

The Legal Risks of Data Loss

A BeCrypt whitepaper paper
written by Shoosmiths solicitors



Introduction

The English philosopher, Francis Bacon, may have stated that “knowledge is power” but of course he never suffered the embarrassment of leaving a memory stick on a train. Barely a month passes without an organisation, frequently in the public sector, suffering damaging publicity as a result of unauthorised disclosure of sensitive data.

In an era when the UK Government itself acknowledges that total security of data is impossible, and the Information Commissioner has described data as a potential “toxic liability” to an organisation, this White Paper explores the risks associated with the potential loss of confidential company data, customer or employee information, provides an overview of the relevant legislation in this area and reviews the best practice and guidance available to assist organisations in handling such data.



The Risks

The risks relevant to the loss of any particular data depend on the exact nature of the data in question.

For example, the possible financial and commercial consequences of the loss of sensitive customer data are obvious. Such data is frequently lost by mere carelessness, but it could also occur by deliberate and/or malicious actions (e.g. an employee seeking to set up a competing business or to tempt key clients to a competitor company when taking up a new position).

An organisation may also be at risk of losing highly important corporate information such as manufacturing processes, trade secrets or other confidential information that is fundamental to the success of the business. In this category of case, the commercial consequences of disclosure could be very significant.

Organisations also neglect the security of employee data at their peril. While this may not cause the high profile commercial damage associated with the loss of customer details or trade secrets, inadvertent disclosure of employee data is likely to be in breach of the Data Protection Act and could leave the organisation open to legal claims by the employees affected (if they can establish financial loss) or alternatively complaints to the Information Commissioner, who regulates this area. While the commercial consequences of such data loss may be minimal, the damage to the morale and confidence of employees could be substantial.



The nature of these various risks can be illustrated by recent cases which have all received wide attention and generated negative publicity for the organisations involved.

“

While the commercial consequences of such data loss may be minimal, the damage to the morale and confidence of employees could be substantial.

”

In December 2008, the Bar Council (the professional body for barristers) had to write to all barristers in order to inform them that, during a break-in at the Council's central London office, a laptop computer and four hard drives had been stolen. The data taken included financial records of barristers who paid by direct debit and also details of complaints made against individual barristers. However, it was clear that the data was protected at least in part, the financial data did not include any passwords, credit card, debit card or personal identification numbers and the Bar Council's view was that the data was appropriately protected for its sensitive nature.

Data losses from Government departments have caused embarrassment across Whitehall and have led to reviews of practice at departments such as Her Majesty's Revenue and Customs and the Ministry of Defence, culminating in the publication of a Cabinet Office report on data handling procedures in Government, see the BeCrypt Data Handling Review white paper for further reading.



The widespread use of service providers also causes further complications. Many examples of significant data loss have occurred not due to the errors made directly by an organisation, but by contractors or suppliers dealing with the data on behalf of those organisations. An example of this occurred in August 2008, when unencrypted data on the 84,000 prisoners held in England and Wales went missing after an employee of the contractor, PA Consulting, lost a memory stick. The missing data included names, dates of birth and, in some cases, information on the expected release of certain prisoners. As a result of this data loss, the member of PA Consulting's staff was suspended, and PA Consulting ultimately lost a lucrative Home Office contract.

“

The missing data included names, dates of birth and, in some cases, information on the expected release of certain prisoners.

”

In September 2008, four CDs containing the details of almost 18,000 staff were lost as they were moved between the payroll department of Whittington Hospital NHS Trust and a third party payroll company. At least the story had a positive outcome, with the CDs being found again later in the same month.

The highest profile data loss was probably that suffered by HM Revenue and Customs in November 2007, when 25 million records containing the names, addresses, dates of birth and National Insurance numbers of the entire HMRC Child Benefit database went missing. This occurred because of a junior member of staff's decision to send the details in unrecorded and unregistered delivery through a courier service to the National Audit Office.



The Government itself acknowledges that complete security of data may simply be impossible. Speaking in early November 2008, following the loss of a memory stick containing the passwords to a Government website used to submit on line tax returns, Prime Minister Gordon Brown explained that it was important to recognise that he could not promise that every single item of information held by the Government would always be safe because mistakes in the communication of information were inevitable.

The Law

The main legislation in this area is the Data Protection Act 1998 which, amongst other things, sets down a number of principles as to how the data controller should handle personal data. These include the fact that the data should be processed fairly and lawfully, that it should be adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed, and that appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing or accidental loss or destruction of, or damage to, personal data.

Sensitive personal data (consisting of certain categories of information about individuals such as their racial or ethnic origin, political opinions or religious beliefs) are covered by further protections on processing that are set out in Schedule 3 of the Data Protection Act.



Given the nature of the data being processed, express consent by the individual is usually required, but the organisation may be able to rely on other, limited, grounds to permit the processing, such as the processing being necessary for the administration of justice or being in the vital interests of the individual in a situation where consent cannot be given (e.g. a medical emergency).

An individual who suffers damage by reason of any contravention by a data controller of any of the requirements of the Data Protection Act is entitled to compensation from the data controller for that damage.

Organisations should also be mindful of the powers of the Information Commissioner to impose fines for deliberate or reckless breaches of the Data Protection Act. This power was granted to the Information Commissioner in May 2008 under the Criminal Justice and Immigration Act and was welcomed by the Commissioner as sending a clear signal that data protection must be a priority.

While the **Human Rights Act 1998** is only directly enforceable against public authorities (such as NHS Trusts, Government departments or local authorities) private sector employers need to at least be aware of an individual's rights under this Act as a claim for breach of the Act might be added to some other form of Tribunal or Court claim.



The main right that is likely to be argued in respect of any loss of data is contained within Article 8 of Schedule 1 of the Human Rights Act. This provides that everyone has the right to respect for his private and family life, his home and his correspondence.

“

This provides that everyone has the right to respect for his private and family life, his home and his correspondence.

”

Should an individual succeed in an argument that the Human Rights Act has been breached, the Court or Tribunal has the power to award damages and also has a broad power to make orders or grant relief as it deems appropriate.

A final consideration is any contractual obligation that might have been breached by the unauthorised disclosure of information. For example, an organisation might have entered into a contract, with a third party, which incorporates terms relating to how the third party's data will be secured or processed. Should these terms have been breached by any data loss incident, then the third party may take legal proceedings for breach of contract.

Guidance

The Information Commissioner regulates this area and while the Codes of Practice that he issues are not binding legislation, they are very useful guidance and will always be considered by Courts or Tribunals in determining any proceedings in relation to any breach of the Data Protection Act.

Relevant guidance includes the Framework Code of Practice for Sharing Personal Information, the Employment Practices Code (which refers to the recruitment of employees, maintenance of employment records, monitoring employees at work and information about workers' health) and Good Practice Notes on certain specific issues such as guidance on data security breach management, security of personal information and guidance on the notification of data security breaches to the Information Commissioner's office. All of this information is available from the Information Commissioner's website: www.ico.gov.uk.

The guidance covers a number of important areas for organisations that will be handling personal information and stresses that any organisation should analyse the potential risks that might flow from an unauthorised disclosure of the information, identifying specific staff who have responsibility for the security of such data, implementing appropriate security and organisational measures to ensure the safety of such data (both technical and physical security) and considering the appropriate levels of security to be applied, such as encryption or password protection.



The data held within the financial services industry can often be particularly confidential and the Financial Services Authority (the “FSA”) has produced a specific report as a result of a review of industry practice and standards in managing the risk of data loss. Although the report deals with the financial services sector, the concerns that it highlights and the steps that it advises firms to take are relevant in all sectors of industry.

This report points out that the FSA supports the Information Commissioner’s position that it is not appropriate for customer data to be taken off site on laptops or other portable devices which are not encrypted. It warns that the FSA may take enforcement action against firms that fail to encrypt customer data off site.

The report also highlighted that many firms do not undertake an appropriate risk assessment regarding the potential loss of data and implementation of data security policies is often patchy. It noted a potential point of weakness in the use of third parties for IT maintenance, backing up of electronic files and archiving of paper documents, with a concern that firms generally relied too much on assumptions that contractual terms were being met, with very few firms proactively checking the security arrangements that the contractors had put in place to protect customer data. It also stressed the risk of data loss via laptops, USB devices and the Internet, highlighting the fact that very few firms seemed to mitigate data security risks by steps such as encrypting laptops and USB devices and blocking web based communication facilities such as hotmail and instant messaging.



The report also stresses that while many firms pass on customers' personal details to third party suppliers, this does not absolve the firm itself from responsibility for data security as it is the data controller who will still need to comply with the principles set out in the Data Protection Act.

Conclusion

Important data, whether relating to customers, an organisation itself, or its employees, is clearly necessary for any organisation to function. To paraphrase the Information Commissioner, such data can be (and often is) both a crucial asset and a toxic liability. The challenge for all organisations is to assess the risks that they face, bearing in mind the categories of the data held, consider the possible consequences of any data loss, and then put in place appropriate and proportionate protections, both technical and physical, to ensure the security of the data as much as is humanly possible.

As the Information Commissioner acknowledged in an interview he gave in October 2008; "things will inevitably go wrong, therefore you should plan for things going wrong". Organisations have to become more aware that holding large elements of personal data creates a significant risk and therefore substantial protective measures are needed in order to secure that data.

Shoosmiths

January 2009

This White Paper contains a general statement of the law and is not a substitute for obtaining detailed legal advice. You should seek specific advice on any particular issue.



About BeCrypt

BeCrypt provides market leading disk encryption, media encryption, data protection, and remote access products that can be configured to the individual needs of your organisation. Our data security products protect the data and information on desktops, laptops, PDAs, USB sticks, mobile devices and removable media such as CDs.

Some of the most secure organisations in the world rely on BeCrypt encryption software to protect their data. We work with global corporates and public sector organisations such as the UK Government and Ministry of Defence on many security development projects.

Our encryption products are certified by the leading security assurance schemes, including CESG Assisted Products Scheme (CAPS), CCT Mark, Defence INFOSEC Procurement Co-Operation Group (DIPCOG) and the Federal Information Processing Standard (FIPS).

Our ground breaking Trusted Client product allows organisations to give mobile workers secure network access from an unmanaged internet enabled PC. Trusted Client can drastically reduce the cost of mobile working and offers significant business continuity gains should office based workers not be able to get to their work place. For safe remote access to the network users simply insert the Trusted Client memory stick and boot up their PC.



All product names referenced within this document are trademarks or registered trademarks of their respective companies.

BeCrypt Ltd disclaims interest in the marks or names of others. While every effort has been made to ensure technical accuracy, information within this document is subject to change without notice and does not represent a commitment on the part of BeCrypt Ltd.

No part of this document may be reproduced or transmitted in any form, electronic or otherwise, without the expressed consent verbal or written of BeCrypt Ltd.

130 Shaftesbury Avenue
London W1D 5EU UK
t: 0845 838 2050
f: 0845 838 2060
Outside UK: +44 (0) 20 3145 1050
sales@becrypt.com
www.becrypt.com