Technology and Telecommunications

bulletin

OVAL Insurance Broking

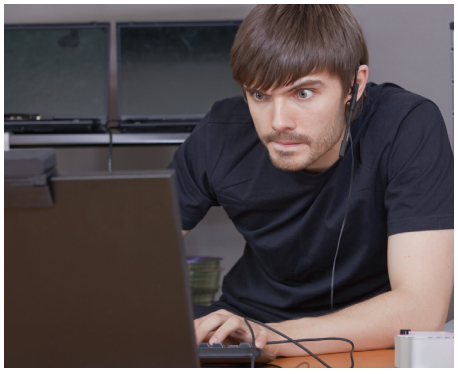
Electronic Data – Can you afford not to be protected?

'Once more unto the breach, dear friends, once more'

Since the Sony PlayStation hack in April of this year the media has been awash with headlines about big businesses being hacked, institutions facing daily attacks and personal information being compromised. Yet these well publicised attacks are just the tip of the iceberg, little is heard in the UK of breaches suffered by professional organisations, small businesses and public bodies. In a recent report by Detica published jointly with the UK Cabinet office "cyber crime" was estimated to cost UK businesses around £27 billion every year.[1]

A Selection of Headlines over the last six months

- **Scots QC rapped for failing to encrypt stolen laptop (Herald Scotland 17 November 2011) (www.heraldscotland.com/news/home-news/scots-qc-rapped-for-failing-to-encrypt-stolen-laptop-1.1135306)**
- **Three quarters of tech firms hit by cyber criminals (City A.M. 21 November 2011) (www.cityam.com/news-and-analysis/three-quarters-tech-firms-hit-cyber-criminals)**
- **Government slams councils over £7m online payment scam losses (v3.co.uk 14 November 2011) (www.v3.co.uk/v3-uk/news/2124871/government-slams-councils-gbp7m-online-payment-scam-losses)**
- **Rochdale Council loses 18,000 residents' details on unencrypted USB stick (v3.co.uk 03 November 2011) (www.v3.co.uk/v3-uk/news/2122401/rochdale-council-loses-residents-details-unencrypted-usb)**



Whilst a whole market has arisen from the proceeds of cyber crime and organisations with an anarchic stance are causing mayhem, it is important to note that it is not just the activities of these groups that can compromise your system. Data can also be lost as a result of:

- Employees either looking to profit or disgruntled at their treatment;
- Industrial espionage looking for trade secrets;
- Extortion, or threat of extortion;
- Careless loss of laptops, phones, memory sticks and other hardware containing data;
- Introduction of malware or virus;
- Accidental actions or inactions of employees, e.g. mis-keying;
- Natural Disasters.

The cost of a data breach hugely depends on where you are conducting business and the type of loss you have suffered. In its report on data breaches in 2010, the Ponemon Institute put the average cost of a data breach in the US at $214 per compromised record[2]. In the UK this figure is £71 per compromised record - up 13% from 2009[3].

The reason for the difference is that in the US, 46 of the States have a legal requirement to notify individuals if they may be affected by a data breach. In the UK there is no similar requirement, however the common consensus is that this is likely to change very soon.

In the UK it is the Information Commissioner's Office (ICO) that governs compliance with the Data Protection Act 1998 and they have the power to commence audits, impose fines of up to £500,000 or to bring criminal proceedings against those breaching the Act.

Under the Act it is the "seventh principle" that is the most commonly breached this is: 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.

So any company that is storing or handling personal data, whether that be customer or employee records, has a duty of care to make sure such measures are in place to prevent unauthorised use or access.

Whilst regular monitoring and a reasonable level of security is almost a mandatory requirement no system is full proof. Security programmes quickly become dated, employees have easier access from the inside, and human error will mean laptops and memory sticks get left on trains. For the companies utilising the Cloud there are the ongoing questions about its security.

Following a security breach where are the costs to a company?

- The major costs of a data breach are in its rectification. These include costs of forensic testing to identify the cause, the solution required to remedy this and the costs required to recover, replace or rekey any lost data;
- There is the cost of notifying customers of potential privacy breach including writing to each customer and the possibility of providing credit monitoring to each one;
- Legal costs and claims made by third parties who have suffered a financial loss following a data breach;
- Costs of complying with regulation and any fines and penalties imposed by the regulator;
- Loss of profits or revenue due to downtime of systems;
- Legal and business costs in defending claims for theft of Intellectual Property (IP).

[1] Detica & Cabinet Office, The Cost of Cyber Crime 2011
[2] Symantec Corp & Ponemon Institute, 2010 Annual Study: US Cost of a Data Breach 8 March 2011
[3] Symantec Corp & Ponemon Institute, 2010 Annual Study: UK Cost of a Data Breach 21 March 2011

Electronic Data – Can you afford not to be protected? - Continued

Whilst the listed costs are financial it must not be overlooked that the biggest cost to a company could be reputational damage, which will often have a far greater impact than any rectification costs as Sony has recently discovered.

A well structured insurance programme will help a company finance these costs and the data recovery procedures should a company suffer a loss, cover can also include Public Relations costs to help limit reputational damage.

Whilst all necessary precautions may have been implemented by a business at its own locations, additional risk lies where there is a dependency on suppliers. The knock on effects of a supplier suffering a data breach need to be considered, this is especially pertinent in relation to the Cloud. It is important to note that businesses that outsource their work to third parties are not transferring the liability that comes with the use of data, under the Data Protection Act 1998 a Data Controller is defined as "a person who determines why and how any personal data will be processed". So whilst a business might use a third party it still has responsibility for any data transferred to that third party. At Oval we provide our clients with a tailored insurance solution that will not only provide cover for the traditional physical exposures of fire and theft, but also respond effectively to modern, non physical perils that are associated with technology.

These include:

- Costs of rectifying a data breach;
- Notification of clients;
- Credit monitoring;
- Compliance with regulatory procedures;
- Where permitted by law costs of fines and penalties;
- Business interruption and loss of profits;
- Managing reputational risk;
- Protection of intellectual property assets;
- Crisis management response;
- Critical value of suppliers and large customers.

In addition we are also able to offer consultancy advice on Network Security, Data Protection and Business Continuity that will help reduce the likelihood of a claim and mitigate the effects as a result of one.

Whilst this article relates to electronic data, do not forget that data can also be stored in other forms such as in paper files, and these can often present a higher risk than electronic data, and the effects to a business can often be the same.

For further information please contact Richard Hodson, Head of Technology, Media & Entertainment 020 7422 0193 or email richard.hodson@theovalgroup.com

The Oval group

Since Oval was established in October 2003 we have built a strong national business by acquiring, and integrating, high quality regional brokers and financial advisory companies.

We hand picked companies that already had excellent reputations in their regions and were known for their attentive approach. Our success is based on delivering first-class service, locally, to clients throughout the UK.

Our clients range from multinationals and small businesses to sole traders and private individuals.

To date, 33 companies have joined the Oval group and we now have more than 1,200 employees across the UK supporting our clients.

As an integrated group comprising insurance, risk management, healthcare and financial advisory specialists, we bring a wider range of expertise to the table.

At the heart of our business is an emphasis on service excellence and total commitment to client care. We constantly aim to exceed your service expectations and we are proud of our client retention rate.

Oval Insurance Broking Limited
Registered Office: 9 South Parade, Wakefield WF1 1LR
Registered in England No: 01195184
Authorised and regulated by the Financial Services Authority.

www.theovalgroup.com