

Security must come first

Sunday, October 05, 2008

Customers giving personal information to an organisation have a right to be protected and not to be exposed due to negligence.

Over the last couple of years we have had an almost constant barrage of news items where personal, and sometimes sensitive personal, information has been lost or stolen by its custodians.

Given the amount of public information on these data losses, one has to ask - how can there be any more? And yet there are. Week after week we are hearing about Bank X and Department Y losing information on its customers and citizens. To paraphrase those oft quoted lines from Oscar Wilde: "To lose personal information once is unfortunate, twice is careless and the third time is unforgivable."

We must also be concerned about the likely amount of data losses that occur that do not make it into the public domain.

When these stories do come to light, much is made of the controls in place on the laptop, USB stick or back-up tape the data was stored on. "It was password protected," they say or, with self-congratulatory smugness, "we applied military-grade encryption to the device", and so on.

In the majority of cases in Ireland to date in which personal information was lost or stolen, there were no real security controls of any sort applied. The one exception to this to date has been the Irish Blood Transfusion Service Board. A laptop of that organisation was stolen during a mugging in New York, but was appropriately encrypted to protect the sensitive personal information stored on it.

However, we must remember that full hard disk encryption is only as secure as the credentials that are used to unlock the encryption and access the system. There are many solutions out there today that will implement full hard disk encryption and they offer many different authentication systems.

Some will use the traditional userID and password, some will require the unlocking via passphrase of a digital certificate and others will require a hardware token as well as a userID and password. Some will even utilise biometrics such as rudimentary fingerprint analysis.

The point is that the devil is in the details as to how a firm chooses to implement authentication options where full hard disk encryption is deployed.

The risk assessment that must be carried out to determine the appropriate controls should take into account the classification applied to the data stored on the device, the likely adversaries in the event of data loss and the types of users that will be supplied with these devices.

The education and security awareness of the users of these devices is also fundamental to the protection of the information assets stored on the devices. We have seen where industry-leading full hard disk encryption has been applied to a laptop, and the userID and password given to the user. The user has then written

down the userID and password on a piece of paper and stuck it to the keyboard area with clear tape so that it would not wear when they were typing.

In this scenario, the policy of the organisation was implemented and senior management would have felt that their investment in encryption would ensure they were protecting their information assets.

However, as the users were not made aware of the implications of their actions, they totally undermined the investment and made the information readily accessible to anyone with physical access to the laptop. Worse than that, once the encryption software had authenticated the user, they were automatically logged into Windows and had access to the remote access services of the organisation.

In effect, the userID and password on the encrypted laptop were the keys to the kingdom; the user now had access to all data on the laptop, if they attempted a remote access server (RAS) connection, they would be automatically connected to the organisation's internal network as it was assumed this was coming from a secure connection.

The picture is now suddenly a disaster - the breach has moved from one single repository of information assets being compromised to all information systems of that organisation, and any of its connected peers, being compromised too.

In my opinion, the data owners and custodians in organisations are responsible for the access controls that are applied to prevent unauthorised access to their information.

For instance, when applications are being developed that allow users to access information systems from RAS devices, the data owners should be querying whether or not there is a requirement for any of that information to exist on the RAS device?

Can the applications be deployed using thin-client solutions such as Citrix or Terminal Services and configured so there is no data footprint on the RAS device at any time? If the RAS user will be working in areas of limited internet access and the internet is the RAS medium in use, can the user work in an offline mode and synchronise data when next connected? If that is the case, does the application support the removal of data locally on the RAS device once it is no longer relevant?

These sorts of questions and decisions will assist in trying to limit the amount of data that could be compromised should the laptop be lost or stolen.

It is no longer acceptable that "road warriors" should be able, or need, to download a complete database or information store of personal data to an RAS laptop, as they will be out of the office for a period of time. If it proves necessary to process information when offline, only a relevant subset of information should be extracted to the encrypted device. This information should then be expunged from the device when appropriate.

Organisations of any size that are gathering personal information on their customers must ensure that they are compliant with the Data Protection Act. The Office of the Data Protection Commissioner will provide specific and pragmatic advice to organisations that are unsure of their responsibilities and the controls that they must apply.

In larger organisations, there is often a Data Protection compliance unit that is

responsible for the registration and management of the relationship with the ODPC. They also have a responsibility to ensure that all data owners are aware of their responsibilities when it comes to personal information and to ensure staff are aware of their responsibilities.

More attention than ever is being placed on the management and security of personal information, and rightly so. The responsibilities on organisations that fall under the terms of the Data Protection Act have increased with the widening in scope of the act to include structured paper-based filing systems, not just IT-based data storage systems.

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