Directive 95/46/EC as implemented in Member States; Data Protection Act 1998 (UK); Personal Information Protection and Electronic Documents Act ('PIPEDA') (Canada); Privacy Act (New Zealand). See further DLA Piper, *Data Protection Laws of the World* http://dlapiperdataprotection.com/#handbook/world-map-section.

41 John Leyden, 'Miscreants rummage in lawyer's silky drawers at will, despite warnings' *The Register* (16 April 2015) www.theregister.co.uk/2015/04/16/law_office_breaches_rife_foia/.

42 The Association of the Bar of the City of New York Committee on Professional Ethics, 'Formal Opinion 2015-3: Lawyers who fall victim to internet scams' (April 2015) www.nycbar.org/ethics/ethics-opinions-local/2015opinions/2161-formal-opinion-2015-3-lawyers-who-fall-victim-to-internet-scams; Ellen Rosen, 'Cybercrime at Firms Triggers Ethical Duties: Business of Law' *Bloomberg BNA* (1 May 2015) www.bloomberg.com/cybercrime-at-firms-triggers-ethical-duties-business-of-law.

confidentiality.[43] It is important for the law to consider the unique position of lawyers and clearly set out what a lawyer's obligations are.

Data security: practical considerations

Data security needs to be addressed in law firms of all sizes, through in-house counsel of small and mid-sized companies, and across all jurisdictions. The areas of risk discussed in this section exist in all practice settings, and the suggestions for addressing the data security issue are relevant for all members of the global legal profession.

Cloud computing

Cloud computing involves storing data and software on a remote server. Users can then access programs and data remotely. Typically, the remote server is operated by a third-party service provider. Cloud computing has been widely adopted because it is more flexible, cheaper and easier to maintain than traditional systems, and information is often more effectively backed up. It does, however, create vulnerabilities for information security, which lawyers need to understand. Cloud computing typically involves shifting control of data to a third party. The law firm necessarily remains responsible for protecting the security of that information.[44] The professional obligations of confidentiality and competence, discussed above, require lawyers to take reasonable care to minimise any risks to confidentiality and security of client information stored in the cloud.[45] Therefore, at a minimum it is important that law firms conduct adequate due diligence on potential third-party service providers, and include contractual terms requiring the service provider to establish and maintain adequate security measures. Lawyers also need to be aware of which jurisdiction the remote server is located in, and thus what laws and regulations need to be considered in managing data security risk.[46]

---

43 Koblentz, n 38 above; E-Law Committee of the Law Society of South Africa, n 25 above; New Hampshire Bar Association, *Ethics Committee Advisory Opinion #2012-13/4 'The Use of Cloud Computing in the Practice of Law'* (2012) www.nhbar.org/legal-links/Ethics-Opinion-2012-13_04.asp; New Zealand Law Society, n 32 above; Law Society of British Columbia, *Report of the Cloud Computing Working Group* (2012) www.lawsociety.bc.ca/docs/publications/reports/CloudComputing_2012.pdf.

44 Solicitors Regulation Authority, *Silver Linings: Cloud computing, law firms and risk* (November 2013), 10.

45 E-Law Committee of the Law Society of South Africa, n 25 above; New Hampshire Bar Association, n 43 above.

46 E-Law Committee of the Law Society of South Africa, n 25 above; Law Society of British Columbia, n 43 above; New Zealand Law Society, n 32 above, 9.

Portable devices

Portable devices such as smartphones, blackberries, tablets and laptops are increasingly used by lawyers for work. Indeed, cloud computing has contributed to the use of portable devices.[47] Remote access facilitates flexible working and can improve client service. However, portable devices and their use on wireless connections often represent weak points for information security.[48] For example, using portable devices on unsecured Wi-Fi represents a clear risk for 'electronic eavesdropping'.[49] All work-related communications need to be made through a secured channel.[50] The risk of portable devices being lost or stolen necessitates encryption of the data on those devices and other security precautions, such as adequate password protection, the ability to wipe a device remotely and the immediate reporting of theft or loss of the device.[51] Confidential information needs to be irreversibly wiped from portable devices before they are disposed of (this extends even to copiers and printers, which may retain images of documents on their hard drives).[52]

Hacking

The range of sensitive information held by law firms and the diversity of potential data security threats create risks for all lawyers. Hackers range from 'script kiddies' (computer whizzes who conduct a cyberattack simply because they can) to sophisticated state actors (as was allegedly the case in the North Korean state attack on Sony). Some hackers are politically motivated, such as terrorist groups or 'hacktivists'. Others are motivated by economic gain, including organised crime groups, competitor businesses and current or former employees.

The diversity of actors and motives means that firms of all sizes can be targeted. For example, a small UK law firm, ACS:Law, had its security breached in 2010 by prominent hacktivist group Anonymous. The hackers were concerned by the firm's 'speculative invoicing' tactics of targeting

47 Solicitors Regulation Authority, *Silver Linings: Cloud computing, law firms and risk* (November 2013), 11.

48 Rhodes and Polley (eds), n 1 above, 9.

49 Solicitors Regulation Authority, *Silver Linings: Cloud computing, law firms and risk* (November 2013), 11.

50 *Ibid.*

51 Martin Prinsloo, 'Keeping Your Law Firm Safe from Cyber Threats' *Broward Daily Business Review* (25 March 2015).

52 Rhodes and Polley (eds), n 1 above, 72.

individuals the firm claimed were engaged in illegal file sharing.[53] The attack resulted in the crash of the firm's website. During attempts to get the website running again, the unencrypted emails sent to those accused of illegally sharing pornography were made publicly visible. Privacy International sued the firm on behalf of the individuals whose information was breached; the lawyer who owned the firm was fined £1,000 by the UK Information Commissioner's Office. The fine would have been £200,000 if the firm had not gone out of business.

In 2012, Anti-Sec, an offshoot of Anonymous, hacked into the servers of the small US law firm Puckett & Faraj and obtained nearly 3GB of emails, numbering tens of thousands of messages and dating back two years.[54] This was in response to the firm's defence of staff sergeant Frank Wuterich, who was accused of leading a group of Marines responsible for the deaths of 24 unarmed Iraqi civilians at Haditha.[55]

In a very different scenario, in 2011 several large Canadian law firms were subject to an 'advanced persistent threat' (APT), which is thought to have originated from a state actor.[56] BHP Billiton made a $38bn bid to take over Canadian-based Potash Corporation. Canadian law firms representing the parties to the transactions, as well as other stakeholders such as the Canadian government and clients of the law firms, were the target of a coordinated attack originating from China. Some experts speculate that the attacks were related to efforts by China's state-owned chemical company, Sinochem Group, to disrupt the BHP takeover bid.[57]

Hackers often rely on malware (malicious software). One type of malware that has gained notoriety is 'ransomware', which holds a target's information and demands money for its return; sometimes, the money is paid and the data deleted anyway.[58] Other malware, called 'botnets', combine part of

---

53 'ACS:Law fined over data breach' *BBC News* (11 May 2011) www.bbc.co.uk/news/technology-13358896; 'ACS:Law solicitor Andrew Crossley suspended by SRA' *BBC News* (8 March 2012) www.bbc.co.uk/news/technology-16616803.

54 R Gallagher, 'Anonymous Splinter Group Anti-Sec Wages War on "Profiteering Gluttons"' *The Guardian* (27 February 2012) www.theguardian.com/technology/2012/feb/27/anonymous-splinter-group-antisec-waging-war.

55 Dominic Rushe, 'Anonymous publishes trove of emails from Haditha marine law firm' *The Guardian* (6 February 2012) www.theguardian.com/technology/2012/feb/06/anonymous-haditha-killings.

56 Rhodes and Polley (eds), n 1 above, 126; Greg Weston, 'Foreign Hackers Target Canadian Firms' *CBC News* (29 November 2011) www.cbc.ca/news/politics/foreign-hackers-targeted-canadian-firms-1.1026810.

57 Rhodes and Polley (eds), n 1 above, 126; Weston, n 56 above. The bid was ultimately blocked by the Canadian government.

58 Solicitors Regulation Authority, *Spiders in the web: The risks of online crime to legal business* (March 2014), 8.

each infected computer's processing power to conduct targeted attacks. An example of using 'spear phishing' emails to install malware on a target system is to email a law firm purporting to be a job applicant, with an attachment that purports to be a CV. The attachment in fact contains a malware program. This should usually be preventable by adequate anti-virus systems, but it has been successful on a number of occasions.[59]

Other risks include 'malicious insiders',[60] allowing lawyers to BYOD (bring your own device), threats based on accidental, inadvertent or natural events and hacking of law firms' business partners.[61] For example, one Washington, DC law firm's external cybersecurity consultant was hacked, exposing the law firm's work for the Chamber of Commerce and resulting in the filing of an ethical complaint against three of the firm's lawyers.[62]

Commercial identity theft

Lawyers should be aware of the risk of commercial identity theft, where clients or members of the public receive emails purporting to be from their firm.[63] This can damage the reputation of the lawyer, the firm and the legal profession, and cause significant loss to clients or members of the public. These scams can be highly sophisticated, drawing on detailed information about the lawyer and law firm. One measure to protect against this risk is to ensure that electronically stored information about a lawyer or law firm is adequately protected or securely destroyed.[64]

Insurance

If a data security breach does occur, insurance is an important way to mitigate the damage. Law firms of all sizes need to examine their insurance policies to ensure that they have adequate coverage for the diverse data

---

59 *Ibid.*

60 The US Department of Justice has brought several cases against Chinese employees who steal intellectual property and trade secrets: Marisa Kendall, 'Feds Charge Chinese Engineers With Stealing Silicon Valley Technology' *The Recorder* (19 May 2015) www.therecorder.com/id=1202726949251/Feds-Charge-Chinese-Engineers-With-Stealing-Silicon-Valley-Technology#ixzz3cfmV6wZl.

61 Rhodes and Polley (eds), n 1 above, 13.

62 *Ibid* 26.

63 'Cybercrime issue is escalating, says SRA' *Solicitors Regulation Authority* (1 June 2015) www.sra.org.uk/sra/news/press/cybercrime-increasing-june-2015.page; Solicitors Regulation Authority, *Spiders in the web: The risks of online crime to legal business* (March 2014), 14.

64 *Ibid.*

security risk environment.[65] The cost of incomplete coverage could be devastating: in 2014, the average cost of a corporate data breach in the United States was $5.9m, a figure that will continue to increase.[66] Lawyers should not assume that any data security breach will be covered by their commercial general liability insurance, professional liability insurance or other policies.[67] If purchasing a specific cyber insurance policy, lawyers should understand that these are relatively new insurance products, with significant variation between policies.[68] Not all policies will fit the unique risk profile of a firm. Data security insurance is an area that warrants a proactive approach, careful attention to detail and, in many cases, consultation with an insurance professional.[69]

What do lawyers need to know?

Lawyers must avoid the trap of assuming that their IT department will protect them from data security risk, or that their firm is too small to be targeted by hackers.[70] As a start, lawyers should know:

- what information their firm stores;
- where it is stored;
- how information is separated out within the firm;
- what technical, physical and administrative protections are in place;
- what is required to maintain the integrity of those protections.

Most security breaches occur as a result of human error of some kind.[71] Lawyers should have a sense of vigilance and an understanding of data security risk. For example, lawyers should understand the risks of opening email attachments and using USB sticks, and ways to spot issues such as unauthorised access or a misbehaving infected computer.[72]

---

65 See Monica Bay, 'Think You Don't Need Cyber Insurance? Think Again!' *Bloomberg BNA* (22 May 2015) https://bol.bna.com/think-you-dont-need-cyber-insurance-think-again/; Michael N DiCanio, 'Preparing for the Inevitable: Insurance for Data Breaches' *New York Law Journal* (19 May 2015).

66 DiCanio, n 65 above.

67 *Ibid.*

68 *Ibid.*

69 Scott J Shackelford, 'Should Your Firm Invest in Cyber Risk Insurance?' (2012) 55(4) Business Horizons 349.

70 Rhodes and Polley (eds), n 1 above, 192.

71 Steve Ragan, 'Law firm says human error to blame for client breaches in 2014' *CSO* (18 May 2015) www.csoonline.com/article/2923023/disaster-recovery/law-firm-says-human-error-to-blame-for-client-breaches-in-2014.html; Blanchard and Blake, n 16 above.

72 Canadian Bar Association, n 24 above.

For lawyers in management positions in medium and large firms, implementing an adequate internal data security framework involves activities such as:[73]

1. Creating an inventory of the digital assets in the firm.
2. Providing training and education to legal and administrative staff.
3. Conducting periodic cybersecurity risk assessments.
4. Developing security strategies and controls. This should include separating out information so that lawyers and staff can only access the information that they need to, thereby reducing the threat of current or former employees intentionally or otherwise breaching the firm's cybersecurity defences. Limiting the access and control granted to partners, who are owners of the firm, will require clear articulation of the risks and how they are best managed.[74]
5. Developing an incident response plan, including understanding any reporting obligations.
6. Examining insurance policies.[75]
7. Implementing oversight of external business and third-party service provider arrangements.
8. Conducting ongoing monitoring and analysis, which is required to maintain the level of security and detect breaches if they occur. It is a scary thought that breaches may continue undetected for months, and indeed breaches may never be detected.[76] The *2013 Trustwave Global Security Report* revealed that in 2012, nearly two-thirds of businesses that became aware that they had been the subject of a cyberattack took over 90 days to discover the breach, with nearly a fifth of firms taking over one year to discover the attack. The value that lawyers intuitively place on confidentiality and privacy will need to make room for monitoring and analysis of computer systems and communications.[77]

The protection principles – prevent, detect, react and deter – are always effective for incident management and timely communication of security events associated with information systems.

---

73 See for example the Rhodes and Polley (eds), n 1 above, 50; Prinsloo, n 51 above.

74 Rhodes and Polley (eds), n 1 above, 109.

75 DiCanio, n 65 above.

76 Solicitors Regulation Authority, *Spiders in the web: The risks of online crime to legal business* (March 2014), 5, citing the *2013 Trustwave Global Security Report.*

77 Rhodes and Polley (eds), n 1 above, 108.

Industry standards and auditing by clients

Law firms are using industry standards as a way to certify their data security protections: the International Organisation of Standardisation (ISO) accreditation 27001 is being taken up by larger law firms, particularly in the US.[78] Indeed, some large clients, such as Goldman Sachs or JP Morgan Chase, require more than an ISO 27001 accreditation, conducting their own audits on firms.[79] A 2014 KPMG survey of FTSE 350 companies found that 33 per cent of respondents audited third parties, such as law firms, on cyber risk.[80]

As clients increasingly scrutinise how their data will be protected, data security is becoming a competitive differentiator. It is large firms that are best positioned to take advantage of this; the cost of acquiring the ISO accreditation, or meeting the exacting requirements of large clients, means that it is often not feasible for small and mid-sized or specialist firms.[81]

Outlook for the global legal profession

Data security has become a risk issue that is truly global in nature. Cyberspace transcends national borders. Threats can originate from anywhere, and all firms are potential targets. Malware is available for purchase online; the commoditisation of cyber tools makes the theft of electronically stored information more widely accessible.[82] However, at present the leaders in law firm data security are top-tier law firms in the US and UK. More needs to be done in less developed legal sectors, where there may be fewer resources and less expertise, but where the risk is no less compelling.

Data security is increasingly resource intensive, requiring technology, expertise, staff training and, for medium to large firms, a well-staffed IT department. One computer security firm quotes the cost for a large law firm to hire them as a cybersecurity consultant (to work with the firm over a period of months to bring its cybersecurity framework up to acceptable

78 Gluckman, n 18 above.

79 *Ibid.*

80 KPMG, *FTSE 350 Cyber Governance Health Check: An insight into the issues of today and tomorrow* (2015), 1.

81 Gluckman, n 18 above.

82 McNerney and Papadopoulos, n 5 above, 1248; Juniper Research, *The Future of Cybercrime & Security: Financial and Corporate Threats & Mitigation*, cited in 'Cybercrime Will Cost Businesses Over $2 Trillion by 2019' (Juniper Research, 12 May 2015) www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion?utm_source=gorkanapr&utm_medium=email&utm_campaign=cybercrime15pr1.

industry standards) at around $130,000.[83] One estimate for the cost of a large firm going through the procedure to obtain a three-year ISO 27001 certification is $30,000.[84]

The global legal profession needs sector-orientated assistance. This is an issue that calls for the legal profession to act collectively to raise awareness and provide education, training and other resources. It is essential for the legal profession to encourage lawyers and law firms to conduct a cyber readiness test and ensure that a specific cyber-incident response plan is in place. There is a role for an international organisation like the International Bar Association (IBA), with its global membership of bar associations, law societies and legal professionals, to assist lawyers to achieve adequate standards of data security and to ensure that the unique position of lawyers is accommodated in legislative responses to data security risk.

Conclusion

Data security should be a risk priority for all members of the global legal profession. There is a pressing need for greater proactivity and engagement by all lawyers. Lawyers cannot rely on their IT department or assume that technology will look after itself. As an initial step, management must take a leadership role in promoting attention and vigilance at every level of a law firm's business. However, addressing the data security issue will be resource intensive, and many lawyers and law firms will benefit from assistance. Moreover, lawyers' professional ethical obligations of confidence, competence and protecting property in their trust requires a risk management approach tailored to the legal profession. It will be important for bar associations and international organisations such as the IBA to raise awareness and provide education, training and other resources to assist lawyers in all jurisdictions and practice settings to protect their valuable digital assets.

83 Gluckman, n 18 above.

84 *Ibid.*