



# Insecurity of Privileged Users

Global Survey of IT Practitioners

---

**Sponsored by HP Enterprise Security**

Independently conducted by Ponemon Institute<sup>LLC</sup>

Publication Date: December 2011

# The Insecurity of Privileged Users

Global Survey of IT Practitioners

Ponemon Institute, December 2011

## Part 1. Introduction

Ponemon Institute is pleased to present the findings of *The Insecurity of Privileged Users* sponsored by HP Enterprise Security. The purpose of this research is to understand the current threats to an organization's sensitive and confidential data created by a lack of control and oversight of privileged users in the workplace. User provisioning systems and security information and event management (SIEM) are currently considered the most important technologies used to control privileged user access to IT resources.

For purposes of this research, privileged users include database administrators, network engineers, IT security practitioners and cloud custodians. According to the findings of this study, these individuals often use their rights inappropriately putting their organizations' sensitive information at risk. For example, the majority of respondents say privileged users feel empowered to access all the information they can view and although not necessary will look at an organization's most confidential information out of curiosity.

We believe respondents have a deep understanding of the potential risks to sensitive data because they have privileged access in their organizations. For purposes of this research, we surveyed 5,569 IT operations and security managers in the following 13 countries: United States, United Kingdom, Germany, France, Italy, Spain, Singapore, Hong Kong, Korea, Japan, India, Australia and Brazil.

To ensure that respondents have an in-depth knowledge of how their organizations are managing privileged users, we asked respondents to indicate their level of access to their organizations' IT networks, enterprise systems, applications and information assets. If they had only limited end user access rights to IT resources, they were not included in the final sample of respondents.

Sixty percent of respondents are at the supervisor level or higher and most report to the chief information officer. On average, respondents have been employed in their current position for slightly more than 7 years. According to 77 percent of respondents, privileged access rights are required to complete their current job assignment. However, 23 percent say the access rights they have are not necessary for their role.

The following practices occur in many of the global organizations represented in this study:

- Not revoking privileged access status after the employee's role changed and providing everyone at a certain level in the organization with such access.
- IT operations is primarily responsible for assigning, managing and controlling privileged user access rights. However, business units and IT security are the functions most often responsible for conducting privileged user role certification.
- Rarely are requests for privileged access immediately checked against security policies before access is approved and assigned.
- Privileged access rights that go beyond the individual's role or responsibilities are often assigned.
- Commercial off-the-shelf automated solutions are most often used for granting privileged user access to IT resources and for reviewing and certifying privileged users' access.
- There is an inability to create a unified view of privileged user access across the enterprise.

## Part 2. Key Findings

Following is a summary of the consolidated global key findings. The major topics addressed in this study are: privileged user access governance, the process for assigning privileged user access to IT resources, critical success factors and barriers to reducing the risks of an insecure privileged user access program.

**Privileged user access is often abused.** The detailed findings section of this paper presents the perceptions respondents have about the management of privilege user access and common practices of privileged users. According to 64 percent of respondents, it is very likely or likely that privileged users believe they are empowered to access all the information they can view and a similar percentage (61 percent) say privileged users access sensitive or confidential data because of their curiosity.

As an indication that a governance problem exists in many organizations, 52 percent of respondents say it is likely or very likely that the organization will assign privileged access rights that go beyond the individual's role and responsibilities. However, organizations in this study seem to do a better job at making sure employees who leave the organization do not continue to have their access rights. Only 17 percent say this is very likely or likely to happen.

**What's at risk?** Forty-two percent of respondents say the risk to organizations caused by the insecurity of privilege access users will increase over the next 12 to 24 months and 42 percent say it will stay the same. Cloud-based applications, virtualization and regulations or industry mandates are the primary reasons for this belief.

General business information followed by customer information are the data types at risk if there is a lack of proper access controls over privileged users and the applications most threatened are mobile, social media and business unit specific applications.

**User provisioning systems and SIEM are the preferred technologies.** When asked to indicate the relative importance of technologies with respect to controlling privileged user access to IT resources, the following were selected: user provisioning systems and security information and event management systems (SIEM) and authentication and identity management.

**Many organizations do have well-defined policies for assigning privileged user access.** While 41 percent say the best way to describe the assigning of privileged user access to IT resources is ad hoc, 39 percent say assignment is determined by well-defined policies that are centrally controlled by corporate IT and another 13 percent say it is determined by well-defined policies that are controlled by business or application owners.

Forty-seven percent say information technology is responsible for granting privileged user access to information resources and 40 percent say is the business unit manager. Most responsible for conducting privileged user role certification are business units (33 percent) and IT security (28 percent).

Commercial off-the-shelf automated solutions are most often used for granting privileged user's access to IT resources and for reviewing and certifying privileged users access.

**Many organizations face a lack of enterprise visibility of access rights making governance difficult.** Almost one-third (32 percent) of respondents are not confident and six percent are unsure that their organization has enterprise-wide visibility for privilege user access and can determine if these users are compliant with policies. The primary reason for this lack of confidence is the inability to create a unified view of privileged user access across the enterprise.

Twenty-seven percent say their organizations use technology-based identity and access controls to detect the sharing of system administration access rights or root level access rights by privileged users and 24 percent say they use a combination of technology and manually-based identity and access controls. However, 15 percent admit access is not really controlled and 11 percent say they are unable to detect sharing of access rights.

What organizations say they do well is to provide evidence of compliance with regulations and industry. Areas where organizations most need to improve include: monitoring privileged users' access when entering administrative root level access, understanding privileged users entitlements that violate policy and enforcing access policies in a consistent fashion across all information resources in an organization.

**The critical success factors.** Budget, identity and access management technologies and security intelligence technologies are the three most critical success factors for governing, managing and controlling privileged user access across the enterprise. Least critical is audits by an independent third party.

**The barriers to delivering and enforcing privileged user access rights.** The top barriers are: cannot keep pace with the number of access change requests that come in on a regular basis, lack of a consistent approval process for access and a way to handle exceptions, too expensive to monitor and control all privileged users and difficult to audit and validate privileged user access changes.

The following are believed to have a very significant or significant affect on privileged user access governance: adoption of cloud-based applications enables the business or end-users to circumvent existing access policies, availability of SIEM and other network technologies, adoption of virtualization technologies and increasing number of regulations.

### **Global perspective**

The potential for privileged access abuse seems greatest in France, Italy and Hong Kong, according to respondents in those countries. Seventy-nine percent of respondents in France say privileged users believe they are empowered to access all the information they can view followed by 76 percent of respondents in Italy and 74 percent of respondents in Hong Kong. The countries where this is less likely to occur, according to respondents, are Japan, Singapore and Germany.

The countries where privileged users are most likely to access sensitive or confidential data because of their curiosity are France, Australia and Italy. Less likely are Japan, Singapore and Germany. Also in France and Italy, according to respondents, organizations are most likely to assign privileged access rights that go beyond the individual's role or responsibilities. This is less likely to occur in Korea, Singapore and Germany.

Respondents in the UK, Hong Kong and Australia are more concerned that the risk to an organization's access governance process will increase. Countries that are more optimistic about the risk are Korea, India and Singapore.

The situations that are most likely to affect their organizations' access governance process, especially for privileged users are: adoption of cloud-based applications because it enables the business or end-users to circumvent existing access policies, availability of SIEM and other security intelligence technologies, increasing number of regulations or industry mandates and adoption of virtualization technologies. Only the US, Germany and France selected the change in the nature and scope of cyber crime as a major influence on access governance procedures.

### Part 3. Implications & recommendations

The findings reveal a plethora of security problems caused by privileged access abuse. We believe enabling technologies are essential to identifying threats posed by negligence and malicious acts. We also recommend the following practices:

- Implement a well-managed enterprise-wide privileged user access governance process that is based on roles and responsibilities. Manage changes to a privileged user's role to ensure that he or she continues to have the correct access rights for a given job function.
- Create well-defined business policies for the assignment of access rights. These policies should be centrally controlled to ensure they are enforced in a consistent fashion across the entire enterprise.
- Understand how to make the case for building an enterprise-wide privileged user access governance process to senior management. Factors to include are the fines and penalties for noncompliance and downtime as a result of negligence that causes operational problems. With respect to data breaches, it is the cost of notification, customer attrition and loss of reputation that can severely impact an organization's bottom line. This will help ensure there is an ample budget and collaboration among business units to enforce privileged user access policies.
- Track and measure your organization's ability to enforce privileged user access policies. This includes its effectiveness in managing changes to users' roles, revoking access rights upon an individual's termination, monitoring access rights of privileged users' accounts and monitoring segregation of duties.
- Ensure that accountability for privileged users access rights is assigned to the business unit that has domain knowledge of the users' role and responsibility.
- Become proactive in managing access rights. Instead of making decisions on an ad hoc basis based on decentralized procedures, build a process that enables your organization to have visibility to all user access across all information resources and entitlements to these resources. Technologies that automate access authorization, review and certification will limit the risk of human error and negligence.

### Part 4. Detailed findings

The majority of respondents (77 percent) say privileged user access rights are necessary for fulfilling their job function or role (see Pie Chart 1). Twenty-three percent say they have these rights even though they are not necessary for their work. As shown in Table 1, 43 percent of these respondents believe they still have this privilege because of their position. Another 34 percent say privilege access, while once necessary, was not revoked after their role changed.

Pie Chart 1: Is privileged access required in order for you to complete your current job assignment or function within the organization?

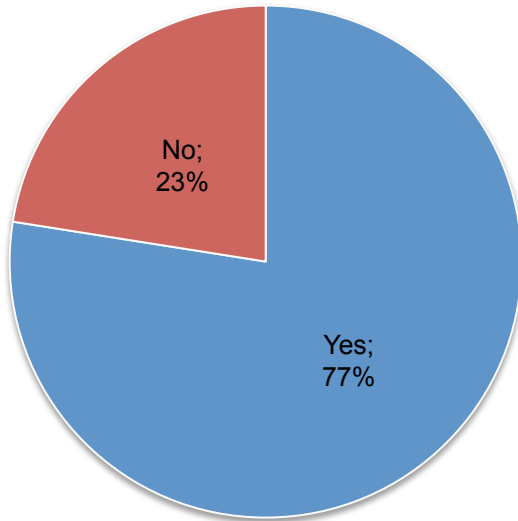
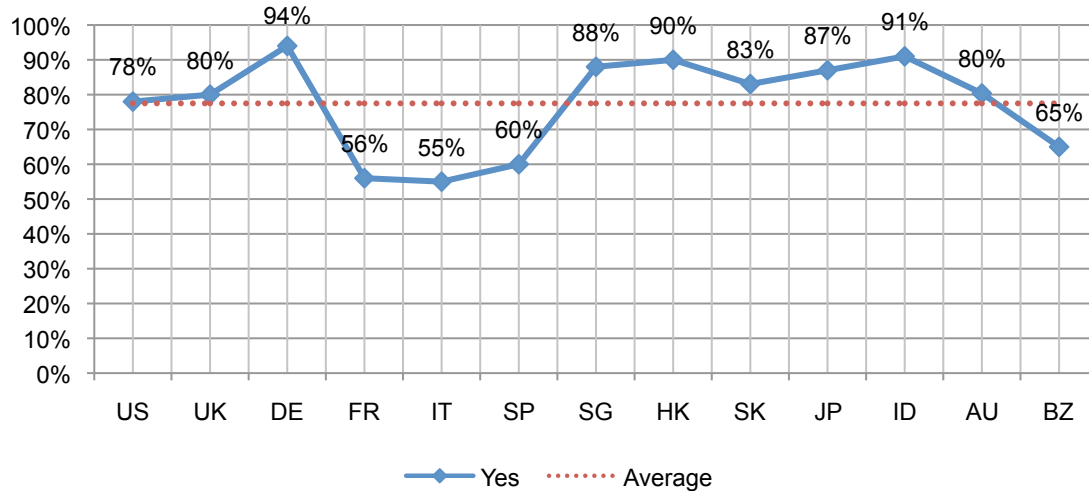


Table 1: If you said no, what is the primary reason you still have privileged access rights? Only one choice is permitted.

Reasons why	Pct%
I needed privileged access in a previous position and it was not revoked after my role changed	34%
Everyone at my level has privileged access even if it is not required to perform a job assignment	43%
The organization assigned privileged access rights for no apparent reason	12%
I don't know	11%
Total	100%

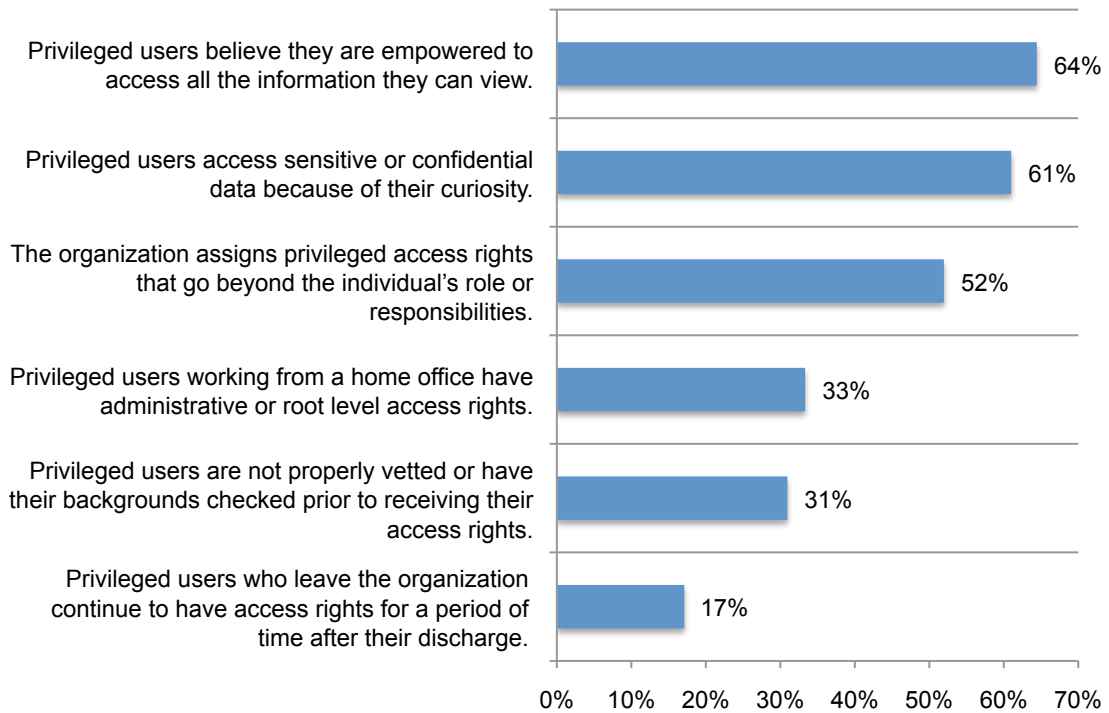
The need for privileged access rights varies among respondents in 13 countries. As shown in Graph 1, 94 percent of respondents in Germany say privileged access is essential. In contrast, only 55 percent of Italian respondents believe this to be so.

Graph 1: Is privileged access required in order for you to complete your current job assignments or functions within the organization? Percentage Yes response



Respondents were asked to assess the likelihood of certain scenarios occurring in their organizations. The most likely scenario to occur, according to 64 percent of respondents, is that privileged users believe they are empowered to access all the information they can view. Sixty-one percent believe privileged users are very likely or likely to view sensitive or confidential data simply because they are curious. Similarly, 52 percent believe privileged users within their organization have access rights that go beyond their role or job-related responsibilities.

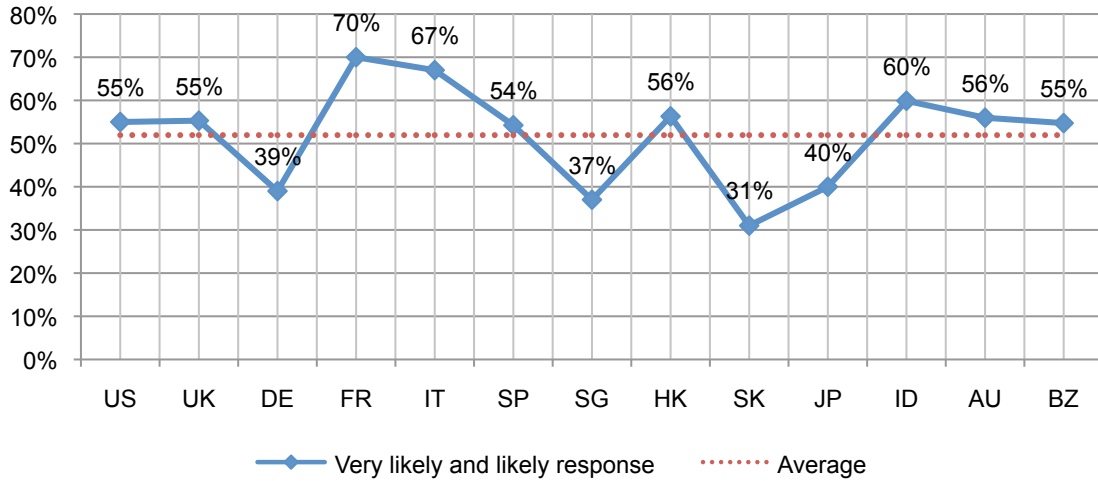
**Bar Chart 1: Indicators of privileged user access governance issues**  
Very likely and likely response



Do privilege access rights go beyond job role or function? In other words, is access governance too lenient and as a result puts information assets at risk? As shown in Graph 2, more than 70 percent of respondents in France and 67 percent of respondents in Italy believe privilege access rights within their organization go beyond role and function. In contrast, 31 percent of respondents in Korea and 37 percent of respondents in Singapore believe privilege access rights are too pervasive.

**Graph 2: The organization assigns privileged access rights that go beyond the individual's role or responsibilities.**

Very likely and likely response

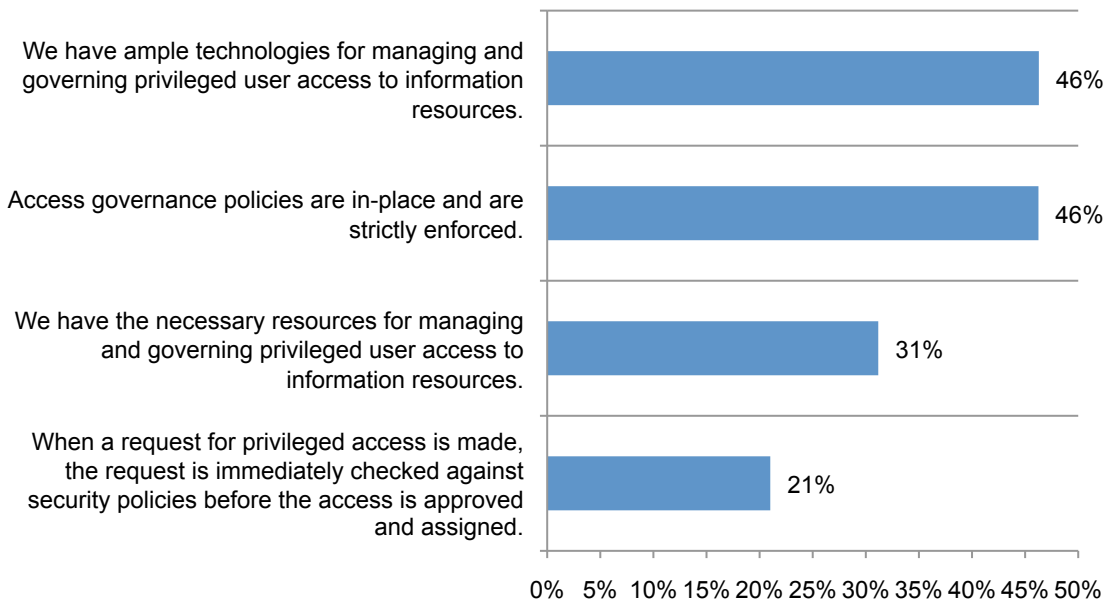


Bar Chart 2 reports four attributions about the state of access governance within respondents' organizations. Each percentage reflects the strongly agree and agree response combined. Hence, a percentage greater than 50 percent suggests a net-favorable response. Inversely, a percentage below 50 percent suggests a net-unfavorable response. All four attributions in this chart are below 50 percent suggesting a net-unfavorable view about access governance in the organizations studied.

Only 21 percent strongly agree or agree that requests for privileged user access are immediately checked against security policies before the access is approved and assigned. Thirty-one percent strongly agree or agree that their organizations have the necessary resources for managing and governing privileged user access to information assets. Forty-six percent believe their organizations have policies that are strictly enforced. The same percentage of respondents believe their organizations have ample enabling technologies available for managing privileged user access to information resources.

**Bar Chart 2: Attributions about the state of privileged access governance**

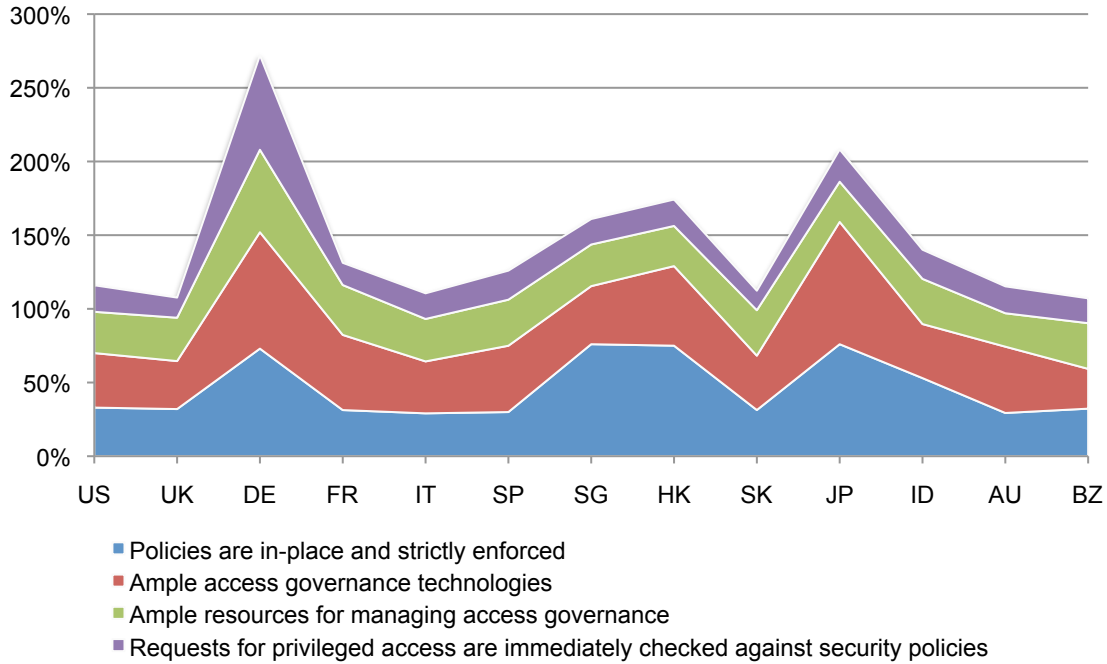
Strongly agree and agree response



Graph 3 presents an area diagram showing respondents' strongly agree and agree ratings to four attributions about the state of privileged access governance within their organizations. A high combined score suggests a stronger access governance regime and a low combined score suggests the opposite. This graph shows Germany achieves the highest combined score followed by Japan. In contrast, the UK, Brazil, Korea, Italy, US and Australia have much lower combined scores.

**Graph 3: Four attributions about the state of privileged access governance**

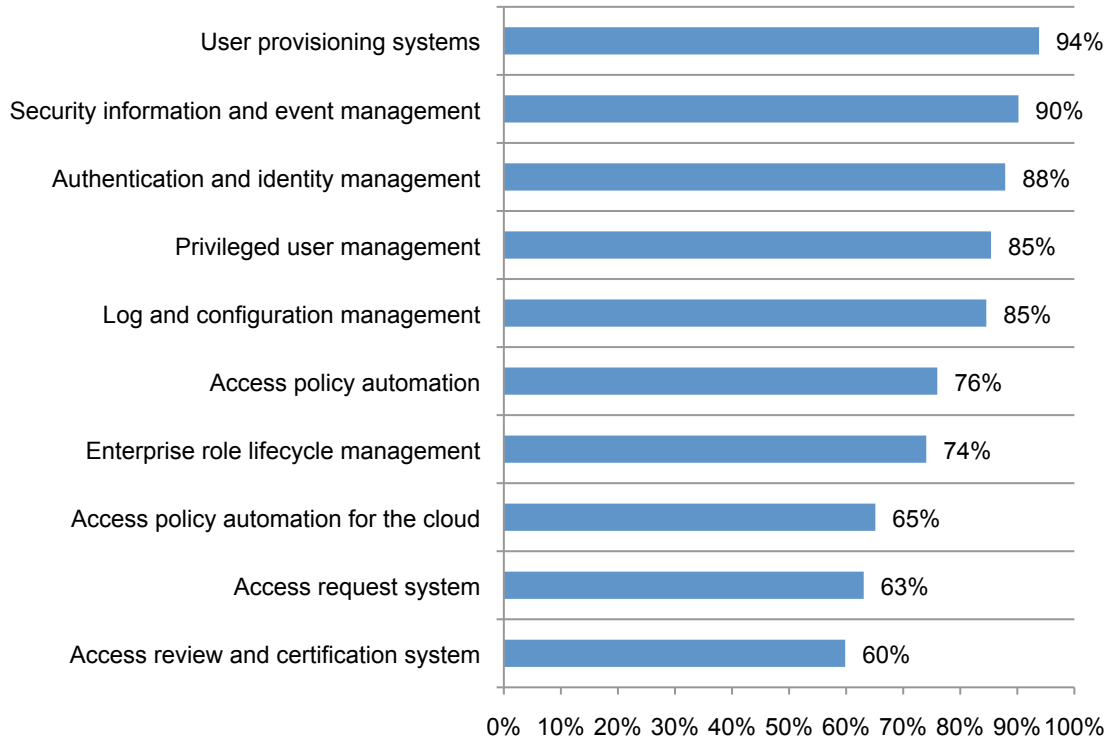
Combination of four separate ratings (strongly agree and agree response)



Respondents were asked to select the technologies presently used within their organizations. They then rated each security technology based on its importance in governing and controlling privileged user access to data assets and other IT resources. The combined very important and important ratings are reported in Bar Chart 3. As shown, the top three technologies rated by respondents as most important are: user provisioning (94 percent), security information and event management or SIEM (90 percent), and authentication and identity management (88 percent).

**Bar Chart 3: Enabling security technologies considered important to achieving a high state of privileged access governance**

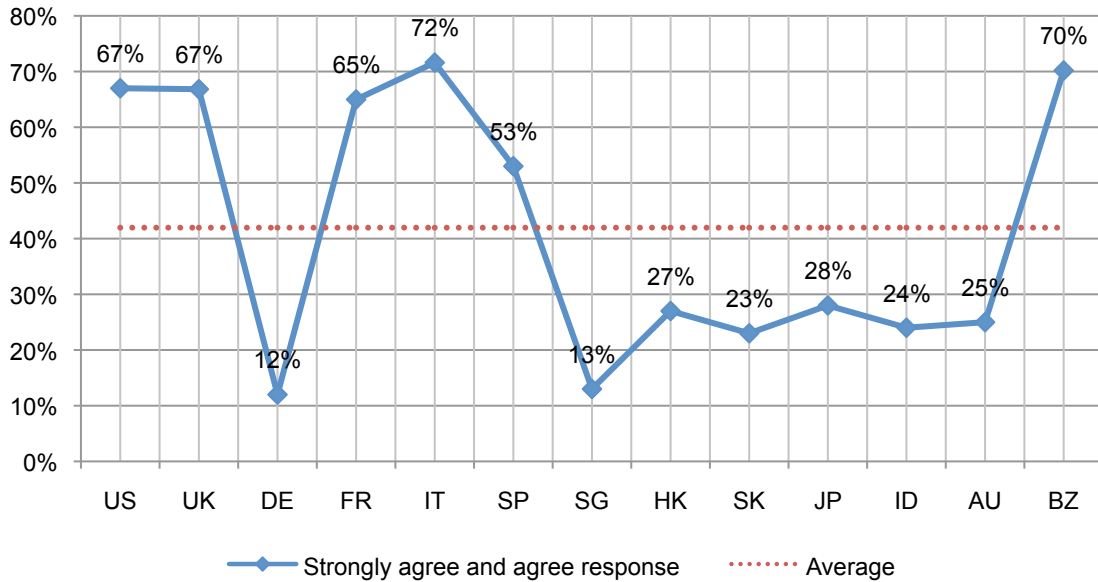
Very important and important response



Graph 4 reports respondents' rating of an attribution dealing with a potentially dangerous practice – namely, the privileged user's ability to circumvent IT security requirements in order to deliver services. Clearly, there are significant differences among the 13 countries studied. On the positive side, Germany (12 percent) and Singapore (13 percent) report the lowest ratings of this attribution. In sharp contrast, respondents in Italy (72 percent) and Brazil (70 percent) report the highest ratings. These results suggest the circumvention of IT security requirements may be a pervasive practice in Italy, Brazil in and several other countries.

**Graph 4: Attribution “In my organization, privileged users are permitted to circumvent IT security requirements if it prevents them from delivering services.”**

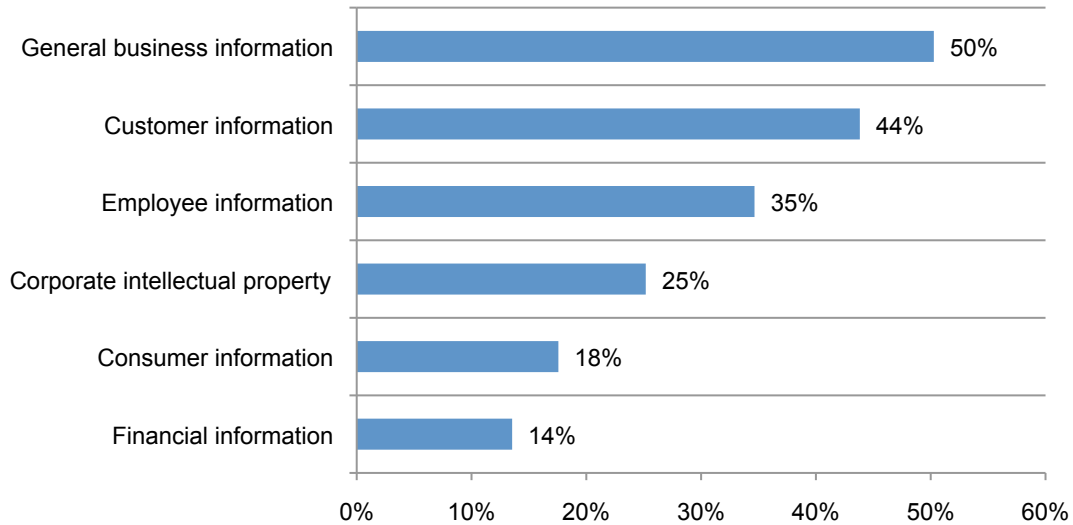
Strongly agree and agree response



Bar Chart 4 shows the data assets most at risk, according to respondents. As shown, general business information (such as documents, spreadsheets, emails and other sources of unstructured data) are considered most at risk because of improper access controls. Customer and employee information are also viewed as high-risk data assets. Financial information is viewed as the least at risk. This finding, at least in part, may be due to access requirements implemented over the past several years in response to regulatory requirements such as Sarbanes-Oxley, Basil II and other comparable standards.

**Bar Chart 4: What types of data assets do you consider to be most at risk due to the lack of proper access controls?**

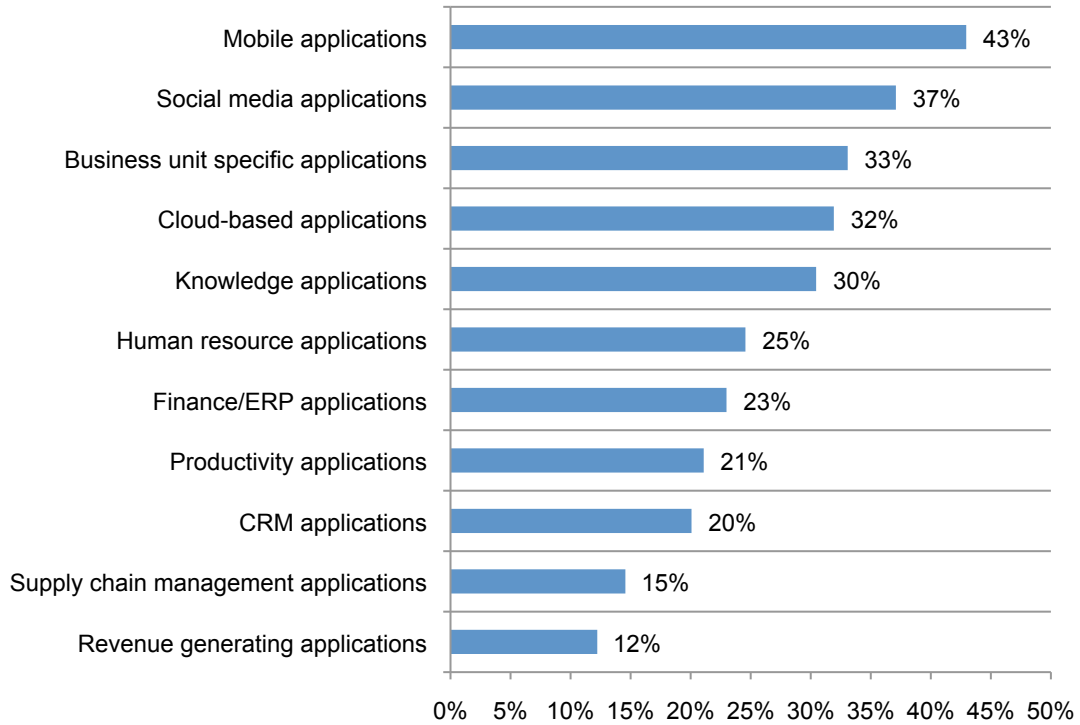
More than one choice permitted



Bar Chart 5 reports the applications most at risk, according to respondents. Mobile applications and social media present the applications with the highest levels of risk because of improper access controls. Business unit specific and cloud-based applications are also viewed as high-risk.

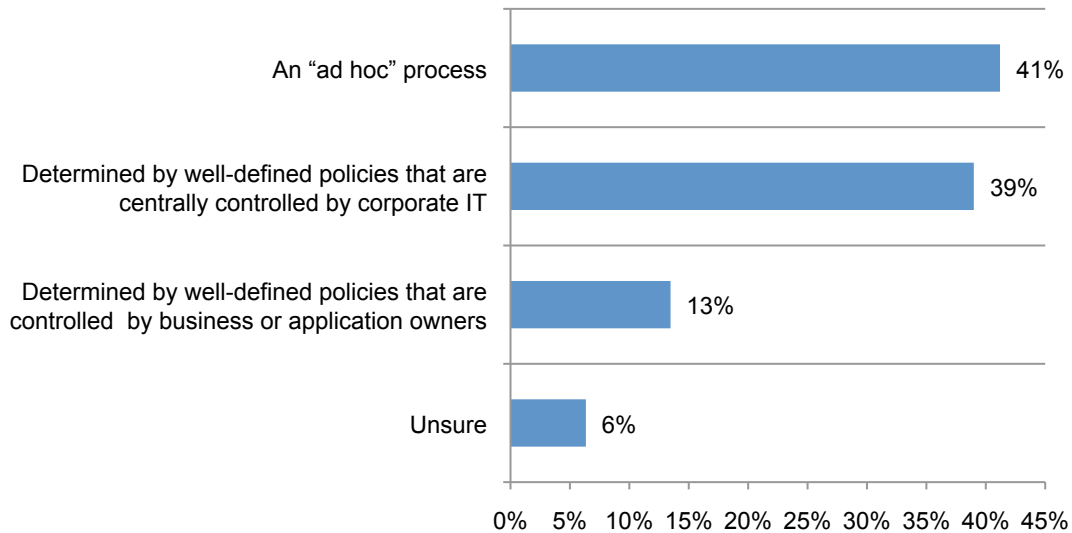
**Bar Chart 5: What applications do you consider to be most at risk due to the lack of proper access controls?**

More than one choice permitted



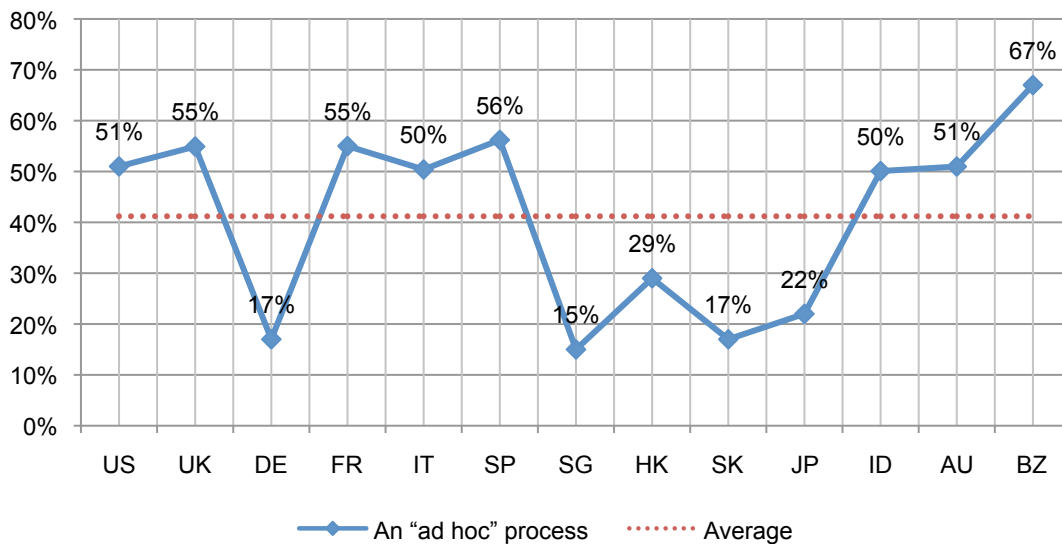
Respondents were asked to define their organization’s process for assigning privilege user access. As shown in Bar Chart 6, 41 percent of respondents say the process is ad hoc. Another 39 percent define their organization’s process as based upon well-defined policies and centrally controlled by corporate IT.

**Bar Chart 6: What best describes the process for assigning privileged user access to IT resources in your organization today?**



Graph 5 reports the percentage frequency of respondents within each country that say their organization’s process for assigning privileged access is ad hoc. As shown, Singapore (15 percent), Korea (17 percent) and Germany (17 percent) are least likely to define this process as ad hoc. In contrast, respondents in Brazil (67 percent) are most likely to see their organization’s process for assigning privileged access as ad hoc.

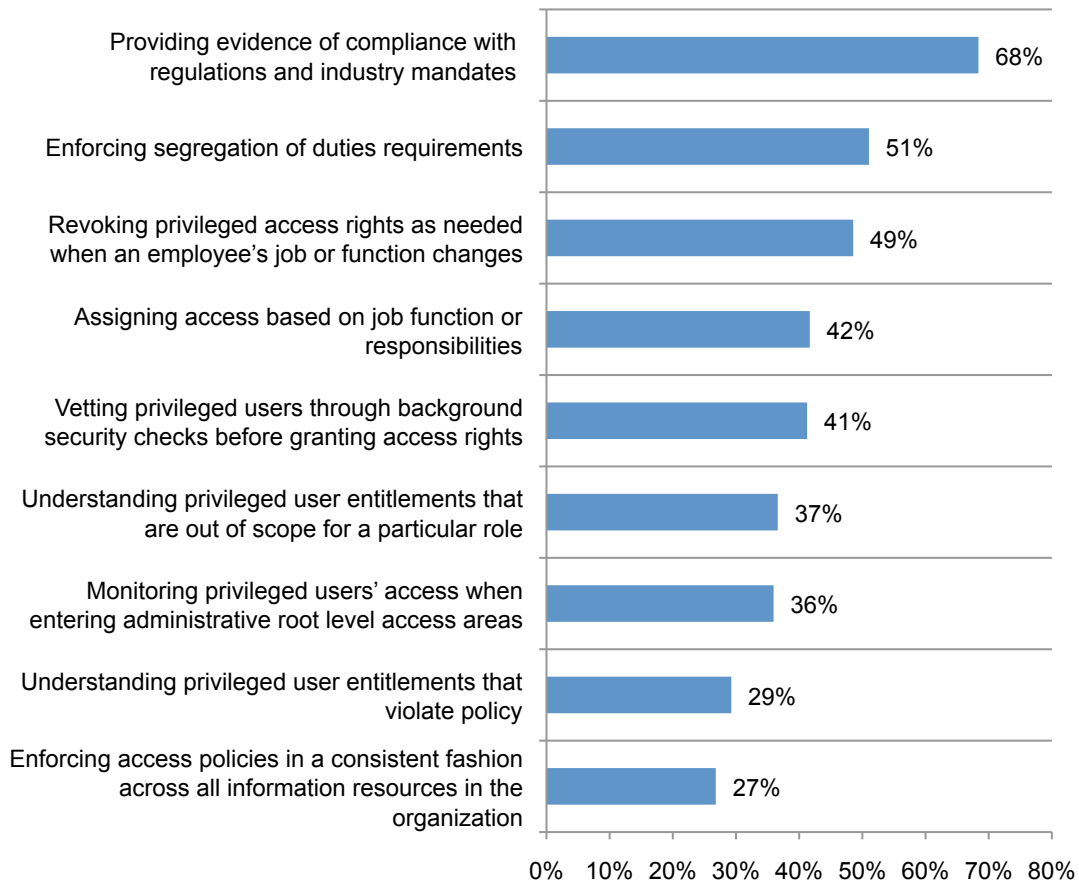
**Graph 5: Respondents who state their organization’s process for assigning privileged user access as “ad hoc”**



Bar Chart 7 provides respondent ratings to a list of best practices. Each rating is defined as the combination of an excellent and good response. A high percentage value suggests a favorable result. Accordingly, 68 percent of respondents say their organizations are excellent or good in providing evidence of compliance with regulations and industry mandates. Fifty-one percent say their organizations are excellent or good in enforcing segregation of duties. Only 27 percent of respondents say their organizations enforce access policies in a consistent fashion. Further, only 29 percent say their organizations have an excellent or good understanding of privileged users' entitlements that violate policy.

**Bar Chart 7: How well does your organization ensure privileged user access policies for the following tasks are strictly enforced?**

Excellent and good response



Pie Chart 2 shows that only a minority of respondents are very confident (19 percent) or confident (19 percent) that their organizations have enterprise-wide visibility for privileged user access. Table 2 reports the reasons why respondents are not confident. As can be seen, 42 percent say their organizations cannot create a unified view of privileged user access across the enterprise. Another 32 percent say their organizations cannot keep up with the pace of change resulting from on-boarding, off-boarding and outsourcing activities, respectively.

Pie Chart 2: How confident are you that your organization has enterprise-wide visibility for privileged user access and can determine if these users are compliant with policies?

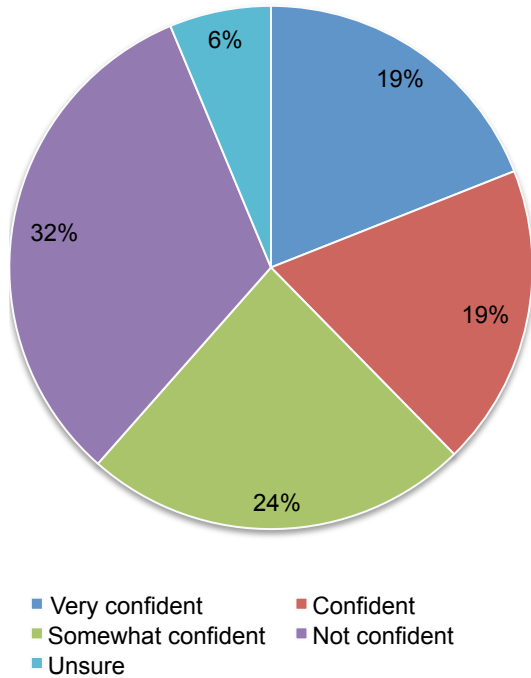
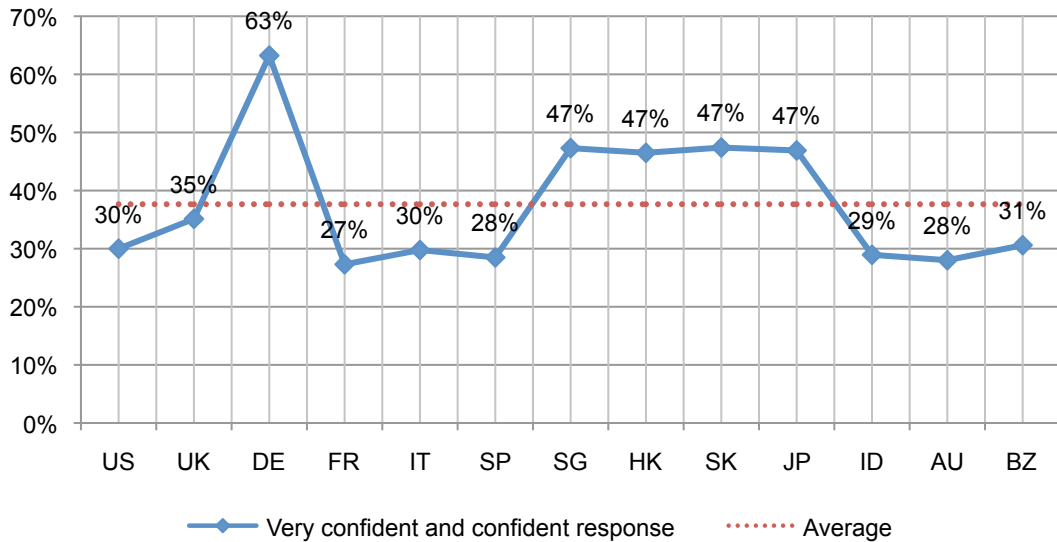


Table 2: If “not confident,” please select one main reason.

Reasons why	Pct%
We cannot create a unified view of privileged user access across the enterprise	42%
We only have visibility into privileged user account information but not entitlement information	13%
We cannot apply controls that need to span across information resources	14%
We cannot keep up with the changes occurring to our organization’s IT resources (on-boarding, off-boarding and outsourcing for management)	32%
Total	100%

Graph 6 reports the very confident or confident response for respondents among 13 countries. As reported, German respondents (63 percent) have the highest level of confidence in their organization's ability to achieve enterprise-wide visibility for privileged user access. Respondents in France (27 percent), Spain (28 percent) and Australia (28 percent) have the lowest levels of confidence.

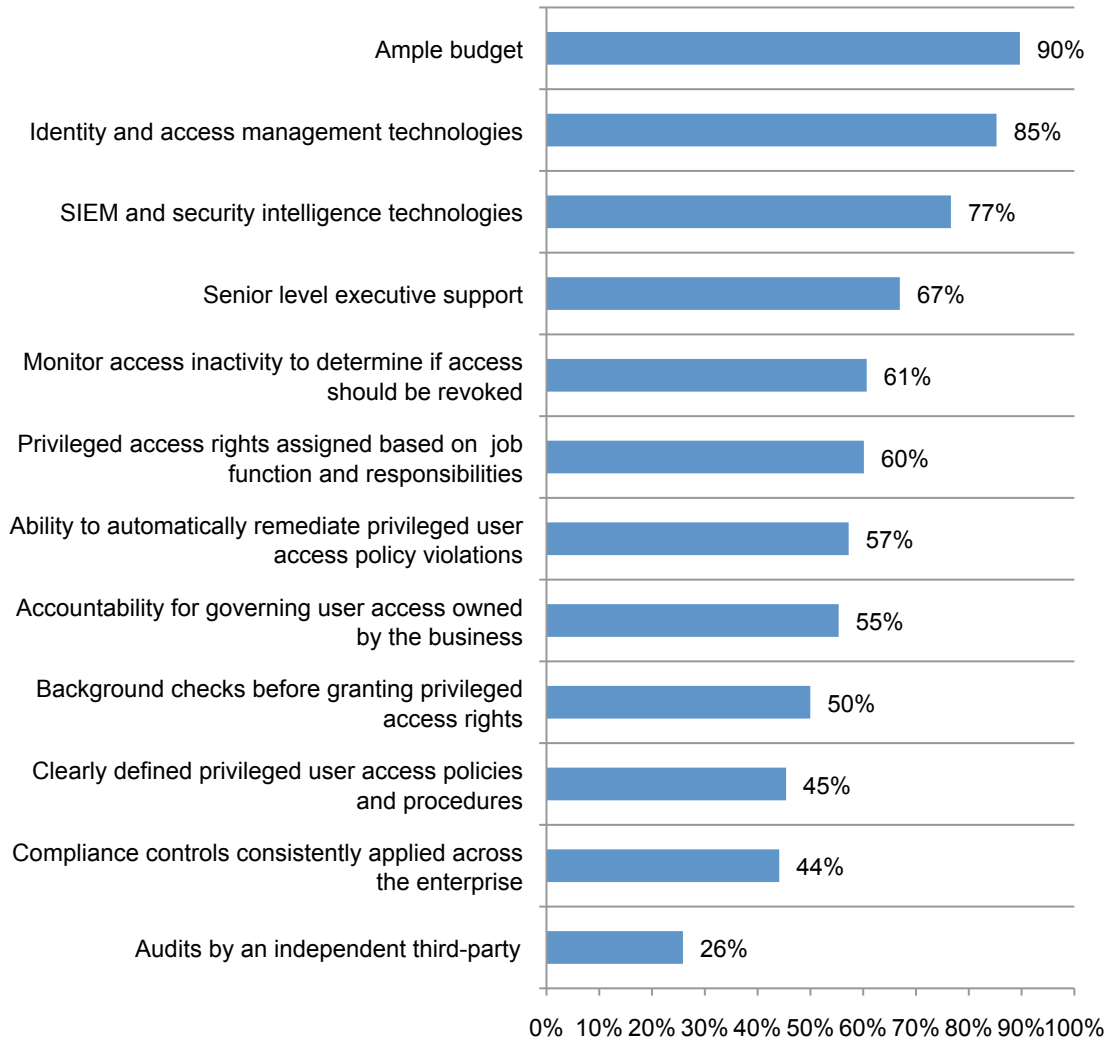
**Graph 6: Respondents who said they are very confident or confident that their organizations have enterprise-wide visibility for privileged user access**



Bar Chart 8 summarizes respondents' very important and important ratings to critical success factors relating to privilege user access governance. The top three most important factors are: ample budget (90 percent), identity and access management technologies (85 percent) and SIEM and security intelligence technologies (77 percent). Least important, according to respondents, is third party audit (26 percent).

**Bar Chart 8: What are the critical success factors for governing, managing and controlling privileged user access across the enterprise?**

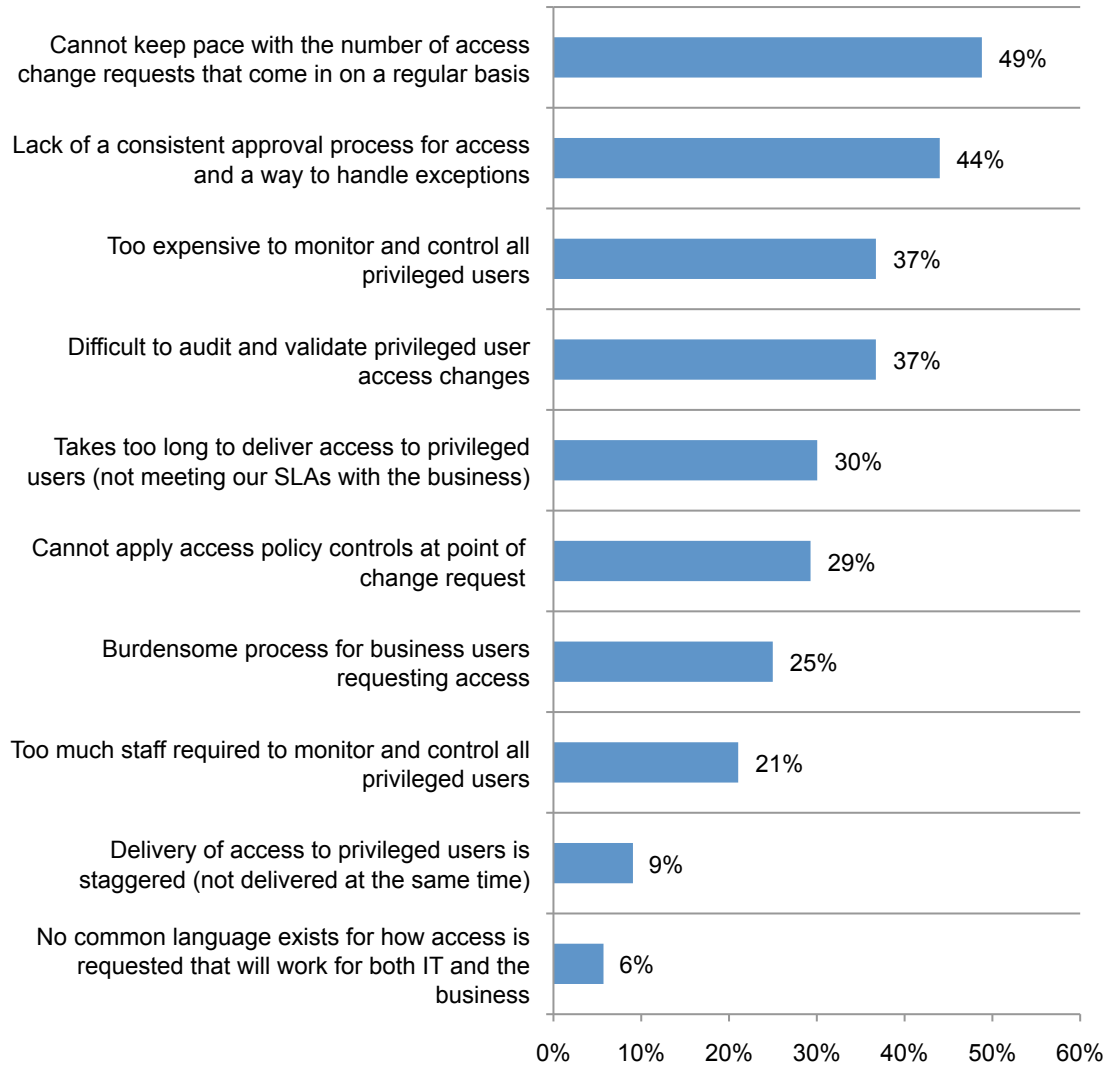
Very important and important response



Bar Chart 9 summarizes the main issues or problems organizations deal with in the delivery and enforcement of privileged user access rights. The top rated problems include workload (49 percent), lack of a consistent approval process over access rights assignment (44 percent) and cost-related issues (37 percent).

**Bar Chart 9: What are the main problems your organization faces in delivering and enforcing privileged user access rights?**

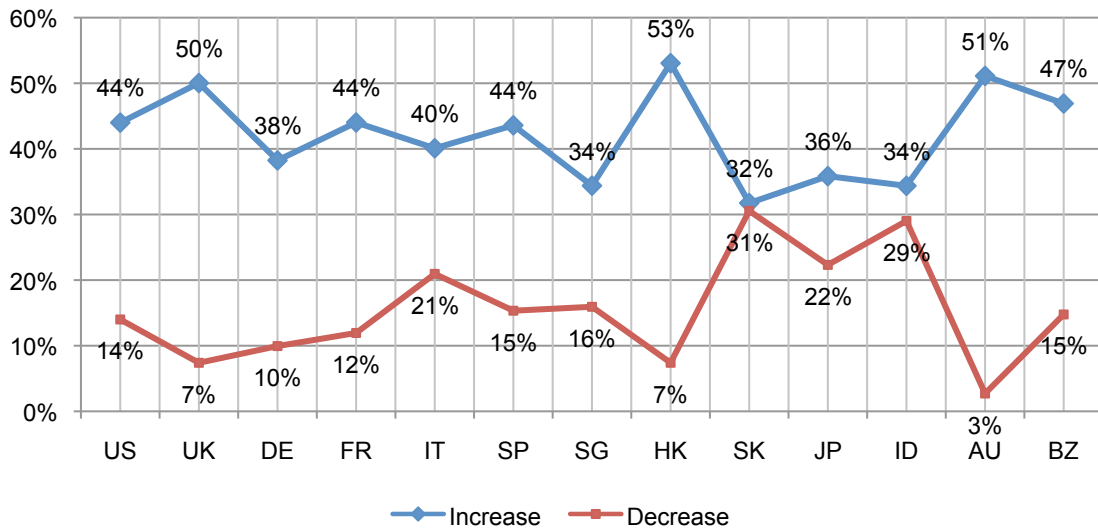
More than one choice permitted



Graph 7 shows respondents generally viewing the risk of privilege user insecurity as either increasing or staying the same. The graph clearly shows that respondents in all countries are more likely to see the risk as increasing versus decreasing. The largest gaps between these two choices include Australia (Diff = 48 percent), Hong Kong (Diff = 46 percent) and UK (Diff = 43 percent). The smallest gaps include Korea (Diff = 1 percent) and India (Diff = 5 percent).

**Graph 7. Do you believe privileged user security risks will increase, decrease or stay the same over the next 12 to 24 months?**

Increase and decrease response



## Part 6. Methods

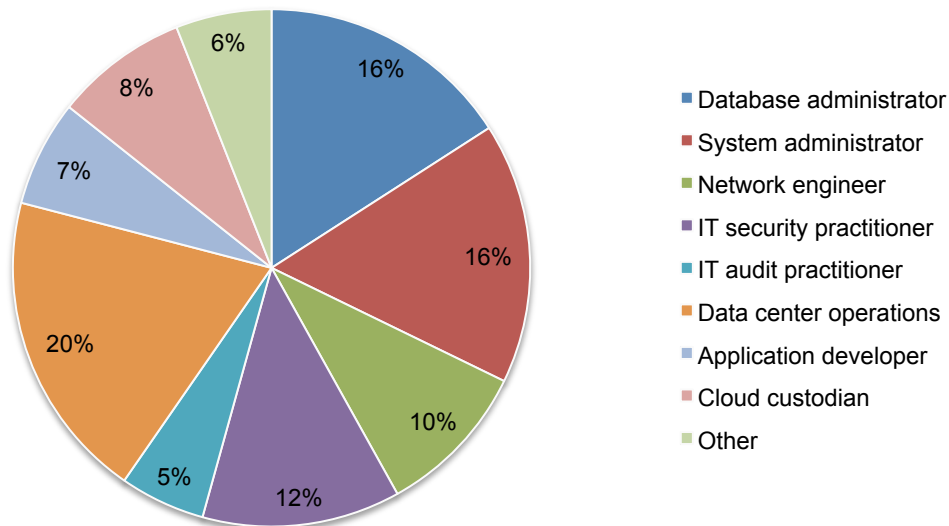
Table 3 reports the survey response statistics in 13 countries. All survey results were collected over a two-month period ending in November 2011. Utilizing proprietary sampling methods, we identified 130,791 individuals for possible participation in our global survey about privileged users in the IT environment. All of these individuals held bona fide credentials in the IT or security fields.

A total of 6,309 survey responses were received. After reviewing surveys for reliability and implementing screening criteria, we achieved a final sample of 5,569 respondents. The overall response rate is 4.5 percent. The largest country sample is the United States (n = 558) and the smallest country sample is Hong Kong (n = 319).

Countries	Abbreviation	Sample frame	Final sample	Response rate
United States	US	16,579	558	3.4%
United Kingdom	UK	11,283	499	4.4%
Germany	DE	14,503	506	3.5%
France	FR	9,981	371	3.7%
Italy	IT	7,895	321	4.1%
Spain	SP	8,009	405	5.1%
Singapore	SG	6,543	328	5.0%
Hong Kong	HK	7,020	319	4.5%
Korea	SK	8,917	442	5.0%
Japan	JP	10,995	493	4.5%
India	ID	15,603	518	3.3%
Australia	AU	4,699	309	6.6%
Brazil	BZ	8,764	500	5.7%
	Totals	130,791	5,569	4.5%

Pie Chart 3 shows the different roles or job functions respondents held that typically define privilege user status in the IT environment. Twenty percent are located in data center operations, 16 percent of respondents are database administrators, 16 percent are system administrators, 12 percent are IT security practitioners, and 10 percent are network engineers.

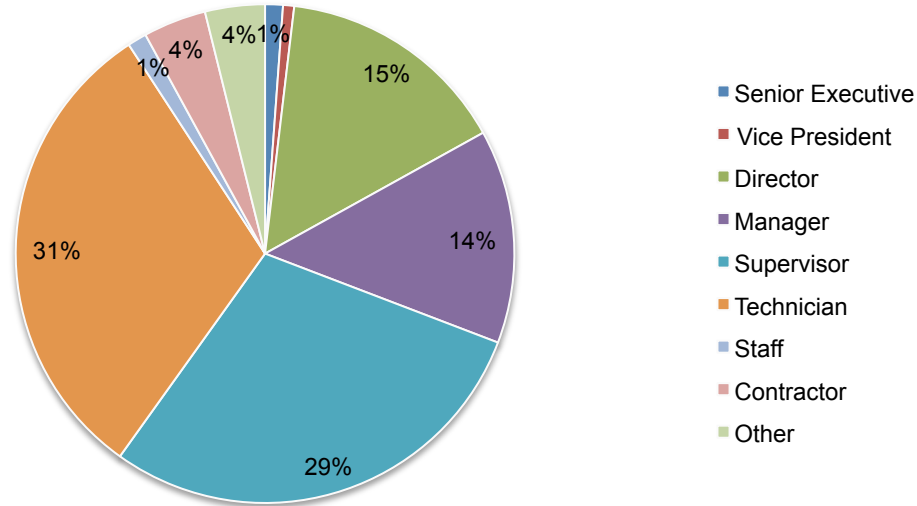
**Pie Chart 3: Respondents' approximate role or job function requiring privileged user status**  
 Respondents have on average 2 privileged roles. Consolidated data for 13 country samples (n = 5,569)



Pie Chart 4 reports the respondents' approximate position level within their organizations. As reported, the majority of respondents are at or above the supervisory level. The largest segment includes 31 percent of respondents who are at the rank-and-file level (a.k.a. technician).

**Pie Chart 4: Respondents' position level**

Consolidated data for 13 country samples (n = 5,569)

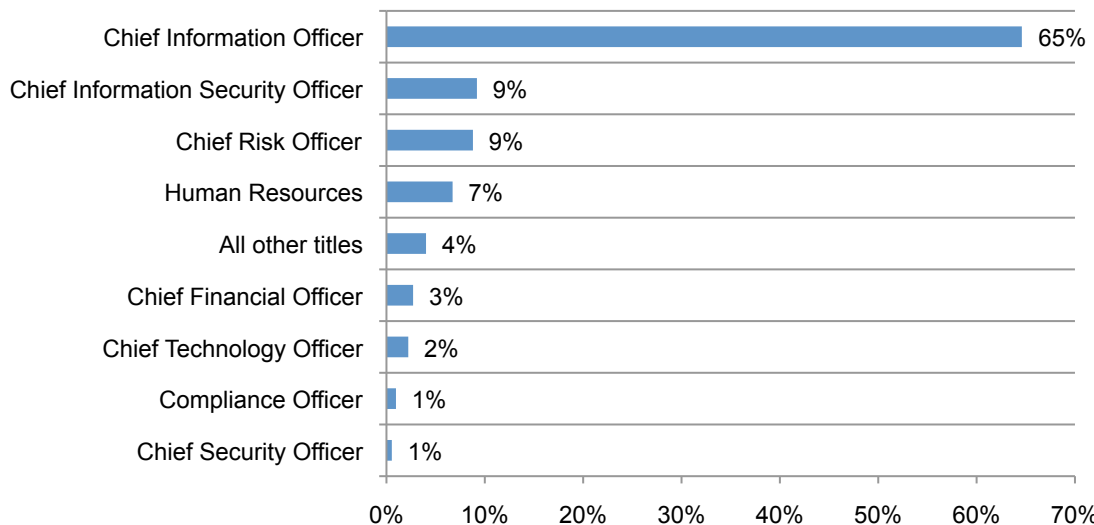


Twenty-seven percent of respondents are female and 73 percent male.<sup>1</sup> The average overall experience in years is 12.3, with a median value of 11.5 years.

According to Bar Chart 10, 65 percent of respondents report up through the organization's CIO or IT leader with an equivalent title. The second and third most frequently cited reporting channels include the CISO and the Chief Risk Officer (both at 9 percent).

**Bar Chart 10: Respondents' primary reporting channel**

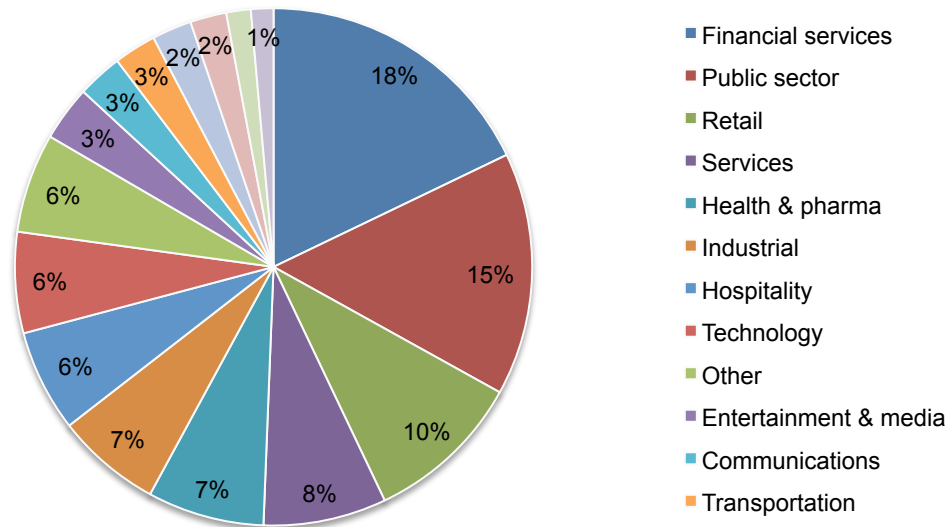
Consolidated data for 13 country samples (n = 5,569)



<sup>1</sup>While the overall sample is skewed to male participants, this result is consistent with numerous studies all showing that the IT field has a larger proportion of males than females worldwide. Studies show this gap is decreasing over time.

Pie Chart 5 reports the industries represented in the present study, consolidated for all country samples. As can be seen, the largest industry sectors include financial services (18 percent), public sector (15 percent) and retail (10 percent). Financial services include retail banking, insurance, payments/credit cards, brokerage and investment management. Public sector organizations include national, state/provincial and local/municipal entities. In some countries, healthcare providers are classified as public sector entities.

**Pie Chart 5: Respondent organizations' primary industry classification**  
 Consolidated data for 13 country samples (n = 5,569)



**Limitations**

There are inherent limitations to survey research that need to be carefully considered before drawing inferences from findings. The following items are specific limitations that are germane to most Web-based surveys.

- Non-response bias: The current findings are based on a sample of survey returns. We sent surveys to a representative sample of IT privileged users located in 13 countries, resulting in a large number of usable returned responses. Despite non-response tests, it is always possible that individuals who did not participate are substantially different in terms of underlying beliefs from those who completed the survey.
- Sampling-frame bias: The accuracy is based on contact information and the degree to which the list is representative of individuals who are IT practitioners who deal with a wide array of issues. We also acknowledge that responses from paper, interviews or telephone might result in a different pattern of findings.
- Self-reported results: The quality of survey research is based on the integrity of confidential responses received from respondents. While certain checks and balances were incorporated into our survey evaluation process, there is always the possibility that certain respondents did not provide responses that reflect their true opinions.

## Appendix: Consolidated Survey Data

The following frequency and percentage frequency tables summarize the consolidated results of this research involving 5,569 privileged users in the IT environment located in 13 countries. All fieldwork concluded in November 2011.

### Part 1. Background

Q1. What best describes your <u>level of access</u> to your organization's IT networks, enterprise systems, applications and information assets? Please select only one choice.	Pct%
Limited (ordinary) end user access rights to IT resources (Stop)	6%
Expanded access rights to IT resources, but not overly broad	10%
Broad access rights to IT resources	42%
Root level access rights to IT resources	31%
None of the above (Stop)	10%
Total	100%

Q2a. Is privileged access required in order for you to complete your current job assignments or functions within the organization?	Pct%
Yes	77%
No	23%
Total	100%

Q2b. If you said no, what is the primary reason you still have privileged access rights? Please select only one choice.	Pct%
I needed privileged access in a previous position and it was not revoked after my role changed	34%
Everyone at my level has privileged access even if it is not required to perform a job assignment	43%
The organization assigned privileged access rights for no apparent reason	12%
I don't know	11%
Total	100%

Q3. What best describes your role in the organization's IT department or related functions? Please check all that apply.	Pct%*
Database administrator	35%
Systems administrator	35%
Network engineer	21%
IT security practitioner	27%
IT audit practitioner	12%
Data center manager	42%
Application developer	14%
Cloud custodian	18%
Other (please specify)	3%
Total	207%

\*On average, respondents chose 2.07 privileged roles. Pie Chart 3 reports this percentage data on a role rather than an individual basis.

<b>Very likely &amp; likely response combined</b>	Pct%
Q4. The organization assigns privileged access rights that go beyond the individual's role or responsibilities.	52%
Q5. Privileged users are pressured to share their access rights with others in the organization.	38%

Q6. Social engineers outside the organization target privileged users to obtain their access rights.	28%
Q7. Malicious insiders target privileged users to obtain their access rights.	20%
Q8. Privileged users are not properly vetted or have their backgrounds checked prior to receiving their access rights.	31%
Q9. Privileged users become disgruntled and leak data or damage equipment.	27%
Q10. Privileged users access sensitive or confidential data because of their curiosity.	61%
Q11. Privileged users believe they are empowered to access all the information they can view.	64%
Q12. Privileged users who leave the organization continue to have access rights for a period of time after their discharge.	17%
Q13. Privileged users working from a home office have administrative or root level access rights.	33%
Q14. Negligent privileged users have at least partial responsibility for data loss or theft.	46%
Average	38%

<b>Part 3. Attributions:</b> Please rate the following statements using the scale provided below each item. Strongly agree and agree response combined	Pct%
Q15. In my organization, access governance policies are in-place and are strictly enforced.	46%
Q16. In my organization, we have ample technologies for managing and governing privileged user access to information resources.	46%
Q17. In my organization, we have the necessary resources for managing and governing privileged user access to information resources.	31%
Q18. In my organization, IT operations are primarily in-charge of assigning, managing and controlling privileged user access rights.	63%
Q19. In my organization, IT leadership determines what access rights are required or necessary for privileged users to complete their role and function.	23%
Q20. In my organization, privileged users are permitted to circumvent IT security requirements if it prevents them from delivering services.	42%
Q21. In my organization, when a request for privileged access is made, the request is immediately checked against security policies before the access is approved and assigned.	21%
Average	39%

**Part 4. Privileged user access governance**

Q22a. Please check all 10 of the enabling security technologies below that are used by your organization.	Pct%
Enterprise role lifecycle management	47%
Access request system	39%
Access policy automation	36%
Access review and certification system	31%
Privileged user management	43%
Security information and event management (SIEM)	46%
Access policy automation for the cloud	35%
Log and configuration management	56%
User provisioning systems	61%
Authentication and identity management	67%
Average	46%

Q22b. Please review all 10 of the enabling security technologies below that are used by your organization. For each item selected, indicate the relative importance of the technology with respect to controlling privileged user access to IT resources.	Pct%
Enterprise role lifecycle management	74%
Access request system	63%
Access policy automation	76%
Access review and certification system	60%
Privileged user management	85%
Security information and event management (SIEM)	90%
Access policy automation for the cloud	65%
Log and configuration management	85%
User provisioning systems	94%
Authentication and identity management	88%
Average	78%

Q23. What types of data do you consider to be most at risk in your organization due to the lack of proper access controls over privileged users? Top two choices.	Pct%
Customer information	44%
Consumer information	18%
Employee information	35%
Financial information	14%
General business information	50%
Corporate intellectual property	25%
Total	185%

Q24. What type of applications do you consider to be most at risk in your organization due to the lack of proper access governance and control? Please select the top three.	Pct%
Finance/ERP applications	23%
CRM applications	20%
Supply chain management applications	15%
Revenue generating applications	12%
Business unit specific applications	33%
Human resource applications	25%
Productivity applications	21%
Knowledge applications	30%
Cloud-based applications	32%
Social media applications	37%
Mobile applications	43%
Total	291%

Q25. What best describes the process for assigning privileged user access to IT resources in your organization today? Please select one best choice.	Pct%
An "ad hoc" process	41%
Determined by well-defined policies that are centrally controlled by corporate IT	39%
Determined by well-defined policies that are controlled by business or application owners	13%
Unsure	6%
Total	100%

Q26. Who in your organization is most responsible for granting privileged-user access to information resources? Top two choices.	Pct%
Information technology operations	47%
Information security department	12%
Compliance department	16%
Business unit managers	40%
Application owners	37%
Human resource department	26%
Unsure	5%
Total	184%

Q27. What processes are used for granting privileged user access to IT resources: Please select the top two.	Pct%
Manual process (i.e. email or phone)	23%
Homegrown access request systems	16%
Commercial off- the-shelf automated solutions	36%
IT Help Desk	17%
Unsure	3%
Other	5%
Total	100%

Q28. What processes are used to review and certify privileged user access? Please select the top two.	Pct%
Manual process (i.e. email, spreadsheets)	21%
Homegrown access certification system	19%
Commercial off-the-shelf access certification system	34%
IT Help Desk	4%
Unsure	16%
Other	6%
Total	100%

Q29. Who within your organization is most responsible for conducting privileged user role certification?	Pct%
IT security	28%
Business units	33%
Audit	5%
Compliance	13%
Quality assurance	5%
Data center management	3%
Other	13%
Total	100%

Q30. How does your organization detect the sharing of system administration access rights or root level access rights by privileged users? Please select the top two.	Pct%
Technology-based identity and access controls	27%
Manually-based identity and access controls	17%
A combination of technology and manually-based identity and access controls	24%
Access to sensitive or confidential information is not really controlled	15%
We are unable to detect sharing of access rights	11%
Unsure	6%
Total	100%

Q31. How well does your organization ensure privileged user access policies for the following tasks are strictly enforced? Combined excellent and good response.	Pct%
Assigning access based on job function or responsibilities	42%
Revoking or changing privileged access rights as needed when an employee's job or function changes or their relationship with the organization is terminated	49%
Enforcing access policies in a consistent fashion across all information resources in the organization	27%
Monitoring privileged users' access when entering administrative root level access areas	36%
Enforcing segregation of duties requirements	51%
Providing evidence of compliance with regulations and industry mandates	68%
Understanding privileged user entitlements that are out of scope for a particular role	37%
Understanding privileged user entitlements that violate policy	29%
Vetting privileged users through background security checks before granting access rights	41%
Average	42%

Q32a. How confident are you that your organization has enterprise-wide visibility for privileged user access and can determine if these users are compliant with policies?	Pct%
Very confident	19%
Confident	19%
Somewhat confident	24%
Not confident	32%
Unsure	6%
Total	100%

Q32b. If "not confident," please select <u>one</u> main reason.	Pct%
We can't create a unified view of privileged user access across the enterprise	42%
We only have visibility into privileged user account information but not entitlement information	13%
We can't apply controls that need to span across information resources	14%
We can't keep up with the changes occurring to our organization's IT resources (on-boarding, off-boarding and outsourcing for management)	32%
Total	100%

Q33. What are the critical success factors for governing, managing and controlling privileged user access across the enterprise? Very important and important response combined.	Pct%
Senior level executive support	67%
Ample budget	90%
Identity and access management technologies	85%
SIEM and security intelligence technologies	77%
Clearly defined privileged user access policies and procedures	45%
Accountability for governing user access owned by the business	55%
Privileged access rights assigned based on job function and responsibilities	60%
Compliance controls consistently applied across the enterprise	44%
Ability to automatically remediate privileged user access policy violations	57%
Monitor access inactivity to determine if access should be revoked	61%
Audits by an independent third-party	26%
Background checks before granting privileged access rights	50%
Average	60%

Q34. What are the main problems your organization faces in delivering and enforcing privileged user access rights? Please select only your top three choices.	Pct%
Takes too long to deliver access to privileged users (not meeting our SLAs with the business)	30%
Too expensive to monitor and control all privileged users	37%
Too much staff required to monitor and control all privileged users	21%
Cannot apply access policy controls at point of change request	29%
Delivery of access to privileged users is staggered (not delivered at the same time)	9%
Cannot keep pace with the number of access change requests that come in on a regular basis	49%
Lack of a consistent approval process for access and a way to handle exceptions	44%
Difficult to audit and validate privileged user access changes	37%
Burdensome process for business users requesting access	25%
No common language exists for how access is requested that will work for both IT and the business	6%
Other (please specify)	2%
Total	288%

<b>Part 5. More scenarios.</b> In your opinion, how will each of the following situations affect your organization's access governance process, especially concerning privileged users? Very significant and significant responses combined.	Pct%
Q35. Increasing number of regulations or industry mandates	56%
Q36. Adoption of cloud-based applications enables the business or end-users to circumvent existing access policies	64%
Q37. Outsourcing of applications and data for management	46%
Q38. The constant turnover (ebb and flow) of employees, contractors, consultants and partners	44%
Q39. Availability of SIEM and other security intelligence technologies	58%
Q40. Constant changes to the organization as a result of corporate reorganizations, downsizing and financial distress	31%
Q41. Adoption of virtualization technologies	56%
Q42. Expanded use of mobile devices in the workplace	51%
Q43. Change in the nature and scope of cyber crime	38%
Q44. The level of risk caused by privileged users abuse or misuse of IT resources	20%
Average	46%

Q45. Do you believe this risk will increase, decrease or stay the same over the next 12 to 24 months?	Pct%
Increase	42%
Stay the same	42%
Decrease	16%
Total	100%

**Part 5. Your role**

D1. What organizational level best describes your current position?	Pct%
Senior Executive	1%
Vice President	1%
Director	15%
Manager	14%
Supervisor	29%
Technician	31%
Staff	1%
Contractor	4%
Other	4%
Total	100%

D2. Check the <b>Primary Person</b> you or your IT security leader reports to within the organization.	Pct%
CEO/Executive Committee	0%
Chief Financial Officer	3%
General Counsel	0%
Chief Information Officer	65%
Chief Technology Officer	2%
Compliance Officer	1%
Human Resources VP	7%
Chief Security Officer	1%
Chief Information Security Officer	9%
Chief Risk Officer	9%
Other	4%
Total	100%

D3. Experience	Mean Value
D3a. Total years of employment experience	12.3
D3b. Total years in current position	7.4

D4. Gender	Pct%
Female	27%
Male	73%
Total	100%

D5. What industry best describes your organization's industry focus?	Pct%
Agriculture	0%
Communications	3%
Consumer products	1%
Defense	2%
Education & research	2%
Energy	2%
Entertainment & media	3%
Financial services	18%
Health & pharmaceutical	7%
Hospitality	6%
Industrial	7%
Public sector	15%
Retail	10%
Services	8%
Technology	6%
Transportation	3%
Other	6%
Total	100%

D7. What is the worldwide headcount of your organization?	Pct%
< 500	12%
500 to 1,000	18%
1,001 to 5,000	26%
5,001 to 25,000	20%
25,001 to 75,000	17%
> 75,000	7%
Total	100%

## **Ponemon Institute**

*Advancing Responsible Information Management*

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

As a member of the **Council of American Survey Research Organizations (CASRO)**, we uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.

## **HP Enterprise Security**

HP is a leading provider of security and compliance solutions for modern enterprises that want to mitigate risk in their hybrid environments and defend against advanced threats. Based on market leading products from ArcSight, Fortify, and TippingPoint, the HP Security Intelligence and Risk Management (SIRM) Platform uniquely delivers the advanced correlation, application protection, and network defense technology to protect today's applications and IT infrastructures from sophisticated cyber threats.