

Citizens suffer as cyber war waged on all fronts

The flow of data is seemingly endless from the public and private institutions that are tasked with gathering, processing and safeguarding our personal information. One would have thought that the introduction of various legislative instruments over the last ten years in Ireland and other jurisdictions would have had an impact, but it doesn't seem to be the case.

We don't need to go into Her Majesty's Revenue & Customs' spectacular loss of the records of 25 million British citizens, but it was certainly one of the high(low)lights of the year.

Just to put it in context, the following are a list of the losses of personal information, both in Ireland, Britain and further.

Department of Social and Family Affairs in Ireland: in 2003, an employee with access to personal information made it available to a relative with criminal intent - it was used to plan burglaries and extortion.

This department was again the subject of attention from the Data Protection Commissioner this year when it was uncovered that staff in the department were supplying private investigators with information in exchange for cash on citizens from the data stored in the department.

The Driver and Vehicle Agency in Coleraine in Northern Ireland had a loss of data in November 2007 that saw the information of more than 6,000 drivers lost in transit on two CDs en route to the Driver and Vehicle Licensing Authority in Swansea.

The British Driving Standards Authority, within the Department of Transport, had to apologise in the last weeks to millions of learner drivers after a hard-disk with their details was lost by a US contractor in the state of Iowa.

In Britain, Revenue & Customs was in the spotlight for seven other data losses in the last 24 months.

In the United States, the Veterans Administration was in the spotlight this year. It lost details on 12,000 staff and veterans after PCs and laptops were stolen. While a concern, it pales into insignificance when compared with the loss of details on more than 24 million veterans and staff in 2006.

Again in Britain, there were losses reported at Leeds Building Society, the Nationwide Building Society (which was fined stg£980,000 by the Financial Services Authority), Norwich Union Life was fined stg£1.26 million for financial losses suffered by customers and so on.

A very useful reference site for these incidents is <http://www.privacyrights.org/ar/ChronDataBreaches.htm>. Other issues that last year threw up were the rise of the Super Botnets.

These armies of infected machines, which were offered for sale on the internet for various nefarious tasks such as spam generation, grew to staggering new sizes. Various estimates of the size of the Storm Botnet have been from 250,000 infected or compromised computers to more than one million.

Alleged state-sponsored cyber warfare has also raised its head this year with the denial-of-service attacks against the internet infrastructure of the most internet-aware country in the world, Estonia.

The Estonians allege that the Russian state was responsible for the overwhelming of their international internet connectivity and this had a significant impact on the state that has such heavy usage of the internet.

The worrying thing for many people with the increased loss of personal data is the use of this information for identity theft and fraud.

After Monster.com was hacked and more than 1.6 million records of job applicants was stolen, significant fraud was perpetrated against people whose data had been stolen in very sophisticated spear-phishing attacks.

In terms of the new year coming, what are we likely to see? More of the same. This means we will see more data losses, and these being exploited, and more people being defrauded. These losses, while often recoverable, can be devastating and extremely traumatic.

It will be interesting to watch the information coming from audits carried out by the Data Protection Commissioner's office in 2008 and also from his counterpart in Britain who is seeking similar powers as those bestowed on the Irish Commissioner.

The HMRC incidents have given the Information Commissioner all the ammunition he needed to get these extra powers.

Rits Group Head Quarters
Information Security Centre
2052 Castle Drive
Citywest Business Campus
Co. Dublin
Ireland

Tel: +353 (0) 1 6420500
Fax: +353 (0) 1 4660468
Email: info@ritsgroup.com
Web: www.ritsgroup.com