

Privileged user management

It's time to take control

October 2009

IT managers everywhere feel overwhelmed with the rising tide of security threats they have to deal with in the face of an increasing regulatory burden. It is not surprising then that they tend to overlook one particular area of IT security, which is the privileged access that they grant themselves and/or their colleagues in order to do their jobs.

The level of access to sensitive data given to privileged users is often the highest any employees have had in the history of business. It is the equivalent of having the locksmith solely hold the keys to the safe, and then requiring them to come and maintain it at any time they wish, alone and unassisted. Whilst such access is necessary, it is most commonly managed on an ad hoc basis or not managed at all and, despite claims to pay heed to regulations, requirements with regard to privileged users are often overlooked.

This report should be of interest to anyone concerned with ensuring that the availability of their IT systems is not impacted by the inadvertent or malicious actions of privileged users, that the use of privileged user accounts is policed and that such accounts cannot be easily compromised by outsiders. It should also be of interest to those with responsibility for ensuring that their organisations' use of IT would satisfy the demands of regulators and, indeed, anyone concerned about the safe keeping of their personal data that businesses are storing ever more of.

Bob Tarzey
Quocirca Ltd
Tel : +44 7900 275517
bob.tarzey@quocirca.com

Clive Longbottom
Quocirca Ltd
Tel: + 44 771 1719 505
clive.longbottom@quocirca.com

Mariateresa Faregna
CA Inc
Tel: +39 2 90464739
mariateresa.faregna@ca.com



An independent report by Quocirca Ltd.

www.quocirca.com

Commissioned by CA

quocirca

Privileged user management

It's time to take control

IT managers everywhere feel overwhelmed with the rising tide of security threats they have to deal with in the face of an increasing regulatory burden. It is not surprising then that they tend to overlook one particular area of IT security, which is the privileged access that they grant to themselves and/or their colleagues in order to do their jobs.

- **Certain employees need to be granted privileged access to various resources in order to do their job; this is especially true for the management of information technology (IT)**
IT managers need privileged access to operating systems, databases, business applications, networks and IT security systems. Such high level access means that any mistakes they make can have serious consequences, and if they abuse their rights for personal purposes the results of their actions can be very serious indeed.
- **Controlling and monitoring their own activities is not high on the agenda of most IT managers**
IT managers feel they have plenty of other issues to worry about with the dangers of malware, the activities of "normal" users and the demands placed by an increasing tide of regulations on the IT infrastructure they oversee.
- **The ISO27001 standard for IT management, which is adopted by about 40% of the respondents to this survey, explicitly states that "the allocation and use of privileges shall be restricted and controlled"**
Despite widespread claims to have adopted the standard, many businesses admit to bad practices with regard to privileged user management (PUM) that are in direct contravention to it.
- **Bad practices include the sharing of privileged user accounts, the use of default usernames and passwords and the granting of far broader privileges than necessary for a given privileged user to do their job**
41% of respondents admitted that their organisations shared administrator accounts between users for operating system access; this rose to over 50% for network administrators.
- **There are plenty of examples of privileged users abusing their access rights or hackers targeting these accounts as their main entry point, underlining the need to put controls in place**
These range from straightforward theft of sellable data, such as credit card details, to the perpetration of complex frauds or the theft of intellectual property. In other cases it is down to pure spite by a disgruntled employee.
- **The technology exists to mitigate the threat posed by privileged users but adoption levels are low**
Just over 25% of European businesses have deployed technology for PUM although many more say they have plans, albeit delayed ones. Such technology allows privileged user access to be managed and monitored and bad practices to be brought under control, enabling the "least privilege principle" where only the access rights needed to carry out a given set of tasks are granted.
- **There are two reasons for prevarication around the deployment of such technology**
Lack of budget is the biggest constraint on the deployment of better IT security although there is little evidence of budgets being cut. However, the main reason for holding back is a lack of awareness amongst IT managers of the dangers of not monitoring and controlling their own activity, even when it is in their own interest. There is likely to be a similar lack of awareness amongst business and risk managers.

Conclusions

It is in the interest of individual IT managers, the IT department as whole and the overall business to have measures in place to control and monitor privileged users. Manual processes are ineffective and do not provide an audit trail that would satisfy regulators. The one way to ensure this is to put in place tools that fully automate the management of privileged user accounts, the assignment of privileged user access and enable the full monitoring of privileged user activity.



CONTENTS

| | |
|--|-----------|
| 1. INTRODUCTION AND TARGET AUDIENCE | 4 |
| 2. THRESHOLDS OF TRUST | 4 |
| 3. THE PRIVILEGED USER CONUNDRUM | 5 |
| 4. SCALES OF RISK | 6 |
| 5. NOT SUCH GOOD PRACTICE..... | 7 |
| 6. WHY PRIVILEGED USERS TURN BAD..... | 8 |
| 7. MITIGATING THE PRIVILEGED USER THREAT | 9 |
| 8. WHY DON'T MORE ORGANISATIONS DEPLOY PUM? | 10 |
| 9. CONCLUSIONS AND RECOMMENDATIONS..... | 11 |
| APPENDIX 1: COUNTRY LEVEL DATA..... | 12 |
| APPENDIX 2: DEMOGRAPHICS AND IT SPENDING TRENDS | 14 |
| ABOUT CA | 15 |
| ABOUT QUOCIRCA..... | 16 |



1. Introduction and target audience

IT managers everywhere feel overwhelmed with the rising tide of IT security threats they have to deal with in the face of an increasing regulatory burden. It is not surprising then that they tend to overlook one particular area of IT security, which is the privileged access that they grant to themselves and/or their colleagues in order to do their jobs.

Whilst such access is necessary, it is most commonly managed on an ad-hoc basis or not managed at all and, despite claims to pay heed to the regulations, specific requirements with regard to privileged users are often overlooked.

This Quocirca report looks at how privileged user management (PUM) is carried out across Europe and is based on interviews with 270 senior IT managers in four vertical sectors (telecoms & media, manufacturing, financial services and government). It includes organisations from most Western European countries and a range of company sizes (see Appendix 2).

This report should be of interest to anyone concerned with ensuring that the availability of their IT systems is not impacted by the inadvertent or malicious actions of privileged users, that the use of privileged user accounts is policed and that such accounts cannot be easily compromised by outsiders. It should also be of interest to those with responsibility for ensuring that their organisations' use of IT would satisfy the demands of regulators and, indeed, anyone concerned about the safe keeping of their personal data that businesses are storing ever more of.

2. Thresholds of trust

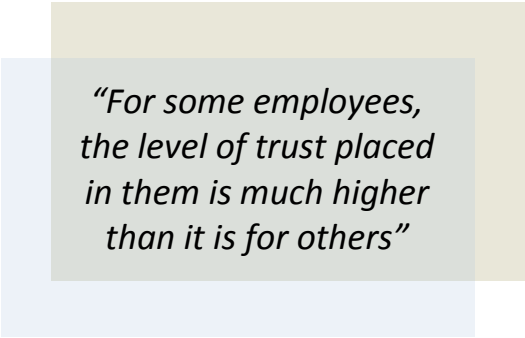
There is an innate desire in human beings to trust one another; if there were not, life would be very hard indeed. When trust breaks down between family members, the family usually fails. Beyond the family we choose friends in whom to place trust. The threshold for that trust may be lower or higher than that we place in family members. For those that find it hard to trust the world is a lonely place.

In the work place, too, a level of trust is essential. However, unlike the bonds of trust we form

amongst friends and family, in business we are often required to deal with people we don't know well. The threshold for trust naturally drops. Furthermore, human-to-human interactions and exchanges of information are sometimes replaced by human-to-machine, so trust is now second-hand.

However, trust must still be there, employees must be allowed to know some of the business's secrets and have access to sensitive data to do their jobs. Sometimes that trust is abused and this can cause untold damage to the business in question.

The abuse is often not intentional; compromise can be accidental, through naivety or carelessness. However, in the area of IT, such behaviour can also leave businesses more exposed to the harmful intentions of outsiders.



“For some employees, the level of trust placed in them is much higher than it is for others”

For some employees, the level of trust placed in them is much higher than it is for others; an accountant may have to see the end of year financial figures long before they are reported to the markets, a cleaner may have keys to the CEO's office and a PA may be privy to their boss's intentions and ideas.

In the area of IT, where so much of a business's data and intellectual property is stored and used, such highly trusted employees are known as privileged users and their access to data can be very wide-ranging. Their privileged status will often give them access to financial data and electronic diaries that they aren't intended to have, and certainly don't need, to carry out their jobs. They may not have the physical keys to CEO's office, but they can potentially access the virtual filing cabinet of anyone from the CEO down.

Despite often being employees of a relatively low rank, the level of access to sensitive data given to privileged users is often the highest any employees have had in the history of business. It is the equivalent of having the locksmith solely hold the keys to the safe, and then requiring them to come and maintain it at any time they wish, alone and unassisted.

Worst still, poor practice can leave privileged user accounts easily accessible to outsiders. If hackers gain access at the privileged, rather than “normal”, user level they are much more likely to be able to achieve their goals. Also, such accounts often have far wider access rights than is necessary in the first place, exacerbating matters.

So there is a need to protect privileged users from themselves, to protect the business from its own privileged users and protect against the possibility of privileged user access by outsiders.

“Despite often being employees of a relatively low rank, the level of access to sensitive data given to privileged users is often the highest any employees have had in the history of business”

3. The privileged user conundrum

IT systems need managing and for this to happen privileged users must have access to their inner workings. When a new database, operating system or application is provisioned it will come with a series of “default” privileged user accounts that will be widely known to many and often documented and easily found on the internet. The privileged user problem starts right here and is at its most insidious.

Commonsense, and many regulatory requirements, say these should be changed immediately, but often they are not. When this is the case, it is not just internal privileged users that have access, but any hacker who may want to take look at a given organisation’s data. The British hacker Gary McKinnon, who the US government want to extradite after he hacked Pentagon IT systems, gained much of his access through privileged user accounts which had been left with the default settings.

So, the privileged user issue is first about managing the privileged user accounts and then about managing the actual privileged users, and in many cases they are not well aligned. Even if the default password is changed, its replacement may still be known by several privileged users who all use the same administrator account. So when something goes wrong it is impossible to prove which one of them was individually responsible.

Some software applications also need to be granted privileged user access and this may mean embedding usernames and passwords in them. These need to be monitored, as does the activity of the software developers writing and testing them.

To bring all this under control requires that privileged users are given unique access; their individual accounts must be the only way of gaining access to IT systems at the privileged user level and their individual activity, whilst operating at that level, should be monitored and audited.

The access granted also needs to be modular; too often privileged accounts are assigned broad “catch-all” access rights that are far wider than is necessary for a given individual to do their job. It is much safer to assign fine-grained access controls at the account level. Such “*appropriate role separation*” ensures privileged users cannot over step the mark, accidentally or intentionally, and, should their accounts be compromised, the unauthorised user is similarly restricted. This is known as the “*least privilege principle*”.

This has become especially true with the increasing use of virtualisation. In the past, granting a given privileged user access to a single physical server still gave them fairly limited

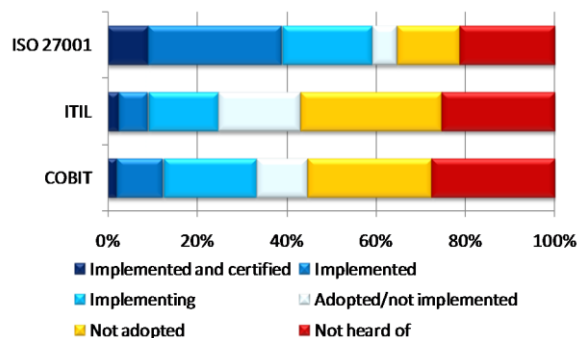
access rights but, if virtualised, there may be many different systems running on the same server to which access is possible, if unlimited rights have been granted at the physical level.

A further benefit of this level of control over the assignment of privileges in virtualised environments is that it allows competing organisations to share the same physical resources. This is increasingly likely with the move to “cloud computing”. For the outsourcers that provide these managed services, the granular granting of privileges and the auditing system management activity is essential.

PUM is not just about protecting the data and intellectual property assets of the business and paying regard to the privacy of employees in general; it is also about complying with the requirements of regulators that are often explicit about privileged users in their requirements.

For example, around 60% of European organisations have implemented or are implementing the ISO-27001 IT security standard (Fig 1). It states that **“the allocation and use of privileges shall be restricted and controlled”**.

Figure 1: Deployment of security standards and methodologies?



The Payment Card Industries Data Security Standard (PCI-DSS), which any business taking credit or debit card payments must adhere to, recommends **“auditing all privileged user activity”** as well as avoiding the use of vendor-supplied defaults for system passwords and other security parameters.

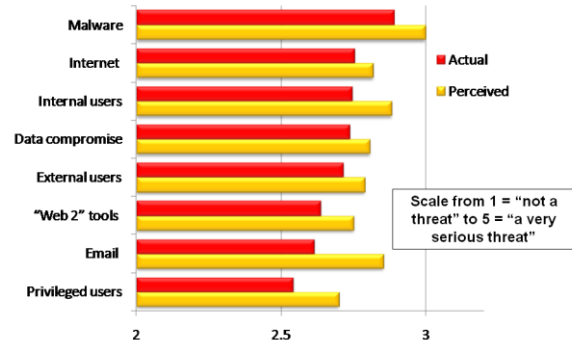
The issue of PUM is being more and more widely recognised. The Italian personal data protection watchdog, Garante Privacy, has recently issued new measures that must be adopted with regard to the management of privileged users. It points out that system administrators are **“key figures for the security of data banks”**. Italian businesses must comply by December 2009. This underlines the fact that the PUM issue is not only about organisations protecting themselves but also about the safe custody of personally identifiable data that governments are increasingly taking an interest in.

Meeting these regulatory demands requires business to have processes and tools in place to control the activities of privileged users but, as this report goes on to show, the majority of organisations do not, even when they claim be complying to such standards.

4. Scales of risk

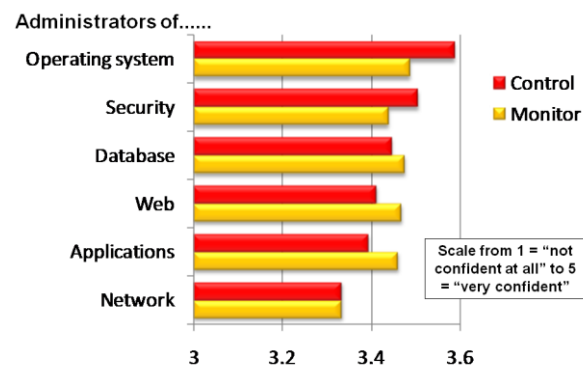
IT managers have plenty to worry about and managing their own privileges is not necessarily high on the list (Fig 2). Indeed, given the demands of regulators, one might expect this is because good practice with regard to PUM is generally in place and the regulators would approve.

Figure 2: To what extent are the following a threat to IT security in your organisation?



Indeed, confidence levels around the ability to manage privileged users are reasonably high (Fig 3). Although it should be pointed out that this varies by industry, telecoms/media companies being the most confident and government organisations the least.

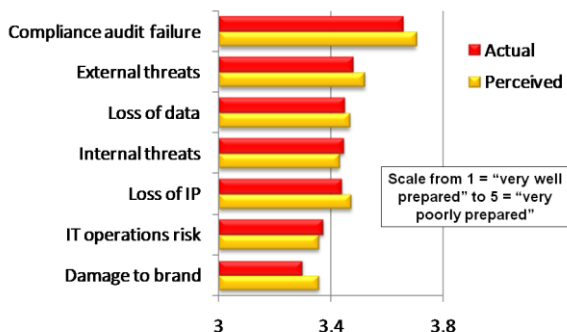
Figure 3: How confident are you that you are able to control and monitor the following types of privileged user accounts?



However, much of this confidence is likely to be down to complacency; it is easier just to trust privileged users to do the right thing—and worry about things that are higher profile and, perhaps, easier to control, such as malware and the day-to-day activities of “normal” users.

Respondents were also relatively confident that they could meet the demands of a compliance audit and worried more about issues like data loss and compromise of intellectual property (Fig 4).

Figure 4: How well prepared is your organisation to protect against the following risks?

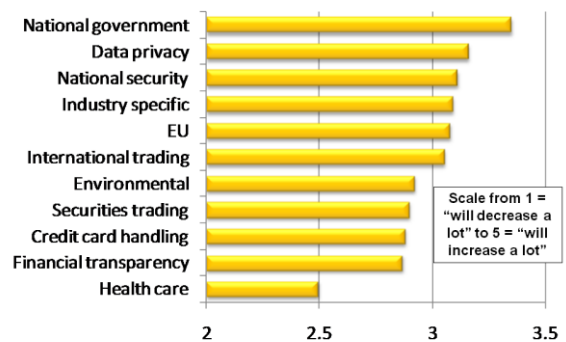


Apart from the fact that no one wants to admit they might fail an audit, if their focus has been on controlling “normal” users and their use of data and communications tools, IT managers may feel they have control over their IT systems and that is a good thing when the auditors turn up. However, the auditors will also ask some awkward questions about the privileged activities of the IT managers themselves, which may leave them feeling rather less confident when the auditors have gone.

The current research showed a tendency for the most senior IT managers (CIO and CISO) to have higher levels of confidence in their readiness to face up to such threats than their more junior reports. This may be best explained by those nearer to the action realising how exposed their organisations are in certain areas, not least when it comes to privileged account access, which they are more likely to be using on a day-to-day basis than their bosses.

In many areas the regulations auditors come to enforce are expected to increase (Fig 5). The new measures from Italy’s Garante Privacy discussed in section 3 are a case in point.

Figure 5: How do you see regulations in the following areas affecting your organisation over the next 5 years?

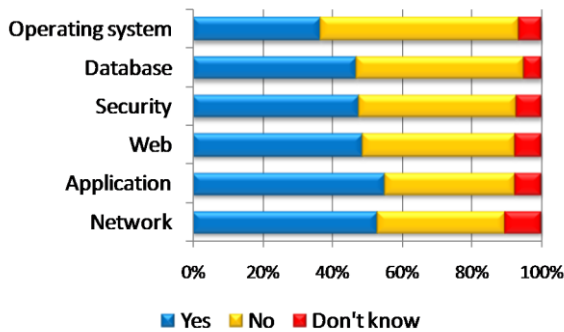


5. Not such good practice

The focus on “normal” users is understandable; there are lots of them, and there is every chance some of them somewhere are up to no good. Hundreds of incidents of users behaving carelessly, stupidly or maliciously come to light every year. However, the truth is, given their limited access rights, the majority of these incidents are benign and, if they turn out to be more serious, generally the user has been accessing a given system via an assigned account, so IT managers know who they are.

However, when a privileged user behaves carelessly or maliciously, their access rights can mean the consequences are far more serious. Just as with “normal” users it is necessary to know who they are but, in almost half of the businesses interviewed for this survey, IT managers admitted that privileged user account sharing is common place (Fig 6).

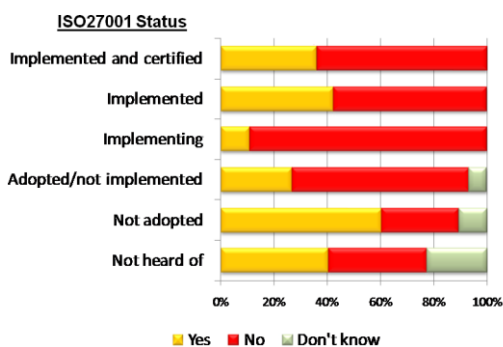
Figure 6: Do you share administrator accounts between different individual privileged users in the following areas?



This is appallingly bad practice that auditors would frown upon. Again, government organisations come out badly, with widespread privileged user account sharing, but so do telecom/media companies, despite the higher levels of confidence they claim in controlling privileged users. This suggests that PUM is an area where some of the issues are not clearly understood, even by organisations that consider themselves well versed in IT security issues.

Significantly, around 41% of organisations that claim to have implemented ISO27001 admit to privileged user account sharing (Fig 7). The figure is still at an alarming 36% for those that claim to have implemented ISO27001 and to have had it certified by an external auditor.

Figure 7: Do you share operating system administrator accounts between privileged users versus ISO2007 adoption



The sharing of accounts is risky enough, but it points towards another very bad practice; shared accounts will often use the system default username and the password may well have been left with those settings or be set to something obvious so that multiple privileged users can remember them.

This is because the practice of privileged user account sharing stems from not addressing the issue when software or hardware was first deployed. The account settings were never changed and the issue of who should have access, how, when and from where was not clearly thought through.

In some cases privileged users may wreak havoc by accident, wiping a disk, deleting a database, disabling “normal” user accounts accidentally—in many cases such issues can be fixed, without causing too much long term disruption, providing a safety net of business continuity good practice is in place elsewhere.

However, if a privileged user goes rogue, then their actions can be highly focussed and very serious indeed. Even the auditing services on a system are not immune from some privileged accounts, and the integrity of system audit logs is therefore vulnerable to inadvertent or malicious actions.

“Around 41% of organisations that claim to have implemented ISO27001 admit to privileged user account sharing”

6. Why privileged users turn bad

In rare cases a privileged user may be a plant—someone who has penetrated a given organisation as an employee or contractor—just to get access to their IT systems. However, there are a number of reasons a once seemingly trustworthy privileged user might go rogue; the most obvious is for financial gain.

This can either be straight forward theft, such as the 2007 case of a “*low level*” database administrator at the US banking services company Fidelity National Information Services who was found to have stolen 2.3 million credit card records and selling them on to a data broker.

It can also be for more in-depth fraud such as that perpetrated by Jérôme Kerviel, the rogue trader who, it was revealed, had lost the French Bank Société Générale €4.9 billion. He was able to perpetrate his fraud and cover his actions for a couple of years because of privileged user access that he had been granted to carry out a previous IT administrator related job, which had not been revoked when he moved to the trading floor.

Another reason is plain spite; a disenchanted privileged user may choose to wreak havoc, just because they can. A former systems administrator of the Swiss bank UBS, Roger Duronio, was convicted in 2006 of sabotaging his employers IT systems in retaliation over a compensation dispute. UBS never reported the cost of lost business, but did say the attack cost the company more than \$3.1 million to get the system back up and running.

Another notorious example involved a UNIX engineer at the US mortgage giant Fannie Mae who was accused with maliciously damaging his employer’s servers in Jan 2009. His privileged access rights were not revoked immediately after being let go from his contract position, leaving a window of opportunity to cause the damage. If the malicious script had gone undiscovered, it would have disabled monitoring alerts and logs, deleted root passwords to 4,000 Fannie Mae servers, and erased all data and backup data on those servers by overwriting with zeros.

The theft of intellectual property by employees leaving one employer for another is also a danger. There are many examples of “normal” users doing this, but privileged users have even greater opportunity with their wide-ranging access rights.

7. Mitigating the privileged user threat

It is possible to get the privileged user threat under control; some methods are better than others. There are two priorities:

- To make sure all the default privileged user accounts are identified and closed down. This can be a huge task; there are operating systems, networking devices, security systems, databases, business applications and many other parts of the IT infrastructure to consider.
- With the default accounts under control it is then necessary to grant privileged user rights in specific areas to those who require it.

Some businesses attempt manual PUM; for example issuing one-off passwords and emailing them around or storing them in sealed envelopes in physical safes. Often access is allowed for a given period of time before the password changes again. This has the obvious flaw that some “*higher level*” privileged user would still have all the access rights that good PUM practice tries to avoid, as well as being non-scalable and cumbersome.

An alternative approach is to increase the privileges of certain users in a standard user management system (for example, the access level rights granted to the operating system) so that they have enough privilege to carry out IT management tasks; but there are a number of problems with this approach.

- It does nothing to aid the monitoring of privileged user accounts in the first place to avoid those default settings being left in place.
- An unscrupulous user with privileges may tamper with log files, to cover their tracks.
- It does not enable the comprehensive monitoring of the privileged user’s actions while they are logged in.
- It does not usually allow for “dual control” where necessary (the practice where certain actions can only be carried out with the sanction of two privileged users).
- With some systems, for example UNIX, a given user’s identity may be lost if they use commands like “su” (substitute user).

However, the best approach is to automate the whole process with purpose-built PUM tools that provide an understanding of the wide range of systems that businesses use and enforces the necessary policies with regard to privileged users. There are many benefits not afforded by other approaches:

- Privileged user accounts can be scanned for and monitored to ensure default settings are never left in place.
- Privileges can be assigned to named users at the account level on a case-by-case basis, with the appropriate granularity of access, enabling the “*least privilege principle*”.
- The way the system is used can be matured over time. The most basic requirements, such as scanning for vulnerable privileged user accounts, can be undertaken straight away. Putting in place the processes that truly follow the “*least privilege principle*” can be achieved in the longer term.
- The activity of privileged users can be continuously monitored; the system will record who checked out a password, when, and what actions they took.
- Compliance with standards and regulations can be audited and proven when necessary.
- In the event of a privileged user account being compromised, auditors will be able research the incident forensically.
- For particularly sensitive systems, it is possible to assign one-time passwords.
- Dual control can be enabled when required.
- Software applications can be granted privileged user rights when necessary and their developers given short term limited access, as and when required, to test them.
- Around the clock support for mission-critical systems by geographically distributed teams can be easily and safely enabled.
- The granular granting of privileges can be extended to the management of virtualised environments.
- PUM tools ease the integration of IT systems when organisations come together following a merger or acquisition. The current research shows such activity to be on the rise during the current financial downturn.

8. Why don't more organisations deploy PUM?

A little over 24% of organisations have some form of manual control in place for overseeing the actions of and controlling the access of privileged users (Fig 8).

Despite availability of more sophisticated systems and the clear case for them, only around 26% have actually deployed a full PUM system (Fig 9) although the high number of organisations that say they have plans, albeit often delayed ones, suggests there is not a complete lack of awareness of the issues, amongst IT managers at least.

However, it is likely the business and general risk managers, whilst not interviewed for this survey, are aware of the high profile IT security issues such as malware and data leakage, but not the lower profile issue of privileged user management.

Figure 8: Do you use manual methods to manage access for privileged users?

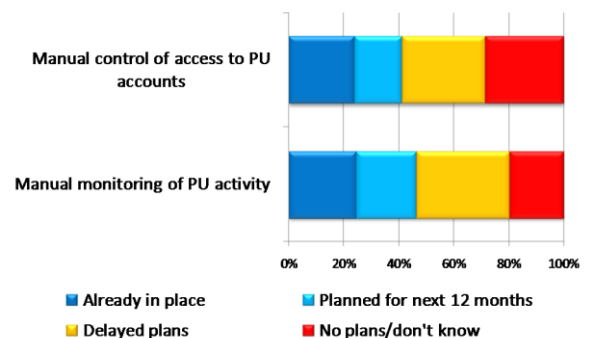
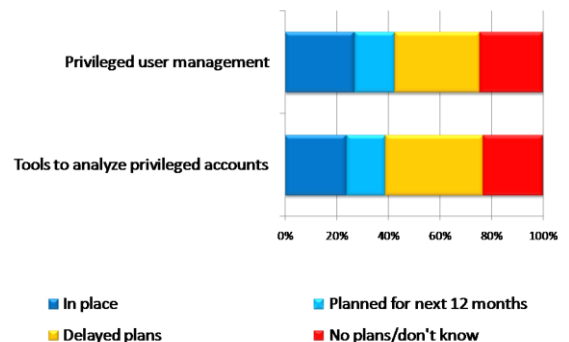


Figure 9: Do you use any of the following types of tools for managed privileged users?



Deployment rates vary quite a bit between industries. Over 37% of telecom/media organisations have deployed automated PUM tools, which helps explain their higher confidence levels with regard to PUM discussed in section 4. Deployment levels drop to 24% for government organisations and as low as 18% for manufacturers.

Deployment rates are slightly higher for larger organisations leading to marginally higher confidence levels in the ability to control privileged users, but such confidence is also high among smaller businesses, perhaps because they find the problem of privileged users is easier to contain. Confidence is lowest with mid-sized businesses that have quite a few privileged users but few tools in place to control them.

There are two reasons businesses prevaricate about investing in PUM tools. One is cost, which stands out as the biggest factor limiting spending on IT security at present (Fig 10), although there is little evidence that the recent financial crisis has led to IT security spending being reduced any more than overall IT spending (Fig 11).

Figure 10: How influential are the following factors in limiting investment in security?

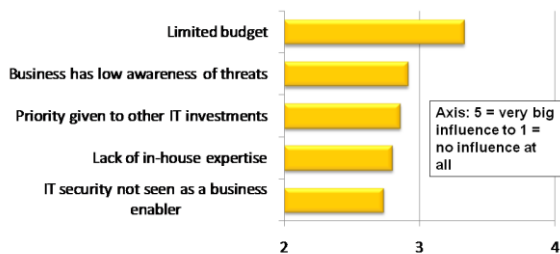
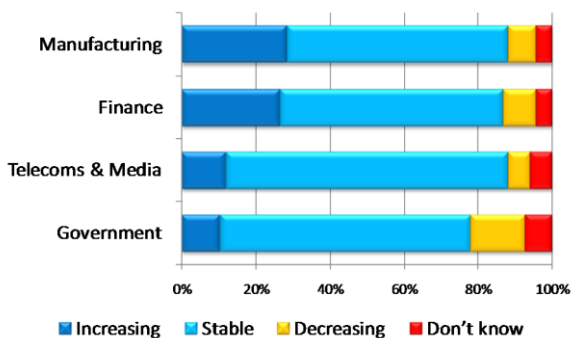


Figure 11: Is the proportion of your organisation's total IT budget is spent on IT security increasing or decreasing?



There is another reason that may explain all those delayed plans, which cannot simply be put down to a financial crisis that has only arisen over the last 18 months or so.

Putting the tools in place to manage privileged users will have to be done by the IT department itself. In other words, IT managers have to be motivated to control and curtail their own activities; for those that consider they are honest and of high integrity, this is counter intuitive. However, the benefits of being able to prove that integrity when necessary are underestimated, and there is also a level of naivety about the potential dangers posed by uncontrolled privileged user access.

Any well intentioned IT management team should recognise that having PUM in place not only catches the occasional bad employee, but also ensures that, should it ever be necessary, their own integrity can be proven. Also, of course, if those tools are in place, their claims to comply with standards such as ISO27001 and PCI-DSS, in the area of privileged users at least, will not be disputable.

9. Conclusions and recommendations

It is in the interest of individual IT managers, the IT department as a whole and the overall business to have measures in place to control and monitor privileged users. Manual processes are ineffective and do not provide an audit trail that would satisfy regulators.

The deployment of PUM tools enables this and allows organisations to mature their use of PUM over time.

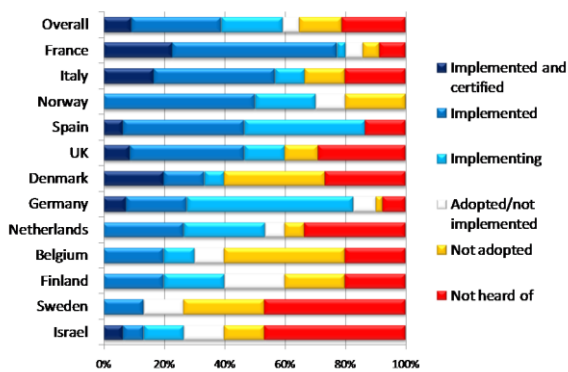
In a world where IT is fundamental to the operations of almost every organisation, the way IT is deployed and managed is ever more complex and IT systems are increasingly the target for fraudsters. The issue of who is trusted to have high level access to the most sensitive systems can no longer be left to chance; it is time to take control.

Appendix 1: country level data

The current research ranges across 14 different European countries (see Appendix 2) and some interesting geographic variations are highlighted in this Appendix. It should be noted that, apart from the UK, Germany, France and Italy, the sample sizes per country are fairly small so many of the findings are only indicative. However, it would seem businesses in some countries are way behind those in others when it comes to dealing with the issue of PUM.

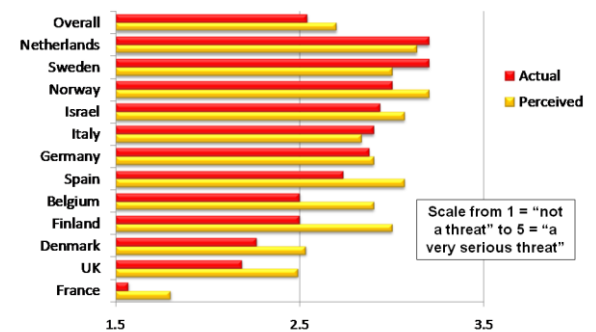
Deployment of ISO27001 varied widely (Fig 12), with France coming out highest and Sweden, Finland, Belgium and Netherlands quite low. The data for France contained more interviews with IT security heads than the other samples, so there may be an awareness, or even defensive, issue here, with people in such roles having more insight in to regulatory compliance or not wanting to admit to be overlooking it.

Figure 12: Deployment of ISO27001 by country



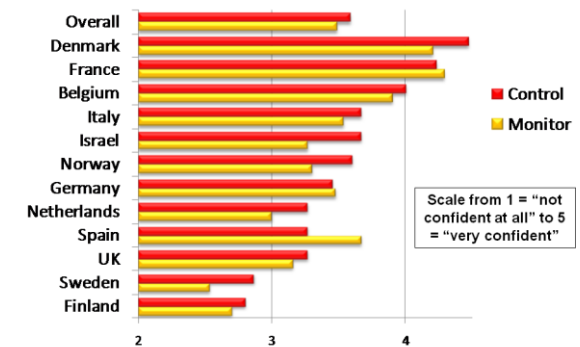
The threat with regard to privileged users is roughly the inverse of ISO27001 deployment (Fig 13). France and UK perceive the least threat and Sweden and Netherlands the most. This suggests that ISO27001 deployment does lead to better practice.

Figure 13: To what extent are privileged users a threat to IT security in your organisation?



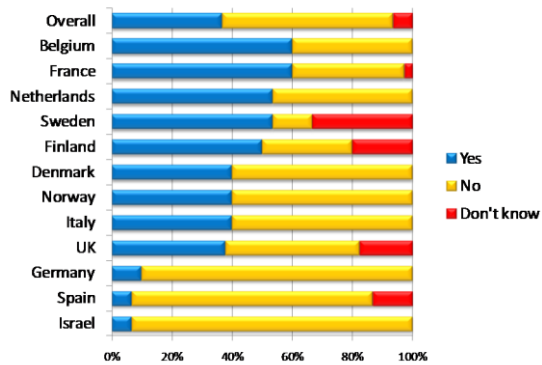
This is supported by figures for confidence for controlling privileged users (Fig 14); France scores highly and Sweden low. Although there are some discrepancies, Belgians seem confident despite low levels of ISO27001 deployment.

Figure 14: How confident are you that you are able to control and monitor privileged user accounts at the operating system level?



However, the bad practices exposed by this report, even for those with ISO27001 deployed, should not be forgotten (Fig 15). France and Belgium report a high degree of privileged user account sharing, whilst for Germany the practice is rare. Here, there is little correlation with ISO27001 deployment; this suggests that the confidence conferred by the standard is general rather than specific, along the lines of "we are ISO27001 compliant therefore we must have privileged users covered".

Figure 15: Do you share administrator accounts between different individual privileged users at the operating system level?



There is also a rough correlation with confidence in controlling privileged users and the use of manual processes and/or automated tools for PUM (Figs 16 and 17). In France, Denmark and Belgium such deployment is widespread, whilst in Spain and Netherlands it is limited.

This is clearly a good finding, as it shows there is a payback for taking action. However, the long list of benefits (see section 7 of this report) conferred through using automated tools should not be forgotten. Manual processes, whilst better than nothing, are a poor substitute for full PUM tools.

Figure 16: Do you use manual methods to control access for privileged users?

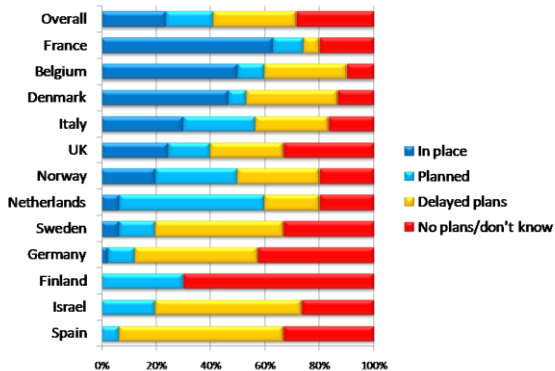
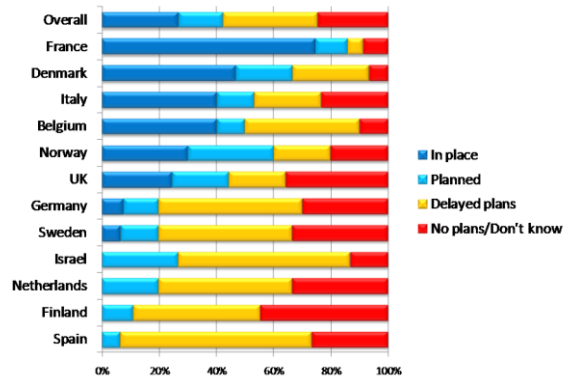
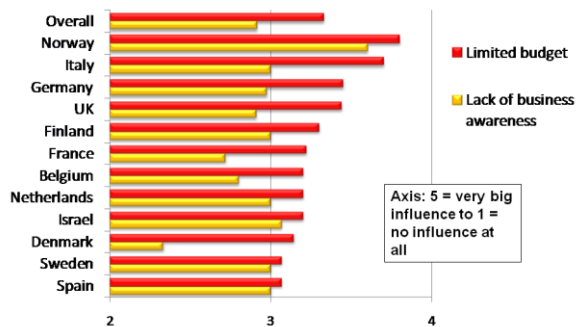


Figure 17: Do you use privileged user management tools?



In no country was a "limited budget" for IT security surpassed by a "lack of business awareness" as a limitation on IT security spending (Fig 18). Norwegians and Italians have the tightest financial restrictions, Sweden and Spain the lowest. Danes worry least about a lack of business awareness, Norwegians the most.

Figure 18: How influential are the following factors in limiting investment in security?



No country in Europe has proved itself immune from the threat posed by bad practice with regard to PUM; the same message should go out to all. The issue of who is trusted to have high level access to the most sensitive systems can no longer be left to chance; it is time to take control.

Appendix 2: demographics and IT spending trends

This appendix shows how the 270 interviews were distributed across the country, industry, company size and job roles categories covered by the survey.

It also shows some more detail by industry of total IT spending, factors that limit security spending and perceptions around IT threats.

Figure 12: Countries covered in survey

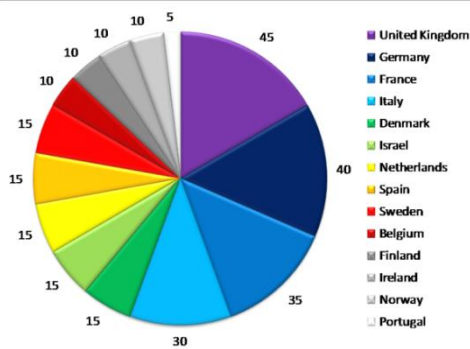


Figure 13: Company sizes covered in survey

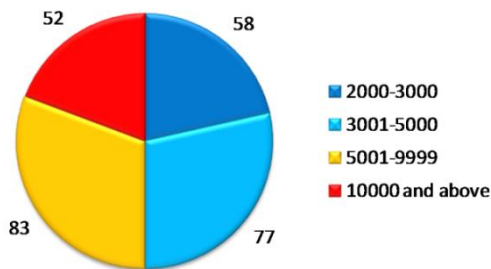


Figure 14: Business sectors covered in survey

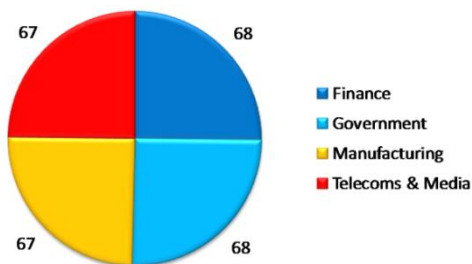


Figure 15: Job roles of respondents covered in survey

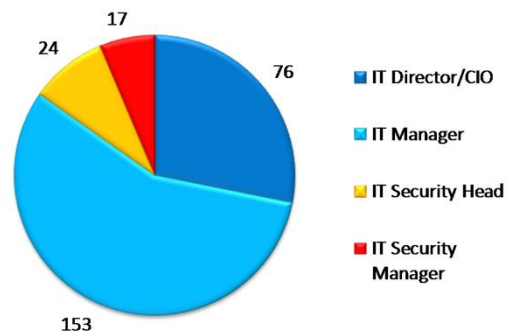


Figure 16: Approximately how much does your organisation spend each year on IT?

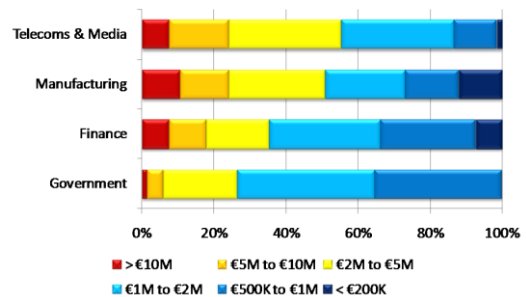


Figure 17: How influential are the following factors in limiting investment in security?

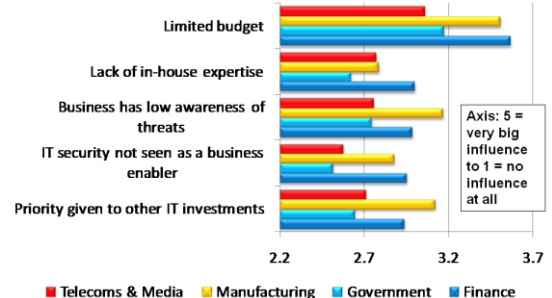
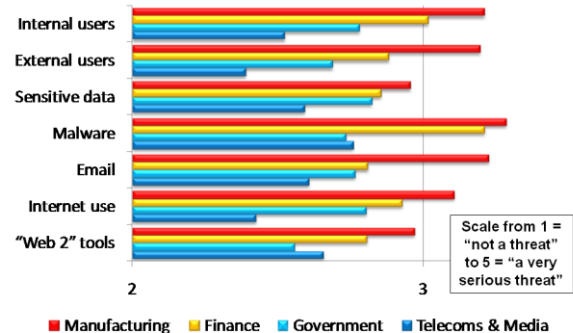


Figure 18: To what extent are the following perceived as a threat to IT security in your organisation?



About CA

CA (NASDAQ: CA), the world's leading independent IT management software company, helps customers optimize IT for better business results. CA's Enterprise IT Management solutions for mainframe and distributed computing enable Lean IT—empowering organizations to more effectively govern, manage and secure their IT operations.

[CA Security Management](#) technologies help customers efficiently and proactively protect and secure their IT environments. We offer a modular yet integrated set of tools that help customers answer key security questions that are essential to the security of their enterprise. Customers can determine who has access to what data, and then track that access to see how deep the user has gone into an application. This is all accomplished by automating and simplifying typically complex, time-consuming processes. By providing complete and integrated Identity and Access Management, and Security Information Management solutions, CA helps customers save time and money, and benefit from a faster time-to-value.

[CA Access Control](#) helps manage regulatory compliance by enforcing policy-based control of Privileged Users and controlling what system resources they can access and what they can do under specific circumstances. It provides a scalable, integrated solution for comprehensive privileged user management and host access control across multiple platforms and operating systems. Managed from a single console, CA Access Control helps secure servers, applications, and devices in a physical or virtual environment, while streamlining authentication across UNIX® and Active Directory systems.

In managing Privileged User passwords, CA Access Control issues passwords on a temporary, one-time use basis, or as necessary. It also helps provide accountability of shared account access for each privileged user beyond server access.

Founded in 1976, CA is a global company with headquarters in Islandia, NY and offices in more than 40 countries. CA had fiscal year 2009 revenues of \$4.3 billion. For more information, visit www.ca.com.

For additional background information on the report please visit www.ca.com/gb/mediaresourcecentre.



REPORT NOTE:

This report has been written independently by Quocirca Ltd to provide an overview of the issues facing organisations with regard to compliance and privileged user management.

The report draws on Quocirca's extensive knowledge of the technology and business arenas, and provides advice on the approach that organisations should take to create a more effective and efficient environment for future growth.

Quocirca would like to thank CA for its sponsorship of this report.

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 firsthand 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>

quocirca