Keep Private Data Safe

These last couple of weeks have dealt some very severe body blows to the trust levels between ordinary citizens in Ireland and the custodians of their personal information.

It emerged in news reports following Freedom of Information requests to the Department of Social and Family Affairs that there had been a breach of their information security within the department.

It would appear that an employee had been supplying personal data on potential extortion and burglary victims to his criminal brother.

This employee had credentials that permitted him to access the Central Records System within the department and it is from here that he was able to gather this information.

Having passed this information to his brother, a number of crimes, or attempted crimes were perpetrated against these people.

This issue came to light following a Garda investigation into an extortion attempt and the subsequent arrest of the civil servant's brother. It would appear that he had a paper printout on his person that contained information on the would-be victim.

Gardai approached the department with the information and an investigation ensued.

What is worrying from an average citizen's perspective is the apparent ease with which this person was able to get access to very sensitive personal information and remove it from the environs of the department.

In too many organisations today there is a situation that once you have been given authentication credentials to the main network-based systems, you have access to all information stored on the networks. There is a level of trust and access applied to all staff regardless of the section they are working in.

Organisations must start to treat information that is held about citizens, as well as other potentially sensitive information as a resource that one should be privileged to access, not entitled to.

There is a responsibility on the data owners within an organisation (and if such a concept does not exist, it must be created) to authorise access to the data at an individual level.

This access must be reviewed on an ongoing basis to ensure its continued accuracy and appropriateness. It is vital that this is performed regularly to ensure that as staff move within an organisation and their job role changes that they do not continue to have access to information that is no longer appropriate.

In the case of the access to information within the department, it would appear from the information released that there were significant volumes of audit trail or logging data available. This would have allowed the investigation to determine with some accuracy the amount of information accessed, by whom and when.

While it's important to record this activity, in many cases it is used only for post incident analysis. However, it should be possible to use this information in a more proactive way.

For instance an application analysing this information on an ongoing basis could warn that a person working within the data protection unit in the department was generating an unusual level of queries, or queries to information that he had had no business need to access.

Another example is that shortly after a person in Limerick won a vast sum on the Euro Millions lottery, there were a significant number of queries within a government department to access the winner's personal details on those computer systems.

This issue is not unique to the Department of Social and Family Affairs. Many organisations, both state and private, will be at risk to this sort of data theft and unauthorised access.

This has to be a focus area for the Data Protection Commissioner in the future. Once an organisation has a valid requirement to maintain information on citizens, they must implement appropriate controls to protect access to that information. The approach must be based on the ‘need to know' principle and the least privilege necessary to carry out one's job role.

Unfortunately, a market has grown for this kind of information. We have seen high-profile incidents linked to criminal behaviour such as the one mentioned above.

There is significant anecdotal comment regarding payments to junior officials in financial institutions as inducements to supply financial records to private investigators. This data has been used by the private investigators in cases of fraud and also for family law cases.

We have been aware of civil servants that have been approached during lunch breaks and requested to get personal information and offered bundles of cash for this.

Apparently, there is a culture in a number of organisations holding significant amounts of sensitive personal information to make queries about celebrities, politicians and coworkers. There is a responsibility on management within any organisation to ensure that this sort of conduct is not acceptable and that any breach of this policy will result in disciplinary action.

Another area that needs attention is the management of potential conduits from the organisation of sensitive or confidential information. While it is difficult to manage the theft of information on paper after printing, it is easier when an attempt is made to remove the data electronically.

This is often the preferred method as the data is more readily usable than if it was printed. The conduits in question would include e-mail, web-based e-mail, USB flash disks and hard disks, CD/DVD burners, portable media players, personal or business-related laptops.

Organisations that have significant volumes of personal information gathered and stored in information systems must start living up to the responsibility that holding such data imposes. It is no longer acceptable not to have Data Ownership assigned and access rights managed.

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