

## CRN - Managing and monitoring the privileged – Nov 2009

By Bob Tarzey, Director and Analyst, Quocirca Ltd

A small group of employees in any organisation will have the ability to wreak havoc on IT infrastructure and the business it is there to serve: they are the privileged users who manage it.

Granting privileges to such users is necessary for them to be able to do their jobs, but when things go wrong the consequences can be dire.

The actions to blame may be unintentional but, because of the high-level access, the 'accidents' of privileged users can be far more serious than those of normal users. They may wipe a disk or crash a server at peak times.

And some privileged users abuse their status. Examples include Société Générale trader Jérôme Kerviel, who used his privileged access to perpetrate a €4.9bn fraud, and UBS systems administrator Roger Duronio, who was convicted in 2006 of sabotaging his employers IT systems in retaliation over a compensation dispute.

It is not just the privileged themselves who are the problem; privileged accounts are often targeted by hackers. Such accounts are often left with default settings at installation, making them easier to access than many 'normal' accounts.

If a hacker gets in this way too, they will have far wider access to the target systems. This is how UK hacker Gary McKinnon broke into the Pentagon's systems in the US.

It is not just in an organisation's own interest to get the privileged-user issue under control; regulators and standards bodies have something to say about the matter too.

The ISO 27001 IT security standard states that the allocation and use of privileges shall be restricted and controlled. The Payment Card Industries Data Security Standard (PCI-DSS), to which any business taking credit or debit card payments should adhere, recommends auditing all privileged-user activity as well as avoiding the

use of vendor-supplied defaults for system passwords.

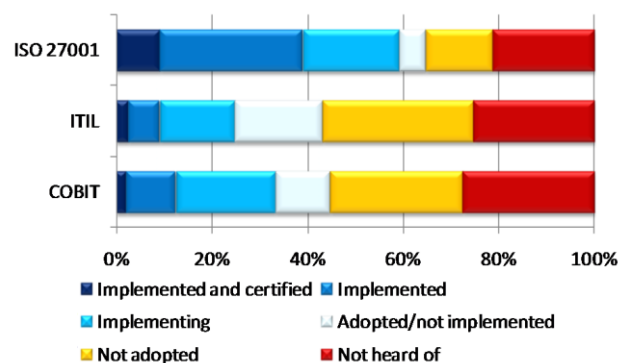
Despite this, when interviewing 270 European IT managers we found many organisations still allow poor practice around the management of privileged users.

You can see our results in the report, Privileged-user management - it's time to take control, which is free at:

[http://www.quocirca.com/pages/analysis/reports/view/store250/item22042/?link\\_683=22042](http://www.quocirca.com/pages/analysis/reports/view/store250/item22042/?link_683=22042)

Take-up of certain IT security standards is high (fig 1). Sixty per cent of respondents said they had implemented or would implement ISO 27001. Even so, about half also admitted to the sharing of privileged user accounts (fig 2) – meaning no one privileged user can be held to account when things go wrong, including some that have implemented these IT security standards (fig 3).

Figure 1: Deployment of security standards and methodologies?



A standard is often implemented gradually and selectively. However, those who are reassured by a given organisation's compliance claims might be shocked to find that underlying weaknesses in IT management can remain.

While all this sounds a bit gloomy, for resellers there are services and product opportunities. An assessment of any organisation that has not addressed the privileged-user issue - and only about 25 per cent have - may expose some of the weaknesses outlined. Then a case can be made for buying tools for privileged-user management (PUM).

Figure 2: Do you share administrator accounts between different individual privileged users in the following areas?

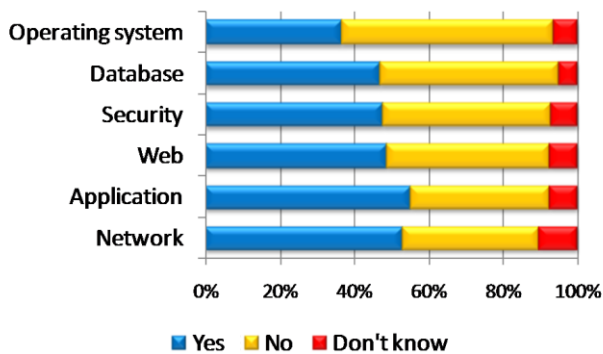
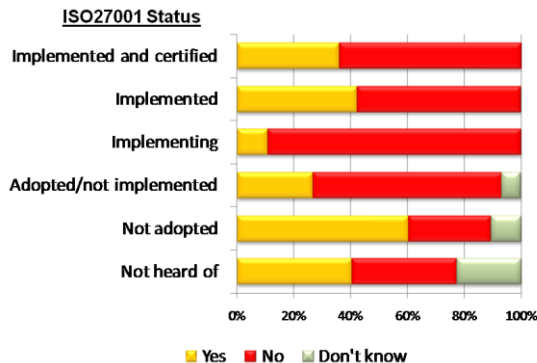


Figure 3: Do you share operating system administrator accounts between privileged users versus ISO2007 adoption



PUM tools allow the monitoring of software, including operating systems, databases and applications, to ensure privileged-user accounts are not left with default passwords and are only granted to certain people. They also enable continuous monitoring of users while acting under privilege, creating an audit trail that protects users themselves and the business.

To sell such tools to IT managers may prove tricky, as they are being asked to limit their own activities. You may need buy-in from business managers as well, who should be shocked at their organisation's exposure via privileged access.

## 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, O2, T-Mobile, HP, Xerox, 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>