CenturyLink®

WHITE PAPER

Law firms and cybersecurity: how can lawyers keep their client data confidential?

Cybersecurity has dominated the global headlines during 2017. In May, ransomware attacks - allegedly emanating from North Korea - caused chaos in the NHS. The following month, James Comey, the former head of the FBI, gave evidence in which he claimed that he had "no doubt" that Russia had attempted to interfere in the 2016 US presidential election by hacking into voter databases. In September, it was revealed that credit ratings company Equifax was hacked and the confidential data of 143 million people was compromised.

According to Lloyd's of London a 'serious' cyberattack could cost the global economy almost £100 billion. The fact is that cybercrime is a growing menace to the whole of society, impacting private individuals, public infrastructure and global business. CenturyLink commissioned research to find out how law firms are tackling their own cybersecurity challenges, and we will consider some of the findings below.

20%

of law firms have experienced an attempted cyberattack in the last month

What are the main cybersecurity risks faced by law firms?

According to the research 20% of law firms have experienced an attempted cyberattack in the last month, rising to 44% over the last year. Each of these attempts is both an attack on the firm's infrastructure and potentially seeks to compromise their data. Although 34% claim they have never been the victim of an attempted cyberattack, whether this belief reflects reality is open to question, argues Joanne Frears, Consulting Solicitor at Blandy & Blandy: *"The average length of time it takes to discover a cybersecurity breach is 196 days and so although it is easy to believe that almost half of all firms have suffered attempted cyberattacks, it is alarming to think that the 34% who claim to never to have been targeted, could simply be unaware that malware has been planted on their system or that perhaps one of their accounts staff is currently being spear-phished! This lack of awareness and preparedness is one of the biggest risks the profession faces."*

Data protection breaches

Since law firms will often be advising their own clients on data protection matters, they need to be particularly aware of, and fully compliant with, all the data protection rules and regulations. Currently, the Data Protection Act is the primary piece of legislation with which law firms need to comply - but they must additionally abide by the Solicitors Regulation Authority (SRA) rules, under which they are responsible for keeping any client data confidential. If client data is compromised, the financial and reputational impact on a firm can be significant and may involve:

- An investigation by the Information Commissioner's Office (ICO)
- An ICO fine of up to £500,000
- Enforcement action by the SRA
- Loss of trust and business by existing clients
- Loss of future business from potential clients due to adverse publicity

It is therefore surprising that less than a third of the firms in the survey believe they are fully compliant with the relevant legislation relating to data protection. Frears notes that: *"The SRA receives about 40 complaints about breaches of confidentiality a month. The obligation to keep client information confidential is enshrined in Rule 4 and as one of the key principles of legal practice, it is a key USP for the profession in an increasingly crowded advisory sector. Breach of Rule 4 can lead to sanction by the SRA and a fine of up to £500,000 from the ICO and all this is well known."* The forthcoming GDPR will bring even more severe penalties for data protection failures (see opposite).

Infrastructure damage

The NHS ransomware attack was not thought to have compromised patient data, but the cybersecurity failings crippled the infrastructure of affected hospitals, proving a stark lesson in the importance of protecting vital IT systems. Law firms can similarly be brought to a standstill if, say, their practice management system goes offline or emails cannot be accessed.

Firms that have made steps towards agile working, without paying heed to the security aspects of their digital transformation, are most at risk. Home based fee earners who are reliant upon IT infrastructure which allows them to work remotely may be unable to do their work, leading to losses in productivity and delays for clients. Going paperless without putting in place effective cybersecurity can prove extremely costly in the case of a cyberattack.

25%

of firms believe they are currently compliant with the requirements of GDPR

Impact of GDPR on these risks - are firms prepared?

The General Data Protection Regulation (GDPR) comes into force across the EU from 25th May 2018. It increases maximum fines for data breaches to €20 million or 4% of annual global turnover and introduces a variety of new data protection rules, including:

- Mandatory breach notification, meaning data controllers will be required to notify the Information Commissioner of any data breaches within 72 hours (if feasible)
- Widening the scope of personal data
- Encouraging "privacy by design" and "pseudonymisation" - when developing new bespoke IT systems, potential cybersecurity issues should be taken into account

According to the research, only 25% of firms believe they are currently compliant with the requirements of GDPR. Frears encourages firms to prepare for the forthcoming rules while they still have time: *"With the advent of GDPR next May bringing greater record keeping and privacy by design obligations as well as the potential of fines for breach of €20m or 4% of annual turnover, those 75% of firms that admit they are not prepared [or don't know if they are prepared] for these changes have a chance to get ready, but time is running out!" She also warns that Brexit will not provide a panacea for GDPR worries: "Perhaps most firms think Brexit is a cure for GDPR, without realising that unless the UK has robust data protection compliance equivalent to GDPR, it will not be able to provide or accept any personal information from EU businesses or EU citizens and most of the UK service and technology industries would fold as a result!"*

What are the motivations for cybercrime which targets law firms?

Although some types of cyberattacks may be motivated by amateur hackers keen to make a name for themselves, a large element of cybercriminality undoubtedly takes place for financial gain. Law firms are particularly vulnerable because they often hold valuable and sensitive client data. Commenting, Frears says: *"Of all complaints to the SRA, only 1% arise from data protection issues, but as all the information solicitors maintain in relation to clients, their businesses, their personal life, property and money matters is highly sensitive and therefore valuable, law firms are often considered easy targets by cybercriminals. Stark stats confirm this perception might be correct when the SRA reports that from the start of Q1 2016 to the end of Q1 2017, £12m in client money was taken by cybercriminals in scams and that 75% of those were 'Friday Afternoon Frauds'."*

How can firms tackle these challenges?

Technical measures

The research found that 43% of law firms are currently moving to a cloud provider (e.g. Microsoft, Google, Amazon) and 23% are moving their servers to a colocation facility. Some firms are outsourcing not just security but the hosting of their applications to cloud providers. Moving away from legacy on-premise IT systems to a cloud or colocation solution can lead to improved cybersecurity, eliminating the security skills gap by enabling the provider to focus on ensuring that security is constantly being optimised and updated, thereby minimising risks posed by external hacking. Furthermore, outsourcing IT effectively hands over the work of supporting and managing the servers to the provider; they 'keep the lights on', allowing the law firm to focus on providing legal advice.

Culture and people

The biggest issue faced by firms in regard to data security, according to the research, is human mistakes; 49% of IT decision makers cited this as a key challenge and over a third noted lost documentation or devices was a major problem. However, only 60% of firms provide compulsory cybersecurity training for their staff. Clearly more needs to be done to change the culture towards data security within firms; technology alone cannot plug all the security holes. Employees and contractors often provide a soft target for hackers and are sometimes a threat themselves (14% of firms say that insider threats are a key challenge).

Although increasing awareness of staff regarding cybersecurity through regular training is the main way to tackle the cultural problem, there are also technical measures which can help to prevent mistakes by people. For example, employees who are given access to a cloud computing resource will no longer need to send unencrypted emails to their personal accounts or use USB sticks to transfer data; and potential insider threats can be better monitored with the use of auditing software and the distribution of individual logins which track any activity.

How can law firms advise their clients regarding cybersecurity?

Firms which have tackled their own cybersecurity challenges will be much better placed to advise their clients in this regard. Understanding the theory of the compliance regime is one thing, but the practicalities of putting in place the necessary data protection and cybersecurity measures brings a greater overall awareness of the difficulties. Some of the ways in which firms can advise their clients include:

- Explaining their key data protection duties
- Carrying out a data protection audit - both under the existing rules and in advance of GDPR
- Advising them on how to implement practical solutions
- Running staff training on data protection issues
- Putting technical measures in place, possibly in conjunction with external IT providers

Top tips on tackling cybersecurity challenges

- **AAA (awareness, audits and assessments)** - law firms should ensure they are aware of all the necessary steps they must take to comply with data protection, especially in advance of GDPR coming into force. They should carry out an impact assessment of their existing data protection measures and audit any relevant contracts and policies.
- **Outsourcing IT** - rather than spending time and money on beefing up their internal security, it may be more cost effective for firms to move their systems to a cloud provider or colocation solution.
- **Staff training** - people are often a soft target for hackers, so changing the data protection culture within a law firm is crucial to plugging the security holes.
- **GDPR** - law firms will often be advising their own clients on GDPR compliance, so it's vital that they get their own house in order first.
- **Digital transformation** - firms which decide to go paperless or introduce remote working without first reviewing their cybersecurity are at particular risk from hacks that affect their infrastructure. A comprehensive digital transformation plan should be made right from the start.

Global Headquarters
Monroe, LA
(800) 784-2105

EMEA Headquarters
United Kingdom
+44 (0)118 322 6000

Asia Pacific Headquarters
Singapore
+65 6768 8098

Canada Headquarters
Toronto, ON
1-877-387-3764

CenturyLink®