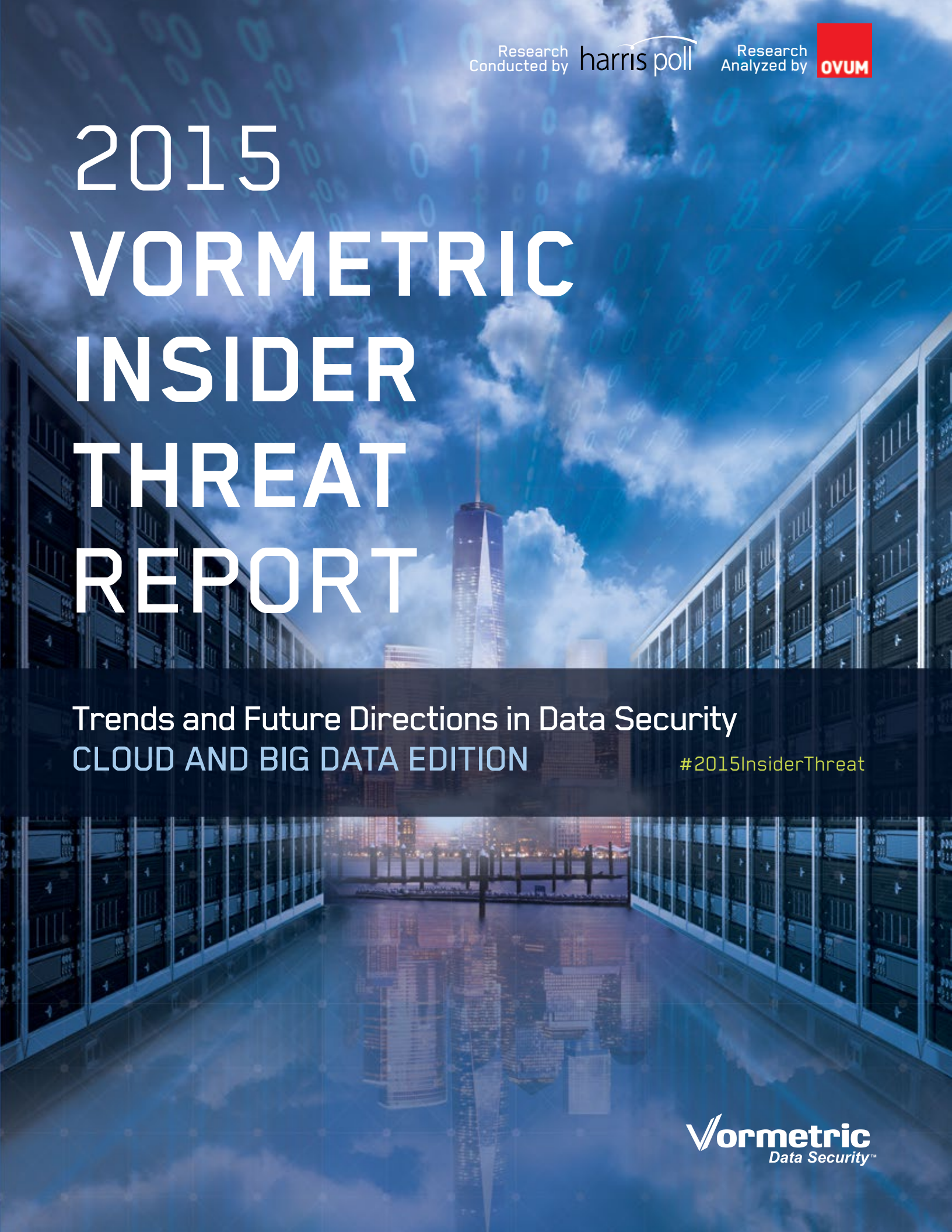

Research Conducted by harris poll
Research Analyzed by OVUM
2015
VORMETRIC
INSIDER
THREAT
REPORT
Trends and Future Directions in Data Security
CLOUD AND BIG DATA EDITION
#2015InsiderThreat
Vormetric
Data Security™

TABLE OF CONTENTS

OUR SPONSORS

Couchbase

CSA

FINANCIAL SERVICES ISAC

rackspace the #1 managed cloud company

fishnet SECURITY

OASIS

carahsoft

PREVENTIA

AZM

M.TECH Your Preferred i-Security Partner

fieldfisher

Raber+Märcker Prinzip Partnerschaft

SUMMARY

Catalyst

The increasing use of cloud services and Big Data projects is causing major security concerns. The Cloud and Big Data edition of the *2015 Vormetric Insider Threat Report* provides up-to-date insight and opinion on the increasing security, risk, and compliance concerns that enterprise organizations face on an ongoing basis. The report is based on survey responses from more than 800 senior business managers and IT professionals from major global markets. It examines their concerns and looks at the changes they want to see implemented before increasing their adoption of cloud and Big Data solutions. Interviews were conducted online by Harris Poll on behalf of Vormetric in September–October, 2014.

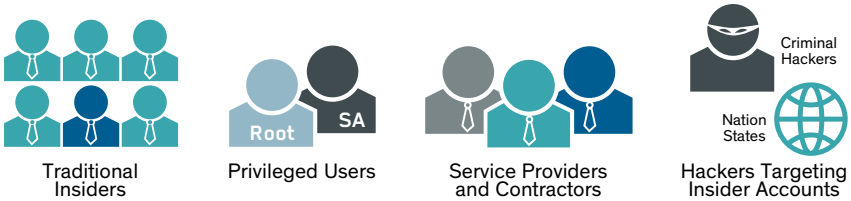
This version of the Insider Threat Report focuses on the increasing use of all forms of cloud technology, and provides information about the security and data protection issues that need to be addressed. Increased risk, the need to manage and protect more data, and a perceived lack of care from cloud service providers are seen as the key progress inhibitors.

Insider threat issues that cause particular concern in cloud and Big Data environments include having to deal with an increasing number of privileged users, including systems administrators who require access to corporate data systems when working on behalf of the cloud services provider. These systems administrator issues, as well as increasingly large volumes of data that need to be protected, are also relevant to Big Data solutions which are frequently implemented using cloud-based services.

*80% of enterprise organizations now make use of cloud-based services and infrastructure systems.**

"Customer organizations should demand high-end protection and strong rule-based security controls as a minimum requirement for doing business with cloud providers."

Where Do Insider Threats Come From?



Traditional Insiders | Privileged Users | Service Providers and Contractors | Hackers Targeting Insider Accounts

*Source Ovum ICT Enterprise Insights—Major Markets Technology Priorities, October 2013—a global study with 6,700 respondents

Ovum view

At a global level, the top three locations where company-sensitive data is stored, maintained, and therefore in need of enterprise-level protection are: databases, file servers, and now, because of the rapid adoption and growth, cloud service environments.

Ovum research shows that globally over 80% of enterprise organizations now make use of cloud-based services and infrastructure systems. The numbers continue to rise, as does the incidence of multiple cloud deployments and interest in Big Data initiatives.

Company-owned databases and file servers may still retain the top two slots when looking at where the bulk of enterprise data assets are stored, but if continued adoption levels are maintained in key global markets (for example, the U.S. and UK), it is only a matter of time before cloud is challenging for the number one position.

The growth in data protection requirements by volume and the consistent direction of travel away from internal application systems puts more pressure on cloud-based service providers to deal with the host of insider and external security threats that continue to inhibit further progress. This is especially the case in more conservative technology markets such as Germany and Japan and in highly regulated industries such as financial services, healthcare, and retail.

Enterprise security, data protection, access control, and compliance concerns are genuine and worrying. Customer organizations should demand high-end protection and strong rule-based security controls as a minimum requirement for doing business with cloud providers. Cloud and software-as-a-service (SaaS) providers need to step up to earn the trust of their enterprise clients and justify their presence in this lucrative market.

Key messages

- More than 80% of organizations use cloud and Big Data services, with 54% claiming to keep company-sensitive information in the cloud.
- Despite these significantly high numbers, further adoption in security-conscious markets including Japan and Germany continues to be constrained.
- Cloud environments at 40% now outstrip databases (38%) and file servers (29%) as the location perceived as being at greatest risk by enterprise organizations.
- Security and compliance concerns continue to inhibit progress, especially when cloud service providers are targeting highly regulated enterprise accounts.

DESPITE ONGOING SECURITY CONCERNS, CLOUD IS SET TO BECOME THE SINGLE MOST IMPORTANT ENTERPRISE OPERATING ENVIRONMENT

Cloud offers an all-encompassing range of services

The term “cloud services” provides an all-encompassing description of the cloud marketplace. For the purposes of the *2015 Vormetric Insider Threat Report*, it includes:

- Infrastructure as a service (IaaS), in which third-party service providers host virtualized computing resources over the Internet on behalf of their clients (software, servers, storage, and other infrastructure components).
- Platform as a service (PaaS), which enables service providers to deliver applications (apps) over the Internet and host a client’s hardware and software using their infrastructure.
- Software as a service (SaaS), in which selected applications are hosted by a service provider and delivered to their clients over the Internet.

Four out of five enterprise organizations already use cloud-based services and the numbers are growing

The top three operating environments, measured by volume of corporate data held, are internally managed databases (49%) then file servers (39%) and in third place, due to the rapid and continuing increases in adoption, is data held in the cloud (30%). At the same time, because of the large data volumes involved, Big Data initiatives (31%) are catching up fast.

In key global markets, particularly the U.S., cloud usage is likely to challenge and ultimately outstrip internally managed systems. Cloud and Big Data usage would undoubtedly be more extensive by now if all the major security challenges had been overcome and usage, access control, and data protection concerns had not held back progress.

Industry-wide numbers show that four out of five enterprise organizations make use of cloud-based services, often working with multiple cloud service providers while also making use of several mainstream SaaS-based services. What the high adoption numbers do not immediately highlight is that usage and multiple adoption rates would be even higher if the security and data protection concerns of business users had been taken more seriously at an earlier stage in the evolutionary lifecycle of the cloud.

To be clear, 80% of organizations make use of some form of cloud-based services, and often there are multiple deployments within each organization.* Of the 20% that say they choose not to make use of the cloud, there will be specific security-related industry, regulatory, and operational reasons why they have been forced to abstain.

"The safety and security of cloud environments is a key concern for enterprises across the globe. The results of this report highlight the need for addressing the risk of data breaches and compliance in the enterprise. The Rackspace managed cloud can provide enterprise customers with security best practices to help them implement appropriate security measures to protect their data."

John Engates
CTO of Rackspace

"CLOUD AND BIG DATA USAGE WOULD UNDOUBTEDLY BE MORE EXTENSIVE BY NOW IF ALL THE MAJOR SECURITY CHALLENGES HAD BEEN OVERCOME."

It is also the case that the global percentage that have chosen the cloud to host mission-critical applications drops down significantly to 54% when security and data protection concerns are taken into consideration. As shown in Figure 1, even that 54% average varies across the major markets. For example the U.S. appears to be more prepared to accept the risk of keeping company-sensitive data in the cloud, with 60% of organizations deploying cloud services that manage company-sensitive information. The percentage figure for the ASEAN region is also high at 56%—but, with everywhere else occupying the lower end of the scale with a mid-forties response, significant levels of reluctance remain.

*54%—The percentage of global organizations hosting **sensitive data** in the cloud.*

*Source Ovum ICT Enterprise Insights—Major Markets Technology Priorities, October 2013—a global study with 6,700 respondents

SaaS—83% of U.S. organizations are very or extremely concerned with SaaS cloud storage environments.

Germany has the highest level of perceived risk for sensitive data in cloud environments at 49% of respondents.

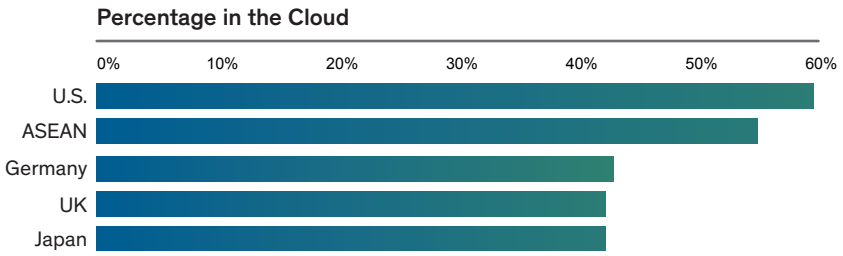


Figure 1: The percentage of organizations holding company-sensitive data in the cloud

Another way of looking at the risk factors linked to the use of cloud-based services when company-sensitive data is involved is to compare actual data usage with and the associated risk levels that senior business and IT managers associate with the cloud. Figure 2 provides a direct global comparison between the volumes of company-sensitive data held within each major operating environment against the perception of risk.

In doing so, it also shows that business and IT managers do not accept that all forms of cloud usage present the same levels of risk, hence the immediately identifiable spike that positions overall cloud usage as very unsafe and the lower levels of risk associated with cloud-based Big Data and SaaS usage.

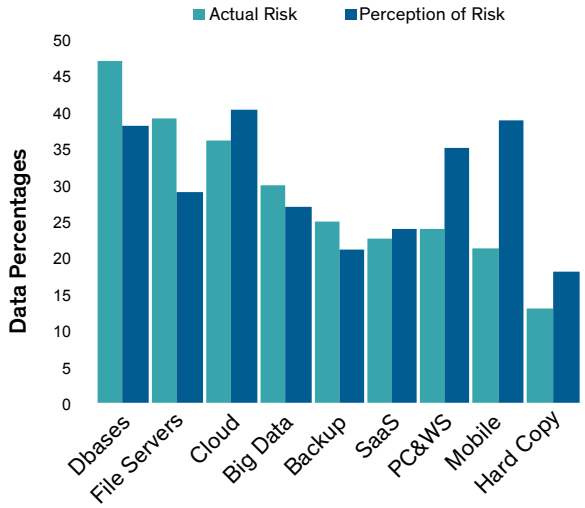


Figure 2: Data risk based on actual volumes of sensitive data stored in each location compared to the perception of risk

Databases and file servers are seen as presenting a risk factor that is significantly lower than the volume of corporate data they hold. This is a reasonable risk position to take because of the general levels of maturity these environments represent and the work that has been done to deploy and maintain security and data management tools.

Nevertheless, cloud, which not unreasonably is seen as a newer and far more risky area of the marketplace, continues to achieve significant growth. In many cases the increased usage involves company-sensitive data, and is being achieved despite a risk score that even exceeds that of ultra-high risk mobile device environments.

Another interesting fact that Figure 2 identifies is the difference in the overall profile of the cloud services model. The general cloud services position is shown as representing high usage and even higher risk, Big Data has lower usage and a comparatively lower risk profile, and SaaS applications are shown as maintaining an even usage and risk position.

SaaS represents an important component of the cloud services sector

SaaS provides the applications and software distribution infrastructure in which applications are hosted by a service provider and made available to clients via the Internet. Popular application services include project and task management and messaging systems, online office and accounting suites, customer relationship management (CRM), enterprise resource planning (ERP), cloud-based backup and storage facilities, and collaboration tools.

Across the cloud services environment there continue to be high levels of enterprise concern about security and data protection that extend across all major business operations. However, as shown in Figure 2, when choices have been made over the use of specific SaaS-based facilities, those services are seen by business decision-makers as being lower risk and having an approval rating that matches the requirements of the operation and the sensitivity of the data involved.

That said, there are specific areas of the SaaS delivery model that continue to cause significant levels of concern to business users. The global average shows that 72% of enterprise respondents are very or extremely concerned about cloud storage within the SaaS environment. That number goes up to 83% when focusing on U.S. organizations. Online backup (65%) and online accounting (65%) also see high levels of concern reported at the global level and increase to 80% and 79% respectively in the U.S. In fact across all elements of the SaaS application market, respondents from U.S. organizations express the highest levels of concern.

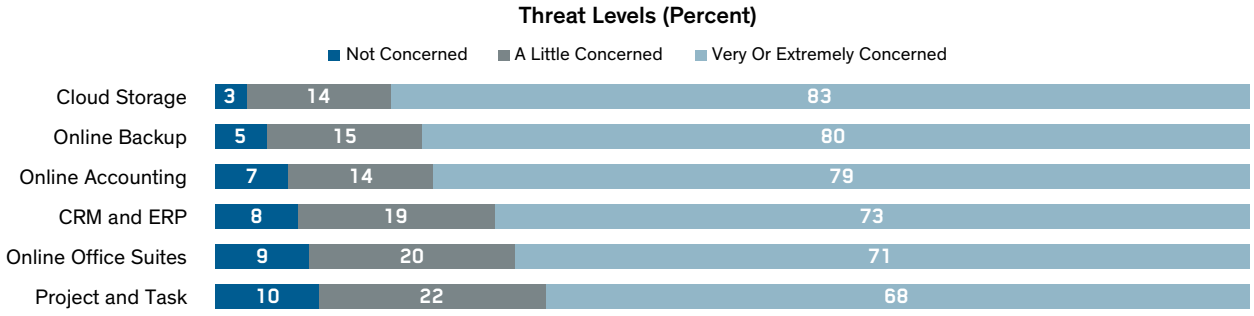


Figure 3: U.S. SaaS security concerns

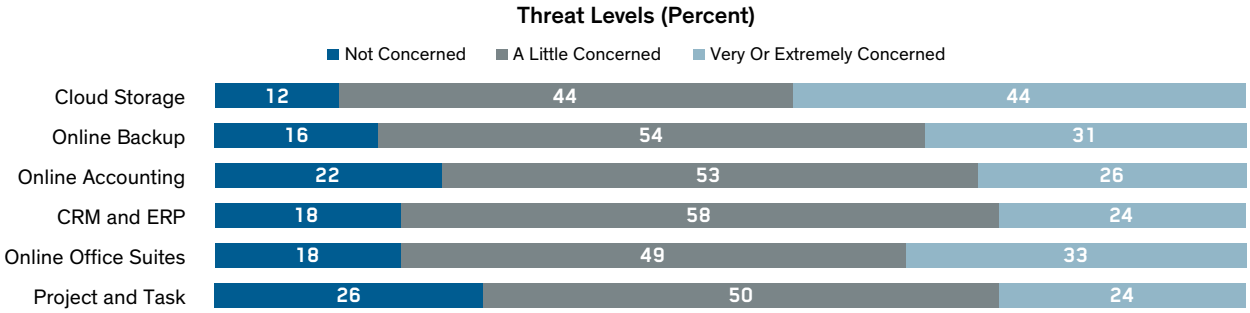


Figure 4: Japan SaaS security concerns

Data protection concerns vary between different markets and industry verticals

The levels of concern about cloud and Big Data operations and the SaaS-based applications used to support those operations vary across different global markets. Based on data volumes held, as highlighted in Figure 5, the markets that show the most concern and that rate the cloud as being the greatest risk to the protection of sensitive data are the U.S. (46%) and Germany (49%). These figures were above the global average, but also highlighted a difference in attitudes between how market dynamics are operating.

Big Data—Low adoption corresponds with low risk perceptions by respondents. Japan—10%.

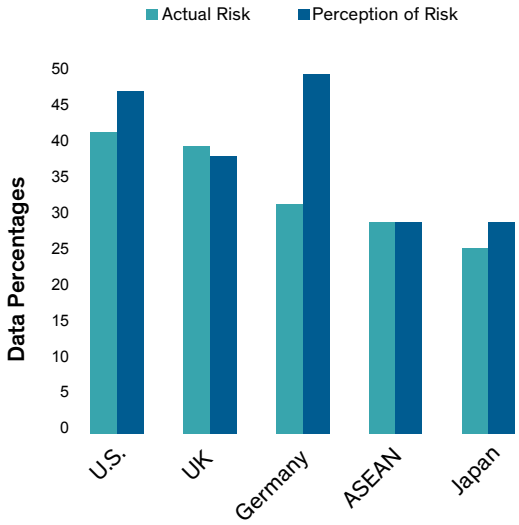


Figure 5: Cloud security, the actual and perceived risks when company-sensitive data is involved—global, regional and country-wide markets

The U.S. has high levels of cloud usage, and forward-looking statistics show that adoption rates will remain higher than the global average. Yet 46% continue to express concern about the market pressures that are forcing them to use cloud services.

In Germany, meanwhile, the adoption rates for cloud services when storing company-sensitive and regulated data are lower, but the levels of concern remain even higher than in the U.S. In fact, at 49% it is higher than in any other developed market, and close to double that of Japan. Significantly, the impact this is having in Germany is very different from that of the U.S. Two thirds of companies in Germany (66%) stated that they have no plans to increase their use of cloud services in the near future because of security and data protection concerns.

Big Data projects also raise security concerns

The U.S. and countries within the ASEAN region report the highest levels of concern when issues of protecting sensitive data in Big Data environments come into play. At the lower end of the scale Japan and Germany report that they see the lowest levels of risk.

Even though Big Data projects regularly rely on the cloud-based service delivery model to support typically high processing and data usage overheads, a lack of advancement and lower usage levels continue to soften the all-round perception of risk.

The survey findings in Figure 6 show that the adoption of Big Data projects within all regions have a direct correlation between usage and perception of risk. Across all regions, the perception of risk reported by survey respondents was slightly but consistently lower than the real risk based on the actual volumes of company-sensitive data held.

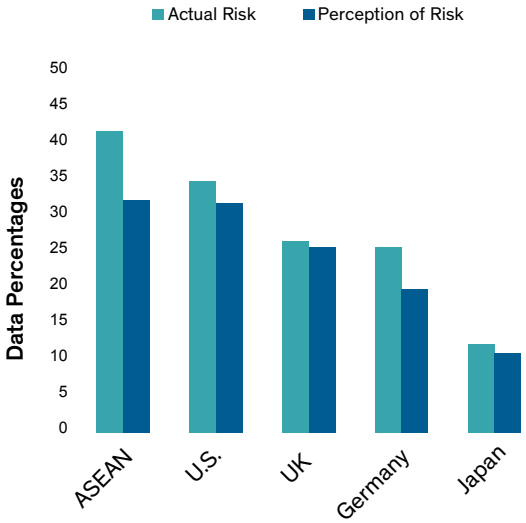


Figure 6: Big Data security concerns

Therefore, for specific markets that express lower levels of concern over Big Data issues such as Japan and Germany, the lower adoption levels help to explain their position.

CLOUD SECURITY ISSUES ARE AT THE TOP OF THE SENIOR MANAGEMENT AGENDA

Data sensitivity has a significant impact across all major business domains

Data security, and in particular the protection of company-sensitive information, is the number one priority for enterprise organizations. This level of prioritization exists because of the explosion in the amount of data that needs to be protected, and the volumes of data now being held and maintained in cloud-based environments. Also, there are additional, cloud-specific, data loss and theft concerns that relate to integral systems management and control services that now need to be maintained away from the control of corporate IT.

Essentially cloud and Big Data issues are about the need to protect more data assets, the distributed nature of those assets, and the growing number of users who are likely to need access. This position posed few surprises to any of the senior business and IT managers interviewed. Figure 7 shows that cloud environments, with 40%, came top of the list when respondents were asked which data storage locations put the enterprise at the greatest risk for loss of sensitive data.

However, despite the risk to business that cloud represents, 40% of survey respondents said that their cloud service operations were used to manage, store, and maintain company-sensitive information and regulated data. There was also a continuity of growth over the coming year because the global average figure for future planned initiatives where cloud and the management of sensitive data would be combined as part of the overall requirement was 52%.

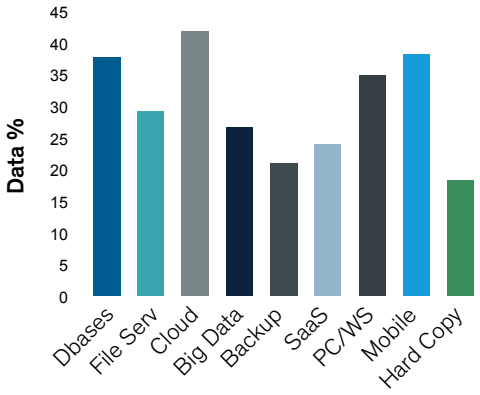


Figure 7: The perception of risk when comparing cloud to other mainstream operations

Although these numbers do not directly relate back to the four out of every five enterprise organizations that currently make use of cloud-based services (because the 80% figure includes all forms of cloud usage*), they are interesting because they focus on organizations that appear to be reasonably content to store company-sensitive data in cloud environments.

This is a relevant issue because the company-sensitive data that needs to be protected in cloud environments is likely to include critical intellectual property, data that is subject to national or international privacy regulations, data that should be protected under industry rules and standards, and data that if it were to be disclosed could cause harm to the organization.

As previously discussed, the high-cloud usage numbers show that the vast majority of enterprise organizations have taken up the cloud opportunity. They also confirm that despite very real security and data protection concerns, organizations continue to make extensive use of cloud-based services.

*Source Ovum ICT Enterprise Insights—Major Markets Technology Priorities, October 2013—a global study with 6,700 respondents

The general direction of travel continues to be towards the cloud, with many public and private sector organizations adopting a "cloud first" strategy. However, this approach tends to be more prominent when new systems initiatives and the deployment of new services are involved. For existing mainframe and server-based implementations, unless strong operational motivations exist, the switch to cloud-based alternatives is happening far more slowly because data protection reservations remain.

"…despite the risk to business that cloud represents, 54% of survey respondents said that their cloud service operations were used to manage, store, and maintain company sensitive information and regulated data."

Security implementations and controls have to be right, or enterprise adoption will stall

The enterprise focus continues to be on the unerring direction of travel towards the use of cloud-based services. Nevertheless, enterprise clients say that adoption levels would be even higher and involve more key enterprise applications if the service providers did more to assail their fears on security, data protection, and data management issues.

Therefore, if they are determined to win more enterprise business, cloud service providers (CSPs) need to take their clients far more seriously when they ask for better protection and more visibility into security and data management matters.

This is an issue that CSPs have to come to terms with. Some are better placed than others, but as an industry the position is very mixed. Some providers are already promoting their "baked in" security protection and management services. Others are still dabbling while building their strategies and are not ready to address the major security and data protection issues that worry the enterprise.

In our opinion, many within the CSP community would benefit from working more closely with specialist security providers to improve their situations. Otherwise, the security concerns highlighted in Figure 8 will continue to be a major stumbling block when organizations make their decisions on which cloud service provider they are prepared to do business with.

THE TOP THREE CONCERNS FOR DATA WITHIN CLOUD ENVIRONMENTS:

- *Privileged user control (94%)*
- *Insider Threat and APT activity (93%)*
- *Concerns over shared infrastructure (92%)*

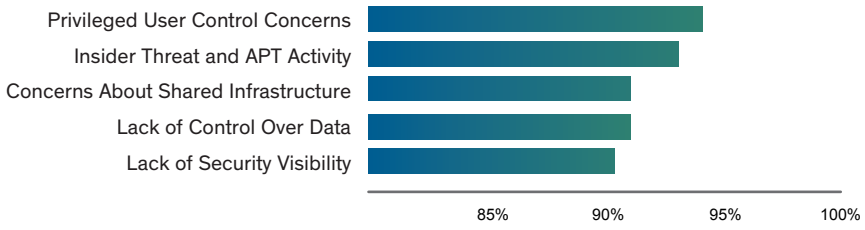


Figure 8: Operational concerns that extend across the cloud services spectrum

As Figure 8 shows, the specific cloud security concerns that were raised by senior business and IT managers are extensive and worry a very high percentage of enterprise clients.

At the top of the list, 94% of survey respondents had serious operational concerns about privileged user abuse (system, cloud, storage, and virtualization administrators) and additional risk caused by employees of the cloud provider. There were similar levels of concern about potential vulnerabilities caused by insider or advanced persistent threat activity (APT) within the service provider domain, raised vulnerabilities from shared infrastructure, and lack of control over the location of data that the service provider may be holding outside acceptable borders.

Of the 94% of senior business and IT managers who said they were worried about privileged user abuse by the cloud service provider's own systems admin staff, 67% said they were very or extremely concerned and significantly only 6% said they were not at all worried.

Very similar results were found across the other top security response categories. For example, 66% said they were very or extremely concerned about APTs and the penetration of their data while under the care of a service provider; only 7% were not at all worried.

About two thirds reported that they were very or extremely concerned about increased security vulnerabilities emanating from the use of shared infrastructure and from the lack of control over the location of sensitive data and associated across border, data-control issues. In both cases only 8% said they were not worried and were satisfied that their services providers had addressed their data protection and compliance concerns.

Collectively, although very high, these results were only slightly above all the other data protection, access control, and malware management concerns that enterprise clients have about the cloud and cloud services in general. There are also major concerns over the lack of openness and visibility into the security measures that CSPs put in place and how they are being operated on behalf of business users.

Worries were also expressed about data custodianship. These included issues of ownership around encryption key management, lack of data privacy policies and privacy commitments. Although it didn't achieve the levels of prominence that it had in the previous years, failure to address compliance issues remained a concern.

In summary, when senior business and IT managers were asked about the issues they have when cloud services are being used, all the usual in-house security and data protection issues were raised, and then more were added as all things to do with the service providers and their staff were discussed.

The U.S. has more cloud related issues than any other region

The U.S. and its enterprise business users have more cloud-related concerns than any other region. This is understandable because the adoption of cloud-based services to store sensitive company information within the U.S. (60%) outstrips other markets, often by a significant margin.

Japan represents the other end of the spectrum. Its support for cloud services is very low when compared to the global average and in particular to the U.S. market position. Survey results show that Japan has the highest percentage of users that currently place no sensitive data in the cloud (17%). The percentage of Japanese respondents that report no plans to expand their use of cloud services in the next year is also high, at 36%. As a direct consequence, Japanese business users express fewer concerns about the data they actually choose to hold in the cloud.

Mature cloud markets are driving further adoption but others are beginning to stall

The global average for cloud usage among enterprise organizations where sensitive and regulated data is involved is 53%. The future figure for the use of cloud locations for the storage and maintenance of sensitive data during the next 12 months is expected to be 52%, which maintains but does not increase the current position.

The numbers are reasonably consistent across all three main areas of cloud usage—IaaS, PaaS, and SaaS. However, with a current global usage level of 60%, SaaS—despite the areas of concern already expressed in this report—is the cloud component that enjoys the highest adoption rates. It achieves wider support in the U.S. than in the rest of the world and, within the U.S., the financial services sector sees the greatest levels of SaaS usage, with 72% of financial services organizations reporting that sensitive data is already deployed within SaaS-based operations.

At the other end of the scale Japan has the highest percentage of users that place no sensitive data in the cloud (17%). Their SaaS adoption rate is 19 points below the U.S. at 47%. But even more worryingly for the cloud sector, expected usage rates for the next year show a decline of 15 points down to 32%.

"The Cloud Security Alliance is dedicated to helping organizations make safe use of cloud computing environments. The report clearly illustrates that organizations still feel at risk from their cloud and SaaS implementations, illustrating the need for education and best practices that enable them to safely benefit from their cloud-based resources."

Jim Reavis
CEO Cloud Security Alliance

Generally, the reported global figures for IaaS, PaaS, and SaaS growth rates, where the use of sensitive data is involved, look steady, but are expected to tail off by a couple of points over the next 12 months. Nevertheless, it is the outperforming U.S. market that is chiefly responsible for sustaining current adoption rates, with strong support from its financial services, healthcare, and retail markets.

The detailed IaaS, PaaS, and SaaS usage numbers are shown in Figure 9.

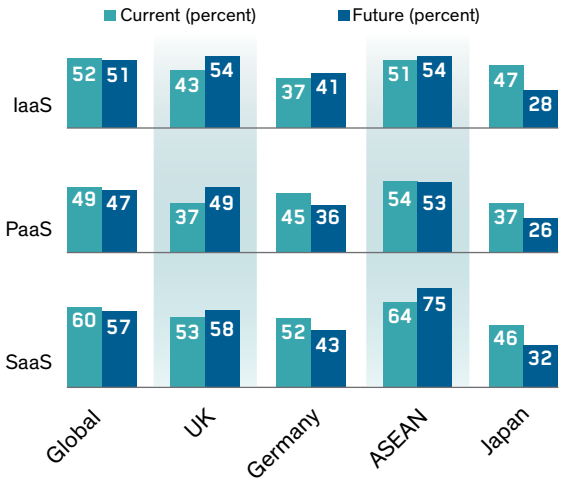


Figure 9: Detailed IaaS, PaaS, and SaaS usage statistics where sensitive company information is being stored

Apart from the U.S., which is currently positioned as the market with the highest percentage of cloud users, the survey response figures show adoption figures that both encourage and disappoint. The emerging markets of the ASEAN region—Indonesia, Malaysia, the Philippines, Singapore, and Thailand—start out with lower cloud adoption numbers than the U.S. and slightly above the global average, but when next year's expectations are taken into account ASEAN at 75% for SaaS is likely to outperform the U.S.

The UK, albeit starting from a far lower base, is the only market that is expected to see increases in cloud adoption rates across all three major sectors—IaaS 43% up to 54%, PaaS 37% up to 49%, and SaaS 53% up to 58%. This also makes the UK one of only a few markets where data stored in the cloud is likely to exceed that of the server market in the near future.

The two major markets that are likely to see a decline in cloud adoption where sensitive data is involved over the next year are Japan and Germany. The projected figures for Japan see reduced adoption across the three cloud sectors—IaaS down from 47% to 28%, PaaS down from 37% to 26%, and SaaS down from 47% to 32%. Germany, however, is down in two and up in one—PaaS down from 45% to 36% and SaaS down from 52% to 43%; IaaS is up from 37% to 41%.

JAPAN AND THE U.S. AT OPPOSITE POLES FOR STORING SENSITIVE DATA IN SAAS ENVIRONMENTS:

- *U.S. 62%*
- *Japan 32%*

This leaves a mixed picture of the cloud services market when company-sensitive data is involved. It shows a global market that is stalling at just over the 50% usage mark, figures that are bolstered by the U.S. and its financial services, healthcare, and retail verticals. It is also receiving increasing interest from the UK as its cloud adoption levels increase and from ASEAN as future interest in the SaaS model exceeds that of all other markets. On the downside, the mature technology markets of Japan and Germany are expressing their concern over cloud security issues by projecting a reduced level of usage over the next 12 months.

The top improvement that would increase adoption of cloud by respondents—Encryption with enterprise control of their keys (55% on their premise—52% at the cloud provider).

Cloud providers need to step up to improve enterprise adoption

To improve the existing levels of cloud adoption, and to take their businesses to the next level, more needs to be done to make the environment more secure and enterprise safe. The specific improvements that senior business and IT managers want to see and believe would improve their appetite for cloud usage is data and security management focused. As shown in Figure 10, they include the widespread use of data encryption and key management across cloud hosted infrastructures. This comes with the popular rider that the management of encryption keys would be better controlled within the enterprise and that without local key management being vested in the enterprise the value of encryption protection is reduced.

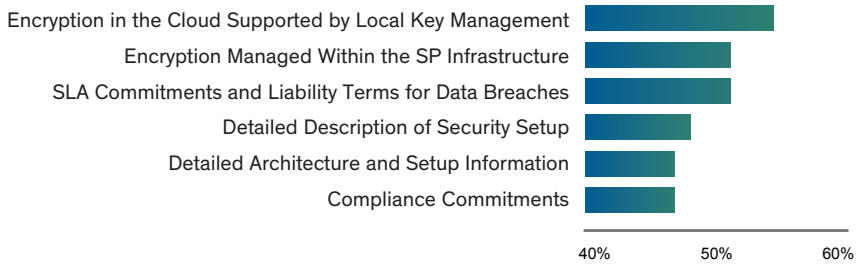


Figure 10: Improvements that are needed to increase adoption of cloud services

Then contractual and SLA issues come into play with the requirement for more visibility and control over service-level commitments and the recognition of liability when data breaches occur. Capabilities, with regards to the delivery of security and security management services, are currently mixed across the cloud provider market. Therefore enterprise clients need to be proactive in forcing the issues. Expectations should be higher; the situation will only improve if enterprise organizations demand security and data protection capabilities from their cloud provider. If they cannot or will not deliver it, there are two choices: buy the services in and bring them along with you, or select a new cloud partner.

*"ASEAN holds more company sensitive data within Big Data environments than any other region"—**41%.***

BIG DATA PROJECTS RAISE DATA MANAGEMENT AND SECURITY CONCERNS

The increased profile of Big Data projects puts security, access control, and data protection on the senior management agenda

The risk factors associated with Big Data projects are wide ranging. In effect there are double jeopardy issues insofar as most Big Data operations are delivered using cloud-based services. Most of the security concerns mentioned in the previous section apply to the use of Big Data facilities. There is a big overlap between Big Data and cloud. Therefore everything to do with remote storage, third-party management, large data volumes, and company-sensitive data protection also applies to Big Data projects.

From an operational perspective it makes perfect sense to do Big Data in the cloud because of the efficiencies and scalability that cloud brings to the table. In particular cloud-based approaches are used because of the Big Data imperative to process, maintain, and store large volumes of data, and from the hardware support position to allow new servers to be spun up and brought online quickly to support high-volume data interrogation and analysis projects.

It should also be recognized that a fair proportion of the data involved is going to be of a classified and company-sensitive nature, which adds to the senior management pain levels as sensitive data may be distributed across Big Data repositories, and these are likely to be run off-premise using the cheapest and fastest service delivery options available.

ASEAN holds more company-sensitive data within Big Data environments than any other region. The adoption rate numbers of respondents from that region that claim to hold company-sensitive data within Big Data operations is 45% and far outweighs that of any other region. Conversely nearest neighbor Japan only has a 12% response and adoption rate on Big Data projects.

Nevertheless, the Big Data security concerns expressed by senior business and IT managers highlighted in Figure 11 make this more than just a data management issue. Moving large volumes of sensitive data to and from cloud environments is operationally time- and bandwidth-intensive. Terabytes through to petabytes of data can be involved. This also puts up bigger operational barriers that go beyond just bringing up new servers when needed and then terminating them once the operation is complete. It involves very large volumes of data, remote storage, third-party management, and access control issues.

"59% of U.S. survey respondents identified privileged users as the biggest threat to their organizations. Failure to adequately handle security requirements, especially around mission critical applications, places an enterprise at significant risk, exposing sensitive data to possible data breaches. With Big Data security at the top of every CIO agenda, every NoSQL deployment should protect sensitive data access for interactive, operational applications."

Ravi Mayuram
SVP Couchbase Engineering

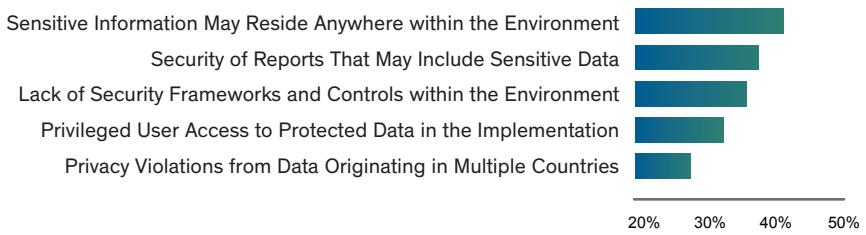


Figure 11: Big Data usage, security, and data protection concerns

There is nothing new behind the principles of gaining business insight into large data sets that drive the current generation of Big Data initiatives. Interest is being driven by the combined inclusion of structured and unstructured data into the analyses. The Big Data technology approach provides analysis from all types of data and produces actionable insight and business information that is targeted at specific projects and business requirements. It involves an information-inclusive approach and is the main reason why usage will continue to increase in the short to medium term.

*Japan with low adoptions rates for Big Data, also has low sensitive data deployments—**12%.***

Big Data projects suffer from serious data protection issues; regional figures highlight further concerns

Big Data initiatives are used to help organizations analyze and extract business intelligence from huge volumes of data. Such projects have significant usage and processing overheads as well as the requirement to keep sensitive data safe. The distributed nature of Big Data environments is a continuing issue that was first brought up in the *2014 Vormetric Insider Threat Survey*. As highlighted in Figure 11 globally and locally it remains the number one concern for organizations that are running analytically based Big Data projects.

The prospect of data residing across geographic boundaries and being drawn in from all available resources makes managers with data responsibility nervous. Hence, the top levels of concern at 41% from the global analysis. It is also worth noting that the U.S. data residency concern level is 44% and that the European response has both the highest (UK 45%) and the lowest (Germany 34%) numbers. See Figure 12.

The Biggest Big Data Concern?—Sensitive data may reside anywhere within the environment.

DATA RESIDENCY CONCERNS FOR BIG DATA ARE HIGH—VARYING FROM 34% (GERMANY AND JAPAN) TO 45% (UK).

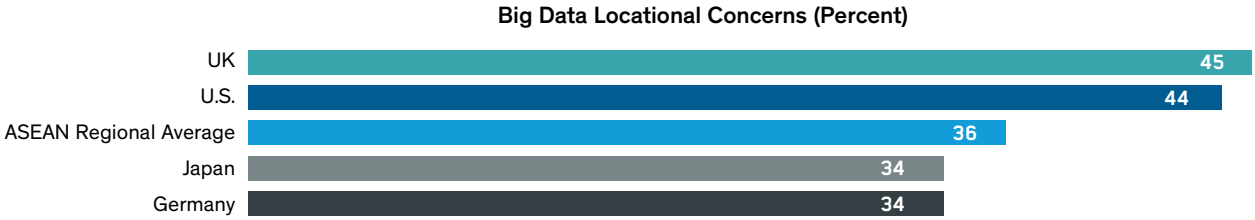


Figure 12: Data residency issues and concerns, showing variations by geography and markets

MANAGEMENT SUMMARY AND RECOMMENDATIONS FOR ENTERPRISES

Cloud and Big Data usage would undoubtedly be more extensive if all the major security challenges had been overcome and usage, access control, and data protection concerns had not held back progress. Enterprise organizations need better protection when using cloud-based services and should be demanding it from their cloud service providers.

Data protection concerns (or to be more accurate lack of data protection) is the major reason why two thirds of senior business and IT managers see the cloud as a worrying, unsafe, and uncontrolled environment. Cloud service providers need to step up to the plate and take more responsibility for security and data protection.

To improve the existing levels of cloud adoption, more work needs to be done by cloud service providers to make the operational infrastructure safer, the environment more secure, and keep enterprise users safe.

Specific security improvements to cloud services environments that senior business and IT managers should be looking for include:

- Better and more inclusive use of data protection and data encryption services
- Key management that remains under the control of the enterprise client
- More visibility into the security facilities that the service provider has available
- More say in how security services are tailored to meet the needs of the organization
- More insight and control over what happens if a data breach occurs

To improve their security services and achieve these objectives, while addressing insider as well as external and third-party threat activity, cloud service providers must be prepared to work more closely with the security industry. They must make better decisions on the data protection tools, security and information management services, and the provision of analysis and reporting facilities that need to be deployed to address quality of service and security issues.

The most effective way to achieve this is to position security at the forefront of cloud and Big Data strategies. Security issues and a lack of trust continue to hold back cloud adoption. Therefore, cloud providers that can meet enterprise security requirements should benefit from the increased adoption of their services, and those that don't should expect to see future opportunities limited to mundane low-risk projects.

TOP 5 CHANGES TO INCREASE ENTERPRISE CLOUD ADOPTION:

- *Additional data protection services*
- *Encryption with enterprise customer key management*
- *Increased security stance visibility*
- *Tailored security service options*
- *Explicit Data Breach commitments*

ANALYST PROFILE–ANDREW KELLETT, PRINCIPAL ANALYST SOFTWARE–IT SOLUTIONS, OVUM

Andrew enjoys the challenge of working with state-of-the-art technology. As lead analyst in the Ovum IT security team, he has the opportunity to evaluate, provide opinion, and drive the Ovum security agenda, including its focus on the latest security trends. He is responsible for research on the key technologies used to protect public and private sector organizations, their operational systems, and their users. The role provides a balanced opportunity to promote the need for good business protection and, at the same time, to research the latest threat approaches.

Author
Andrew Kellett
Principal Analyst Software
IT Solutions, Ovum
andrew.kellett@ovum.com

HARRIS POLL–SOURCE/METHODOLOGY

Vormetric's 2015 Insider Threat Report was conducted online by Harris Poll on behalf of Vormetric from September 22-October 16, 2014, among 818 adults ages 18 and older, who work full-time as an IT professional in a company and have at least a major influence in decision making for IT. In the U.S., 408 ITDMs were surveyed among companies with at least $200 million in revenue with 102 from the health care industries, 102 from financial industries, 102 from retail industries and 102 from other industries. Roughly 100 ITDMs were interviewed in the UK (103), Germany (102), Japan (102), and ASEAN (103) from companies that have at least $100 million in revenue. ASEAN countries were defined as Singapore, Malaysia, Indonesia, Thailand, and the Philippines. This online survey is not based on a probability sample and therefore no estimate of theoretical sampling error can be calculated.

ABOUT VORMETRIC

Vormetric (@Vormetric) is the industry leader in data security solutions that protects data-at-rest across physical, Big Data and cloud environments. Vormetric helps over 1500 customers, including 17 of the Fortune 30, to meet compliance requirements and protect what matters—their sensitive data—from both internal and external threats. The company's scalable Vormetric Data Security Platform protects any file, any database and any application's data—anywhere it resides—with a high performance, market-leading solution set.

FURTHER READING

To read the *2015 Vormetric Insider Threat Report—Global Edition*, please visit www.vormetric.com/InsiderThreat/2015.

2015 **VORMETRIC** INSIDER THREAT REPORT—*CLOUD AND BIG DATA EDITION*

Vormetric.com/InsiderThreat/2015

Vormetric
Data Security™