

Hit where IT hurts

Tim Walker looks at computer-related crime and its potentially damaging consequences for law firms

Electronic data is everywhere – on our PCs, laptops, phones, memory sticks, even in our wallets – so it's not surprising to learn that it can sometimes fall into the wrong hands.

Computer crime is on the increase, posing a threat to all organisations, but also – interestingly – creating business opportunities for legal and forensics firms.

Martin Baldock, vice-president and general manager of Stroz Friedberg's UK offices in London and Leeds, explains: "There is a vast amount of data out there and all it takes is one so-called 'bad leaver' (someone who leaves a company bearing a grudge) to potentially damage reputations or threaten intellectual property."

Baldock has more than 25 years' experience in the IT industry, where for nearly a decade he has focused on forensic technology applications, including electronic discovery, investigations, and computer forensics. He previously held the general manager position at Data Genetics International Ltd, the UK forensic technology company, which was acquired by Stroz Friedberg.

For companies, Baldock's advice is simple: "You must put in place robust policies for your employees about IT use. In order to do this you have to first identify the value of the data you hold and carry out a risk assessment. Then take appropriate measures, but don't get carried away – if you make the whole security system too complex, employees get confused and end up writing down passwords, etc, and that defeats the object."

He adds: "Limit access to data to the right people (identify who needs to see HR records for example). Around 80 per cent of breaches involve people on the inside of an organisation – remember that people commit crimes, not machines. Have good, sensible policies and monitor use."

Baldock advises that all portable devices



be encrypted so that harm is mitigated if they fall into the wrong hands.

Understandably, he says that if there is a problem you must bring in outside help. There are sound reasons for this, he argues: "You need someone to come in who is independent, who doesn't know the people involved, who can look objectively at the evidence. You also need that specialist expertise that my company and others can offer. For instance, we can examine a computer and discover data that has been deleted. The evidence landscape in such cases is vast now – and gets bigger every day as technology moves on, so the techniques for tracing security breaches have to keep pace too."

Stroz Friedberg has become a trusted resource for corporations, counsel, individuals, government agencies, and the courts, in matters ranging from theft of intellectual property to lost laptops – and all other matters, digital and investigatory.

While computer crime is a major threat to legal firms, it also presents

opportunities, according to Timothy Pitt-Payne, a barrister in private practice at 11 Kings Bench Walk.

He explains: "Organisations need to have robust policies and contracts. For example, restricted covenants in employment contracts need to be constantly updated as technology changes. That is an opportunity for legal firms in terms of advice and in offering help with drafting clauses."

Pitt-Payne specialises in both information and employment law, so is well placed to talk about threats and opportunities in this area. He urges law firms to protect their reputations and intellectual property by making rules which are proportionate but not over-ambitious. For example, restricted covenants which are too restrictive are virtually worthless, he says.

"Weigh up what can be protected and what cannot. For example, it is very difficult to prevent people using information which is inside their heads, but if it is physical data it is easier to police."

If the worst happens, he says, bring in outside help because evidence-gathering is difficult and a legal minefield, especially if it involves covert operations.

Pitt-Payne, who has acted for both parties in such cases, continues: "Companies where people are the number one resource – such as legal firms – are very vulnerable, so these need particularly robust policies on IT use."

Research suggests that nearly three-quarters of employees have stolen corporate documents and information when leaving a job, many justifying it in the belief that they felt the information partly 'belonged' to them.

And it's a problem which firms need to be tackled from the start, says Jason Dainty, Partner at Kempner Robinson, a specialist IP law firm set up in May this year. The company deals with IP work including patents, trademarks, copyright and design work as well as breaches of confidence. He says legal firms need to get smart if they want to ensure their intellectual property and sensitive client data are not open to theft by disgruntled and ex-employees.

The ease with which documents and files can be accessed and communicated electronically, fuelled by

a 'culture of acceptability', means that IP theft is now 'rife' – not only in the UK but across the globe.

An expert on brand protection and strategy, Dainty also advises on a wide range of commercial IP agreements, and he says that it is incumbent on law firms to ensure they have safeguards in place to counter the threat of IP theft.

He says: "There's no doubt that technology is a double-edged sword – everyone in the modern workplace who uses a computer which does not leave the traditional physical paper trail has the potential to access and use sensitive company information; it's certainly a lot easier than printing off 500 sheets from a ring-bound file

"As an employer, you don't want to disrupt people's day-to-day work, but there is a delicate balance to be struck, and you have to make sure that employees know from the start what is, and is not, acceptable conduct. You can restrict the use of portable media storage such as USB sticks and CDs, and at the very least make sure that sensitive information is only accessible to those who need to have access.

"But it's also about having effective electronic monitoring systems in place –

emails, the internet, databases. You have to know what's going on, and that might mean calling in IT experts to set up such a system."

Bob Russell of the Forensics Telecommunications Service (FTS), is a former police officer. He says the potential for theft of intellectual property has obvious implications for law firms in terms of the volume of sensitive data, such as client details, which they hold.

Russell gives this advice: "Early reporting or contact can often be vital in obtaining advice for the preservation of evidence and to avoid any deleted data being overwritten.

"It is absolutely critical that throughout any investigation that we are asked to carry out, the data is treated with extreme security and care, as computer-held information is extremely fragile.

"Any evidence needs to be both forensically and meticulously collected and recorded, so that it can be presented later, whether that is for the firm's own use or indeed whether the courts become involved in terms of action against someone."

The message is clear – be prepared and, if you suspect there is a problem, bring in the experts. ■