ATTORNEYS PRACTICE AND INTERNET RELATED RISKS

1. INTRODUCTION

The management of risk is a considered business decision and a competitive weapon. Law firms are, thanks to their nature, exquisitely fragile and unstable businesses. They can be stabilized, however, stability is a process, a consistent pattern of action over an extended period of time.

Attorneys permanently face the spectre of complaints and law suits. Their conduct often leads to claims against the Attorneys Fidelity Fund and Attorneys Insurance Indemnity Fund. They must do all they can to protect their firms, their clients and the Funds from practice management risks.

The best way a law firm can avoid complaints and possible claims is by analysing its policies, processes, and procedures for weaknesses and devising appropriate ones to minimise risks.

Information technology has brought immense benefits and advantages to law practices. The opposite is also true in that information technology has brought about risks to both the law firm and its clients. These risks have the potential to cripple a law firm by *inter alia* violating the rules of confidentiality or leading to loss of information – both of which can lead to claims. This note briefly discusses internet-related risks and how to deal with them.

2. INTERNET RELATED RISKS

2.1 Social Networking

Social networking does not introduce something fundamentally different into the profession. It is just a new mode of communication; its use in the profession is both inevitable and appropriate. The potential problems created by, or feared in, social networking really fall into five categories:

- the breach of client confidentiality through online exchanges of information that characterise social networking sites,

- the creation of online contacts via the network that are ethically improper,

- the creation of unintended attorney-client relationships via the network,

- the violation of rules regarding advertising and solicitation, and

- the use of such sites to improperly gather information.

Blogs appear on the internet as personal journals with various contributors and a variety of topics. A blog is an easy way to get information out very quickly. For lawyers blogs are a way to inform current clients, attract potential clients and market legal services. A blog has been described as being able to establish an attorney as the "go to" person in a specific area of law, if that attorney puts up content that is current, informative, and insightful.

The experts view blogs in two types, namely informational blogs and advisory blogs. The latter offers legal advice and therefore increases the risk of a professional indemnity claim. An advisory blog can also inadvertently create an attorney-client relationship.

Informal blogs present information or offer discussion forums. It is advisable that the information be presented in a general, non-biased manner. A blog allows you a presence on the internet. It is absolutely **not** a place to dispense legal advice.

An attorney should take extra care not to establish an attorney-client relationship in this way. A blog is seen as no different from engaging in a conversation at a cocktail party.

A blog is borderless as it can be viewed anywhere. Does this mean other provinces' ethics rules apply? Firms that actively market to potential clients in provinces in which they are not registered will need to consider whether they are required to comply with the rules of those provinces.

E-mail is the most basic form of internet-based communication, useful for communicating with clients and transmitting documents. Similar to a blog, with e-mail, an attorney can create alert systems to keep clients apprised of recent statutory or case developments.

Internet may be used to:

- Create online chat or negotiation rooms with clients and other parties,

- Create controlled-access, allowing entry only to those with permission to view some or all of a client's legal file online. EXTRANETS permit clients and lawyers to share, in real time, document databases, legal research and memorandums and other relevant case materials,

- Create online libraries customised to particular clients or subject matter.

The internet and its related tools can assist law firms in providing legal services to clients,

but these same tools can also be sources of risk that must be monitored closely:

- The greatest risk to law firms with an internet presence is that they may not always know who their clients are. Many websites provide prospective clients with forms enabling them to engage attorneys. Other sites allow prospective clients to contact attorneys through e-mail, and some attorneys spend time in chat rooms discussing legal issues. These activities create risks in that attorney-client relationships may be created before any evaluation for appropriateness has been performed.

- The ability to communicate electronically has increased the risk of inadvertent disclosure of confidential information. E-mails and other electronic communications can easily be directed to an unintended recipient by mistake. This creates the possibility of professional indemnity exposure.

- Law firms request and create a great deal of data, which must be kept under lock and key. Attorneys collect significant amounts of personal information about their clients. The information is placed into databases within the firms' records. It is observed that databases in the legal industry are hazardous because too often minimal requirements or none, are placed on legal firms to install adequate IT security systems.

Sensitive electronic data can be exceptionally damaging if they fall into the hands of motivated cyber criminals. The uncontrolled leak of client's data could damage integrity of relationships.

Attorney-client privilege is the most important concept in the legal field because it protects communications between attorneys and their clients. The legal industry may have made some strides in data protection by using basic virus and spyware programmes, but it has yet to address issues of outbound e-mail protection. Given the vulnerability of e-mail systems to the threat of hackers, it is difficult for the e-mail user to remain confident in the security of electronic communications. This debate is particularly germane to attorneys acting within the ambit of the attorney-client privilege. Attorneys who wish to use e-mail to communicate with clients should consider the degree of security it offers and its implications for the attorney-client privilege. E-mail communications become computerised records when saved and are subject to discovery requests during litigation.

Hackers are not the only threat to the security of e-mail communications.

Other dangers include:

- **the lack of guaranteed security for transmissions between different e-mail systems.** Mis-transmissions can occur because different e-mail systems use different addressing schemes. For a message to be sent properly between systems, its address must match the addressing scheme of the recipients system. If the format does not match, the message will not be delivered or could be delivered to an unintended recipient. Imperfectly addressed messages could be sent to unintended recipients,

- the accessibility of e-mail messages by e-mail providers,

- **the informal use of e-mail** which may result in legal problems. Users may tend to view e-mail as more temporary and approach it more spontaneously than paper messages. Consequently offensive messages might be sent through e-mail that would not otherwise be sent in a formal letter. Thus, this informal use of e-mail makes it a potentially large source of damaging information.

- **the disorganisation of computerised information in general**. This is a practical concern about e-mail maintenance. Information stored in a computer system is often disorganised with files frequently not organised into subdirectories. If potentially privileged information is not segregated from non-privileged information, litigation can necessitate the time-consuming task of sorting files.

- **the difficulty of destroying computerised information**. Unlike paper documents, information stored in a computer is difficult to destroy. Deletion does not remove a document from a system. A user with an over-the-counter utility programme can retrieve the remnants of the deleted document. Even documents that have been overwritten can be deciphered. Without application of retention and destruction policies to computer records, a problem is created.

Without a clear and appropriate records-management policy, early destruction of electronic documents could lead to violations of an attorney's ethical and legal obligations. The risks posed by improper destruction of electronic documents are especially clear in the context of discovery. If an attorney permits or aids destruction of documents that should have been retained, the attorney may be subject to sanctions. In an American case, *Coleman (Parent) Holding Inc. v. Morgan Stanley and Company Inc.* 2005 WL 679071 (Florida Circuit Court, 1 March 2005 and 2005 WL 674885 (Fla.Cir.Ct.) Morgan Stanley stated that it may sue its former counsel for the $1.5 billion verdict it suffered because the court

determined that its law firm did not respond appropriately to discovery requests for electronically-stored documents.

3. **MANAGING INTERNET RISKS**:

3.1 SCREENING TECHNIQUES - It is important for law firms to use appropriate screening techniques to avoid unintended attorney-client relationships.

A conspicuous **disclaimer** should be placed on the firm's website clearly stating that no attorney-client relationship exists unless and until expressly agreed to by all parties, preferably in a written **engagement letter** specifying the identity of the client, the scope of services to be provided, and the fee payable (at a minimum).

Another suggestion is to switch off the comment feature in your blog to avoid spam comments or other inappropriate replies being posted.

A disclaimer should be used to clearly point out that the blog, or the firm's website does not give legal advice. Generally posting content on a website for all to read is not considered to be the provision of legal services, however in some scenarios, blog entries could constitute legal advice. Once an attorney refers a client to information posted on his blog, the referral could be construed as providing advice using the blog.

When blogging, an attorney should review the regulatory rules on advertising.

In Beazley Brief, issue 20, February 2010, an American lawyer and risk management practitioner, David Jargiello, offers some common-sense advice that you should ensure that you know where you are and who you are talking to. He observes that when discussing the propriety of lawyers' social networking, there is a tendency to treat the practice as monolithic when in fact it is not. Jargiello stresses that the websites which are for communication among lawyers skirt the edges of an attorney-client relationship (e.g. Free Advice.com). It is therefore imperative to know your audience.

Respect client confidentiality even online. An attorney has no right to post confidential clients' information, for example on his Facebook.

Social networking sites are inappropriate for attorney-client communications and should not be used as a vehicle to provide legal advice. **Do not practice law on Facebook!**

3.2. SECURING CONFIDENTIAL COMMUNICATION IN THE INTERNET

If law firms do not take reasonable measures to ensure that their electronic communications are private and secure, there is a risk that privileged information will be compromised.

Law firms should use restricted means of communication, such as encryption. **Encryption** is one form of protection that should be used for all confidential information that is transmitted over the Internet. Users without the proper key, that is, unauthorised recipients or browsers, cannot read encrypted messages. However it is unlikely that all of the firm's clients will have encryption hardware and software. Everything being equal, encryption is better than, and preferable to, using a disclaimer to an e-mail. Disclaimers are easily ignored. Law firms need to know what is going on in the technology realm and update their security practices to protect their clients' data.

Information must still be protected even whilst it is stored in the computer. **Authentication** is one measure that may be employed to identify anyone seeking access. A **password** is the most common authentication device used to prevent user impersonation. It must be well chosen and changed frequently. Using a password only once, enhances authentication. **Digital signature** is another authentication tool that confirms to a recipient with certainty, who signed the document and that nothing contained therein has been altered.

A **firewall** can be used in a network that is connected to the internet. It is explained as policing traffic to internal systems. A firewall can log and examine all network connections, filter incoming communications, require authentication, restrict access to selected systems, and block certain services.

Partitioning is another tool that can be used to safeguard confidential information. It is applied so that internal computer resources are inaccessible. Confidential documents should not be stored on a system accessible to the public. Likewise a publicly accessible system should not be run on a firm's internal network.

The use of a **direct modem link** ensures that messages are transmitted directly between modems over telephone lines. Because these messages do not have to pass through a third-party computer, security risks are minimised.

Consider implementing a **service access policy** to assess what types of connectivity with other systems will be permitted. For example if e-mail is the only needed service, then a firm can restrict other forms of access, such as file transfer protocol (FTP).

Information can further be protected by **converting word documents to PDF or some other non-changeable format** before e-mailing them. The PDF format permits a party to read the document but does not enable that party to make changes or to read a previous version.

The use of a large network enhances the hacker threat, since larger networks are accessible to proportionally more hackers. **A small private network** or the use of the same commercial provider may be advisable.

3.3 RECORDS-MANAGEMENT POLICY

A clear policy that governs retention and destruction of electronic documents is imperative for attorneys and their clients. Law firms may consider employing a person responsible for overseeing their client data management, to ensure that electronic data are retained and

are accessible as and when necessary to comply with discovery requirements on a timely basis.

In concluding, when using electronic media such as a blog, e-mail, and internet, the following checklist might be used-

- Include a disclaimer
- Do not offer legal advice
- Avoid creating attorney-client relationships
- Have regard to your law society's advertising rules
- Have an e-mail policy
- Enhance your technology's security by using:
    - encryption
    - a firewall
    - a partition
    - the conversion of documents to PDF formats
    - an access service policy
    - authentication tools
    - a direct modem link (where possible)
    - a small network (where possible)
    - the same commercial service provider
- Obtain waiver from clients regarding e-mail communication
- Ensure that your attorney-client relationship is reduced to writing.

Shadrack Maile

Attorneys Fidelity Fund.

Shadrack@fidfund.co.za