

# Keeping an eye on your data



A year is a long time in the financial markets, and this last year has been a particularly long and torrid one for many firms working in the financial sector.

Given the size and number of new concerns that now populate the regulatory agenda it would be easy to forget what was on the FSA's mind a year ago when it published "Data Security in Financial Services".<sup>1</sup>

This has inevitably slipped into the background given the focus on the banking sector, toxic assets etc. However it certainly will not have gone away. In fact, as the dust settles and work continues on a revised and more intrusive regulatory regime, data security is certain to come back on to the agenda.

So what has your organisation been doing to get its data security into shape? Will you be able to pass an FSA review on this subject which will inevitably come?

Let's remind ourselves what the FSA was saying a year ago.

## Governance

- Firms need to consider data security as a specific issue – it's not just an IT issue.
- The right people at the right level of seniority need to be involved.
- A risk assessment of the whole business should be carried out, using outside expert help if necessary.
- Ensure policies and procedures are relevant and implementable by front line staff.

## Training and awareness

- Make sure that your staff understand the policies and procedures and can work with them.
- Staff must understand that data is an extremely valuable commodity for criminals.
- Don't assume that your staff know what they have to do.
- Focus on high risk areas.

## Recruitment and vetting

- Vetting of staff should take account of the data and fraud risks the organisation is running.
- Organisations must understand the vetting procedures utilised by the recruitment agencies they use for both temporary and permanent staff and supplement these where necessary.
- Any threat posed by existing staff should be considered and back checking performed where appropriate.

## Controls

- Controls in offshore operations are your responsibility.
- Access rights – generally speaking, too many people have too much access to too much information! All access should be granted on a need-to-know basis.
- Everyone should have an individual user account, protected by a strong password.
- Risk-based monitoring of access to customer data should be considered.
- How effective is your customer authentication process?

<sup>1</sup> See [http://www.fsa.gov.uk/pubs/other/data\\_security.pdf](http://www.fsa.gov.uk/pubs/other/data_security.pdf)

- Data back-ups should be as treated as securely as the data that is backed up.
- Access to the internet and email must be controlled appropriately.
- You should be aware of the risks posed by key-logging devices, and consider regular sweeps on a risk basis.
- Laptops pose an obvious problem where they are taken offsite and are not fully encrypted.
- Portable media including USB devices and CDs need good management to mitigate against data security risks.

### Physical Security

- An area where many firms fall down, but which can be supported by a robust security entry system to premises.
- Entry passes are a typical weak spot in many firms. A delay in cancelling passes of leavers is an example. An effective starters and leavers process is vital.

### Disposal of customer data

- Many firms are quite good at disposal of hard copy, paper based data records. However, when was the last time you checked the procedures at your outsourced offsite storage facility?

- Disposal of electronic equipment holding data is less robust. PCs are all too often disposed of with the hard drives still intact. That is all useful data.

### Management of third party suppliers

- How does the third party manage and secure your data?
- Who has access to it
- How is it transferred between the two firms?
- Does the third party have equivalent staff vetting procedures?
- Don't rely on the contract to absolve you of responsibility in the event of a breach.

There is a lot to be considered when thinking about protecting your data from improper use. Imagine the consequences of client information getting into the wrong hands. Clearly, the financial consequences can be pretty bad. The inconvenience of fraud on your clients will not endear you to them. But most significantly, the hit on an organisation's reputation can be catastrophic.

Kingston Smith Consulting has highly experienced practitioners in the field of data protection and information security. We would be delighted to meet to discuss any concerns you may have in this area and work with you to implement cost-effective measures to address them.

---

## About Kingston Smith Consulting LLP

Kingston Smith Consulting is the specialist consulting practice associated with the top 20 accountancy firm Kingston Smith LLP.

Kingston Smith was originally formed in 1923 and the firm has grown to its current position through organic growth and mergers. Kingston Smith is a member of KS International which is an association of independent accounting firms in 49 countries around the world:

Argentina	Australia	Austria	Bangladesh	Belgium
British Virgin Islands	Canada	China	Cyprus	France
Germany	Guernsey	Hong Kong	Hungary	India
Indonesia	Ireland	Isle of Man	Israel	Italy
Japan	Jersey	Luxembourg	Macau	Malaysia
Malta	Mauritius	Mexico	Netherlands	New Zealand
Norway	Pakistan	Peru	Philippines	Poland
Portugal	Russia	Singapore	South Africa	South Korea
Spain	Sweden	Switzerland	Tunisia	Turkey
United Arab Emirates	United Kingdom	Uruguay	USA	

### Kingston Smith Consulting LLP

Devonshire House, 60 Goswell Road, London EC1M 7AD, UK Telephone +44 (0)20 7566 4000 Fax +44 (0)20 7566 4010  
 info@kingstonsmithconsulting.co.uk www.kingstonsmithconsulting.co.uk

A list of partners is available for inspection at the above address.

Registered in England and Wales as a Limited Liability Partnership: No OC341786 Registered office: Devonshire House, 60 Goswell Road, London EC1M 7AD