



Press release

Widespread Bad Practice in 'Privileged User' Management Threatens Security in European Organisations, Survey Reveals

Some 41% of respondents who state they have implemented the ISO27001 standard still have bad practices such as sharing privileged user accounts.

Core News Facts

- 1.** Widespread privileged user management bad practice within European organisations is revealed in a survey commissioned by CA, "Privileged User Management—It's Time to Take Control".
- 2.** Some 41% of the respondents who state they have implemented the [ISO27001](#)* standard still had bad practice among their trusted IT administrators who have wide-reaching power of access to systems. Even for those who state they have implemented ISO27001 and had it certified by an external auditor, the figure is 36%.
- 3.** Respondents are not fully aware or overlook the risks associated with bad privileged user management, as they ranked the threat lower than other security concerns such as malware, the Internet, internal users, and Web 2.0 tools.
- 4.** Despite the availability of sophisticated systems, only 26% have actually deployed a full privileged user management system. 24% of organisations have some form of manual control in place for overseeing the actions of and controlling the access of privileged users. However, a reliance on manual processes for monitoring and controlling privileged users is time-consuming, excessively expensive, unreliable, and prone to errors.
- 5.** To read the full survey, please visit: ca.com/gb/mediaresourcecentre

London, U.K, October 20, 2009 – CA (NASDAQ: CA), the world's leading independent provider of IT management software, today announced the results of a European study revealing that widespread privileged user management (PUM) bad practice is threatening the security of European organisations. The new survey, "*Privileged User Management—It's Time to Take Control*", was carried out by the research company Quocirca on behalf of CA in 14 countries (Belgium, Denmark, Germany, Finland, France, Ireland, Israel, Italy, the Netherlands, Norway, Portugal, Spain, Sweden, and the UK). A privileged user is typically the IT or network administrator responsible for maintaining systems and keeping them available; it also includes operating system, business application, security and database administrators. Generally, they have been allocated



access rights within a business IT infrastructure which are significantly greater than those available to the majority of IT users.

Significantly, 41% of the respondents who state they have implemented the ISO27001 standard still had some non-compliant practices such as sharing privileged user accounts; this points to further bad practice like the use of default privileged account user names and passwords. The figure is still at an alarming 36% for those who state they have implemented ISO27001 and had it certified by an external auditor.

In recent years, many serious cases have emerged which highlight the dangers of underestimating and overlooking the risks that can ensue from a lack of control over the activity of privileged users. In cases where administrators and/or privileged users are given excessive privilege, or where they share their access with other people, they can cause significant deliberate or accidental damage. Moreover, there are also many instances of hackers targeting privileged accounts and successfully gaining access to critical business applications and data. Examples include the straightforward theft of sellable data such as credit card details, to the complex fraud or the theft of intellectual property.

Despite these threats, the research reveals that controlling and monitoring the activities of privileged users is not high on the agenda of IT managers. Respondents rank PUM below seven other actual security threats to the organisation (scoring 2.54 out of 5 on an index of threat), below malware (2.9), the Internet (2.7), internal users (2.7), and Web 2.0 tools (2.6). Moreover, there is a high degree of misplaced confidence surrounding the ability to manage privileged users. Respondents are also relatively confident that they can meet the demands of a compliance audit and worry more about issues like data loss and the compromise of intellectual property.

According to the *"Privileged User Management—It's Time to Take Control"* research, 24% of organisations have some form of manual control in place for overseeing the actions of and controlling the access of privileged users. However, a reliance on manual processes for monitoring and controlling privileged users is time-consuming, excessively expensive, unreliable, and prone to error.

Despite the availability of more sophisticated systems and the clear case for them, only 26% have actually deployed a full PUM system. However, the high number of organisations (48%) that say they have plans (albeit often delayed ones) suggests it is



on their agenda, but is not a priority. Budget availability may be a reason for this prevarication (scoring 3.3 out of 5 on the scale of limiting factors), although 85% state that the budget spent on IT security is either stable or increasing as a proportion over overall IT spending. Ultimately, it is likely that the main reason for holding back is an under appreciation of the risks presented by privileged users.

Country Differences

The research also reveals an interesting variation between the countries participating in the survey. The countries most likely to share administrator accounts between individual administrators are France (60%) and Belgium (60%), followed by the Netherlands (53%). By contrast, respondents in France were the most confident about being able to monitor and control privileged user accounts (scoring 4.26 on a scale of 1-5). The countries least likely to share administrator accounts between privileged users are Spain (7%), Israel (7%), and Germany (10%). 63% of French organisations participating in the survey rely on manual monitoring of privileged user activity, following by Belgium (50%), and Denmark (47%).

Vertical Industry Findings

Examination of the different industry sectors taking part in the survey also reveals wide variation. 43% of organisations in both the Telecommunications & Media and the Government sectors admit to sharing operating system administrator accounts between different individual administrators. This falls to 29% in the Manufacturing sector. Ironically, Telecommunications & Media organisations are the most confident about being able to monitor privileged user accounts (scoring 3.7 out of 5 on an index of confidence), whereas Government is weakest (3.5). Telecommunications & Media is ahead in deploying privileged user management solutions, with 37% already having a system in place, compared with 18% of Manufacturing organisations. Finally, 34% of Telecommunications & Media already have tools in place to monitor and control the activities of privileged users, followed by Government (25%), Finance (22%), and Manufacturing (13%).

“This landmark research provides conclusive proof that organisations are overlooking a crucial area of IT security—the privileged access administrators grant to themselves or their colleagues in order to do their jobs,” says Tim Dunn, Vice President, Security Business EMEA, CA. “While such access is necessary, it is most commonly managed on an ad hoc basis and, despite claims to pay heed to the requirements of regulators, requirements with regard to privileged users are often overlooked. It is in the best



interests of individual IT managers, the IT department, and the overall business to have measures in place to control and monitor privileged users. The deployment of privileged user management tools enables this and allows organisations to mature their use of privileged user management over time. Privilege User management is key to compliance, to reducing risk exposure, and to protecting critical business applications.”

Bob Tarzey, Analyst and Director, Quocirca Ltd. comments, “The research reveals clearly that while it is in the interest of individual IT managers, the IT department, and the business itself to adopt measures to control and monitor privileged users, it is not a priority. Manual processes are ineffective and do not provide an audit trail that would satisfy regulators. The one sure means of achieving watertight privileged user management is through the automated management of privileged user accounts, the assignment of privileged user access, and 360-degree monitoring of their activities.”

The “Privileged User Management—It’s Time to Take Control” research was conducted by Quocirca, a primary research and analysis company specialising in the business impact of ICT. A total of 270 interviews were conducted during June 2009 with IT Directors, Senior IT Security Managers, and other IT Managers in four vertical sectors: telecommunications & media, manufacturing, financial services, and government.

In addition, CA today announced new product releases and integrations that help address security and compliance challenges, including [CA Access Control 12.5](#) which provides technology to support privileged user and password management. Please visit <http://www.ca.com/us/press/release.aspx?cid=217987> to learn more about today’s news.

To download a copy of the survey report, please visit <http://www.ca.com/gb/mediaresourcecentre>

** The ISO27000 series of standards for IT management states that “the allocation and use of privileges shall be restricted and controlled”*



About CA

CA (NASDAQ: CA) is the world's leading independent IT management software company. With CA's Enterprise IT Management (EITM) vision and expertise, organizations can more effectively govern, manage and secure IT to optimize business performance and sustain competitive advantage. For more information, visit www.ca.com.

Quocirca is a leading primary research and analysis company, specialising in the impact emerging and evolving technologies have on businesses of all sizes. Based in the UK, Quocirca's primary research reach is world-wide, investigating, analysing and reporting on the perception of decision makers and influencers in the end user environment around technologies within their businesses.

Connect with CA

- [CA Social Media Page](#)
- [CA Newsletters](#)
- [CA Press Releases](#)
- [CA Podcasts](#)

Trademarks

Copyright © 2009 CA. All Rights Reserved. One CA Plaza, Islandia, N.Y. 11749. All other trademarks, trade names, service marks and logos referenced herein belong to their respective companies.

Press Contacts

Sarah Atkinson

CA
Vice President, Communications, EMEA
Tel: + 44 1753 242191
Sarah.Atkinson@ca.com

Mariateresa Faregna

CA
Public Relations Manager, Italy
Tel. +39 02 90464.739
mariateresa.faregna@ca.com