

Security relies on new technologies (banks and data leak prevention)

By Bob Tarzey, Service Director, Quocirca Ltd, March 2008

Banks and other financial institutions tend to be slightly ahead of their counterparts in their use of advanced network technologies and network security. This is not surprising given the sensitivity of the data they deal with and the degree to which they have to share their data with external organisations.

Given this it must be rather depressing for IT managers working in banks that despite their efforts the press coverage around leaked financial information has been so bad over the last six months or so. Some of the reasons for this are largely beyond the control of the banks themselves.

Many of the data leaks have been due to the carelessness of third parties. Sloppy handling of credit card details by retailers, government departments cavalier in their handling of citizens' data or consumers falling victim to scams. What can the banks do?

First they need to make sure that whatever dangers outsiders expose them to they know who is doing what on their own systems. This requires strict asset management and auditing of access to data and how it is used. But it needs to go beyond this.

Internal processes for handling data need to be clearly defined and easy to follow. It is all too easy to blame a lowly employee for being daft enough to put an unencrypted disk in the post, but they were only trying to do their job and poor processes allowed them to copy the data to disk in the first place. Accountability needs to be pushed upwards to those who define the processes.

It is not just banks' employees that need better education it is customers too. Customers like internet banking and the immediate access it gives them their own financial affairs. Nearly all customers are on the same side as the banks, they don't want to provide thieves access to their accounts any more than the banks do. But many are still duped by seemingly obvious scams.

Much financial fraud is not down to direct access to individual accounts but is through fraudsters applying for loans etc by successfully passing themselves off as a respectable individual. With a list of details including names, address, dates of birth and account details that the UK government at least, seems to make so readily available to anyone, this can be all too easy to do.

Here banks can invest in technology that can spot when a PC is likely to be used for making fraudulent applications. Vendors like Iovation provide technology that spots anomalous activity, such as serial loan applications from a single device and maintains a library of known rogue devices.

Banks will never be able to completely curtail bad data management practices by outsiders, but ultimately it is the banks and the banks alone that have responsibility for who can access their systems and who they dish our money to.

If banks can demonstrate firstly that they are not themselves responsible for data leaks, that they share data with 3rd parties securely and that when data is leaked their access controls and processes for handling potentially fraudulent applications are water tight then they should be able maintain customer confidence.

Not getting all this right can prove very expensive. It is not just the immediate financial losses incurred through theft and the compensation that might have to be paid to customers. It is the more serious long-term damage to brand reputation and the loss of customer confidence and loyalty that is likely to entail.

Quocirca's report "Banks and data leak prevention" is free to readers at http://www.quocirca.com/pages/analysis/reports/view/store250/item20679/?link_683=20679

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>