



Greig Ross Associates

Bringing Business Clarity and Value to IT

IT & DATA SECURITY LAPSES: MAKE SURE YOU'RE NOT NEXT

There is nothing the press loves more than a new security scandal – and there seems to have been an endless succession of them in recent times. The recent loss of 25 million names and addresses from the child benefits data base was described as “catastrophic” by the man responsible for data protection in the UK. But there seems to be plenty more that is yet to surface, according to Richard Thomas, the Information Commissioner. Apparently he has received a series of confidential enquiries from both public and private sector companies, confiding in him about problems with security inside their organisations.

Protecting confidential information is a business requirement, and in many cases also an ethical and legal requirement. Furthermore, it has also become a substantial element in operational and reputational risk. Of course, the importance of good governance and risk management is now well accepted, and retail financial services has more than its fair share of such disciplines. But none of these things necessarily mean that organisations are on top of the issue. Unfortunately the introduction of new systems, technology and changed processes has tended to disguise vulnerabilities – until they come to light in a glare of publicity with amazement as to how such a situation could have arisen. In many instances security breaches are not caused by technology failings but by a lack of common sense, inadequate communications and inappropriate delegation of responsibility. Lenders should be aware of the issues at stake, and of the best way forward in mitigating the increasing security risks their complex operations are running.

This article explores a few of the different security issues which we have uncovered during Health Check reviews in the last twelve months. It also highlights some high profile cases in this and other business sectors, where organisations have incurred substantial fines and reputational damage.

Mismanagement in processing data records

If you look at the Information Commissioner’s Office’s (ICO’s) own web site you will see that in January of this year the ICO took enforcement action against Carphone Warehouse. According to the Press Release, the investigation revealed that Carphone Warehouse and TalkTalk had been opening customer accounts in the wrong name and passing inaccurate information on to credit reference agencies and debt collection agencies. Security failings had also led to customers being able to view other customers’ account details online.

Unfortunately, from our experience this lack of processing governance and proper rigour in data checks and balances applies also to retail FS. We have come across all three issues in banks and building societies, i.e.:

- Opening customer accounts in the wrong name;

1 Trainers Brae, North Berwick, EH39 4NR.



Greig Ross Associates

Bringing Business Clarity and Value to IT

- Passing inaccurate information to credit reference agencies; and
- Customers being able to view other customers' account details.

All of these instances are, uncomfortably, far from rare. In addition, it is quite surprising how different mortgage lenders have differing views on how long certain pieces of personal information should be kept. The Data Protection Act stipulates that personal data should not be kept longer than is necessary; but we see that many organisations do not embrace the concept of data ownership, and in many cases data is retained significantly longer than is necessary, largely out of ignorance of the regulations involved.

Theft of remote IT devices

All retail FS organisations use a combination of laptops, PDAs and other mobile devices in the normal course of business operations. Indeed, laptop sales have now eclipsed those of desktops, a million Blackberries are sold each month and recent estimates suggest that a third of businesses now have people working away from the office for more than 20% of their time. That is why, according to Information Age, the number one most adopted strategy in 2007 was “Encourage/Support Remote/Mobile working”. The flip side of this march forward is that these devices are specifically vulnerable to theft; and in many instances, unfortunately, the information on them is not locked down or encrypted. Quite apart from the cost and inconvenience of the theft and the loss of internal business information is the far more serious loss of customer and internal staff personal information. And thefts of mobile devices, complete with personal data, are becoming a regular occurrence.

The most high profile case in the mortgage lending sector was that of Nationwide, fined £980,000 last year by the FSA for allowing the theft of a laptop containing millions of customers' records. Interestingly this was from an employee's home, and indeed Nationwide claimed that the information on it could not have been used for identity fraud as there were no PIN numbers, passwords or account balance information on it. Given that the missing data was therefore not nearly as comprehensive as it might have been, nor the manner in which it was lost particularly negligent, the scale of both the negative publicity and the FSA fine is the clearest warning that organisations dare not run this type of risk. More recently the ICO found Skipton Financial Services (SFS) in breach of the Data Protection Act following the theft from a SFS contractor of an unencrypted laptop containing the personal information names, dates of birth, national insurance numbers and investment amounts of 14,000 SFS customers. The ICO ruled that SFS should have had appropriate encryption measures in place to keep the data secure.

Another high profile case happened in January of this year. Marks & Spencer broke the law by allowing the details of 26,000 employees to be held on a laptop without the protection of encryption, according to the Information Commissioner's Office; and the

1 Trainers Brae, North Berwick, EH39 4NR.



Greig Ross Associates

Bringing Business Clarity and Value to IT

laptop, and the information on it, was stolen. Marks & Spencer have been ordered to ensure that all laptop hard drives are encrypted by April of this year, and could face criminal charges if it fails to comply with the enforcement notice issued by the ICO.

Disposal of Personal Data

High street banks are throwing customer information into bins outside their premises in breach of the Data Protection Act, according to privacy watchdog the Information Commissioner. After naming and shaming them, the Information Commissioner's Office (ICO) has forced 11 banks and financial institutions to sign an undertaking to stick to the Principles specified for the handling of customer data in the Data Protection Act.

Although businesses have been aware that such practices are unlawful it is amazing that major financial institutions are carelessly discarding their customers' information and not taking security seriously. If they do not, they not only risk further action from the Information Commissioner but also risk losing the trust of their customers. The British public is becoming increasingly security conscious, as the rise of personal shredding machines testifies, and in this light it is clearly vital that customers feel confident that banks and other organisations are safeguarding their personal information. Whilst cost-cutting within retail branch environments often seems to be blamed for this type of local administrative shortcut, it is a poor defence and one that will cut no ice with the media or the ICO.

Indeed, I sometimes wonder whether the senior management is actually aware of the detailed working practices of their staff. In many instances there is a gap between what the board and senior executive believe is happening and the people on the ground who are entrusted with operational processes. We recently uncovered a collection of complete electronic data files which the senior team had believed were being regularly destroyed, but which were actually lying in cardboard boxes in a warehouse, and scheduled to be dumped along with other office rubbish.

Passwords

In all organisations there is recognition that certain controls are necessary to protect sensitive information and prevent unauthorised access. In this regard, the focus tends to be on implementing ever more sound and complex security arrangements such as single sign-on, complex passwords and identity management. However, to give some indication on the vulnerability of passwords, in a survey carried out on commuters at London's Victoria Station a few years ago, two out of three workers gave complete strangers their company password upon request. In addition we regularly encounter the following situations:

- People transferred to new departments still have the ability to view and amend data from their previous departments

1 Trainers Brae, North Berwick, EH39 4NR.



Greig Ross Associates

Bringing Business Clarity and Value to IT

- Staff who have left the organisation still have access to the business systems up to five years after they have left

Passwords can be a maze, simply because of their proliferation. Anyone who has more than one pin number to remember understands the problem when confronted with trying to complete a transaction. In one organisation we visited last year some employees had twenty two different passwords many of which were changing monthly. Their imagination and ingenuity was stretched to the limit in managing to write down these passwords while keeping them concealed. The problem is intensified when businesses have mixtures of full time, contract and part time employees, and adds a new dimension when work is sent off-shore.

Then there is the management of these password systems. IDC provide a frightening insight into the hidden cost of password management:

1. Each year the average large company with four to eight applications spends 0.83 hours per user managing passwords
2. For 5,000 users this requires more than two to four full time help desk workers dedicated to password management alone
3. 60 percent of all users call the help desk at least once per month to get help with a password, at an average of 25 minutes per call
4. For 5,000 users this means many hours in lost user productivity per month.

But passwords themselves are vital for PC security, even within the office. One client had a recent break-in which resulted in the thief taking the only items they could get their hands on: a single desktop computer, which was not locked down.

Licenses

Do mortgage lenders have the correct number of licences for running their business? In our experience the answer is often no. The Federation Against Software Theft (FAST) promotes the legal use of software by enforcement, lobbying and education. In a recent software audit of 2,500 PCs at a UK financial institution FAST discovered over 5,800 illegal digital music files. Most of these files had been illegally downloaded by people in the IT department – those normally tasked with combatting the problem. We are aware of one or two clients who are reviewed annually by FAST; and more often than not new licences require to be purchased as a result. In 2004 FAST moved from seeking civil to criminal prosecutions.

Sometimes, however, organisations have too many licences, rather than too few – and usually for the same reason of lack of proper control. We regularly come across this situation with mortgage lenders. In one case a client had been continuing to pay for ten licences even though the software had stopped being used two years previously.



Greig Ross Associates

Bringing Business Clarity and Value to IT

Clean Desk Policy

In a recent survey a sizeable number of organisations admitted that their employees did not remember the last time they saw their desk because it was so cluttered with documents. Quite apart from the benefits in terms of efficiency and paper reduction, there is a view that locking important documents away at night improves security. We have found that many mortgage lenders have a fully operational clean desk policy, although there are still a few which do not. A number of these admit that important information, including customer records, passwords and personnel information is open to view and violation; but they do not have this as a priority to address.

Disaster Recovery

It is surprising just how many organisations do not have a disaster recovery plan and have no guidance as to what to do in the event of a serious loss of service. For those that do, it is again surprising how expectations at the Board level are not matched with ability on the ground. In one organisation which had most elements in place, and robust checks supposedly carried out by the IT department, we discovered that the user departments were unable to access the systems from the secondary site despite these having been tested regularly by the IT department for the previous three years.

Double-checking of the disaster recovery processes at another client closer revealed that some of the key supporting systems were simply not being catered for in the event of a system failure. These supporting systems were essential to performing the day to day business operations. At another site the IT Director, who had since departed, had started down the road of daily backups to the offsite location but had not completed the job. Nevertheless the business had continued to run with only part disaster recovery for the following three years, in the belief that everything was professionally in hand.

The Way Forward

Nowadays Mortgage Lenders are all too aware of IT security issues and spend some significant time trying to ensure that good practice and governance is put in place. Our experience however, has shown that both the time taken, and the effectiveness of the governance processes, varies quite significantly from business to business. Larger organisations have dedicated teams of security specialists, all suitably qualified and working to appropriate security standards. However, the more complex the environment the more scope there is for problems. In other organisations, particularly where there is a strong third party relationship, there tend to be much weaker plans and processes, and a lack of security ownership and responsibility.

Given that these are audit and control issues, many Mortgage Lenders understandably – but mistakenly – believe that their external auditors and other external governance bodies



Greig Ross Associates

Bringing Business Clarity and Value to IT

will detect problems and bring them to their attention. It is vital to remember that these organisations' principal focus is compliance, and although they do stray into security their involvement here tends to focus on more text book issues. Whether lenders' key concern here is their customers, the media or the regulator, these are issues that cannot simply be treated as minor administrative matters. They are deeply linked to your organisation's operational and reputational risk. Give them a closer look, before your stakeholders do.