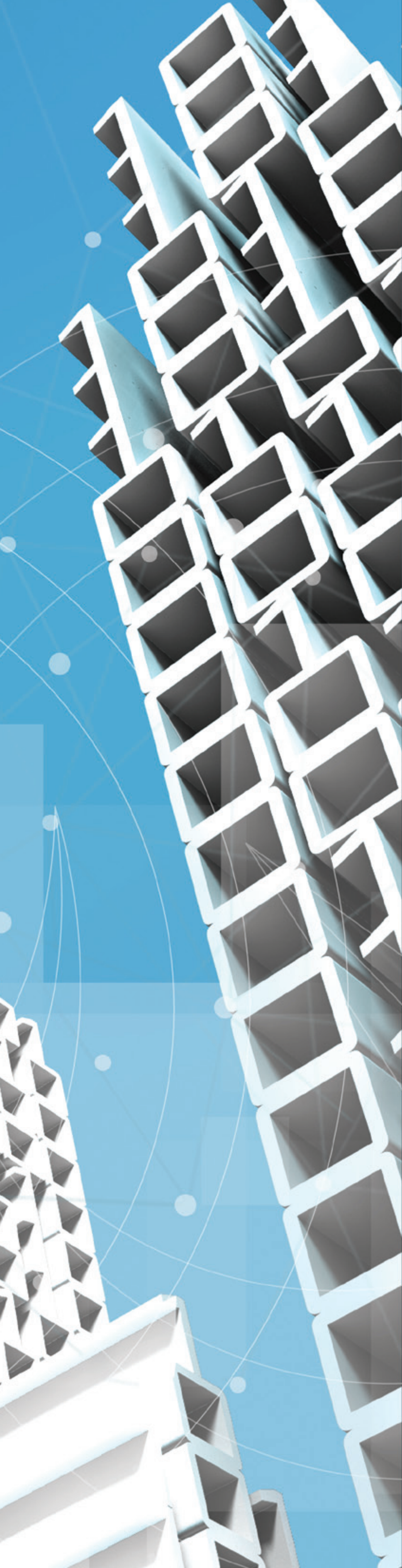

A Websense® White Paper written by Shoosmiths Solicitors

FOREWARNED IS FOREARMED:
SHOOSMITHS ON DATA LOSS

websense®
ESSENTIAL INFORMATION PROTECTION™

Table of Contents

Introduction 3

Causes and Risks. 4
- Causes 4
- Theft 4
- Hacking 4
- Malicious Action 4
- Carelessness 4
- Lack of understanding and awareness 5
- Inadequate procedures 5

Law – Some legal elements in the U.K. 6
- Data Protection 6
- Financial Services 7
- PCI DSS Compliance 7
- Human Rights Act 7

Some Recent cases 7

General Guidance 8
- Use of personal and portable devices 9
- IT security 9
- Outsourcing 9
- Personnel 10
- Training and awareness 10
- Accountability 10

Conclusion 11

Introduction

"The ICO takes data protection breaches extremely seriously. Any business or organisation that is processing personal information in the UK must ensure that they comply with the law, including the need to keep data secure."

In this white paper, we will look at some of the risks surrounding data security and data loss, the legislation relevant to this area and the best practice and guidance available to assist organisations in their attempt to avoid embarrassing, costly and damaging data breaches and to mitigate their impact if they do arise. This paper does not aim to be a complete guide but it aims merely to highlight some of the issues that businesses face in relation to data security and data loss.

Causes and Risks

Data is a valuable and essential asset for any organisation to operate effectively and, where it exists there is the risk that it will be lost, damaged or intercepted. With organisations collecting, generating and storing more and more information, rapid technological advances and changing business practices it will come as no surprise that the risk of data loss and the likely consequences of any breach are increasing too.

The types of data that organisations collect and use are broad ranging and expanding. They range from personal data (as defined by the Data Protection Act 1998 ("DPA") relating to employees, customers, targets and suppliers for example), financial data (which may or may not be personal data for the purposes of the DPA) and strategic and commercially sensitive information to anonymised, statistical and non-confidential information. The risk posed by any security breach would therefore depend on the nature and volume of the information involved. We will discuss the specific risks of data loss later in this paper.

Causes

Data loss can occur for various reasons and indeed can be the culmination of several different factors. Common causes range from theft, hacking and other malicious actions to mere carelessness, lack of awareness and inadequate procedures to protect it.

Theft

Personal data is lawfully bought and sold throughout the world however, unfortunately the illegal trade in personal data is also a lucrative and growing business. This means that, to our dismay, the opportunist criminal is always looking for ways to obtain customer lists for onward sale.

Hacking

The recent security breach suffered by Sony Playstation demonstrates that whilst organisations are continually endeavouring to ensure that their security measures are insurmountable and that their data is out of reach, even the most sophisticated of security systems is vulnerable to attack by the inquisitive and savvy hacker. With the increasing use of portable devices and Wi-Fi, organisations are now more vulnerable to attack than ever.

Malicious Action

The employees of an organisation are arguably its most valuable asset. However, they can also be its weakest link. Employees often need to access commercially sensitive, strategic and personal data in order to perform their roles, however, all too often we hear of the aggrieved employee who disclosed information in order to damage its employer (step forward the former employee of a large Oil company who disclosed the names and addresses of senior personnel to an environmental activist group causing threat to safety as well as massive reputational damage for the company[1]). In addition, we also commonly hear of the previously loyal employee, who decided to set up in competition with its former employer and in return for its long service and loyalty, takes customer lists with him/her in order to get a head start.

Carelessness

We are all human and therefore susceptible to human error. However, with changes in the way we work on a day to day basis (increased home working, remote access and working on the move using portable devices), the potential impact of our careless actions is much greater and much more difficult to contain. To mention an example, there was the recent incident where an employee of a Consulting firm lost an unencrypted memory stick containing the personal details of thousands of prolific criminal offenders and the highly publicised loss of the HMRC computer disks containing the personal details of millions of UK taxpayers.

1 Widely reported but please see www.business.timesonline.co.uk/tol/business/...article7025711.ece

Lack of understanding and awareness

It is surprising that despite numerous significant and highly publicised security breaches and the increase in levels of identity fraud, many individuals still do not place any real value on the protection of confidential and personal data even when it is their own. A recent study[2] revealed that 60% of people questioned on the street would disclose their individual computer passwords in return for a £5 department store voucher. This lack of value we place on our own personal data goes some way to explaining why individuals working for organisations that process personal data do not place any importance whatsoever on the protection and proper treatment of another person's information.

Inadequate procedures

If an organisation does not have adequate and enforceable policies and procedures in place to protect data from loss, destruction and disclosure, the risk of a data loss taking place is immediately increased.

Our business practices are changing. Workplaces are experiencing vast increases in the level of home and remote working, use of portable media (both belonging to the organisation and personal to the employee), sharing of information at local, national and international levels and outsourcing. Each of these factors means that data is constantly being taken outside the immediate control of the organisation responsible for protecting it thus making its ability to protect it, more difficult.

Regardless of how data is lost, the potential impact any loss may have for the organisation, its employees and the individuals to whom it relates may be significant. A data loss can have serious personal, financial and commercial consequences depending on the type and volume of data lost.

Where the loss involves personal data, the risks for affected individuals can range from personal embarrassment and inconvenience to real harm and distress. From an organisation's perspective the loss of data could lead to legal claims from affected individuals and/or complaints to the Information Commissioner's Office ("ICO") and where the data includes employee information, it could damage employee morale and confidence. In addition, the reputational damage that adverse media attention will attract is unquantifiable but without doubt, significant. Where the data loss involves commercially sensitive and/or strategic information, this could also affect the organisation's reputation, market position and ultimately, its profitability.

An inevitable consequence of all of the above is the diversion of valuable time, effort and resources away from business critical projects and towards breach management, complaint handling and liaising with the ICO. This is something that few organisations can afford in this difficult economic climate.

With the increasing frequency at which individuals are using personal devices for work purposes, we must acknowledge that this practice could present a greater risk for the organisation. The types of devices being used include blackberries and 'tablets'. Whilst on initial thought, it might appear to be an effective cost saving measure for an organisation, as the device will not appear on the organisation's asset list and is not within the organisation's control, it is difficult for an organisation to keep track on where its data is being accessed from. In addition, it is also difficult for an organisation to monitor compliance with its policies without also interfering with the individual's personal use of the same device. It also raises the question as to whether or not holding company data on personal devices 'muddies the water' in terms of who actually owns that data. What is clear is that in the event of a data security breach involving the personal device and work related information viewed on it, responsibility for protecting that data (and liability for failing to protect it) will rest with the organisation on whose behalf it is collected.

2 "Passwords are an easy giveaway", Research undertaken by Symantec and reported in Which?, September 26, 2008.

Law – Some legal elements in the U.K.

Data Protection

The main piece of legislation governing this area in the U.K. is the DPA which sets out eight principles that all organisations processing personal data must comply with. The principles state that personal data should be processed fairly and lawfully, should only be processed for specified purposes, should be adequate, relevant and not excessive and should not be kept for longer than necessary.

An important principle however for the purpose of this paper is principle seven of the DPA which states that personal data must be processed subject to "appropriate technical and organisational measures" to protect it against unauthorised and unlawful processing or accidental loss, destruction or damage.

The DPA does not define what will constitute "appropriate" in every instance and this must therefore be decided on a case by case basis, taking into account, the nature of the data being protected and the likely damage that would arise in the event of that data being lost, stolen or damaged. "Sensitive personal data" is defined by the DPA and includes information about an individual's racial or ethnic origin, political opinions, sexual orientation, medical history and religious beliefs. Due to its very nature, it attracts a higher level of protection than general personal data and therefore a higher level of protection will need to be in place where it is involved in order to satisfy the requisite "adequate" condition.

In the event of a data breach, the data controller (the organisation which determines the purposes for which the data is processed and who is at all times responsible for compliance with the DPA) can be liable for damages if an individual can prove that it has suffered damage through the data controller's breach of the DPA.

In addition, since May 2010, the ICO has the power to impose substantial fines (up to a maximum of £500,000 per breach) on organisations who commit a serious breach of the DPA. Whilst the ICO has indicated that it is its intention to only exercise this right in relation to the most serious of cases, the threat of a significant monetary penalty remains.

Since the ICO was granted the right to impose substantial fines, only 6 organisations have been fined under the regime with the highest fine levied to date being £120,000 in June 2011. This was levied against Surrey County Council[3] when sensitive personal information was emailed to the wrong recipients on three different occasions.

In addition to the power to impose substantial fines, the ICO also has the right to issue information notices, enforcement notices and undertakings requiring organisations to provide information and to take specified steps to achieve compliance within strict timescales. Whilst these are not widely published by the ICO, they will appear on the ICO website and will inevitably be picked up by journalists looking for a topical scoop.

Finally, the ICO is moving towards a compulsory breach notification scheme (and indeed one already exists for some sectors) and whilst this is not a legal requirement, it is now recognised good practice to notify where ICO Guidance suggests. The ICO Guidance indicates that in the event of a breach, the data controller must carry out a risk assessment to decide whether or not the breach is serious enough to notify to the ICO. This assessment should take into account (amongst other things), the nature of the data involved, the volume of data involved, the measures that were in place to prevent unlawful use (i.e. encryption) and the risk that the breach poses for individuals. If, taking those factors into account the organisation decides that it should notify, the notification must set out, amongst other things, details of the breach, action taken by the organisation to mitigate the impact of the breach, action taken to remedy the breach and proposed steps that will be implemented to ensure that it does not happen again.

3 ICO News Release: 9 June 2011.

Financial Services

Organisations operating in the financial services sector are also subject to regulation by the Financial Services Authority ("FSA") which imposes additional obligations on organisations that are subject to it. In contrast to the ICO, the FSA has the power to impose unlimited fines and in August 2010 it fined Zurich Insurance almost £2.3 million, the highest fine ever for data security failings[4]. This fine was imposed where the FSA found that Zurich had failed to have adequate systems and controls in place to prevent the loss of confidential information belonging to 46,000 customers. Bank of America is currently facing a class action lawsuit alleging that the bank compromised the private financial records of thousands of customers. Those reporting on this action have opined that the legal penalties for the bank could run into billions of dollars[5].

PCI DSS Compliance

Any organisation that processes payments by card is required to comply with the Payment Card Industry Data Security Standards ("PCI DSS") which aim to protect card payment details from abuse by fraudsters. The Payment Card Industry Security Standards Council ("PCI SSC") is responsible for managing the security standards, while compliance with them is enforced by the founding members of the PCI SSC (being American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc). Failing to comply with PCI DSS carries various implications which include increased processing fees being charged by the card issuer, a bar on the processing of credit card transactions by the issuers and fines of up to £250,000 for each instance of non-compliance.

Human Rights Act

Public authorities and private companies which undertake public functions are subject to the Human Rights Act 1998 and data security will be relevant in terms of the individual's right to respect for his private and family life, his home and his correspondence (Article 8). A data loss involving their personal data might infringe this right. If an individual succeeds in claiming that his human rights have been breached, then the Court or Tribunal has the power to award damages or to make orders or grant relief to the individual.

In addition, where a data loss arises as a result of an organisation failing to comply with its contractual obligations and/or its duties of care, this can give rise to legal claims for breach of contract and/or negligence by individuals affected by the breach.

Finally, it is worth pointing out that where an organisation makes personal data available to third party service providers, the originating organisation will at all times remain responsible (as data controller) for the processing of that data in accordance with the DPA. In the event of a breach by the third party service provider (the data processor), any investigation, fine and/or enforcement action will be directed towards the data controller so it is in its best interests to ensure that it is adequately protected in these circumstances. (See further comments below under Guidance.)

Some Recent cases

In recent years, the reporting of data loss and security breaches has become more and more newsworthy. For high profile companies, a publicised data loss can have a serious impact from both a financial and reputational perspective. For small businesses, one significant data breach could be enough to cause the decline of an otherwise successful business.

4 www.fsa.gov.uk/pages/library/Communication/PR/2010/134.shtml

5 "In case with National Security implications, Bank of America faces angry customers over outsourcing and government capture of their financial data", Association of Certified E-Discovery Specialists, August 2011, Vol 2, No. 26.

One of the most high profile data losses in 2011 took place in April when Sony Playstation lost the records of 77 million users as a result of hacking. Of the records stolen, 3 million were registered UK users and the breach is being investigated by the ICO. Sony has experienced further data security breaches since April thus resulting in further negative publicity. The losses these data security breaches present for Sony have been broadly quantified at $170m[6].

The Sun newspaper has also released information that its website was hacked in July 2011 and that thousands of people who have entered their competitions may have had personal information, including their addresses and dates of birth, stolen. It has reported the breach to the police and the ICO[7].

The health service appears to be a repeat offender when it comes to data security. KPMG's Data Loss Barometer report[8] states that 25% of all breaches in 2010 took place within the healthcare sector and in July 2011 alone, the ICO found six health organisations to be in breach of the seventh principle of the DPA having failed to take appropriate technical and organisational measures to protect the personal data they hold. This has prompted the ICO to state that "security of data remains a systemic problem [in the health service] [...] The policies and procedures may already be in place but the fact is that they are not being followed on the ground.[9]"

The use of unencrypted laptops and memory sticks continue to present a problem with the ICO obtaining 9 undertakings from various organisations that have lost data in this way to improve their levels of compliance and to encrypt laptops. KPMG's Data Loss Barometer report states that over a third of data loss in relation to portable media involves portable hard drives, which are becoming increasingly targeted by thieves because of their capacity to hold a large amount of data but are becoming smaller and easier to hide.

General Guidance

Whilst the comments below refer specifically to the DPA and FSA and to the protection of personal data and financial information, the principles apply across the board and if followed should go some way to protecting all commercially sensitive and other data stored by the organisation.

The ICO has issued various Codes of Practice and Guidance Notes to assist organisations in achieving compliance with the DPA. Whilst these are not binding legislation, they do provide helpful guidance in terms of what the legislation requires and how the requirements can be applied in practice. In addition, they provide some comfort to organisations who comply with them as, in the event of proceedings in relation to any data security breach, the Courts and Tribunals hearing the proceedings will, in reaching their verdict, take into account whether or not the Codes of Practice and Guidance have been followed. In addition, the FSA issued in April 2008 a guidance document called "Data Security in Financial Services" which sets out detail in relation to the controls that FSA regulated organisations should have in place to prevent data loss by their employees and third party suppliers.

The Codes of Practice and Guidance Notes issued by the ICO are all available to view on the ICO website at www.ico.gov.uk and these provide both generic guidance for compliance as well as topic specific guidance. We would recommend all companies should review for themselves the Practice and Guidance notes as issued by the ICO.

---

6 Widely reported but please see www.digitaltrends.com/.../sony-network-breach-to-cost-company-170-million
7 www.ontrackdatarecovery.co.uk/data-recovery-news/articles/the-sun-admits-data-security-breach037.aspx
8 www.datalossbarometer.com/14965.htm
9 "Health Service must get it right on data security says ICO", News Release: 1 July 2011.

In terms of basic guidance, organisations are advised to conduct a risk assessment exercise, to find out exactly what personal data they hold, the nature of the data held and the risks that would arise in the event of a breach involving that data. This will enable the organisation to determine what security measures need to be put in place to protect it. How can an organisation even start to consider how to protect the data it holds if it doesn't know the nature and extent of that data in the first place?

The next step is to implement appropriate measures to protect it. These will involve IT security measures, physical security measures and measures to ensure the reliability of personnel who have access to personal data. These will need to be backed up by robust, comprehensive and enforceable policies, compliance with which should then be actively monitored and enforced.

The measures set out in this note are not intended to be an exhaustive list that guarantee compliance but merely an outline of some measures that can be taken, all companies should assess their own systems and policies to try to limit the risk of any data loss. We have identified some specific and current vulnerabilities which should be given particular attention:-

Use of personal and portable devices

The use of personal and portable devices for work purposes is now widespread and is difficult to monitor and control. All portable devices should be encrypted to prevent unauthorised access to information held on them, should be recorded on the organisation's asset list, should only permit access to the organisation's server through a secure route and should be password protected. However where the portable device belongs to the employee some additional steps need to be taken to mitigate the risk of a data loss taking place. In particular, their use will need to form part of the organisations internal policies and procedures. Policies should specify that if use of personal devices for work purposes is permitted, employees must comply with relevant security measures, they must be encrypted and the employee should be required to notify the organisation immediately in the event of loss or theft. In addition, in order to resolve the issue regarding ownership of work related data held on personal devices, this too should be specifically covered off in the organisations' internal policies and procedures which should stipulate that data viewed through a portable device regardless of ownership of that device, will at all times remain with the organisation. If the use of personal devices is not permitted, this should be stated and enforced. Whilst many organisations do monitor the use of devices owned by it, it is extremely difficult to do this with personal devices where the user will use it both for work and personal purposes. The simplest resolution appears to be prohibiting the use of personal devices for work purposes.

IT security

IT security has always been relevant to the protection of confidential and personal data however, because of technological advances, the vulnerabilities, and therefore the requisite measures that need to be implemented, are constantly changing too.

Outsourcing

Outsourcing is on the increase and it is vital that data controller's protect themselves against inadvertent breaches of the DPA through their service providers by ensuring that where third parties are granted access to an organisation's confidential and personal data, control over that processing is retained by the originating organisation. This will involve a written contract being put in place, spot checks being carried out and due diligence being conducted on the service provider. In addition, organisations should carefully consider what parts of its business it wants to outsource and ideally, sensitive parts of the business would be controlled in-house.

Personnel

Personnel are often considered to present the greatest risk in terms of an organisation's data security. Appropriate background checking should therefore be carried out on individuals who will have access to confidential and personal data, compliance with policies should be monitored and enforced and each contract of employment should place appropriate obligations and restrictions on the employee in terms of dealing with such data. In addition, measures should be put in place to ensure that access rights are removed on termination and that all equipment and company information is returned on termination.

Training and awareness

Lack of awareness and understanding of the importance of keeping confidential and personal data secure is a key vulnerability and this can only be rectified by ensuring that all personnel who access such data are trained to recognise confidential and personal information and on how it should be treated. An organisation can have no recourse against an ill informed employee.

Accountability

Finally, in order for the above measures to take place, be implemented, enforced and updated, there must be some accountability within the organisation setting out which individuals are responsible for which aspects of the overall project. Otherwise, things will not get done or will become outdated and the vulnerabilities will re-appear.

It is also important for organisations to have a plan for how to react to any breach if or when one does arise. This is just as important as having measures in place to prevent the breach taking place in the first place and the ICO will place a high degree of importance on an organisation's reaction to the breach as part of any investigation. This plan should set out how the organisation will contain and recover from the breach, assess the ongoing risk presented by the breach, how the organisation will decide who needs to be notified of the breach (if anyone at all) and how it will evaluate the breach and respond to it to prevent further breaches taking place.

Conclusion

Data security is a minefield and has been referred to by the ICO as a "toxic liability". As mentioned above, where data is held, the risk of loss, damage or theft will not be far away. All that organisations can do is to carry out a risk assessment, put in place and enforce "appropriate" measures to try to prevent a data breach taking place, regularly check the adequacy of those measures and compliance with them and plan for how the organisation will react in the event that a breach does occur.

The ICO, FSA and individuals expect a high degree of security to be in place to protect data however; all recognise that accidents do happen. The question that must be considered is whether or not, in the event of a breach taking place, the organisation involved can contain it and be confident that they had done enough to try to prevent it.

Shoosmiths
August 2011

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. While the information contained in this white paper has been prepared in good faith, no representation or warranty, express or implied, is or will be made and no responsibility or liability is or will be accepted by Websense or by any of its affiliates, respective officers, employees or agents in relation to the accuracy or completeness of this information or any other written or oral information made available to any interested party and any such liability is expressly disclaimed.