A tangled **web**

It has been said that there are two types of firms: those that know they have been attacked by cybercriminals, and those that don't yet know. ***Francis Dingwall*** *looks at how to prevent attacks, and how to mitigate them when they do happen*

Francis Dingwall *is a solicitor and partner in Legal Risk LLP*

Cybercrime is a recent phenomenon, exploiting the vulnerabilities of computers and the internet, and it is therefore difficult for a busy practitioner to get to grips with. However, the process to follow in addressing the threats it poses is the same as with other areas of exposure: identify the risk, evaluate it, take steps to manage it (whether rejecting it, mitigating it or transferring it), and monitor it.

LAW FIRMS: THE WEAKEST LINK

Identifying the source of the risk is easy enough. Cybercrime is a business. Cybercriminals are not spotty teenagers in their bedrooms, but professionals in sophisticated organisations. Cybercrime is an industry, reportedly churning out 250,000 items of new malware a day.

The business community has woken up to the risk and has been addressing the threat. Even so, the law firms who serve those businesses, and hold their most confidential data, have lagged behind. Cybercriminals probe to find the weak points, and in November 2011, the FBI held a meeting with 200 law firms in New York where they explained that cybercriminals considered law firms to be a "backdoor to the valuable data of their corporate clients". Firms in the UK have suffered numerous attacks, which have caused losses from client accounts running to millions of pounds, to say nothing of the value of the confidential data stolen.

The legal world is taking note: the American Bar Association published *The ABA Cybersecurity Handbook* in October 2013. Also, The Solicitors Regulation Authority (SRA) published *Spiders in the web: the risks of online crime to legal business* in March 2014.

PAPER: SECURE BUT INCONVENIENT

Data has been stored and transmitted on paper since the time of the Pharaohs. It is a fairly secure medium. As it is physical, it can be locked up: premises can be secured and filing cabinets locked. Transmission via Royal Mail, DX or courier is safe. There are vulnerabilities, including 'social engineering' threats (which used to be known as 'confidence tricks' or 'cons'), but by and large, it is secure.

However, paper was not a convenient medium for storing or transmitting data. It is difficult to share the data other than by physically copying pages, and the data cannot be manipulated.

ELECTRONIC DATA: CONVENIENT BUT INSECURE

Storing and transmitting data electronically is a lot more convenient. The data is portable and accessible at all times. It is easy to manipulate, such as by using the tracking changes functionality in Word or Excel. The data can be shared by email.

But when IT suppliers gave us electronic data and the new channels of communication, they omitted to mention one key factor: lack of security. The convenience comes at a price. What makes it convenient is exactly what makes it insecure. The cybercriminal exploits the lack of security inherent in the technology.

What exposes a law firm to the vulnerabilities of electronic data storage and transmission? There are different issues for different people. The world divides into 'digital immigrants' (those born before 1985) and 'digital natives' (aka Generation Y, or 'millenials').

DIGITAL IMMIGRANTS

Anyone born before 1985 has had to adapt to the new technologies. Some take to them well, but many are baffled.

The key issue for digital immigrants is understanding technology: if you don't, how can you hope to understand the threats? As a solicitor, you have an obligation of competence. If you use any of the new technologies, you have an obligation to gain a basic understanding of that technology, including its vulnerabilities.

Take an example from the past. When telephones were first introduced, all calls went via an operator at a public exchange, who could listen in. A solicitor who used a telephone to speak to their client had an obligation to understand that limitation to the confidentiality provided by a telephone call. The same obligation applies today to the newer technologies.

Understanding the technology does not require you to be able to build it or repair it, but you do have to understand the essentials, and the vulnerabilities. Only then can you start to appreciate what the threats are. The solicitor must understand what "phishing" is, what "vishing" is, what a "man in the middle" attack is, what a "Trojan horse" is, how "ransomware" operates. Additionally the solicitor must understand where the threats come from: for example, that if you act for an unpopular corporation, you can expect attacks from "hacktivists".

DIGITAL NATIVES

Millenials have grown up with Facebook, Twitter, Instagram. They are perhaps too much at home with it all, and they have a low desire for, or expectation of, privacy. They have grown up in a world where they

share information freely. A study, 'Do Millenials believe In Data Security', in the *Harvard Business Review* (available at tinyurl.com/mco2o6s), concluded that they value convenience over security, and will use their familiarity with the technology to work around security policies. They often keep their passwords in plain sight, and do not hesitate to use personal accounts for work purposes and vice versa.

The issue for digital natives is perhaps to have a full recognition of the duty of confidentiality required of a solicitor, as follows.

- Chapter 4 of the SRA Code of Conduct (you keep the affairs of clients confidential), reflects the fiduciary duty that a solicitor owes. See also Principle 10: protect client's assets.
- Corporate clients often demand evidence of the quality of the information security their solicitors can provide, and they may demand the certification of ISO 27001.
- Solicitors also have obligations to the Information Commissioner, and under the Data Protection Act 1998.

Millenials who do not hesitate to upload work documents on their personal accounts should be mindful of the Solicitors Disciplinary Tribunal's decision in SRA v Crossley (case no. 10726-2011). Mr Crossley's firm, ACS Law, took on the file-sharing community, which punished him with a DDoS (distributed denial-of-service) attack, in the course of which they extracted and published confidential information held by the firm. He was criticised by the tribunal for his use of his personal account: "The use of a 'home' web hosting package (which failed in any event) was inappropriate, inadequate and put confidential data at serious risk ...". Mr Crossley was suspended for two years.

WHO IS RESPONSIBLE FOR INFORMATION SECURITY?

There are two key issues in terms of responsibility here: vulnerabilities, and the duty of confidence. When the IT team suggests that the firm stores its data in the 'cloud', whose job is it to ask where it will actually be stored? Storing data on the cloud means nothing more than outsourcing your servers. Who will be in charge of the servers? Who will be able to look at the data? Will the data always be available? What if the owner of the servers becomes insolvent: will the firm be able to recover its data?

The temptation is to say that this is all the responsibility of the IT team. However, as with business continuity, the issues go beyond IT. There are essentially three aspects:

1. Technical – this is the IT issue.
2. Physical – this is about protecting the facilities and infrastructure from intruders.
3. Administrative / management – this embraces four areas:
   - risk assessment (identifying and evaluating the risk, and proposing ways to address it), taking into account the extent of the duty of confidentiality,
   - ensuring personnel are competent, trained, trustworthy and managed (dishonest, disaffected or departing personnel are one of the biggest threats, as are new people, who are most likely to open the door to a phishing attack, by clicking on a phishing email's attachment);
   - disaster planning, and planning the response to an attack; and
   - audit and monitoring.

The firm needs an information security function to handle these issues. Within a large firm, there may be a dedicated information security manager with a team; in a small firm, it may be a role that the partner responsible for risk management will take on.

BUILDING YOUR DEFENCE

Having identified the risk and evaluated it, the firm must tackle it. There will be a number of defensive layers.

The first will be locks: putting digital locks on the digital doors into the firm's data.

That leads on to the next layer of defence: training. However good the locks are, they will be ineffective if a cybercriminal can persuade an employee to open the digital door. That is the social engineering aspect of cybercrime: using the traditional skills of the conman in new ways. Humans are the weakest link. Staff need to understand what, for example, 'spear phishing' is: the criminal targets the particular employee, looking at any social media the employee uses, to see who they might be expecting an email from, and then posing as that individual. Firms should maintain awareness by, for instance, a fortnightly email circulated to all staff, telling them about the latest horror story or a new and ingenious form of attack.

The next layer of defence may consist of passing some of the cybercrime risk to the firm's clients, by putting provisions in the retainer letter or terms of business: a common one is to invite the client to use an encrypted mode of communication, and warn them that they use unencrypted email at their own risk.

The firm may reject aspects of the cybercrime risk, by declining to participate in certain media, or by setting rules which prohibit employees from vulnerable practices. For example, the firm may want to prohibit the use of web-based personal email and/or online file-hosting services. The firm should consider carefully its position on BYOD (bring your own device), in terms of whether to let the firm's employees put the firm's data on their own devices, and if so, what stipulations to make about encryption, and how to enforce it.

The firm may transfer the cybercrime risk to insurers by purchasing cyber liability insurance. You should look carefully at the extent of the cover being offered.

The last layer of defence will be planning the response to an attack. The instinctive response may be to hide the attack, in the hope of preserving the firm's reputation, especially if the firm's information security is not all it should be. That is fatal: in the recent attack on Sony, it was commended for informing the FBI within hours. In some attacks, every minute can count.

Finally, you should assume that there will be an attack, if it hasn't already happened. It has been said that there are two types of firm: those which know they have been attacked, and those which don't yet know they have been attacked. If you are not persuaded, visit the 2014 Information Security Breaches Survey (available at tinyurl.com/mnejsbt). It makes for sobering reading.