Simmons & Simmons

Data Security – mitigating risks and dealing with incidents

January 2009

Contents

Introduction

Data security has developed into a high profile risk area for both businesses and public sector organisations. The treatment of data and data security breaches are now front page news and incidents result in significant damage to reputation and goodwill. According to the research conducted by the Information Commissioner's Office ("ICO"), the public considers protecting personal information to be the second most socially important issue (placing it above issues such as the environment, the NHS and terrorism).

Data security is also receiving much greater regulator and governmental scrutiny. Both the ICO and sector specific regulators such as the Financial Services Authority ("FSA") have turned their focus closely on data security in the course of the last year and the UK Government is also taking visible steps to improve in this area.

According to the Information Commissioner:

"...alarm bells must now ring in every organisation about the risks of not protecting people's personal information properly..."

The FSA gives the following stark warning in its report on data security (April 2008):

"Overall, data security in financial services firms needs to be improved significantly. Many firms, particularly small firms, still need to make substantial progress to protect their customers from the risk of identity fraud and other financial crime."

Data security is an issue faced by every organisation and failure to maintain proper data security will result in liability and damage to an organisation and its reputation.

Data security - law and regulation

The main source of law in the United Kingdom in relation to data security is the Data Protection Act 1998 (the "DPA"), which relates to the protection of "personal data".

Personal data means data which is stored on automatic equipment or a "relevant filing system" (broadly, a structured manual filing system) and which relates to a living individual who can be identified from that data (or from that data in combination with other data). English case law has refined this definition by stating that, in order to qualify as "personal data", the information should be biographical in some significant sense and have the individual as its focus. However, subsequent ICO guidance on the meaning of "personal data" suggests that the court's interpretation of the DPA may be overly narrow. In any event, organisations will generally want to interpret the meaning of this expression conservatively, to ensure their compliance with the DPA.

The DPA sets out, among other things, the eight Data Protection Principles with which organisations that are subject to the DPA must comply. Data security is the subject of the seventh Data Protection Principle, which provides as follows:

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

This statutory obligation means that organisations must guard against all forms of destruction, loss, alteration, access and disclosure, whether they are accidental, unlawful or unauthorised and caused by the organisation, its employees or third parties. However, this requirement is not absolute in that it only requires organisations to take measures which are appropriate, having regard to the state of technology and cost, the nature of the data and to the harm that might result from unauthorised or unlawful processing or accidental loss/destruction/damage.

Organisations must also take reasonable steps to ensure the reliability of employees who have access to data and, where contracting with a third party supplier who is to access or use personal data, ensure that the supplier complies with the relevant organisation's instructions and complies with the security obligations set out above.

Businesses may also be subject to sector specific regulation. For instance, financial institutions are required to put in place appropriate systems and controls and the FSA is focussing particularly at present on systems and controls relating to data security. Other industries and professions have their own regulation or professional standards that can be breached in the event of a data security incident.

In addition to applicable law and regulation, a data security incident may well cause a breach of confidentiality obligations owed to individual and corporate customers, suppliers, employees, former employees or other third parties.

Potential legal liabilities

Under the DPA, the ICO may impose fines on organisations, find directors and officers individually liable, order organisations to pay compensation to the individuals affected or require organisations to give public undertakings.

The following two routes are available for the ICO to enforce the DPA in respect of data security failures:

- Enforcement notice route: The ICO may send an enforcement notice to the party at fault, specifying the actions which need to be taken to remedy the fault and the timeline within which such actions must be taken. If the party at fault does not comply with the notice, it may then be fined.
- Direct imposition of fines: If there has been a deliberate or reckless commission of a serious breach of the DPA, the ICO may impose a fine without first sending an enforcement notice. This is a relatively new power for the ICO (it only entered into effect in May 2008 via the enactment of the Criminal Justice and Immigration Act 2008), but the level of the fines that may be imposed has not yet been set.

Failure to deal appropriately with data security may also result in a wide range of other potential sources of liability and recriminations ranging from civil liability (whether for breach of contract or a claim for compensation under the DPA), fines and criminal sanctions (under sector specific regulation) to public naming and shaming by the ICO.

Dealing with data security risks

Managing data security requires a comprehensive adoption of a culture of security throughout an organisation. Data security is not just an IT issue. Steps have to be taken by an organisation to address data security and these steps include:

- Governance: appoint a senior manager with overall data security responsibility, supported by a committee with representation from relevant areas of the organisation (including human resources, security, IT, legal and compliance and internal audit).
- Policies: develop policies that are proportionate, accurate and relevant to staff's day-to-day work and encourage open and honest communication (and follow a set process) where an incident arises.
- Training and awareness: raise awareness of data security issues and offer training which provides practical examples of when they may arise and actively test employees' knowledge (as opposed to relying on employees seeking out and familiarising themselves with relevant policies).
- Staff recruitment and vetting: vet staff, including temporary staff (particularly those with access to large amounts of customer data).
- Control access: access rights to personal or sensitive data should be granted on a "need to know" basis and access should be monitored on an ongoing basis. Best practice should be observed in relation to the use of passwords, including by requiring that number/letter and upper case/lower case combinations are used (which are harder to crack) and requiring frequent changes. Laptops and portable media should be encrypted and portable media should only be used to store personal or sensitive data where there is a genuine operational requirement and the relevant staff have been authorised to do so.
- Physical security: restrict physical access to areas where large amounts of personal or sensitive data is accessible and robust security systems should be implemented in relation to such areas. Desks should be kept clear and filing cabinets should be locked.
- Disposal of customer data: identify "confidential waste" that is in paper form and adopt a secure process for its disposal (for example, shredding before disposal). Hard drives and portable media containing personal or sensitive data should be properly wiped (using specialist software) or destroyed before they are disposed of.
- Managing third party suppliers: conduct due diligence of third party suppliers' data security standards before entering into agreements with them and then conduct periodic audits of compliance on an ongoing basis. Also, data should be only be transferred to third party suppliers via secure means.
- Compliance: monitor, on an ongoing basis, compliance with data security policies and training across all relevant areas of the organisation.

Dealing with data security incidents

If a data security incident occurs, urgent action is needed. In the financial sector, the FSA's recent enforcement action (particularly in the Nationwide case, where a delayed reaction was taken into account when determining the seriousness of the breach) has shown that a failure to act swiftly and methodically to incidents is likely to increase the level of fine imposed.

The ICO's guidance on data security breach management focuses on the following four main steps that organisations should take in relation to data security breaches:

- Containment and recovery: This step involves, in the first instance, the establishment of a team to deal with the incident that is appropriately resourced, having regard to the nature and size of the incident. The organisation should then take steps to recover the lost equipment or data and, where applicable, isolate or close elements of its systems. Different responses are appropriate to different scenarios and so a theft will necessitate a different response to data damage; whereas data damage may be remedied simply by the use of back-up tapes, a theft should be reported to the police.
- Assessment of ongoing risk: In assessing the ongoing risk it is important to ascertain the nature of the data lost or damaged, whether the data was encrypted and the number of individuals who may be affected (and how they are likely to be affected). Also, the circumstances that gave rise to the loss or damage may be continuing and so may need to be addressed.
- Notification of breach: An important consideration is whether to notify the individuals who may be affected. The DPA does not expressly require notification but the ICO does regard it as best practice where notification helps individuals to manage their risk. Also, sector specific rules may apply and there may be a contractual requirement to notify specified parties of breaches. It is important to note, however, that there is a risk that notifying individuals can be counterproductive; it may alert criminals to the fact that data has been lost and its significance. Organisations should also consider whether their regulators need to be notified.
- Evaluation and response: After the dust has settled, organisations should conduct a detailed analysis of how the data security incident arose together with a methodical plan to avoid similar incidents occurring. In our experience, entities frequently find the aftermath of a data security incident to be a useful point at which to put in place procedures for addressing similar incidents in the future.

How we can assist you in relation to data security

Simmons & Simmons International Data Protection and Privacy Group has significant experience in advising organisations in the public and private sectors on data security issues, both on a proactive and a reactive basis.

We can assist you in relation to the following areas, among others:

- Compliance audits: We can assist you with auditing your data security arrangements, report on any deficiencies and make recommendations in relation to address deficiencies.
- Development of information security policies: We can assist you with developing an information security policy, taking into account best industry practice.
- Training: We can provide training to staff in relation to data security compliance.
- Specific projects: We can conduct privacy impact assessments in relation to specific projects.
- Contracts with third parties: We can advise you on the drafting and negotiation of provisions that needed to be included in agreements in order to assist you in complying with the DPA and regulatory requirements relating to security. Also, we can advise on best practice in relation to data protection related contractual provisions generally.
- Dealing with data security incidents: We can assist you with assessing the potential liability that may arise in connection with a data security incident, taking action against third parties and the management of related communications.

Simmons & Simmons
January 2009

Alexander Brown
Partner
T +44 (0)20 7825 4954
E alexander.brown@simmons-simmons.com

Lawrence Brown
Associate
T +44 (0)20 7825 3053
E lawrence.brown@simmons-simmons.com

Offices

Abu Dhabi
Level 10 The ADNIC Building Sheikh Khalifa Street
PO Box 5931 Abu Dhabi United Arab Emirates
T +971 (0)2 627 5568 F +971 (0)2 627 5223

Amsterdam
PO Box 79023 1070 NB WTC H Tower
Zuidplein 100 1077 XV Amsterdam The Netherlands
T +31 (0)20 890 99 00 F +31 (0)20 890 99 99

Brussels
Avenue Louise 149 b 16 1050 Brussels Belgium
T +32 (0)2 542 09 60 F +32 (0)2 542 09 61

Dubai
Level 7 The Gate Village Building 10
Dubai International Financial Centre PO Box 506688
Dubai United Arab Emirates
T +971 (0)4 709 6600 F +971 (0)4 709 6601

Düsseldorf
BroadwayOffice Breite Straße 31
40213 Düsseldorf Germany
T +49 (0)2 11-4 70 53-0 F +49 (0)2 11-4 70 53-53

Frankfurt
MesseTurm Friedrich-Ebert-Anlage 49
60308 Frankfurt am Main Germany
T +49 (0) 69-90 74 54-0 F +49 (0) 69-90 74 54-54

Hong Kong
35th floor Cheung Kong Center
2 Queen's Road Central Hong Kong
T +852 2868 1131 F +852 2810 5040

Lisbon
Simmons & Simmons Rebelo de Sousa
Rua D. Francisco Manuel de Melo 21
1070-085 Lisbon Portugal
T +351 21 313 2000 F +351 21 313 2001

London
CityPoint One Ropemaker Street
London EC2Y 9SS United Kingdom
T +44 (0)20 7628 2020 F +44 (0)20 7628 2070

Madeira
Simmons & Simmons Rebelo de Sousa
Av. Zarco nº2-2º 9000-069 Funchal Madeira
T +351 291 20 22 60 F +351 291 20 22 61

Madrid
Simmons & Simmons Mochales & Palacios
Calle Miguel Angel 11 5th floor
28010 Madrid Spain
T +34 91 426 2640 F +34 91 578 2157

Milan
Corso Vittorio Emanuele II 1 20122 Milan Italy
T +39 02 72505.1 F +39 02 72505.505

Moscow
Simmons & Simmons CIS LLP
Gogolevsky Boulevard 11
119019 Moscow Russia
T +7 495 646 9300 F +7 495 646 9301

Padua
Largo Europa 1 35137 Padua Italy
T +39 049 8750672 F +39 049 8753675

Paris
5 boulevard de la Madeleine 75001 Paris France
T +33 (0)1 53 29 16 29 F +33 (0)1 53 29 16 30

Qatar
5th floor Al Mirqab Tower Al Corniche Street
PO Box 23540 Doha State of Qatar
T +974 483 9466 F +974 483 9584

Rome
Via di San Basilio 72 00187 Rome Italy
T +39 06 80955.1 F +39 06 80955.955

Rotterdam
PO Box 190 3000 AD Weena 666
3012 CN Rotterdam The Netherlands
T +31 (0)10 404 21 11 F +31 (0)10 404 23 33

Shanghai
33rd floor Plaza 66 1266 Nanjing Road West
Shanghai 200040 People's Republic of China
T +86 (0)21 6249 0700 F +86 (0)21 6249 0706

Tokyo
Simmons & Simmons in association with TMI Associates
23rd floor Roppongi Hills Mori Tower
6-10-1 Roppongi Minato-ku Tokyo 106-6123 Japan
T +81 (0)3 6438 5255 F +81 (0)3 6438 5256

Simmons & Simmons