Safeguarding IP in the legal sector

Despite investments in cyber security, legal firms are risking catastrophic damage to their clients' and their own businesses by failing to adequately protect sensitive data stored on laptops, portable devices and removable media.

The imperative of secure gatekeeping

Legal firms hold a wealth of sensitive data on behalf of clients, including patent data, merger and acquisition information, details of commercial negotiations and customer contracts. Safeguarding this information is clearly a central responsibility.

As the custodian of many of the most valuable intangible assets belonging to their clients, legal firms hold a privileged position. This position is based totally on trust in the legal firms' ability to protect that data.

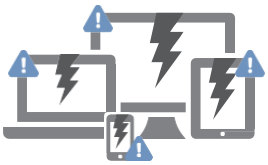
Keeping this information secure in the face of a wide array of threats is critical.

The crippling cost of IP theft

The loss of any sensitive client data or intellectual property can have devastating consequences for both the client and the legal firm.

For the client the impact of a competitor gaining access to research outputs, proprietary designs or details of commercial negotiations could mean lost customers, reduced competitiveness and lower profitability. These clients may never see a return on their R&D investment.

For the legal firm, a data breach is likely to destroy client trust and gravely damage their reputation.



In the year 2014/15 there were 82 separate data breach incidents reported involving members of the legal profession.[1]

The growing threats to the legal sector

Subject to threats from a range of sources, legal firms are increasingly a target for cyber-crime. Attackers include organised cyber-criminals, governments, their clients' competitors and disgruntled employees.

Legal firms are often seen as both high-value and relatively soft targets. Breaching the defences of a legal firm could expose the IP and trade secrets of multiple businesses in one hit. Indeed, in 2014 the UK Information Commissioner, Christopher Graham, highlighted the legal sector as an area of particular concern, and it has been reported that GCHQ regard law firms as "the soft underbelly of UK plc"[2].

The security weak spot of unsecured devices

Data breaches occur for a variety of reasons, but most are the result of malicious attack or human error. Recent research revealed that:

- 47% involved a malicious or criminal attack
- 25% involved a negligent employee or contractor.[3]

In particular, the loss or theft of unencrypted devices is causing concern. ICO figures show that Q1 2015/16 saw a 22% increase in this type of data breach. Given the large numbers of mobile professionals across the legal sector, there is a huge amount of sensitive client data being carried around on laptops, tablets and mobile devices. Consequently, legal firms are particularly exposed to data breaches from unsecured devices.

[1] https://ico.org.uk/action-weve-taken/data-security-incident-trends/ [2] http://www.itv.com/news/2013-06-13/britains-gchq-intelligence-agency-prepare-to-come-out-of-the-shadows-to-combat-cyber-crime [3] 2015 Cost of Data Breach Study, Ponemon Institute/ IBM

The risks that must be addressed

Common data protection failures are leaving Legal firms exposed to the loss of clients' critically important IP;

Policy black holes

Companies lack policies governing how data is managed and protected on portable devices – often accompanied by limited employee awareness of what *they* can do to reduce risk.

Failure to protect data at rest

Businesses fail to adequately protect data stored on desktops, laptops and portable media because they mistakenly assume that password protection or Endpoint Protection technologies adequately protect the data from a determined cyber criminal.

Data leakage via portable devices

Businesses fail to prevent data being easily copied onto unencrypted portable media (such as USB drives and smartphones) – one of the most common sources of IP theft.

Over-restrictive or complex security

If security prevents people doing their jobs effectively, employees are likely to find ways to bypass it – creating new vulnerabilities.

Limited visability & control

Businesses are often unclear about what data needs protecting, what devices are being used to store that data and how the data is being used and copied.

In a market where trust is a key driver of value, protecting clients' IP has never been more vital for legal firms.

Simple solutions for IP protection

Preventing IP from being stolen from laptops, PCs and portable devices, Becrypt's suite of data protection solutions safeguards business value and reduces the risk of compliance failures.

Secure your data at rest

Approved by the UK government to secure classified data (up to TOP SECRET), Becrypt's Disk Protect provides highly secure, full disk encryption for Windows laptops, PCs, tablets and servers – keeping data secure in the event of the theft or loss of a device.

Prevent data leakage

With full event reporting and audit trails, Becrypt's Port Control, *Connect Protect*, defends companies from data leakage and malware by preventing unauthorised access to, and use of, externally connected devices. Policy can be applied at device, user or group level, and devices can be white-listed by make/model, unique device ID or a signed device process.

Flexible sharing

Supporting multiple users on a single device, *Disk Protect* gives flexibility without risk by eliminating password sharing. Becrypt's Media Encryption, mShare, encrypts data on external storage devices such as USBs.

Easy implementation

Saving time and minimising the need for end-user involvement, Becrypt's *Enterprise Management* (BEM) enables quick and easy roll-out of our data protection products across thousands of devices. Active Directory integration allows easy importing of users, organisational units and security groups.

Fully manage, control & audit

BEM's centralised management system ensures full visibility and control of user activity, enabling the creation, application and updating of policies to end-points, users or groups. It also allows fast risk assessment in the event of a lost or stolen device.

To find out more about protecting device estates from IP theft, contact the experts.

contact@4ITSec.com

01603673787

#becrypt.com