Data security: Protecting your information assets

In the first of a two-part series of articles on data security breaches, Ashley Hurst, Partner, and Louise Lambert, Senior Associate, at Olswang LLP consider some of the major legal issues that can arise in an information security crisis

Ever since the widely reported Sony PlayStation data breach, the security of personal data has been rising up the board agenda for large businesses.

But it is not just the leaking of personal data that is a concern for businesses.

The protection of intellectual property and confidential information can be even more important to some businesses, notwithstanding the fact that the regulatory risks are lower.

With targeted cyber attacks increasing in their scale and frequency, regulators imposing significant fines on private companies for data protection breaches, and the forthcoming overhaul of the data protection regime, there has never been a better time for businesses to take a closer look at this area.

In the first part of this two part article, we look at why these issues are important and at some of the legal challenges that arise in an information security crisis.

In the second part, we will provide some guidance as we look at the practical consequences of security breaches, how to respond in an information security crisis and the steps businesses can take to reduce their risk.

Hitting the bottom line

According to a recent survey by PwC, in 2013 93% of large organisations and 87% of small businesses suffered a security breach.

The average cost to a large organisation of its worst security breach was £450,000 - £850,000, or £35,000 - £65,000 for a small business.

Most serious security breaches were due to multiple failings in people, processes and technology; the root cause in many cases was a failure to educate staff about security risks (source: 2013 Information Security Breaches Survey, BIS/ PwC).

In many cases, the security breaches involved the loss or unauthorised disclosure of personal data in breach of the Data Protection Act 1998 (DPA).

In 2010, the UK's data protection regulator, the Information Commissioner's Office (ICO), acquired the power to impose fines of up to £500,000 for serious breaches of the DPA, and in 2011 similar powers to enforce the Privacy and Electronic Communications Regulations.

The ICO may impose a fine (known as a 'monetary penalty') if it is satisfied that:

(a) there has been a serious breach of one or more of the data protection principles;

(b) the contravention was of a kind likely to cause substantial damage or distress; and

(c) either the contravention was deliberate or reckless, in that the data controller failed to take reasonable steps to prevent it.

Between 2010 and June 2013, the ICO has imposed a total of 40 fines, of which the vast majority related to security breaches.

The highest ICO fine for a security breach to date is £325,000, with the average being around £90,000.

Whilst the majority of fines have been imposed on public sector data controllers (many of whom are obliged to disclose breaches under Cabinet Office guidance), private sector businesses are not immune from fines.

In January 2013, Sony was fined £250,000 by the ICO over the PlayStation hack which took place in 2011. This is the largest fine imposed on a private sector business to date and the third largest fine ever imposed by the ICO.

More recently, in June 2013, fines of £125,000 and £100,000 were imposed on two private companies found to be responsible for over 2,700 complaints to the Telephone Preference Service or reports to the ICO concerning unsolicited calls.

Data controllers in the financial services sector are also no strangers to significant fines.

The Financial Services Authority, recently replaced by the Financial Conduct Authority and the Prudential Regulation Authority, has handed out penalties of up to £3 million in the wake of a number of high profile failings involving customer data, including £1.26 million to Norwich Union in 2007, £3 million to HSBC in 2009 and £2.2 million to Zurich in 2010.

Legal changes on the horizon

The fines imposed to date by the ICO are, however, considerably lower than the fines which might apply in future under the proposed EU General Data Protection Regulation which, if adopted according to the European Commission's timetable, could come into force as soon as 2016.

Amongst various new proposed requirements for data controllers, Article 79 of the draft Regulation provides that "the supervisory authority shall impose a fine up to 1 000 000 EUR or in case of an enterprise up to 2% of its annual worldwide turnover".

For the largest global businesses, 2% of annual worldwide turnover is enough to make board members sit up and take note.

In addition to the draft EU General Data Protection Regulation, there is also a draft Directive which would impose new obligations on e-commerce platforms, social networks and key infrastructure providers to have formally documented security policies, undergo security audits and report cyber attacks to national authorities.

The Network and Information Security (NIS) Directive is broader in scope than the EU General Data Protection Regulation, because it will impact upon the integrity and business continuity of networks and services generally, regardless of whether personal data is compromised. For example, the Directive will also cover intellectual property, which is often the target of cyber attacks.

Risks and legal issues in an information security crisis

There are many different types of information security crises, ranging from the theft of a laptop to a major computer hack, but the issues are often the same and can include the following:

- reputational damage;
- regulatory action or criminal investigation or prosecution, leading to fines and other penalties;
- business disruption;
- legal claims for compensation from customers or employees; and
- disclosure of commercially sensitive material to competitors.

To make matters worse, many of these issues arise simultaneously, the result of which can be panic, poor judgment and lack of control.

Whilst in any information security crisis, the initial focus will be on containment and establishing what has gone wrong, those in charge will very quickly need to address a whole range of legal and commercial issues.

"Whilst in any information security crisis, the initial focus will be on containment and establishing what has gone wrong, those in charge will very quickly need to address a whole range of legal and commercial issues"

The matters that should be addressed include those set out under the headings that follow.

Vulnerability/data containment

Practical and legal steps can be taken to track down the data in question and determine the extent to which it has already been disseminated.

For example, disclosure orders may be obtained against third parties to reveal the identity of a hacker or orders obtained to restrain the use of the data, even if the identity of the culprit is unknown.

Regulatory issues

A number of regulatory issues may be raised in an information security crisis.

Where the data constitutes personal data, the UK currently has a voluntary regime for notifications to the Information Commissioner.

However, there is a presumption that when the breach is serious, organisations will file a report with the ICO.

Where there is an international element, reporting obligations in other jurisdictions (which may be inconsistent with those in the UK) also need to be considered.

Where the data are held by an entity subject to specific regulation (for example the Financial Conduct Authority), additional reporting to the relevant regulator may be necessary and/or advisable.

In some circumstances, it may be appropriate or necessary to liaise

(Continued on page 8)

(Continued from page 7)

with the police. This may be the case particularly where Computer Misuse Act 1990 or Regulation of Investigatory Powers Act 2000 issues are engaged.

Reputation management

Often there will be significant and adverse media coverage of a data security incident. Sometimes there will be a concern that the information itself will end up with a media organisation.

In these cases careful management of the organisation's reputation will be crucial.

Third party notification and complaints

It will usually be prudent to notify affected individuals about the incident and in some cases to provide guidance to help them protect themselves against heightened risks, such as identity theft.

The incident may also give rise to potential legal claims from affected third parties which will have to be considered.

Claims against third parties

It may be that the data breach was caused by the actions of a third party, such as a contractor.

In such cases, consideration may be needed as to whether it is possible to make a claim against that third party for the loss incurred.

With significant costs of managing the incident mounting up, a potential claim against a third party may need some urgent attention. There may be a number of tactical decisions to be made about matters such as the time at which greatest leverage can be exerted over contractors, their visibility in any reputation management issues, and their co-operation with any ensuing internal investigation or regulatory scrutiny.

Employment

Where the loss of data has been due to the activities (whether deliberate or accidental) of one or more employees, disciplinary action may be called for. This may include suspension, or even dismissal, of the employees involved.

Also, where the data in question concerns employees, they may themselves have complaints and potential legal claims against the company.

Legal privilege

If the incident is serious, often an investigation is undertaken. This may be conducted internally (for example by internal audit).

Where an investigation is conducted by third party advisers, ensuring that all necessary steps are taken to secure legal privilege is important to protect the organisation.

Legal privilege is, of course, also relevant to other communications at all stages during and after the immediate crisis.

It is very easy, however, to list these issues in calm conditions. When the storm hits, the theory needs to be supported by proper procedures and sound judgment, which comes from experience and preparation.

In the second part of our article, in the next issue of this journal, we will provide guidance as to the practical steps that can be taken both during an information security crisis and to prevent a crisis from happening in the first place.

Ashley Hurst and Louise Lambert
Olswang LLP
ashley.hurst@olswang.com
louise.lambert@olswang.com