



Key Contact

Chris Harris
charris@bovill.com

“...there is often a lack of a co-ordinated approach and too much focus on IT controls”

London office
82 Blackfriars Road
London
SE1 8HA

Phone: 020 7620 8440
Web: www.bovill.com

DATA LOSS IN FINANCIAL SERVICES FIRMS – RECOGNISING THE THREAT

July 2008

Overview

Having controls in place to recognise and minimise the risk of loss and theft of data is a key tool in the fight against financial crime. FSA’s Principle 3 requires firms to take reasonable care to organise and control their affairs responsibly and effectively with adequate risk management systems. This is expanded upon in the Systems and Controls Sourcebook which requires firms to “take reasonable care to establish and maintain effective systems and controls for compliance with applicable requirements and standards under the regulatory system and for countering the risk that the firm might be used to further financial crime”.

Financial services firms generally hold much customer data which is necessary for them to carry out their business effectively and compliantly. Customer data is identifiable personal information about a customer held in any format, such as NI numbers, addresses, date of birth, family circumstances, bank details and medical records and is a valuable commodity for criminals, for example to facilitate identity theft. Having effective controls in place to protect and secure such data is also the responsibility of the firm under the Data Protection Act 1998.

In 2007, the FSA conducted a review of data security controls in financial services firms. The results were published in April 2008 and concluded that poor data security is currently a serious, widespread and high-impact risk to the FSA's statutory objective to reduce financial crime. In many cases FSA found that firms failed to identify the value criminals place on data and also underestimated the risk of loss or theft of customer data.

The review reported that the resources firms dedicate to data protection, including the prevention of loss and theft of data, are often inadequate. The FSA found that even when resources are adequate, there is often a lack of a co-ordinated approach and too much focus on IT controls. Many firms fail to assess the risk of their exposure to data loss or theft incidents and firms often fail to consider the wider risks of identity fraud arising from a significant case of data loss. Some firms have a greater concern about adverse media coverage than about being open and transparent with their customers. There is often also a failure to allocate accountability for data security to a single senior manager, which often results in significant weaknesses in systems and controls.

Which areas should firms be considering?

It is clear that data security is not something that is just dealt with by IT. It goes much wider than the controls around hardware, software and laptops. We highlight below some of the additional actions that can be taken.

Data Security Policy

Firms should have a well defined and understood policy. The FSA found that larger firms had adequate policies but the implementation was “patchy”. Training of the relevant

front line staff is also important to get right here. It should not focus only on legislation and should cover how people are expected to implement the policies on a practical basis. It is also important to test staff's understanding of the policies and what they should do in various real life situations.

Vetting of Staff

It is important that all members of staff are vetted but, from a data security perspective, some should attract more scrutiny than others. It is often senior staff that go through the most stringent checks, with little consideration of the risk that junior staff with access to large amounts of customer data might pose. The FSA found that very few firms conduct criminal records checks on junior staff and few firms do repeat vetting during the course of employment to determine whether the individual's circumstances have changed, thus making them more susceptible to corruption and financial crime.

Access to Records

Access to computer records is usually well controlled in larger firms where there are likely to be controls in place to allow access only to the data relevant to the role of the individual. In smaller firms, it is not unusual for staff to have access to all client data regardless of whether they need it. A further consideration here is the control of access to paper records.

Paper Records

Notwithstanding some high profile examples of firms failing to dispose of customer records properly, there are generally good controls surrounding the disposal of confidential paper with most firms shredding sensitive documents in a secure fashion.

Storage and transfer of electronic records

Encryption of data is the appropriate approach here. Not everyone completely mitigates the risk of data loss via laptops, USB devices and the internet. Few firms lock USB ports and CD writers or encrypt laptops and USB devices. Some do not use password protection on handheld devices. The FSA also stated in their report that many firms fail to recognise the need to block web-based communication facilities such as internet mail and instant messaging.

When transferring data to and from third parties, it is sensible to use a secure internet link. Some data is transferred via email, internet, or on portable media (CD, USB stick etc) which are not encrypted. As has been reported in the Press sometimes computer disks do not reach their destination. Once more, the FSA pointed to rare occasions when firms have sent unencrypted data by unregistered post.

Third Party Suppliers

There are further issues to consider in relation to data security when some functions of the business are outsourced e.g. clearing and settlement. Some firms use third party suppliers for IT maintenance and backing up electronic files and archiving/disposal of paper documents. Firms should proactively check how their third party suppliers vet their employees, and the security arrangements they have in place to protect their client data; and at a more basic level, consider the risk of allowing office cleaners and security staff access to their business premises.

Properly considering all of the relevant data security issues, together with an appreciation of how they potentially relate to financial crime, means there is more work for firms' compliance officers and money laundering reporting officers. Firms need to ensure they are adequately covering these areas in order to combat effectively the ever resourceful criminal.

Manchester office

**Barnett House
53 Fountain Street
Manchester M2 2AN**

Phone: 0161 247 8562
Web: www.bovill.com