

A BIBA broker's guide to...

Cyber risks

2014 - Issue 2

Part 1: Data protection



Contents

Introduction from BIBA	03
What are cyber risks?	04
Data Protection Act	05
Data security	06
Case study - Jala Transport	08
Data breach response	09
Planning for future regulatory change	10

This series of legal supplements is brought to you through a partnership of BIBA, DAC Beachcroft and Zurich. We hope that you find DAC Beachcroft's legal expertise, Zurich's industry knowledge and BIBA's desire to share these with you helpful and we welcome any suggestions for future subjects.



Introduction

Like death and taxation, data breaches and IT network integrity problems have become a fact of life. Hardly a week goes by without some organisation or another admitting an embarrassing data breach to its customers and implementing costly and time consuming remediation. According to Symantec, 2013 was the year of the mega breach. It is little wonder that the cyber risk insurance market has seen significant growth recently, providing BIBA brokers with exciting opportunities to develop new products.



STEVE WHITE
CHIEF EXECUTIVE
BIBA

However, cyber security issues are not just a concern for big organisations. Statistics show that 40% of cyber-attacks are directed at firms with fewer than 500 employees*. This guide is aimed at helping brokers understand existing data protection rules and prepare for future regulatory change from the European Union (EU).

Changes to EU law will make it harder for many organisations to remain silent about data breaches in future. The draft General Data Protection Regulation updates the EU's data protection rules and puts individuals back in control of their personal data. One way of doing this will be to allow people the right to know when their data has been hacked: organisations will have to notify their national supervisory authority of serious data breaches within a set period so that users can take appropriate measures.

Having a plan about how to prevent your business data being compromised in the first place or how to respond in the event that things have gone wrong will become increasingly important in future and you are to avoid your business becoming another statistic.



What are cyber risks?



Hans Allnutt
Partner
DAC Beachcroft LLP



Rhiannon Davies
Associate
DAC Beachcroft LLP

DAC beachcroft.

The word “cyber” appears in national and international headlines with increased frequency. Global corporations suffer at the hands of hackers and rogue employees who take down networks and steal millions of personal and financial records.

In an insurance context, “cyber risk” encompasses risks arising out of an organisation’s reliance on electronic systems and networks. These are not sector specific and affect any company with an online presence or that use electronic systems to conduct business.

Cyber risks can give rise to both first party losses and third party liabilities. For example, a denial of service attack or computer virus that prevents a company from trading could give rise to a claim under business interruption insurance. The theft of personal data or intellectual property from an organisation’s electronic systems could result in regulatory investigations and claims as a result of breaches of data protection and privacy laws.

Such is the breadth of this area, we have decided to focus on third party liabilities associated with data security and privacy in this issue. We shall turn our attentions to first party cyber risks and in particular, business interruption, later this year.

The Data Protection Act 1998

“Personal data” means data from which you can identify a living individual. Where the ability to identify an individual from one source of data depends on separately held information, the data held will still be “personal data”.

The threshold for what constitutes personal data is quite low. An employee’s email address contains the employee’s name and where they work. A quick browse of the company’s website might say how long the employee has worked at the company and what their role is, making this “Personal Data”.

Additional controls relate to the processing of “sensitive personal data” which is a special category of personal data including physical or mental health and criminal records.



The eight principles







The DPA sets down eight legal principles for processing personal data.

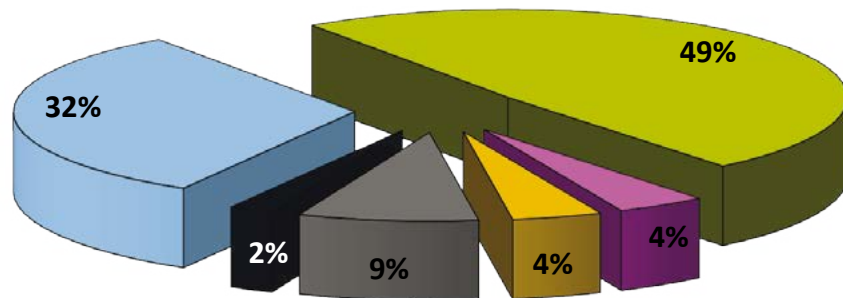
Principle	Personal data processing must be...
1	Fair and lawful
2	For specified and limited purposes
3	Adequate, relevant and not excessive
4	Accurate and up-to-date
5	Not kept longer than necessary
6	Processed in line with data subject’s rights
7	With adequate security
8	Not transferred outside the EEA unless adequate protection is in place

Data security

The 7th data protection principle states that appropriate technical and organisational measures are taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. More than 90% of the Information Commissioner's Office's (ICO) enforcement actions relate to a breach of the security principle.

Reasons for ICO Fines: 2010 - 2013

-  Physical Loss/Theft
-  Disclosed in Error
-  Breach of PECR*
-  Inadequate web security
-  Failure to dispose securely
-  Inaccurate data



*The ICO also issues fines for breach of the Privacy and Electronic Communications Regulations ("PECR") which apply to any organisation that sends out marketing and advertising by electronic means.

Organisations should:

- design and organise security to fit the nature of the personal data held and the harm that may result from a breach;
- be clear about who in the organisation is responsible for information security;
- make sure the right physical and technical security is used, backed up by robust policies and procedures and reliable, well-trained staff; and
- be ready to respond to any breach of security swiftly and effectively.

Particular risks arise when organisations appoint "Data Processors" to act on their behalf. "Data Controllers" are those that determine the manner and purpose of the processing of personal data. Data Processors merely act on the instructions of the Data Controller.

Data Processors currently have no obligations to comply with the DPA; however Data Controllers are obliged to:

- choose a Data Processor that provides sufficient guarantees about its security measures to protect the processing;
- take reasonable steps to check that those security measures are followed; and
- contract with the Data Processor to limit what it can do with the personal data and the security levels that should apply.

In practice, this means auditing a Data Processor before entering into the contract and throughout the duration of the contract.



Case study: Jala Transport Limited

On 3 August 2012, Jala Transport's ("Jala") owner was driving to work. As he stopped at a junction, a thief reached through an open window and snatched the driver's briefcase, which contained a hard-drive containing a database of 250 clients including names, addresses, contact numbers, dates of birth, nationalities and passport numbers. The hard-drive was password protected but was unencrypted. Jala voluntarily notified the ICO of the breach.

Despite Jala being the victim of a theft, the ICO considered that Jala had failed to take appropriate measures to secure the data held on the hard-drive. Jala should have encrypted the data and placed the briefcase in the boot of the car.

The ICO found that the data subjects could suffer substantial distress knowing that the data had been disclosed to unknown third parties and fined Jala £5,000, a reduction from £70,000 in recognition of Jala's voluntary notification.



Lessons learnt

- Consider the effect a loss of data could have on data subjects and ensure appropriate security measures are taken;
- Do not leave devices holding personal data in unsecure locations;
- Encrypt personal data – a password is not enough;
- Keep a secure back up of all personal data; and
- In the event of a breach, consider notifying the ICO to seek their guidance and cooperate with their enquiries.

Data breach response

Generally, there is no legal obligation on most companies to notify the ICO in the event of a data breach. Only "CSPs" (e.g internet providers and telephone companies) have a mandatory obligation to notify the ICO of breaches of personal data under the Privacy and Electronic Communications Regulations 2003 ("PECR").

What are serious breaches?

The ICO has stated that "serious breaches" should be voluntarily reported. The ICO describes the following as factors that will indicate the severity of the breach:

1. **Detriment:** the potential for the breach to cause "detriment" to individuals, e.g. financial loss, physical damage and emotional distress.
2. **Volume:** there is no fixed number of records but the greater the number of records have been lost, the more likely notification that will be required.
3. **Sensitivity:** where the release of data, however small, could cause a significant risk of individuals suffering substantial detriment and distress, then notification will likely be required. A release of sensitive personal data (as defined in s.2 DPA) is most likely to cause such distress. Even a single record could trigger the need to notify if the information is particularly sensitive.

Once notified, the ICO will then consider the nature of the breach and analyse whether the organisation is properly meeting its responsibilities under the DPA.

The ICO recommends the following approach to data breach management:

Contain: Isolate the breach, appoint someone to head up the investigation, appoint forensic experts and report to the police, if necessary.

Recover: Can the data be physically recovered or restored?

Assess: What type of data is it? Is it sensitive? Who does it relate to? How many people does it affect? What harm might the individuals suffer?

Notify: Does the ICO or another regulatory body, such as the Financial Conduct Authority (FCA), require notification? What about the police, customers, insurers, banks or other professional bodies? Consider the seriousness of the breach and the information the ICO will require. Use the ICO's breach notification form.

Evaluate: What needs to be put in place to avoid a repeat breach? Perform a thorough risk assessment and make someone responsible for data security.

Plan now for future EU data protection regulatory change



YASMIN DURRANI
DATA PROTECTION
OFFICER
UKGI, ZURICH



In March 2014, the European Parliament voted in favour of the draft EU Data Protection Regulation, designed to provide a single set of data protection rules to all 28 EU member states. These are expected to be finalised in late 2014 or early 2015, with a 24 month transition period, and while 2017 may seem a long way off, now is the time to be planning ahead to respond to the requirements in an efficient and effective manner.

There are a number of key changes in the current draft to be aware of and a few are listed below:

- **Right to data portability**-people will be able to transfer their data between service providers more easily. However, this data must be transferred in an electronic format which can be easily reused. While this is beneficial for individuals, it could be seen as contradictory to the need to protect data.
- **Right to erasure**-people will be able to request firms to delete their data if there are no legitimate reasons for keeping it.
- **Dedicated data protection officers** must be appointed by organisations processing personal data of more than 5000 data subjects in any 12 month period.
- **More comprehensive privacy notices** must be used on all communications with customers to ensure they understand how their data is collected and how it will be used.
- **Profiling**, as detailed in Article 20, of data subjects is permitted, as long as consent to do so has been obtained from the individual. However, if this profiling affects the interests of the data subject, paragraph five states that profiling should not be solely based on automated processing. Therefore, an element of human assessment should be included.

The impact for brokers

Brokers must be aware that business processes and systems may need to be changed to comply with this regulation. For example, triage processes for new customers may need to change to ensure profiling is not 100% automated; this may require the hiring of staff and additional investment in operational change.

The consequences of breaches

Data breaches would need to be reported to the relevant national supervisory authority in the country of the organisation's main establishment without undue delay, and where possible, within 72 hours.

In the cases of serious data breaches, sanctions may be more stringent, with proposed fines of €100 million or 5% of global annual turnover (whichever is the highest). This is likely to have a huge impact on smaller brokers, who should be aware of this and adjust their contingency plans accordingly.

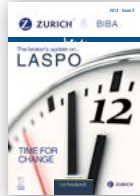
The EU Data Protection Regulations will in general be beneficial for business, and clear up some of the current ambiguity from Europe regarding data protection. However, brokers and insurers alike must be aware of the key changes to the EU's requirements, and should act now to plan for the future.



Other guides in this series are available from the BIBA website – www.biba.org.uk



Employment Law



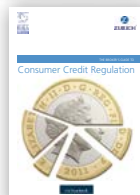
LASPO



Advertising, marketing and branding



Claims



Consumer Credit Regulation

British Insurance Brokers' Association
8th Floor
John Stow House
18 Bevis Marks
London
EC3A 7JB

Find a broker helpline: 0870 950 1790
Member Helpline: 0844 77 00 266
Fax: 020 7626 9676
enquiries@biba.org.uk
www.biba.org.uk