

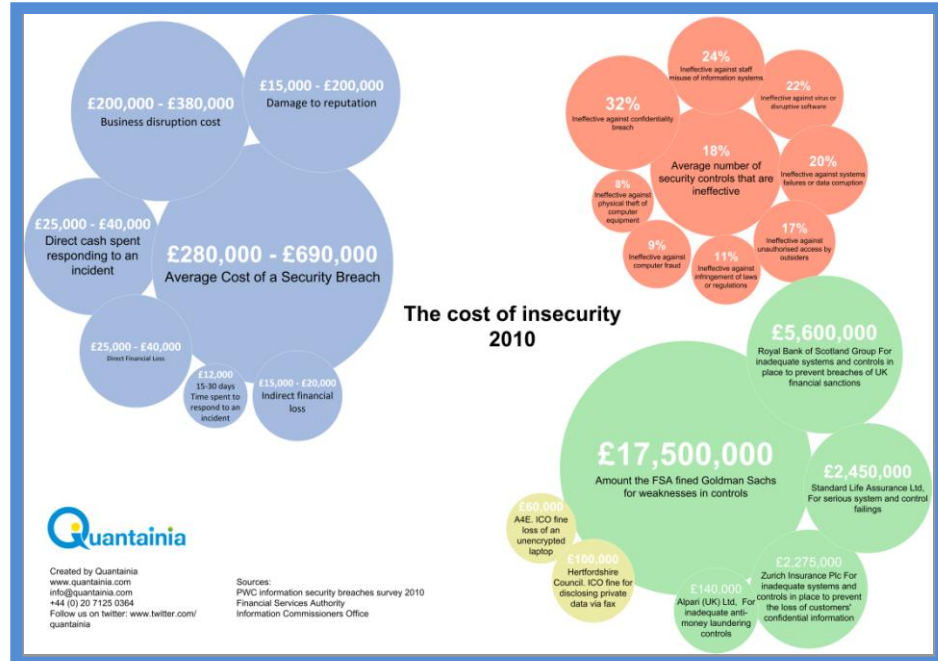
# The Cost of Insecurity

Javvad Malik & Simon Walker  
December 2010

**2010** has been notable for a number of reasons, the advent of a coalition government in the UK, followed by swinging spending cuts, and a turbulent economic picture. In a regulatory sense, too, 2010 stands out: increasingly active regulators have increased fines for organisations which are found to have failed to comply with basic levels of protection around data. A new record was set with the £17.5 million FSA fine on Goldman Sachs. Moreover, the emphasis has broadened – rather than the ICO and FSA focusing solely on the financial sector. Both Hertfordshire County Council and A4E were the subject of fines for weak controls around personal data. At the same time, other regulation continues to apply – many organisations are struggling with PCI-DSS compliance, not only in the commercial sector, but also in the state sector, where cards are important for covering payments for basic services.

## ***Effective Information Security Management isn't about implementing a few technology solutions and neither can it be outsourced.***

While no definitive source of data exists, available indicators suggest the average cost of a security incident has continued to increase over previous years. This is a result of two factors; the ever-increasing reliance on technology in business process, and the increasing sophistication of attackers.



At the same time, many organisations appear to have not yet taken adequate measures to protect their information assets—sources suggest that, in a test sample, 32% of controls were ineffective against confidentiality breaches. Hence, old problems can still be seen to persist.

The UK Government, despite the downwards pressure on spending, is taking the evolving cyber threat landscape seriously. Some £650m is the projected spend on protecting both national infrastructure and individuals. This is of huge significance, as it represents a shift of emphasis from merely protecting the elements of state, to accepting the importance of protecting wider interests, including the digital elements of the UK economy.

***The right mechanisms need to be in place. The monitoring and analysis capability, the right management structure, technology, business process, and vitally, the human factors.***

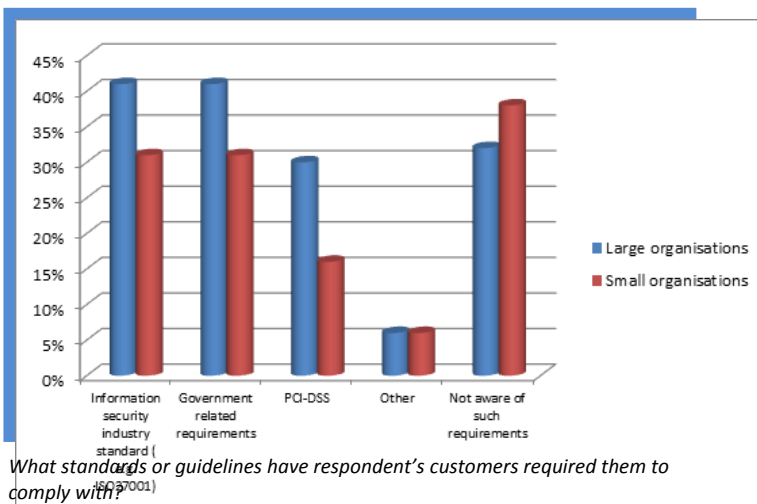


## What the future holds

In June 2010, the Chancellor of the Exchequer, George Osborne, announced plans to abolish the FSA. One of the fundamental reasons for this change is the perception, justified or otherwise, that the FSA had not been adequately successful in its mission around regulating the financial sector and, importantly, protecting the financial sector's customers.

What is likely to follow is the raft of new regulatory agencies wishing to make their mark, in part by being more rigorous than the FSA. This is strongly suggestive of a more complex, and more rigorous, regulatory environment. At the same time, new standards are in the process of emerging; the British Standards Institute has standards in development around the security of data in a medical context (ISO/TC 215 / SC WG7 N 815 and ISO/TC 215 / SC WG 4 N 818), while there have been discussions around a new standard for information security management, focused on the economic aspects

If regulators are seeking to make examples, then they are likely to initially focus on high profile subjects. This will inevitably mean more fines for the financial sector, as well as other bodies which have extensive sets of personally identifiable and financial data: local government, marketing firms, legal practices, healthcare bodies and retailers would all fall into this category. This is likely to have a trickle-down effect – larger organizations will increase pressure on their suppliers and partners to demonstrate the effectiveness of their controls around data as a condition of doing business. This effect is already discernable. Over the past two years, banks in the UK have considerably ramped up the level of scrutiny on third party bodies which handle their information.



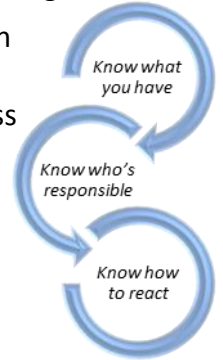
What standards or guidelines have respondent's customers required them to comply with?

Source: PwC information security breaches survey 2010

## An ounce of prevention...

While old problems still persist, the costs of failing to address them are set to increase. Moreover, this applies not merely to large organizations, or to those sectors which have traditionally had the highest emphasis on information security controls, but also new sectors, and the suppliers of large businesses.

A defence in depth approach is vital, spanning not merely technology, but also business processes, your staff, and your business partners, suppliers, and customers.



Three key principles are essential to doing this:

### 1) Know what you have

Knowing what you have is critical – this allows you to gauge both whether existing controls are sufficient and effective.

### 2) Know who's responsible

Everyone in an organisation should know who's responsible for information security. All key stakeholders need to be aware of what is needed from them – management, technologists, and staff alike. A clear statement of the requirements on each stakeholder needs to be documented in a policy.

### 3) Know how to react

There are two levels to this. The first level is the immediate mechanism for reacting to an incident; the second is the process for examining the root cause of an incident.



Javvad Malik  
Simon Walker

Quantainia

Hamilton House, Mabledon Place, London. WC1H 9BB

+44 (0) 20 7125 0364

E: [info@quantainia.com](mailto:info@quantainia.com)

[www.quantainia.com](http://www.quantainia.com)