DATA PROTECTION

Public bodies and businesses often hold large amounts of sensitive customer information. What procedures should they be considering to protect it from loss or theft?

When the PlayStation Network – a portal for PlayStation 3 users – suspended service in April 2011 it emerged that the network had been hacked. The personal information of millions of customers, including names, addresses, email addresses, dates of birth, account passwords and even payment card details was at risk.

In January 2013, owner Sony Computer Entertainment Europe Limited was fined £250,000 for what the Information Commissioner's Office (ICO) described as "one of the most serious [breaches] ever reported to us". In its ruling the ICO added that the attack could have been prevented had Sony's software been up to date.

This breach followed a number of high-profile privacy and data protection infractions, which were highlighted during the course of the Leveson Inquiry. In January too, more than 250,000 Twitter users had their accounts hacked.

Every organisation holds information on its customers and with this comes a legal responsibility to protect it. So what procedures should be in place to protect against its loss or theft?

"Organisations like ours need to review what data we hold, how we hold it and what we do with it," says Travelers Europe Head of Legal and Compliance, John Abramson. Organisations need to be aware of the requirements of the Data Protection Act (DPA) in the UK and Ireland.

ORGANISATIONS NEED TO BE AWARE OF THE REQUIREMENTS OF THE DATA PROTECTION ACT (DPA) IN THE UK AND IRELAND

The DPA defines two types of data: personal and sensitive. 'Personal' is data by which a person can be identified, such as a name, address or a UK National Insurance number. 'Sensitive' is data such as medical and criminal records. Under the DPA, organisations that hold these types of data are legally obliged to process it fairly and lawfully, to obtain the explicit consent of the subject before processing sensitive data and to take appropriate measures to prevent unlawful processing or disclosure.

On the latter point, the ICO website outlines a number of different security measures that organisations should put in place to protect the data that they hold. These include steps such as installing a firewall and viruschecking software on computers, encrypting personal information held electronically, shredding all confidential paper waste and checking the physical security of your premises. There's also an onus on organisations to provide staff with training so that they're aware of potential security risks and know not to do anything that could allow the

leaking of information and bring an organisation into disrepute.

ORGANISATIONS ARE RESPONSIBLE FOR THE ACTIONS OF THEIR THIRD PARTY SERVICE PROVIDERS

Organisations are responsible for the actions of their third party service providers which has become ever more important in an age where outsourcing back-office functions and using call centres overseas has become common. "Not every country in the world has the same level of data protection as the UK, Ireland or other countries in the EU," cautions Abramson. "Countries like India, Singapore and the Philippines have different data protection laws, but it is an organisation's responsibility to ensure that any data it transfers to a third party is handled with the same level of protection as in the UK and Ireland."

As a result there are various levels of protection that organisations can impose on their outsource providers. "There could be procedures put in place to prevent workers being able to download any data," says Abramson "This might include preventing people coming to work with briefcases, writing materials or electronic devices. Workers might also be screened when they come into a building and when they leave. And when they are accessing data they could be given careful password access and only access the data that they need in order to fulfil the part of the contract that they are working on."

In addition to the legal imperative to make sure that personal information is held securely in the UK, Ireland and overseas, there's a commercial argument for having good procedures in place, according to the ICO. "Good information handling makes good business sense," it says on its website. "Organisations that look after people's data correctly will enhance their reputation, increase customer and employee confidence, and by ensuring that the information is accurate, save both time and money."

For those organisations that don't take these responsibilities seriously, the ICO issues the following warning, "The recent monetary penalty of £250,000 we issued to Sony Computer Entertainment Europe Limited following a serious breach of the Data Protection Act shows that irrespective of a company's size, all organisations owe it to their customers to keep their information secure," says the ICO spokesperson. "We have published a range of guidance and offer support to organisations to help them achieve this, but will consider taking action where it is clear that an organisation has failed to meet its legal obligations under the Act." ■

THIS ARTICLE FIRST APPEARED WITHIN TRAVELERS CODE RED, SPRING 2013 ISSUE.

Click here for more information on our Technology products for the IT & Communications and Electronic sectors

INDUSTRY*Edge*®

LEGAL CONFLICTS

The complexities surrounding an individual's right to privacy under the Data Protection Act, with the legal requirements imposed by the Freedom of Information Act (FOI), was underlined in a case that came before the Court of Appeal in December 2012.

The claimant, who was resident at a secure facility for children run by Durham County Council between 1980 and 1984, appointed a solicitor to make a civil claim for damages for the injuries he suffered while in the secure unit. Under the terms of the Data Protection Act the claimant's solicitor contacted the council to request his personal files from the facility, yet these files were redacted by the council to protect the identities and privacy of other children who were named in the record.

The claimant's solicitor argued that the other children could be potential witnesses and that withholding their names prevented his client from having a fair trial. The case came before the Court of Appeal, which ruled that the names of the other children should be disclosed as part of a trail of enquiry.

BRING YOUR OWN DEVICE

Over the past decade or so, there's been a cultural shift in the way that organisations operate, with a significant increase in the amount of home working and employees undertaking more work-related tasks on devices such as smartphones and tablet computers. As a consequence, there's a greater opportunity for breaches of security, yet the legal requirements on businesses remain the same regardless of where employees are working and what device they're working on. To ensure that the company abides by the law and stops breaches occurring, Travelers has put in place a series of security measures, says John Abramson.

WE ONLY ALLOW THE USE OF MEMORY STICKS THAT ARE ENCRYPTED AND THAT CAN ONLY BE USED ON A COMPANY LAPTOP OR COMPUTER

"We only allow the use of memory sticks that are encrypted and that can only be used on a company laptop or computer," he explains. "So if somebody loses a memory stick with data on it, it can't be accessed. Our laptops are similarly protected and people can only work from home on a Travelers laptop. We don't allow any access to our system from a computer that isn't subject to our own security system."

Similarly, if a Travelers employee loses an iPad or BlackBerry, the memory of the device can be wiped remotely. "If a lost BlackBerry is found it will have factory settings and no data on it," says Abramson. "We're very conscious of the fact that people routinely work remotely on iPads and Blackberries. That's just the nature of work today, so we've had to take the necessary steps to protect our clients' data."

Travelers Insurance Company Limited
61-63 London Road, Redhill, Surrey RH1 1NA
Europa House, Harcourt Centre, Harcourt Street, Dublin 2, Ireland
Travelers Insurance Company Limited is authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority in the UK and is regulated by the Central Bank of Ireland for conduct of business rules.
Registered office: Exchequer Court, 33 St. Mary Axe, London EC3A 8AG. Registered in England 1034343. Registered as a branch in Ireland 903382.
travelers.co.uk **travelers.ie** TRV2400