

Security - plugging and avoiding data leakage

By Rob Bamforth, Principal analyst, Quocirca Ltd

All organisations depend on safe, reliable and secure storage of their digital records, but the challenge of securing this information is becoming more difficult due to expansive global networks, more users and increased data portability and mobility.

This internetworking means that physical and logical perimeters around the organisation no longer apply, so the security of applications, the end points of access and the data itself needs to be taken even more seriously and become more fine grained – focused directly around the items being secured.

In addition, despite the melting away of the perimeter, the security risks for all organisations have always been from internal as well as external sources. These can come from the deliberate or accidental acts of employees, or weaknesses in business processes.

External threats vary from those that threaten the resilience of the business – terrorism, weather disruption or communications breakdown – where records might still be 'lost', to those that are malicious or deliberate acts for financial gain, sabotage, notoriety or a prank – stealing, spying and hacking.

Whether as a result of an accident or deliberate act, the end result is that data has leaked outside the organisation, with potentially disastrous consequences. Some accidental data loss may appear to only necessitate a simple short term cost to repair or recreate, but could have further negative impact on corporate image or increased regulatory scrutiny in the longer term.

Deliberate acts are likely to have far more direct consequences to actual data and the concern that it may have fallen into the wrong hands, but the accidental leaks are more likely to cause indirect consequences, such as damage to a brand.

The first objective in mitigating internal or external vulnerabilities is to define which particular resources need to be protected the

most, and identify the range of threats they face so that appropriate measures can be put in place.

It is important to distinguish between information that is critical or sensitive – for example customer, patient or accounting records – and information that is simply a collection of public knowledge. Somewhere in between lays general purpose internal information, such as emails, where content may vary from mundane to secret and care needs to be taken to ensure suitable protection is in place.

While the organisation's physical perimeter could at one time be relied upon to provide a level of protection, the use of open networks like the internet, wireless and public cellular networks, mobile devices and tiny high capacity storage devices mean this is no longer the case.

Information can be detected and snooped while travelling over these networks and small smart devices are highly vulnerable to loss or theft. Organisations now have to focus their security efforts on specific resources - the applications/databases, end devices used for access, the users and the records themselves.

Those with access to managed information need to understand how and why the information is being protected, and their role in ensuring it is kept secure. The onus is then on the organisation to keep security processes as simple as possible to accomplish the level of security required.

This means identifying where security needs to be tight, and where it can be relaxed, and to distinguish how policy or controls should be applied.

If the organisation is providing tools that can offer more security, users need to be fully educated in the effective use, and must appreciate the consequences of incorrect actions.

The best way to set this out is as follows:

- **Start with a pragmatic and granular security policy based on business needs.** This should follow good common business sense that can be easily justified as a means of protecting the organisation's assets, but still operating to fit within day to day working practices.
- **Engage users with consultation, not prescription.** Any policy must be well communicated throughout the organisation and delivered using well understood business procedures. Involving users early will generate trust and encourage responsible behaviour in return. They need to appreciate any security challenges faced, understand the measures being put in place to tackle them, and how they play their part.
- **Automate procedures with technology where possible.** If the policy dictates the use of strong passwords, encourage or compel users to change these regularly, and have systems automatically refuse passwords that are too short or simple. Anti-malware and firewall protection must be installed on every device and updated regularly, but it is important to make sure that these products themselves do not render the very devices they are there to protect unusable – so choose carefully. Known risk areas such as mobile devices must be properly configured by default and before deployment.

- **Train users before, support during.** Run comprehensive training, use workshops and user participation to establish best practices and etiquette that everyone can buy into. From then on ensure users are kept informed and updated with any changes and that they have a simple and straightforward route for getting support in the event of a security problem. One number to call, one website to visit, one email address for support.
- **Strictly enforce policy to show they are important.** Policies must have consequences to be effective, and there are times when rules must be enforced. These must be clear and understood from the outset, so that violators are not surprised. As with any form of disciplinary practice, enforcement should scale according to severity and frequency of the problem.

Records management security is not something that should be buried deep in the IT department, or seen as an arcane art, but as a set of business principles with the intention of ensuring efficient and safe functioning of business processes. Just as all individuals play their part in their respective business processes, so they all play a part in ensuring security.

About Quocirca

Quocirca is a primary research and analysis company specialising in the business impact of information technology and communications (ITC). With world-wide, native language reach, Quocirca provides in-depth insights into the views of buyers and influencers in large, mid-sized and small organisations. Its analyst team is made up of real-world practitioners with first hand experience of ITC delivery who continuously research and track the industry and its real usage in the markets.

Through researching perceptions, Quocirca uncovers the real hurdles to technology adoption – the personal and political aspects of an organisation’s environment and the pressures of the need for demonstrable business value in any implementation. This capability to uncover and report back on the end-user perceptions in the market enables Quocirca to advise on the realities of technology adoption, not the promises.

Quocirca research is always pragmatic, business orientated and conducted in the context of the bigger picture. ITC has the ability to transform businesses and the processes that drive them, but often fails to do so. Quocirca’s mission is to help organisations improve their success rate in process enablement through better levels of understanding and the adoption of the correct technologies at the correct time.

Quocirca has a pro-active primary research programme, regularly surveying users, purchasers and resellers of ITC products and services on emerging, evolving and maturing technologies. Over time, Quocirca has built a picture of long term investment trends, providing invaluable information for the whole of the ITC community.

Quocirca works with global and local providers of ITC products and services to help them deliver on the promise that ITC holds for business. Quocirca’s clients include Oracle, Microsoft, IBM, Dell, T-Mobile, Vodafone, EMC, Symantec and Cisco, along with other large and medium sized vendors, service providers and more specialist firms.

Details of Quocirca’s work and the services it offers can be found at
<http://www.quocirca.com>