Chris Robinson

Legal Consultant
Clarity & experience
in corporate law

Where's my Blackberry?

Data protection comes of age – is your law firm taking it seriously? (UK)

It's hilarious, isn't it? MI6 officer leaves his laptop in a cab. HMRC loses unencrypted data disk in the post. Building society employee's computer is nicked from his home. Medical records found in car park. Council loses children database on memory stick. Only this week, sensitive Scottish court records discovered at recycling bank. There are so many of these stories, and we all enjoy a laugh at the incompetence of these large organisations in protecting our personal information. After all, this only applies to big, faceless institutions managing huge databases – doesn't it?

Data protection law has been around for a long time, but it hasn't been taken terribly seriously by anyone outside of large data centres – except as an excuse to not tell anyone anything: "can't answer that – data protection". We used to tell our clients not to worry unduly – make sure you register, but if you get anything wrong all you will get is a telling-off and guidance on how to do better next time.

But now data protection has come of age. Sit up and take notice. In November the Information Commissioner's Office (ICO) levied its first fines, under stronger powers given it last year. Hertfordshire County Council was fined £100,000 for inadvertently sending child protection case papers by fax to the wrong number. Who hasn't sent a fax or email to the wrong address? Yet the council should, apparently, have had procedures to stop this happening. What procedures, exactly?

The second fine was even more concerning for businesses. A private company, A4e, was fined £60,000 for the loss of a laptop, stolen from an employee's house, containing unencrypted data on 24,000 people.

Data protection doesn't only apply to big databases – the Hertfordshire case concerned only a handful of people, though the information was of the most sensitive kind. It doesn't only apply to professional data processors; it can apply to any business. And good intentions aren't enough: failure to have adequate security and procedures can lead to large fines, even with the intervention of errors or criminals. Keeping data on a PC inside a locked private house wasn't good enough protection.

+44 (0)7770 601840 – chris@cirobinson.co.uk – www.clarityincorporatelaw.co.uk – 58 Augusta Avenue, Northampton NN4 0XP LinkedIn http://uk.linkedin.com/in/chrisrobinsonlawyer . On behalf of Chris Robinson Ltd (registered in England and Wales no 7246040 r/o as above) which does not provide legal services to the public and which advises clients only as agent on behalf of law firms regulated by the Solicitors Regulation Authority. When I am not retained by another regulated law firm, services are provided by Excello Law Limited.

That led me to think about the attitude of the legal world. Solicitors take client confidentiality very seriously, in terms of their own conduct, but many have not translated that into action on data security or, for that matter, physical security. They think of it as a duty to the client, but not about the other data subjects who may be referred to in their files. Legal practices hold vast amounts of personal data, much of it of a highly sensitive nature. Deeds and will may be kept in a safe, but there is little or no security on paper files, which are stored openly, carried around on public transport and taken home. Many lawyers' computer systems have no security on internal access to data beyond an access-level password. They have firewalls and virus protection. But usually no protection at all against unauthorised access or copying by legitimate users of the system, or anyone in possession of their passwords. Data is not segmented or internally password-protected.

Access to the servers from the internet is usually tightly controlled, but once in, there are no restrictions on access to client data. Unencrypted email is universally used for almost all communication, and unencrypted attachments are sent that could include large amounts of personal data. Worst of all is the approach to home and mobile working. Data may be freely transferred to work or personal laptops and mobile devices. Mobile devices with weak passwords or PIN numbers allow access to the entire system, or at least to email records.

Solicitors have always relied on their integrity and professional conduct to enforce confidentiality. Systems are devised to prevent casual disclosure of information, but they are not designed to withstand deliberate, criminal attack. Most solicitors would feel that there is not much chance that they will be victims of deliberate espionage or malicious attacks.

Then there was the ACS Law case, in September 2010. ACS, a small law firm, acted for copyright holders trying to sue P2P file sharers for copyright infringement. It got court orders against ISP's forcing them to disclose lists of users with details of internet usage, allegedly including their access to pornography. BT, and possibly others, sent the data to ACS as unencrypted email attachments – Excel spreadsheets. You wouldn't have done that – would you? Then the libertarians of the file-sharing community mounted an illegal denial-of-service attack on ACS's website. In attempting to restore the site, ACS's IT people accidentally allowed access to internal data, including their email archive – which was promptly stolen and distributed across the net. ACS could yet be fined up to £500,000 for this breach. Clearly that should not have happened. But it was a mistake, made by a technical person. How is a law firm supposed to supervise an IT specialist to make sure he never allows external access to data?

More worrying still, the unencrypted attachments were the main source of the data stolen. What could ACS have done to protect that information? It naturally archives its emails, even if deleted by its users. It also backs up the archive and everyone's inboxes. So multiple copies of any attachment will be created, even if the user did not save the attachment – or correctly saved it with a password.

This is the heart of the problem for law firms. We deal in evidence. We are instinctively more worried about losing access to data than we are about others gaining access. People leave, and passwords get forgotten. We lawyers hate to throw anything away. We get sued if we can't prove exactly what advice we gave to Mrs Jones on the phone in 2005, or we can't explain why clause 24 was deleted in draft 3, or we forgot the family history told to us five years earlier. Professional standards such as Lexcel require us to ensure that other people in the firm have access to client information if the lawyer is absent for any reason. The drive to be efficient and keep costs down requires us to share information quickly.

Part of data protection is the deletion of data that is no longer required, but I have yet to meet a lawyer who thought that any document or record could be discarded. Try persuading them that they should be deleting all records of incoming emails from the other side in litigation because they contain personal data! It's evidence in the case.

So what should we be doing? The ICO's guidance is quite clear, and it does not match with what many lawyers have been doing. Review your security with an eye on protecting the privacy of all data subjects, not just your client. Make sure your data is secure even if someone steals your PCs or servers. Identify particularly sensitive items, either because of the nature of the information or the number of data subjects, and take particular precautions, including password-protecting individual documents and preventing their removal from the office, in hard copy or unencrypted electronic form. Ban anyone from working on computers outside the office unless all client data is stored on an encrypted drive with a strong password. Prevent anyone from transferring data to CD or memory stick without getting authorisation, to include checking the security of the data. Promote a culture of data security, including password security.

For now, this will still be an imperfect solution. We need to communicate with outside parties and to transfer data to them. Email encryption is still not widely accepted in the world at large, due to the need for both parties to operate the same system, so email traffic is likely to remain vulnerable in transmission. Make sure your records of incoming and outgoing emails are stored on encrypted drives and that your access passwords are strong, and not remembered by the user's PC – which Outlook rather encourages. Check that your backups of data are as secure as the originals. If necessary, implement a password management system to securely record the passwords needed to access protected data.

I have done all this myself, to give clients and data subjects the best protection possible against unauthorised access to my home PC, laptop or smartphone, my wireless network or my email communications. I tell my clients to anonymise bulk information they may send me about their employees or customers wherever possible, and to password protect the information. But no-one has yet shown me how to prevent the mis-keying of a fax number, the loss of a document in the post or accidentally attaching the wrong file to an email. At least by being seen to try, we should be protecting ourselves from the savage criticism that will flow from doing nothing.

I should say that nothing in this article relates in any way to any of the firms I work with – I have no cause for concern about any of them.

Chris Robinson
Solicitor (England and Wales)
January 2011