

# How to prepare a risk assessment audit

## *A Financial Services Perspective*

This whitepaper is intended to assist UK-based financial service professionals when assessing areas of data security risk in their practice.

The paper highlights two main risk areas surrounding information security in financial practices; data loss and data exposure, and presents a framework for developing a risk assessment audit. It is of use to both sole practitioners and firms offering financial advice or services within the United Kingdom. For more information on data protection - visit the Financial Services Authority website (<http://www.fsa.gov.uk/>).

# Contents

1.0 Introduction	3
2.0 Purpose and structure	3
3.0 Risks to data	4
3.1 <i>Data Exposure</i>	4
3.2 <i>Data Loss</i>	4
3.3 <i>Risk perception</i>	5
4.0 Causes	6
4.1 <i>Causes of Data Exposure</i>	6
4.2 <i>Causes of Data Loss</i>	6
5.0 Risk assessment	7
5.1 <i>Identifying information assets</i>	7
5.2 <i>Threats, likelihood and impact</i>	7
5.3 <i>Risk reduction, avoidance and transfer</i>	7
6.0 Conclusion	9

## 1.0 Introduction

Data security regulation in the UK is changing. As of April 6<sup>th</sup> 2010 the Information Commissioners Office can issue fines of up to £500,000 for any breaches of the Data Protection Act. This is a sharp increase in the previous maximum fine of only £5000 but is reflective of a growing impatience amongst UK regulatory bodies.

In recent times, cases of company data loss or exposure have become a common feature in national tabloid and broadsheet newspapers. Regulation authorities like the Financial Services Authority (FSA) see these incidents as a direct threat to the reputation of the UK financial services industry. The new fining system and a subsequent awareness campaign is designed to stop the growing number of negligence cases and move to replace confidence in the UK financial services market, both domestically and abroad.

Much of the media coverage on incidents of data exposure and loss have been linked back to basic insecurities in data backup and encryption methods. Firms and individuals are being encouraged to seek out more secure, reliable and manageable data protection solutions if they are to meet current regulatory requirements and maintain goodwill.

## 2.0 Purpose and structure

This document is designed to assist responsible professionals in understanding the risks involved when managing business data and to help raise awareness to the causes of data loss and exposure. It will present a framework for producing a risk-assessment audit in a financial practice. This aims to assist sole practitioners and IT administrators employed by firms, in devising plans to manage their own and client-sensitive data.

It is good practice to review risk-assessments regularly in light of market developments. Further guidance on data security in financial services can be found on the Financial Services Authority website ([www.fsa.gov.uk](http://www.fsa.gov.uk)).

## 3.0 Risks to data

There are two key areas of risk involved when handling business data. Whether it is client specific or internally relevant, the exposure or loss of sensitive data can have a severely detrimental effect on an organisation.

### 3.1 *Data Exposure*

Laptops and other mobile devices are now common place and widely used throughout the financial services industry. The widespread connectivity, while improving productivity, has also made it easier for unauthorized bodies to access sensitive data and use it for unauthorized purposes. Data outside office walls is more vulnerable and difficult to manage, highlighted by the growing number of exposure cases and fraud related crimes in the media.

Between late 2007 and late 2009 over 800 data security breaches were reported to the Information Commissioner's Office (ICO)<sup>1</sup>. The most common incidents of exposure are related to lost or stolen unencrypted USB drives and laptops although virus attack and employee misuse are also a frequent alternative cause of blame.

The consequence of data exposure is often difficult to monetise. While issued fines are significant, the damage to company or professional reputation may result in longer-term penalties. Indeed, the FSA has the right to suspend or remove a company from the financial services industry altogether if they believe it to be appropriate.

### 3.2 *Data Loss*

While exposure is an issue that garners the most attention from regulatory bodies and the media, data loss can have an equally damaging effect on a firm. Uninhibited access to intellectual property and client information is critical for ensuring the on-going efficiency of a financial services practice.

The FSA actively promotes a number of retention-related regulations to ensure files and evidence can be reproduced on demand. One example being the requirement to securely store client financial records for up to seven years, monitored under current audit laws of the Inland Revenue. In addition to the obvious legal ramifications of not being able to produce certain information on demand, several productivity issues related to lost data.

Instances of data loss are strongly linked to unreliable or untimely methods of backup. Hardware and software failure, corruption and human error happen unexpectedly and unless a reliable backup copy of data is available for recovery, it can lead to missed deadlines, lost intellectual property and potential damage to goodwill. One of the key problems experienced by accountants when they lose data is an inability to access their client's files.

1. 'Report data breaches or risk tougher sanctions, warns the ICO (<http://www.ico.gov.uk>)

### 3.3 *Risk perception*

While many firms and professionals are to some extent aware of the risks of data exposure and loss, statistics show that remarkably little is being done to negate them. According to a 2008 ICT report from the British Chambers of Commerce, while 67% of firms are concerned about security aspects of doing business electronically only 49% of smaller businesses carry out regular assessments on vulnerability.

A FSA survey conducted in 2009 found that many firms failed to identify all aspects of the data security risks they face for three main reasons:

1. Some do not appreciate the gravity of the risk;
2. Some do not have the expertise to make a reasonable assessment of key risk factors and devise ways to mitigate against them;
3. Many fail to devote or coordinate adequate resources to address this risk.

Following the findings of this report the former Information Commissioner, Richard Thomas, stated:

“I am disappointed – but not altogether surprised – that the FSA has found that financial services firms, in general, could significantly improve their controls to prevent data loss or theft. The blunt truth is that all organisations need to take the protection of customer data with the utmost seriousness. Getting data protection wrong can bring commercial, reputational, regulatory and legal penalties. Getting it right brings rewards in terms of customer trust and confidence.”<sup>2</sup>

2. Data Security in Financial Services ([http://www.fsa.gov.uk/pubs/other/data\\_security.pdf](http://www.fsa.gov.uk/pubs/other/data_security.pdf))

## 4.0 Causes

To better prepare for the risks related to data loss and exposure it is important to identify what their key causes are.

### 4.1 *Causes of data exposure*

For the sole practitioner, small or medium firm, the most common causes of data exposure are associated with:

- Laptop loss or theft;
- USB or external hard-drive loss or theft;
- Virus infection;

Recent figures from police forces show that over 34,000 laptops are reported stolen each year in the UK<sup>3</sup>. A research project by Dell found that more than 3,300 laptops are lost or go missing at the eight largest airports in EMEA each week<sup>4</sup>.

The frequent loss of USB memory sticks by NHS employees recently saw a campaign led by members of ISEEU Global to ban the use of the devices altogether as a number of high profile misplacement cases hit the headlines<sup>5</sup>.

Microsoft also frequently promote the fact that consumers and businesses can easily become victims of a security breach if they unwittingly download files which are shared online and breach copyright.

### 4.2 *Causes of data loss*

The most common causes of data loss for financial firms are associated with:

- Hardware failure;
- Software corruption;
- Virus attack;
- Human error.

Hardware or system problems are by far the most common causes of data loss. It could be hard-disk drive failures, memory errors or incidents of power loss. The significant problem is that the majority of program data is stored on a computer's hard-disk. Software failure is also another common cause of data loss especially if downloaded or installed programs are buggy or poorly designed.

Viruses can also cause data loss, sometimes in the efforts made by users to remove the virus from their system or by the virus itself. Human error - another possible source of lost data - usually related to accidental file deletion or overwriting good data with bad data.

3. 'Laptop Theft – An Insider's Guide To Not Becoming Another Statistic (<http://creativematch.com/viewNews/?91257>)

4. The Human Factor in Laptop Encryption: US, UK & Canadian Studies, Dec 2008 (<http://www.ponemon.org/data-security>)

5. Call for security warning on USB memory sticks in NHS (<http://www.bjhcim.co.uk/news/2010/n1003042.htm>)

## 5.0 Risk Assessment

After understanding the causes and consequences of data loss and exposure, firms should assess what they are already doing to negate data security risk in their practice. Carrying out a risk assessment audit will help individuals and organisations develop a rigid data protection plan. The extent of these plans, however, will depend on a number of factors.

For a sole practitioner any risk assessment is likely to rely on the effective protection of data stored on a laptop or desktop computer. For the IT administrator of a medium-sized firm, a risk assessment may go on to form a comprehensive network protection policy. To ensure that the appropriate level of consideration is taken, the subject should ask themselves a series of questions:

### 5.1 *Identifying information assets*

The first action is to identify and categorise information assets. What resources am I using? Whose data am I responsible for? Most people probably already know which information is the most sensitive or valuable; for example, confidential client data, staff salaries or internal management papers. Each of these might form a category of data requiring a particular level of protection.

Identifying the various categories of information held is an essential prerequisite to securing it appropriately and effectively.

### 5.2 *Threats, likelihood and impact*

The next stage of the risk assessment process is to map the range of threats to those information assets. This process could point to a different range of (sometimes overlapping) threats; for example, theft by a third-party will compromise an information asset's confidentiality, whilst staff error could affect its integrity; a power cut or mains water leak may affect the same document's availability.

Threats are usually summarised by short descriptions. The simplest way to assess likelihood and impact is to categorise each as high, medium or low.

### 5.3 *Risk reduction, avoidance and transfer*

The final part of the risk assessment process is to identify effective countermeasures. These will depend on the nature and source of a threat, along with its likelihood and potential impact. Opportunities can then be found to reduce risk to an acceptable level, avoid it or transfer it.

With any risk management solution – some amount of risk will always remain. However, one of the advantages of a systematic approach to information security is that the level of residual risk that a firm or individual finds acceptable can be established. Once established, appropriate management decisions can be made.

A comprehensive risk-based assessment of information security can be a complex task. One way of ensuring that it is approached systematically is by using an appropriate template or table. To aid in the process of risk-assessment, taking into account existing and future threats, individuals may wish to use the example template and listed threats illustrated below as a starting point:

Information Security Risk Assessment Example Template					
Asset	Description of threat	Likelihood	Impact	Countermeasures	Residual risk
Accounting management software databases on office servers	Hardware failure; computer virus; Fire, flood or theft by third party. Risk to integrity and availability of client and personal data	M	H	Employ a reliable off-site backup programme Maintain a professional firewall Encrypt backup data copies Secure premises Locked rooms Alarm systems, etc.	L
Electronic files stored on employee laptops	Theft by third party; Accidental loss, Decentralised distribution of practice data. Risk to confidentiality, integrity and availability of client data	M-H	H	Employ an effective laptop encryption solution Adopt a centralised backup process	L
Information in electronic comms between Office A and Office B	Access by third party. Risk to confidentiality, integrity and availability of client data	M	H	Implementation of encrypted internal comms (VPN) Maintain an active firewall	L
Electronic communications traceable for seven years	Hardware failure; Computer virus; Access by third party Risk to confidentiality, integrity and availability of client data	M	M	Implement a secure off-site archiving solution	L
Hard copy client files	Theft by third party. Risk to confidentiality, integrity and availability of client data. Fire and Flood.	M	H	Secured premises Locked rooms Alarm system in offices Locked filing cabinets/safe Clear desk policy Visitor access procedures Staff training and awareness	L

The table shows the different types of asset along with a description of a few example threats each faces (fire, flooding and theft is common to many), the likelihood, impact, countermeasures and an assessment of residual risk. In this simple example, levels are ascribed to high (H), medium (M) or low (L) categories. Note that the assets listed are just examples; not all assets or risks will be relevant to all practitioners of finance; some risks and assets will be subjective and should be assessed accordingly.

Hard copy data risk-assessment is also different to electronic data risk-assessment. In practice, firms will want to make a comprehensive list of all threats to the different types of asset and may want to group types of assets together in respective risk assessment tables. A straightforward H/M/L categorisation scheme for each group may nevertheless be sufficient. Risk can be managed by reducing its likelihood or its impact. It is rarely possible to eliminate a threat though one way to do so – perhaps as a way of managing unacceptably high risk that cannot be otherwise reduced – is to cease a particular activity.

For a small or medium-sized firm the task of analysing risk and identifying countermeasures is, potentially, time consuming and specialist. To some degree it is likely to be a team effort and firms may need to seek expert advice. At the very least, a detailed risk-assessment process will serve to raise awareness.

## 6.0 Conclusion

Technological developments will never cease - their acceptance and adoption is the only true way to uphold a professional reputation. Firms and individuals who perform best in years to come will embrace the benefits that technology brings and take approaches to data management challenges seriously.

Effective data security relies on understanding and professionally managing information assets. Good information management is the lifeblood of all knowledge-based professions and industries, and can only contribute to overall efficiency and profitability.

Information security is one of the foundations of trust that will underpin the financial profession in the 21<sup>st</sup> century. In the longer term, it is to be hoped that the reputation of a firm that takes information security as seriously as the management of other aspects of its practice, will maintain their reputation.

## Backup Direct – Your business in safe hands

For helpful information on how you can improve your data security policy, contact Backup Direct on 0800 0789 437 or [sales@backupdirect.net](mailto:sales@backupdirect.net).

Backup Direct specialise in data protection services to financial services that remove the risk, hassle and cost of managing IT. Online backup, data encryption, email security and archiving, managed firewall and help-desk. Visit [www.backupdirect.net/finance](http://www.backupdirect.net/finance).