Saving face, and money, through data security

Data security experts have a long running saying that there are two types of businesses; those who have lost data and those that will, Sean Hargrave **discovers**

"If data cannot be used by a third party, because it's encrypted, then the FSA rules maintain there has been no security breach."
Nick Cater

Losing business critical data has always been a disaster for those left to rebuild databases and carry on running divisions without the necessary digital files. In today's tough business climate, however, there is also a financial imperative.

High profile cases of companies and government departments losing customer data have not only proven the huge embarrassment and brand damage which can accompany a lapse in security, they have also shown the financial cost. The Information Commissioner's Office (ICO) and FSA have shown themselves ready and willing to use their powers to enforce a company that has lost customer data to reveal the security lapse as well as pay a large fine. Two years ago Nationwide was fined nearly a million pounds by the FSA following the theft of a laptop from an employee's house which had details of 11 million customers.

Remote and secure

Whilst many SMEs may think that backing up a database periodically on to a spare drive might be sufficient to ensure they do not lose customer data, Nick Cater, Director of Field Operations, Europe at Iron Mountain Digital reveals that there are many problems with this informal do-it-yourself approach.

"If you're going to back up data it really has to be stored in a separate, secure location, otherwise it's just as likely to get lost, stolen or damaged as the original," he says.

"You also need to automate the process so back-ups happen automatically and don't rely on someone remembering. Companies need to prioritise the data that changes the most often as well so that is backed up more frequently than data which does not change so rapidly."

"If we know a computer has been lost or stolen we have a special system for wiping it the next time it connects to the internet." Nick Cater
Nick Cater

Encryption key

Iron Mountain Digital operates a range of 'storage-as-a-service' options which back-up company data remotely for clients from desktops, servers and laptops. The crucial point, Cater insists, is back-ups are not solely sufficient; data needs to also be protected by encryption.

"When you're backing up you need to first encrypt it so it can't be intercepted and read at any stage and you also need the data on your desktops and laptops to be encrypted so people can't just download and steal information.

"If you're going to back up data it really has to be stored in a separate, secure location, otherwise it's just as likely to get lost, stolen or damaged as the original."
Nick Cater

"It's particularly important for laptops because they stay outside of the office a lot of the time, so you need to allow them to be backed up beyond the office through a secure wireless broadband connection. You also need to make sure that the data on them cannot be read by anyone should they steal or find the laptop.

"It's a crucial point because if data cannot be used by a third party, because it's encrypted, then the FSA rules maintain there has been no security breach. It's a simple step which could save SMEs a lot of worry over losing data and facing the embarrassment and a large fine for a security lapse."

Focus on data

An extra weapon in the arsenal of a business seeking to protect its business critical data comes in a special facility Cater reveals is programmed in to systems so a stolen computer can be wiped clean.
"If we know a computer has been lost or stolen we have a special system for wiping it the next time it connects to the internet," he reveals.

"It adds an extra level of security and gives extra peace of mind to companies to know that not only is the data encrypted but it can then be later removed altogether."

It underlines a recent shift in thinking away from the days when computer security centred on protecting computers, servers and laptops from being physically taken.

Today, the major risk is not in a computer being stolen but rather the loss of the data on it because it is not only worth far more to the company than the actual equipment but there is also the very real fear of public humiliation and a large fine to compound the misery of not having taken information security seriously enough.

Protecting retail data

Poundland, the cut price retailer, was prompted by the loss of a laptop (which fortunately contained no data of value) to work with Iron Mountain Digital to protect its corporate data.

It wanted to ensure that laptops could be secured, backed-up and then wiped if a device was stolen or lost. It ran a successful test of the company's back-up and data defence products before rolling out the technology to a hundred mobile devices used by its senior and area managers. It further plans to roll out the technology to its Hong Kong operations.

Nick Cater, Director of Field Operations, Europe at Iron Mountain Digital reveals, like many clients, Poundland was prompted in to action by embarrassing stories of lapses in the media and wanted to be in keeping with guidelines issued by the Information Commissioner's Office.

Mo Rahman, IT Services Manager at Poundland confirms that the retail chain was essentially looking for technology which, for a set budget, would leave its managers assured corporate data was safe.