

Lawyers and Data Security - Why They Just Don't Get it!

Your honour, I put it to you that members of the legal sector are guilty of gross negligence! The legal profession is often perceived as the savviest of all the professions however, when it comes to respecting customer confidentiality, it would seem they are just as clueless as other professionals and organisations who have hit the headlines in recent months. Ignorance is no defence. So what is?

According to a recent survey, conducted in the UK amongst lawyers from 100 law firms taken from a cross section comprising small firms to multi-national practices, 24% had misplaced at least one mobile device containing confidential documents. These losses leave the data saved to the device vulnerable to exposure with case-notes, contracts and client details typically at risk. Worryingly 37% believed that if they did lose their mobile device it would be insecure as a hacker, or identity thief, is cleverer than the average lawyer and could access the data it contains.

It's alarming to note that on many of these unprotected devices, lawyers are storing a variety of highly sensitive information including business emails - 85%, work contact details - 65%, client contact details - 50%, firms data - 42%, client records - 34%, contracts - 32%, case files - 28% and even security details like passwords and access codes - 16%!!!! A staggering 4% of legal respondents didn't use any security whatsoever.

To give an idea of the scale of the problem, the ever popular blackberry/PDA is now the most preferred device that lawyers use to store their information with 67%, compared with 63% using their laptops, 41% using USBs or memory sticks, and 21% now using a smartphone such as the Apple iPhone. Seven percent use an MP3 or Tablet PC and the majority use a combination of all of these devices.

One common misconception is that data is protected if it is secured with a password, as was the case for over 90% of the misguided lawyers consulted during this survey. Robert Schifreen ex-hacker, and now an IT security consultant, is of the opinion that "Passwords alone are inadequate if confidential sensitive information is residing

on a mobile device. Cracking software can be downloaded from Google that can break the average password in less than 30 minutes. The only answer is, if sensitive data is stored, it must be encrypted." Data security advice from the Information Commissioner's Office in the UK is to encrypt any information held electronically if it will cause damage or distress if it's lost or stolen.

Although it's worrying that so many unprotected devices have gone missing over the past few years, in reality the true cause of alarm is that that one in five lawyers are using their own mobile device to store corporate and sensitive information – a disclosure which will throw every respecting IT department into total apoplexy. These devices often slip under the companies IT security radar and out of the IT departments control so they can neither be secured, backed up or ownership of the information they contain reclaimed if a lawyer were to leave the organisation.

How do you secure the data that's mobile from never getting into the wrong hands?

As a starting point the questions that need to be examined are the types of information the organisation holds that is stored on mobile devices and how easy would it be for the device to be lost or stolen. The answers will have a great impact on security concerns and risks and will dictate the type and amount of security needed.

As a general rule, this is a best practice guide to securing data:

- 1. Encrypt The Data.** Encrypt the data on every device carried if it's sensitive. This survey found that 13% of those lawyers that had lost a mobile device were

Lawyers and Data Security - Why They Just Don't Get it!

confident it couldn't be breached, or used against them, as this small percentage of law firms were security savvy enough to encrypt the data residing on them. A data protection policy must be deployed that ensures all handheld, laptop, desktop and other removable media (like USB sticks) are encrypted, managed and controlled centrally which then enables the IT department to be able to suspend access if the device is misplaced or stolen.

2. Protect The Data Wherever It Is. If data is lost it doesn't matter what device it was on, data is data! Don't fall into the trap of assuming that the only devices you have to protect are the ones that the organisation owns. Employ a solution that can detect devices trying to connect to the enterprise and sync up with corporate data regardless of type of device, or whether they are corporate or personally owned.

3. Do Not Impact IT Operations. Make sure the encryption solution is transparent to end-users and doesn't interfere with any operational activities. Enforcing an untenable solution is nonsensical. Involve select personnel, at various levels, across all departments to ensure all viewpoints are considered and any necessary changes to working practices viable.

4. Centrally Manage the Data Protection. IT departments should never leave data security up to the end user, they don't have the time or the knowledge, and it certainly wouldn't be considered "reasonable and appropriate" (the underlying theme of mobile security regulation) if the device, and the data contained, was lost or stolen. It is imperative that it is controlled and managed centrally. This can also reduce TCO (total cost of ownership) as machines don't need to be locked down or brought into the office to be updated.

5. Prove It. Corporate Governance requires organisations to not only have security, but be able to prove it is effective. When a device is lost or stolen then the company has to decide if a "breach notification" needs to be issued, along with all the expense and embarrassment that goes with it. However, if there is a reasonable belief that the data was encrypted – and you can prove it – then you do not have to notify the affected individuals whose information has been lost as it is not at risk. By using a solution that includes a central management console, every machine that is protected reports back to say that it has received the latest instruction and confirms that it has been carried out, keeping all the proof centrally.

Enterprises must include data protection throughout the mobile data lifecycle in order to help them meet state and federal regulatory requirements for information data security. Following these five steps will help your company to enjoy sustainable security for all end points and devices.