Personal Data Loss

This has been a very bad year for the average punter worried about the level of effort companies are putting in to protecting his or her private information managed by that company.

While there is strong legislation in place in the Data Protection Act in both the UK and Ireland, it would appear that many organisations are still not managing the personal and private information of their customers or employees properly.

Through 2006, we have heard of many stories of personal information being accessed in an unauthorised way in the United States of America. The type of information that was compromised in these cases was usually Social Security Numbers, name and address, date of birth, bank account details etc. These led in many situations to people suffering a level of fraud as their identities were stolen, or attempts were made to steal them. For anybody that this has happened to, it is an incredibly stressful and unpleasant experience. People feel violated and it can end up in their whole world being turned upside down. It can take months, or even years to recover your good name and previous credit history.

During the latter part of 2006 we saw a number of instances in the UK of similar losses or unauthorised access to personal information. These ranged from confirmed unauthorised access and breaches of databases by employees in a number of UK Government departments to the loss of data due to hardware theft. In London, a laptop containing the payroll and pension details of 15,000 Police officers was stolen from the offices of an external IT consultancy company. These officers would naturally be concerned about their personal information being available in the public domain, not just from a financial fraud perspective but also from a personal security perspective.

This theft was just one of a number of examples in Europe this year where laptops in particular belonging to external auditors or consultants were lost or stolen and was subsequently found to have personal, sensitive data on them. In many circumstances, the storage of this type of information on an unencrypted laptop was in breach of policy within the companies, but this is of little solace to those whose details have been compromised.

Many financial institutions are investigating the areas of outsourcing to help manage costs in different areas of their business. Areas such as call centres, information technology and records management have been the most common areas to be outsourced, and yet these are often the ones with access to the most sensitive information. In an area such as records management or the offsite storage of backup tapes, there is often little or no effort taken to perform a risk analysis on the change in work practise. For instance, very few organisations today are taking the effort to update backup software/hardware with encryption capabilities if they make the decision to outsource their backup media management to a 3rd party. Earlier this year, Bank of America lost backup tapes with the detailed financial records of more than one million Government employees. GE admitted to losing the details on more than 50,000 on a laptop that was stolen from a hotel room.

This will definitely be one of the hot topics for 2007. Organisations must ensure that where they have databases of information on their customers and employees,

©Rits 2005

access to this information must be granted on a need to know basis, this access is audited and reviewed on a regular basis and that the security controls protecting this data are regularly reviewed. In Australia this summer it was found that staff in the Government agency tasked with managing the databases that control social security benefits such as unemployment and pension payments. There were nearly 800 breaches by more than 600 staff gaining unauthorised access to this data.

Last year, an undercover reporter was able to purchase a CD-ROM from a call centre employee in India that contained the personal information of thousands of customers of a company that outsourced their call centre to India.

Just because stories are not making the headlines in Ireland with regard to large-scale personal information theft, it does not mean it is not happening, or about to happen.

On a lighter note, it appears that the hacking community out there have a little too much time on their hands! Online games such as Second Life and World of Warcraft are being targeted by these people. Second Life owners Linden Labs recently had to shut down most of their 2,500 servers to clean up a outbreak of “grey goo”. This is not some sort of plasma ejected during an intergalactic sneeze but is actually a reference to a Worm that was unleashed in the online worlds of Second Life. Gamers were attracted to bouncing gold rings in the online world and on contact caused them to replicate. All this to the audio sounds from Sonic the Hedgehog….. World of Warcraft, another online game with multiple players has also been plagued by attacks within the game.

We are now heading into a season where the IT security professionals are on a heightened state of alert. The holiday season is usually a time of increased hacking activity. A number of reasons have been attributed to this and they include the fact that college students are on holiday and have time on their hands and many people are buying computers for the Christmas gift season and are not often aware of the risks etc. The same principles as always apply for a safe online experience this Christmas; Up to date anti-virus software, a firewall and apply the software patches from companies like Microsoft as soon as possible. Don’t open attachments received via email, even if they appear to be from someone you know unless you are expecting that specific file.

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

©Rits 2005