



Safeguarding Your Reputation

In this article David Tomlinson, managing director for leading data security company, Data Encryption Systems (DES), takes a detailed look at how encryption can safeguard a company's reputation - and at the same time protect against unnecessary fines. Tomlinson's article explains in detail how simple encryption is to use and why it should be as common place in an organisations policies and procedures as installing antivirus software.

"A reputation for a thousand years may depend upon the conduct of a single moment."

English author, Ernest Bramah (1868-1942)

Loss of reputation

In February 2007, the Financial Services Authority fined Nationwide Building Society almost £1m for failing to have effective systems and controls to manage its information security risks. The failings came to light after the theft of an unencrypted laptop from a Nationwide employee's home.

The 'crime' was especially heinous when the FSA discovered that Nationwide was not aware that the laptop contained confidential customer information and did not start an investigation until three weeks after the theft.

The Nationwide fine followed close on the heels of the revelation by the TJX Companies group in the US of a massive data breach in which an 'unauthorised intruder' gained access to its systems over an 18 month period, and made off with nearly 46 million credit and debit card numbers of customers in the US, Canada and the UK. The data loss has so far cost TJX around \$17m, not to mention its reputation. It's not unreasonable to suggest that ultimately, it may cost the company its independence as well.

At the heart of these data breaches, and particularly at Nationwide, is companies' - or their staff's - unwillingness or inability to consider using encryption to safeguard their data. The reason has until now been the reasonable complaint that encryption sounds and has been difficult to use.

Protecting data

But its usage has arguably never been more vital because there is no such thing as an organisational perimeter any more. Data has to be taken out of the building, and information has to travel around between mobile workers, business partners etc. How should that data be protected? Well, encryption is the obvious answer, but there are numerous stories of customers struggling - and failing - to use encryption effectively.

Its perceived user-unfriendliness and fears of being left high and dry without their data has left users willing to take a risk, preferring to carry their unencrypted laptops with them at all times. Here are just a couple of examples I've come across:

We had engineering staff working over the Christmas break to complete a critical project for a major client. But everything had stopped while we awaited the final system design documents. After two or three hours struggling with the then leading data security product, our customer's head of software development finally uploaded a plain copy to our FTP site and asked us to encrypt it at our end. Faced with missing a project milestone he was forced into taking a risk with extremely sensitive data.



On another occasion, we were due to take delivery of documentation relating to banking security. Although we had signed a series of tightly worded non-disclosure agreements, when we asked how the documents were encrypted, the client's senior executive explained that they were no longer encrypted. She had recently made a transatlantic flight with the same information which was to form part of a critical technical presentation and found that the content couldn't be decrypted.

"I know its company policy to encrypt this information," she said, "but I haven't encrypted it because the last time I was at a conference, I couldn't access my presentation. Now, I'm 'once bitten, twice shy' when it comes to using it again. I didn't encrypt it because it was too important - I was afraid of not being able to decrypt it again."

Making encryption second nature

These examples sum up the current lack of confidence in encryption. Yet really, using encryption should be as easy as driving a car. You don't need to understand the technology to be able to use it. You just need someone to make the technology usable. These days no-one worries about using a choke on a car. You simply assume there is an engine management system. Likewise, if you use a microwave, you don't need to know how it works, just that it works!

The impetus towards more effective business use of encryption is now greater, because the current spate of data breaches has attracted the interest of the Information Commissioner, Richard Thomas, who has labelled them 'unacceptable'. Speaking at the launch of his annual report in July, Thomas said, "How can laptops holding details of customer accounts be used away from the office without strong encryption? How can millions of store cards fall into the wrong hands?"

Thomas's involvement, together with that of regulators such as the FSA, as Nationwide has found, means that encryption is now very much on the corporate agenda. What we need to do now is make it as second nature as firewalls and antivirus.

Easier said than done

How do we do that? Well, at the heart of the problems with public acceptance of encryption are training and terminology issues. Suppliers are continually coining new terms that even hard-bitten security analysts find hard to understand, never mind the public. You may recall a Not the Nine O Clock News sketch back in the 90s, which took the Mickey out of the public's lack of knowledge of hi-fi terms such as Dolby, tweeters, decks, gramophones, and amps. It's something like that with encryption.

There are also those so-called encryption specialists who say users 'keep asking the same stupid questions' when they don't understand. This is because the 'specialists' simply haven't taken the time and trouble to explain things correctly. What we need to do is sensibly 'dumb down' encryption, and get rid of the terrible terminology, so that users can be confident, and not hesitant, over its usage.

In these days of political correctness, it can be easy to cause offence by a misdirected email. That is why within organisations, both staff and management must be careful about what people can read, and protect companies' staff from each other, even when it comes to office 'funnies'. At DES all users have the DESlock+ email encryption tool installed; the company has produced an encryption key deliberately named 'Adult

Humour' which staff can request after taking responsibility for reading their workmates jokes. By encrypting these email messages, those without this key are saved the effort of taking offence.



Granular folder encryption

Some might say the answer to safeguarding data is to encrypt complete hard disks. Indeed, the US government positively encourages the companies it does business with to offer full disk encryption. But is it really necessary?

I believe selective encryption of information on PCs, rather than blanket encryption of the whole disk, is a much more practical alternative. Full disk encryption became popular when Gartner advised encrypting the hard drive, but it is only a partial solution. If I need to get my PC fixed by the IT department they need to have the entire disk decrypted first. If I just keep sensitive data in an encrypted folder, I do not have to decrypt anything: I just need the key to use the folder.

If you like the file, folder and email encryption are the locked cabinets and the safe; full-disk encryption is like locking the door. If an engineer arrives to service the air-conditioning (upgrade the anti-virus software), we have to let him in the door (past the full disk encryption). But we don't have to give him access to the locked cabinets (the company payroll files). Full disk encryption will allow you to do even stupid things with your data: leave your notebook in a taxi, bus or pub. And it will protect your data against the (probably) non-technical thieving-types. But it won't do anything to protect the data you need to send or save away from your computer. Granular folder encryption will allow you to do clever things with your data: encrypt files and folders with different encryption keys, encrypt email and attachments, make encrypted archives of your work and share all of this information securely with both exclusive and overlapping workgroups. But for those days when you forget to file that critical document in an encrypted folder, shut down and run for the train, full-disk encryption will also look after you.

The reality is that for most companies dealing with government and other large organisations, encryption is a "tick in the box they must have." And it's likely that within 3-5 years, encryption will be as prevalent as firewalls and antivirus, because if you want to be an approved supplier, you'll have to comply with the rules. And that doesn't just mean large firms - it will also affect the smaller organisations who work for those big companies. We are seeing that already happening with the need for companies to be Payment Card Industry (PCI) compliant for the safety of credit card data.

Ensuring encryption is on the business agenda

The PCI Data Security Standard (PCI DSS) requires merchants (and their partners) to encrypt certain cardholder information. Most US states now have laws that require merchants to announce when they have erroneously disclosed personal financial information that was not encrypted. Indeed, Visa and MasterCard can levy fines of up to \$500,000 for breaches in which the merchant failed to implement security measures. In my experience, these fines are larger and generally occur more often in situations where the merchant failed to use encryption. So encryption should undoubtedly be on your business's agenda.

Some of DES's users - such as Reading Borough Council, who have rolled our data encryption product, DESlock+ out to their mobile workforce (non-expert IT users such as social and care workers), have demonstrated in spades that encryption can work for their staff. What we now have to do is persuade all companies that file encryption - not necessarily disk encryption - is straightforward to do, and will pay off in the long-term. After all, as Nationwide and TJX have proved, what price can you put on any loss to your company's reputation?

- ends -