

Lawyers Found Guilty of Failing to Defend Their Clients

A quarter of law firms admit to losing confidential information.

(Vocus) October 27, 2008 -- Your honour, I put it to you that members of the legal sector are guilty of gross negligence! 24% of UK legal firms have confessed to misplacing 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. That's the shocking discovery by Credant Technologies, a company specialising in IT security, in its survey amongst 100 legal firms across the UK to ascertain how this well-informed sector view "security, mobile devices and end-point protection".

37% of lawyers 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. A paltry 13% of those that had lost a mobile device were confident it couldn't be breached, or used against them, as only this small percentage of law firms were security savvy enough to encrypt the data residing on them.

Lawyers are naïve when it comes to security

This survey was conducted amongst the legal profession, 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. Over 90% of lawyers believe their data is protected because they are securing it with a password. An unacceptable 4% don't use any security whatsoever. However, an educated third of lawyers interviewed are protecting their information with encryption.

Robert Schifreen ex-hacker, and now an IT security consultant, said "Passwords are just inadequate if you have confidential sensitive information residing on a mobile device. You can download cracking software from google that can break the average password in less than 30 minutes. These findings show just how naïve the legal profession is when it comes to data security and I suspect other professions are just as bad, if not worse! The only answer is, if you store sensitive data, you must encrypt it."

One in five lawyers use their own device to store clients information

The survey further revealed that one in five lawyers use their own mobile devices to store corporate and sensitive information – (a disclosure which will throw every respecting IT department into total apoplexy), as these devices slip under the companies IT security radar and out of the IT departments control so they can neither secure them, back-them-up or claim ownership of the information they contain if a lawyer were to leave the organisation.

Case notes, contracts and security details all left unprotected

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%!!!!



Lawyers love their Blackberry's & PDAs more than their laptops

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.

Michael Callahan VP Global Marketing at Credant said ““It’s worrying to note that so many unprotected devices have gone missing over the past few years, but personally I’m more concerned by how many personal mobile devices are being used by lawyers which clearly by-pass any security procedures set-up by the legal firm. This creates an uncontrollable environment for the IT security staff as they simply can’t keep track of which devices they’ve secured and which they haven’t. Our advice is to implement a data protection policy that ensures all handheld, laptop, desktop and other removable media (like USB sticks) are encrypted, managed and controlled centrally which then enables the IT guys to be able to suspend access to the information if it is misplaced or stolen.”

Credant recommend these following top tips to securing data on the move

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

- 1 Encrypt the data on every device you carry if it’s sensitive.
- 2 Get a solution which can detect devices trying to connect to the enterprise and sync up with corporate data.
- 3 Make sure the encryption solution is transparent to end-users and doesn’t interfere with any of your operational activities.
4. IT departments should never leave data security up to the end user. It is imperative that this is controlled and managed centrally This can also reduce TCO (total cost of ownership) as machines don’t need to be locked down or bought into the office to update them.
5. Corporate Governance requires you now to have security and can prove it. Use a solution that includes a central management console – that way every machine is protected and can be tracked.

Follow these steps and your company will be able to enjoy a sustainable security policy for all end points and devices.

This survey was conducted amongst lawyers from 100 law firms in the UK taken from a cross section comprising of small firms to multi-national practices. The survey was conducted by an independent survey company for Credant Technologies on “security, mobile devices and end-point protection”.

For further information please contact Yvonne Eskenzi on 020 71832 832 or email [Yvonne\(at\)eskenziipr.com](mailto:Yvonne(at)eskenziipr.com).

About CREDANT Technologies

CREDANT Technologies is the market leader in endpoint data protection solutions that are critical components of an endpoint protection platform. CREDANT’s data security solutions preserve customer brand and reduce



the cost of compliance, enabling business to “protect what matters.” CREDANT Mobile Guardian is the only centrally managed endpoint data protection solution providing strong authentication, intelligent encryption, usage controls, and key management that guarantees data recovery. By aligning security to the type of user, device and location, CREDANT ensures the audit and enforcement of security policies across all computing endpoints. Strategic partners and customers include leaders in finance, government, healthcare, manufacturing, retail, technology, and services. CREDANT was selected by Red Herring as one of the top 100 privately held companies and top 100 Innovators for 2004, and was named Ernst & Young Entrepreneur Of The Year 2005. Austin Ventures, Menlo Ventures, Crescendo Ventures, Intel Capital, and Cisco Systems are investors in CREDANT Technologies. For more information, visit www.credant.com.

###



Contact Information

Yvonne Eskenzi

Eskenzi PR for CREDANT

<http://www.credant.com/>

020 71832 832

Online Web 2.0 Version

You can read the online version of this press release [here](#).