Data security comes under the spotlight

Mar 05 2009 Bridget Treacy and Natalie Hunt ***Complinet exclusive***

Bridget Treacy

Senior management recognition of the impact of financial crime, and the need to invest in combating it, play an important role in tackling the problem, according to the Financial Services Authority's stakeholder survey. In the current economic climate, financial crime is likely to increase and companies must be vigilant in ensuring that they have in place effective security procedures to prevent financial loss for customers. The FSA's survey highlights the fact that data security has gained greater visibility as an issue. Consequently, the FSA intends to undertake further work to focus on identity theft in the context of offshoring, marketing and systems and controls. Senior management responsibility for data security is an emerging theme for regulators.

FSA stakeholder survey: key issues raised

International market research authority GfK NOP undertook the financial crime stakeholder research for the FSA, which was published in January 2009. The primary objective of the research was to assess the impact of financial crime and to consider the ongoing effectiveness of the FSA in managing financial crime since the previous report published in 2006. The research's findings are hardly surprising, but it is interesting to see that:

- senior managers, particularly in large firms, are increasingly recognising the importance of financial crime;
- financial loss to clients is a greater concern to firms than financial loss to themselves;
- identity fraud is expanding its reach, with increased evidence of "phishing", spamming and online crime, deliberate targeting of lost data, alongside old fashioned methods of identities stolen from the post; and
- 55 per cent of firms responded that their firm had increased their focus on data security and ID theft over the last year.

The research pre-dates much of the current economic turmoil, although respondents noted the impact of high profile data losses on the way in which they address data security and noted that data breaches dovetail with an increase in ID theft and crime. The quantitative research suggests that data protection now has greater priority within firms than previously.

In addition to canvassing opinion on the incidence of financial crime generally, the research asked stakeholders to assess the effectiveness of the FSA in meeting its statutory objective to ensure that firms have adequate systems and controls in place to tackle financial crime. Overall, the FSA's strategy of seeking to reduce the opportunities for crime, rather than dealing merely with the consequences of crime, was

praised. In particular, respondents appreciated the FSA's role in raising public awareness of the potential for financial crime.

Interaction with other regulators

One issue raised for further consideration was the perceived need for the FSA to act consistently with, and to cooperate with, other regulators. This need for cooperation and consistency between regulators is frequently raised as a concern by firms dealing with data breaches. At present, the FSA has the power to impose fines on firms which fail to ensure adequate systems and controls. The first high profile data breach involved the Nationwide Building Society in 2007 which was fined almost £1m following a stolen laptop. In that case the FSA emphasised that the level of fine (which had been discounted by 30 per cent in response to Nationwide's cooperative approach) was intended to act as a deterrent and reflected the fact that the firm's internal procedures for dealing with a data breach incident were lacking.

Since Nationwide, the HMRC data breach occurred. This fundamentally changed public awareness of and tolerance for poor data security procedures. HMRC triggered a raft of reports and much criticism of the enforcement powers of the Information Commissioner who, in the arena of data breach, exercises concurrent jurisdiction to that of the FSA. During 2008, the Criminal Justice and Immigration Act was passed, amending the Data Protection Act 1998 to give the Information Commissioner the power to impose fines for serious breaches of the Data Protection Act, including security breaches. It is widely anticipated that those powers will come into effect later this year and that the Information Commissioner will impose fines of a similar order of magnitude to those imposed by the FSA to date. Firms regulated by the FSA are keen to learn how the Information Commissioner and FSA will cooperate in the exercise of their overlapping powers to fine for serious data breaches.

A further issue highlighted by the research is that respondents were reluctant to comment on the interaction between the FSA and other crime agencies such as the Serious Organised Crime Agency and the National Fraud Strategic Authority. It appears that there is not enough general knowledge of how these agencies work together.

Management take ownership of data security

There is an emerging trend, highlighted by the research and underscored by the current economic climate, of stakeholders seeking to ensure that senior management are accountable to stakeholders. This trend is also evident in the context of data security. Most recently, the Information Commissioner launched a "personal information promise", a series of data protection promises to which an organisation would publicly indicate its commitment by a senior executive signing the promise. Although the Information Commissioner's Office does not consider the promise to create any additional legal risk for firms which sign up, there is understandable caution from many organisations about committing to "go further than just the letter of the law" (as required by the promise) when handling personal information. Of significance is the fact that the promise needs to be signed by a senior executive. This is part of the Information Commissioner's drive to ensure that data protection and data security are board level issues.

Data security as a key issue for 2009

Data security will remain one of the key risk issues for the year ahead. The pressures of the current economic climate, the expectation of the general public that their data will be safeguarded and a focus by regulators on data security will ensure that this issue remains at the top of the risk agenda. In a market which seeks senior management accountability for regulatory failings, data security will become a board level issue, if it is not already.

• ***Bridget Treacy*** *is a partner at Hunton & Williams and leads the UK Information Management Practice. She may be contacted at btreacy@hunton.com.* ***Natalie Hunt*** *is an associate in the UK Information Management Practice at Hunton & Williams and may be contacted on nhunt@hunton.com.*

This article first appeared on Complinet on www.complinet.com on March 05 2009. For a free trial of Complinet's services, please contact client support on client.support@complinet.com or +44 (0) 870 042 6400.