

Identify to comply—strategies can ensure good control through identity management

By Fran Howarth, Principal Analyst, Quocirca Ltd

Compliance is a word on everyone's lips. But it does not just mean regulatory compliance. Rather, all firms need to ensure that compliance is enforced.

One of the most pressing concerns for organisations is ensuring that sensitive data does not leak out of the company, potentially leading to damaged reputations or financial loss.

To guard against this, organisations are increasing their investments in security technologies, from point solutions such as content filtering to prevent leakages to full-blown identity management systems.

While hackers are targeting specific organisations or individuals to steal valuable information, looking for vulnerabilities in networks that can be exploited, most of the incidents of data loss that have been in the press recently were caused by inadvertent actions of employees or, in some cases, by carelessness.

According to a latest survey by the Computer Security Institute, insider abuse of network access may be the most prevalent security problem facing organisations. This was reported by 59 per cent of respondents. Identity management systems solve the problem of policing who is accessing what, when and what they have done with the information afterwards.

Such information is vital for proving through audits that effective security controls have been put in place and that organisations comply with set policies.

Putting in the hard work

This fact is not lost on organisations. The same survey found that, after compliance with regulations and data protection in

particular, solving identity management issues is seen as the second most pressing concern for companies.

However, putting in place an identity management infrastructure is a long and arduous task. During a recent webinar in which Quocirca participated, attendees were polled on what identity controls they had implemented. All firms polled indicated they realised the importance of compliance auditing and securing access to computers, systems and data, with most putting such controls in place in their businesses.

But security policies are only useful if a company can ensure they are enforced. One of the best ways to do this is to tie all actions taken to the individual perpetrator.

Respondents were asked whether they thought user name and password combinations were sufficient for tying a user's identity to their actions.

Our results showed organisations agree that stronger authentication is required for users, with most on the road to supplying network users with some form of additional security token providing an additional layer of security.

However, all organisations experience employee churn and not all staff members leave with a rosy view of the company. To prevent anyone causing deliberate harm at a time their loyalty is likely to be weakest, access rights should be revoked as soon as possible after their employment has ceased preferably immediately.

Still a long way to go?

Yet the results of the poll indicate that 44 per cent of organisations open a considerable window of opportunity for miscreants to do their

deeds. It is harder bringing someone to account when they are no longer your employee.

The poll suggests that compliance is an issue facing every organisation. Also, all respondents accept they do need stronger authentication of network users.

Such authentication provides more reliable evidence that security policies are being enforced by making individuals more accountable for their actions.

Identity management systems ease the burden of proof required for passing compliance audits but for many organisations, watertight identity controls remain a nirvana yet to be reached.

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>