Research Conducted by harris poll

Research Analyzed by OVUM

2015 VORMETRIC INSIDER THREAT REPORT

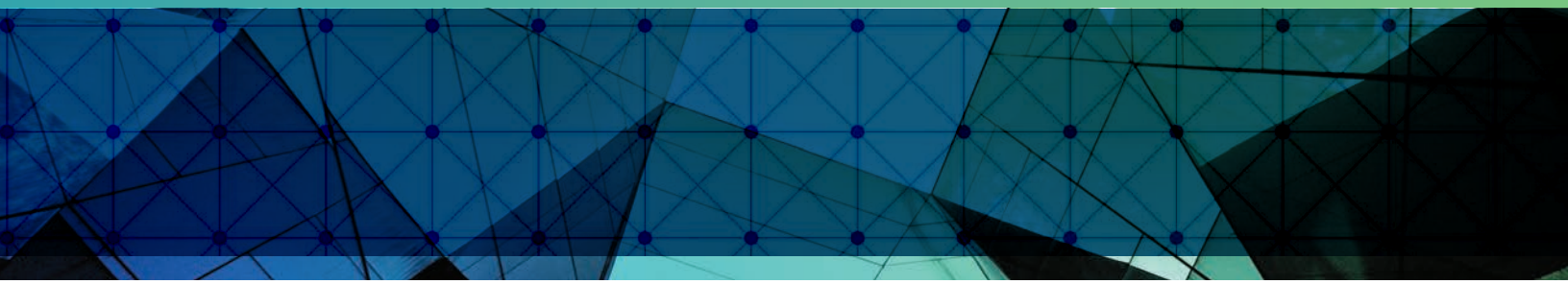
Trends and Future Directions in Data Security

GLOBAL 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

EXECUTIVE SUMMARY

Catalyst

Insider attacks on corporate data and the resultant losses to affected businesses have been relentless during the last 12 months. The negative effect on the victims, often well-known organizations, makes recovery difficult and the impact long-lasting.

The global edition of the *2015 Vormetric Insider Threat Report* provides present-day insight and opinion into the host of data breach threats that enterprise organizations face on a daily basis. The report is based on survey responses from 800 senior business managers and IT professionals in major global markets. Their views on the changes that are needed to keep business systems safe are insightful, as are their opinions on the types of user that put key business information assets at most risk.

Insider threats are caused by a wide range of offenders who either maliciously or accidentally do things that put an organization and its data at risk. The insider threat landscape is becoming more difficult to deal with as the range of miscreants moves beyond employees and privileged IT staff. It now includes outsiders who have stolen valid user credentials; business partners, suppliers, and contractors with inappropriate access rights; and third-party service providers with excessive admin privileges. Unless properly controlled, all of these groups have the opportunity to reach inside corporate networks and steal unprotected data.

INSIDER THREATS:

- *Traditional Insiders—Employees, Management, IT, Contractors*
- *Outsider Compromise of Insider Credentials*

Overview

Results from the *2015 Vormetric Insider Threat Report* show that insider threat awareness levels have increased. Only 11% of respondents felt that their organization was not vulnerable to insider attacks and a very large percentage (93%) were looking to increase or maintain existing spending on IT security and data protection in the coming year. Nevertheless, on several important areas of data protection, threat perception and actual levels of risk were not well aligned, and Ovum as the author of this report recognizes that urgent action is needed if genuine improvements are to be made.

From an overall security perspective it was good to see that a high proportion of organizations were looking to increase or at least maintain their security spending levels in their attempt to protect themselves against insider threat

40% of organizations experienced a data breach or failed a compliance audit in the last year.

89% feel vulnerable to insider attacks.

activity. Less understandable was the logic behind some of the scattergun approaches to how hard-won data protection budgets would be spent and the deliberations on where the corporate data that is most at risk actually resides.

Business obsession with mobile devices and the culture of bring your own device (BYOD) skew the perception of risk further. By comparison to the large enterprise data stores, the volumes of company-sensitive data held on mobile devices is relatively small. Nevertheless, we don't believe that the issues that are playing out here are really about comparative data volumes. Mobile data protection concerns are more about the existing lack of control over mobile devices that enterprises have, how those devices are being used, and importantly not knowing what company-sensitive data may have been copied to them. In our opinion, most of these usage and data protection issues could be addressed through improved data monitoring and increasing data protection through the use of encryption.

Implementing best practices, reputation and brand protection, and then compliance were the top three reasons why organizations were looking to do and spend more to protect their important data assets from insider activity. They are all reasonable objectives. Nevertheless, it continues to be the case that compliant organizations still suffer security breaches, and an organization's reputation and brand image will only remain untarnished for as long as the data protection actions it takes maintain a safe-haven status for customer- and business-sensitive data.

Summary of findings

- Globally 89% of respondents felt that their organization was now more at risk from an insider attack; 34% felt very or extremely vulnerable.
- When asked about who posed the biggest internal threat to corporate data, a massive 55% of respondents said privileged users, nine percentage points behind on 46% were contractors and service providers, and then business partners at 43%.
- Databases, file servers, and the cloud hold the vast bulk of sensitive data assets, but for many mobile is perceived as a high-risk area of concern.

"34% (OF RESPONDENTS) FELT VERY OR EXTREMELY VULNERABLE."

INSIDER THREATS AND THE HIDDEN RISKS WITHIN YOUR ORGANIZATION

The threats are real and need to be addressed

The last 12 months have seen a continuous catalog of loss and data theft as organizations across all major markets and industry verticals have had to admit their security and data protection shortcomings. The effect of insider threats and the continuing legacy of targeted breaches at Home Depot, JP Morgan, Target, Vodafone, Sony, and many others determine that fixing the problem has moved beyond the sole responsibility of IT.

"For business leaders the current data protection position is rapidly becoming untenable."

The Target ramifications continue and for Home Depot, the world's largest home improvement retailer, investigations into its more recent payment systems breach are ongoing. The impact on brand and reputation and associated legal ramifications for all of these high-profile organizations are likely to be so damaging that senior management and board-level executives will be obliged to take responsibility. In the case of the Target breach this has already happened, with the CEO paying the ultimate price and having to resign.

For business leaders the current data protection position is rapidly becoming untenable. Most readily acknowledge that increased spending on security is unavoidable, but few seem to have a clear vision over where and on what types of protection their security budgets should be invested. Ovum research shows that security spending increases during 2014 have once again exceeded the 10% mark, and our projections suggest that 2015 will see similar levels of double-digit growth. The main problem that is emerging is not so much about the amount being spent, but more about the lack of focus and the need to target spending on areas that will control access and protect data and in so doing make a real difference to business and data protection.

"...few seem to have a clear vision over where and on what types of protection their security budgets should be invested."

The most dangerous insiders have privileged access

For far too long systems administrators and business users with privileged access to the most sensitive corporate data have had open access, with few controls placed on their rights of entry. Even today only half of all business organizations have deployed privileged access/identity management (PAM or PIM) technology. But what has changed, and is clearly reflected in the Insider Threat Report survey results, is that senior management concerns over privileged user access have reached the top of their security agendas.

They now understand the damage that a rogue user with admin rights can do, and they recognize that if this type of user is not properly monitored and controlled the damage to the business can be far-reaching. Also, if a privileged user's credentials are acquired by an external attacker, as US investigators say was the case when a hacker stole the credentials of a system administrator at Sony and orchestrated the recent high-profile data breach, the opportunity to gain free access to key information repositories or deploy malware is likely to be extensive. As shown in Figure 1, at 55% the *2015 Vormetric Insider Threat Report* positions the privileged user risk group a massive 9 percentage points above the next highest category, which unsurprisingly given the notoriety of Edward Snowden and the uproar following the Target and more recently the Home Depot breach is a group

"… at 55% the 2015 Insider Threat Report positions the privileged user risk group a massive 10 percentage points above the next highest category."

consisting of third-party contractors and service providers (46%). In third place and not far behind were business partners who have access to company networks (43%).

In our opinion the top three priority sequence is correct, but other areas of the report highlight that more work needs to be done to ensure that the insider access rights these groups have are properly monitored and better controlled.

At the same time, insider access controls for other high-risk groups should not be ignored. The survey results suggest that other IT staff, many of whom have all the skills required to instigate an insider attack, are to a large extent being overlooked. A similar argument can be made for maintaining additional access and monitoring controls over highly skilled senior managers and executives who often have unfettered access to the organization's most sensitive data.

Ovum recommends that all user groups with internal access to business systems should be monitored and the access to corporate data they have should be appropriate and no more than they need to fulfil their specific roles. Currently only 58% of organizations have technology in place that allows them to control privileged users and only 56% monitor and audit privileged user activities, so more still needs to be done.

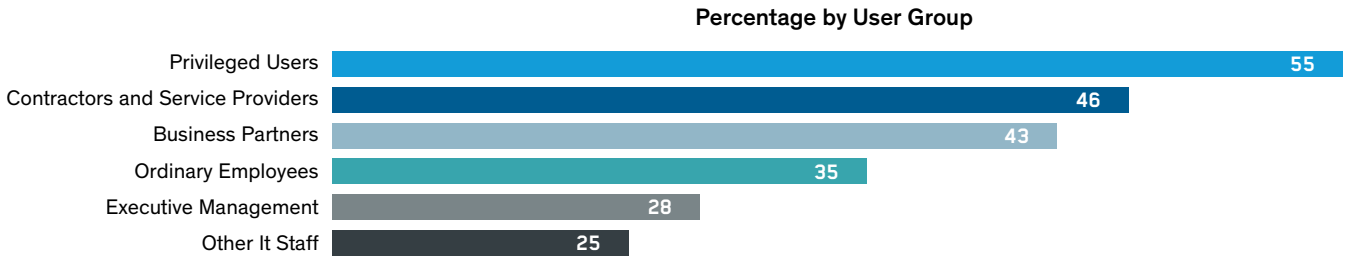


Figure 1: The global position for insiders who pose the largest risk to an organization

Globally, concerns about insider threats continue to grow

The number and size of insider breaches continues to rise year on year. But realistically, outside of the US where almost all data breaches have to be reported and acted upon, the numbers represent only a proportion of the breaches that often remain unreported or have taken place and not yet been identified.

Average breach detection timescales are still measured in months; the published numbers may at last be dropping down towards the 200 day mark. But, given that the breach-detection timescales are still far too high, it is not surprising to find that almost nine out of ten senior management respondents to the survey (89%) felt their organizations were vulnerable to an insider attack. Some 33%, one third of all respondents, said they felt their organizations were very or extremely vulnerable.

These are the global average findings and as the diagram shows there are regional differences. US and UK organizations felt most at risk, yet in other countries with similar risk profiles, their senior executives don't feel quite as concerned. For example, German organizations have the highest respondent numbers that do not feel at risk from insider threats and the lowest levels that felt vulnerable.

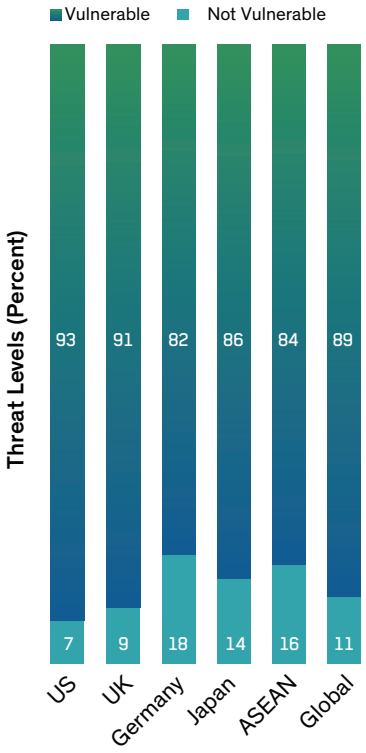


Figure 2: Vulnerability of organizations to insider threats

The global average shows 89% of organizations as being vulnerable and only 11% reporting that their organizations were safe. These figures confirm that most organizations are concerned about the impact of insider threats and overall do not feel that they are in control of the situation.

Only 11% report that their organizations are safe from insider threats.

TOP 3 LOCATIONS WHERE DATA IS AT RISK IN VOLUME:

- *Databases (47%)*
- *File Servers (39%)*
- *Cloud (37%)*

Corporate servers and databases pose the highest risk, yet spending remains stubbornly focused on endpoint and mobile

The top three locations by volume where company-sensitive data is stored and must be protected are: databases (47%), file servers (39%), and the rapid growth area for cloud service environments (37%). The position is fairly consistent across most major geographies and mainstream verticals including financial services, healthcare, and the retail sector.

Along with the ubiquitous use of databases and servers, cloud and more recently big data take-up levels now force a stronger protection case to be made. Growing data volumes, when put alongside worries about a lack of control over third-party access; the use of third-party admins; and data locational issues when foreign intervention and legal sovereignty come into play, make the case for improving cloud-services data protection. Also, as more data needs to transition between on-premise systems and cloud and big data environments, organizations need to make use of more inclusive data protection facilities to control and protect their data as it moves between corporate systems.

Another discussion that should take place revolves around the perception of risk that mobile devices and user mobility bring to the table. By comparison only 20% of sensitive company data is held on mobile devices and, of that 20%, a large proportion is being held on company-owned laptops and other company-protected mobile devices. In our opinion the discussion isn't really about the data volumes involved, and if it were, 20% is still significant enough to cause anxiety. But the real concern for the 70% of business managers who were worried about mobile device protection is firmly about the lack of control over the mobile devices that are in use. It is also about not having enough information to know what data has been copied to those devices and not having the controls in place to stop copies of company-sensitive data being made.

Good quality monitoring and access control technology provide part of the answer. Irrespective of where the data is being held, it is important to know and be able to control who gets access and what they can do with that access. This provides the ability to highlight and report on misuse

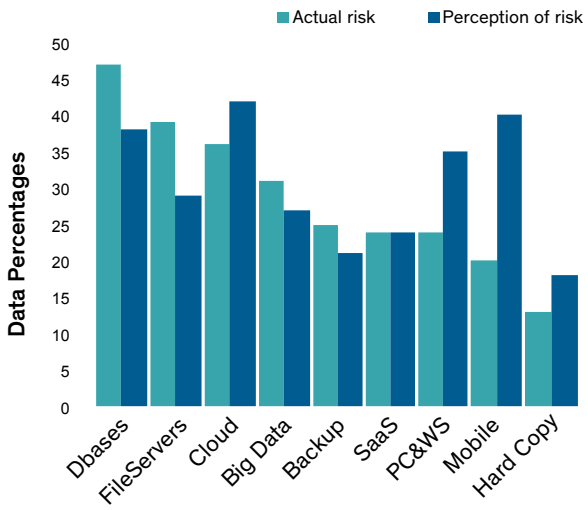


Figure 3: Data risks based on actual volumes of sensitive data stored in each location compared to the perception of risk

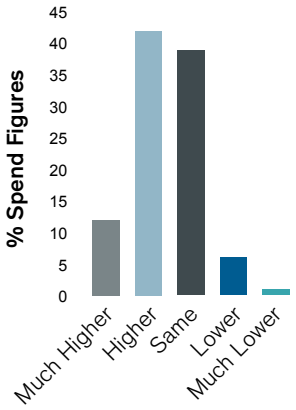


Figure 4: Global spending on security solutions during the next 12 months

that could otherwise put company-sensitive data at risk.

Figure 3 shows the difference between the perceived potential damage from mobile devices and where sensitive data is located. It is close to a 70/20 position. The global average shows 70% of respondents are more worried than they should be about a 20% exposure to risk. Indeed, at a more local level in the ASEAN and US markets the levels of concern are at a high of 86% and 81% respectively.

In our opinion and as highlighted, the risk comparison should focus more on data volumes—how the high volumes of sensitive data held on databases, servers, and in the cloud are protected and managed, rather than the lack of control over mobile devices and how they are used. By volume mobile data levels are low, but devices, locational use, and the mainstream lack of control beyond the firewall are all contributing factors.

"56% of respondents will be looking to increase their security spend to deal with insider threats."

Businesses are spending more on security software to address the threat

The Global Insider Threat Report shows that only 7% of responding organizations believe that next year they will be in a position to spend less on data protection and information security than was the case this year. Sadly, unless there are exceptional circumstances, we would make a case to show that even this small percentage of organizations are probably wrong. The global survey results show that 56% of respondents will be looking to increase their security spend to deal with insider threats next year and the remaining 37% will be spending at least as much as they are now.

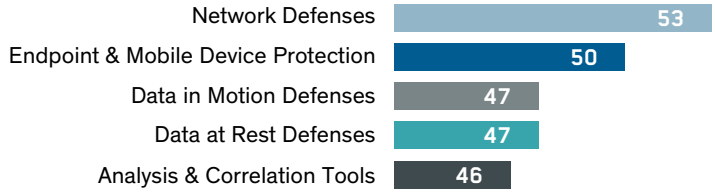


Figure 5: The leading categories where organizations plan to increase security spend during the next 12 months

What is not so clear is how well organizations are going about targeting their increasing, but often hard won security budgets. The scattergun approach that sees increases spread across a wide range of security protection solutions suggests that there is still a significant amount of firefighting going on.

Ovum believes that better results would be achieved by targeting the available funds on risk-based strategies to deal with the protection of sensitive data, monitoring and reporting on usage, and controlling user access. In this respect there do appear to be some positive signs including the increased use of encryption-based data protection tools for data at rest and for protecting data in transit when traveling between corporate systems.

Data breach protection replaces compliance as the number one priority

In Ovum enterprise surveys conducted over the last two years, improving security, risk, and compliance have been the top priorities for enterprise clients. For many the security and risk elements were seen as the drivers for achieving the ultimate goal of remaining compliant with industry and regional regulations. This has consistently pushed the issue of compliance to the head of many enterprise security initiatives, often without enough thought being given to wider enterprise protection requirements. Unfortunately, there are far too many organizations that are able to tick all the compliance boxes but their defenses have not proved to be good enough to prevent insider threats and data theft. Sony, Target, and Vodafone were all compliant at the time they suffered a data breach.

Although it continues to be true that budget contributions for compliance projects remain easier to get from the board, which can help when looking to fund security breach protection strategies, it is often the case that compliance regulations lag behind real-world data protection requirements. Therefore, a more holistic approach is needed to address immediate data breach protection requirements, while delivering security solutions that are capable of evolving to deal with the changing compliance agenda.

The 2015 version of the *Vormetric Global Insider Threat Report* sees the previous obsession with compliance being overhauled by an increased focus on data breach protection. Preventing data breaches, contractual requirements, and protecting intellectual property all scored better than in previous surveys and significantly "achieving compliance" now drops down the priority list.

The reasons why are clear. The last 12 months have seen a continuous flow of high-profile organizations reporting that their security has been breached, including data theft by employees and others with insider status. The numbers don't lie; over 40% of organizations reported that they had either experienced a data breach or failed a security audit in the last year. Senior managers are feeling threatened as data losses mount up. In some extreme cases the CEO has had to go, taking levels of responsibility up to board level and well beyond the usual sacrificial lamb at CISO level.

What this does mean in practical terms for data protection is a stronger focus on implementing best-practice solutions that are relevant to enterprise protection.

"FOR THE FIRST TIME, PREVENTING DATA BREACHES, CONTRACTUAL REQUIREMENTS, AND PROTECTING INTELLECTUAL PROPERTY ARE NOW HIGHER PRIORITIES THAN COMPLIANCE."

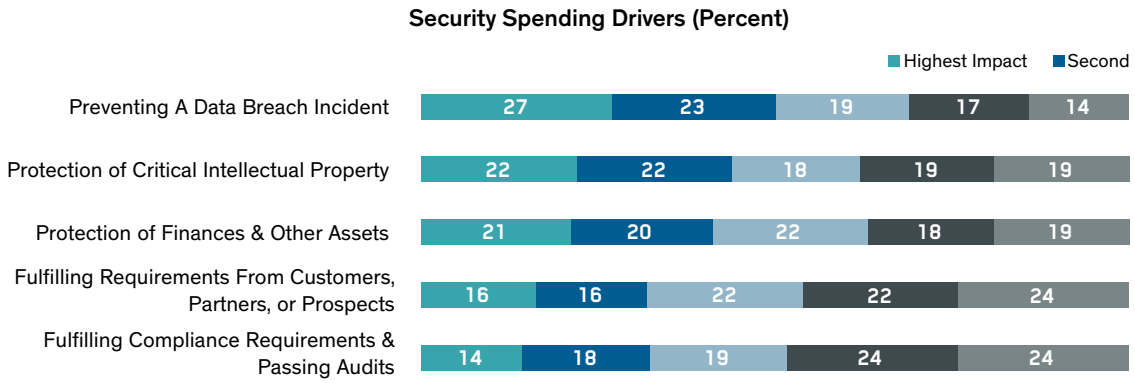


Figure 6: The business protection spending drivers for organization's ranked by priority (1–5)

The most effective data protection technologies and the ones most frequently deployed by enterprise organizations were database and file encryption products, data access monitoring solutions, and data loss prevention technologies. As shown below, these topped a long list of protection solutions and were considered by enterprise respondents to offer the most effective protection against insider threats. Surprisingly tokenization, which has compliance-related uses, came bottom of the list. This may be due to restricted knowledge about the specific benefits the technology has. For example, if organizations need to protect data for specific purposes such as fulfilling payment card industry data security standard (PCI DSS) compliance, tokenization has scoping advantages over other forms of encryption that ensure the scope of audit requirements is reduced, as well as enabling the data to be used by other systems without compromising security.

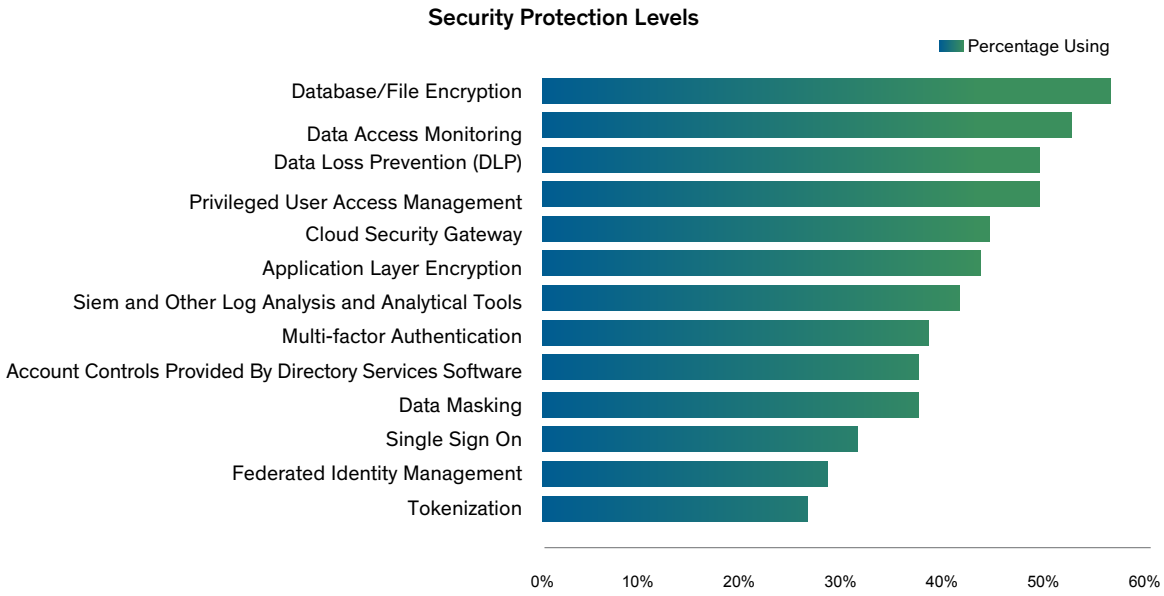


Figure 7: Protections solutions used by enterprise organizations against insider threats

THE MOST EFFECTIVE DATA PROTECTION TECHNOLOGIES:

- *Database and file encryption*
- *Data Access Monitoring*

THE IMPORTANCE OF PROTECTING FROM DATA BREACHES VARIES:

- *US 46%*
- *Global 39%*
- *Germany 18%*

REGIONAL DIFFERENCES–HOW VIEWS ON INSIDER THREATS VARY BETWEEN DIFFERENT REGIONS

The report highlighted many regional data protection variations, some of which were influenced by particular situations. For example, in the US over 1 in 5 organizations reported that they had experienced a data breach (22%) in the last 12 months, and 33% were looking to do more to protect company-sensitive data as a direct result of seeing the damage caused to a competitor following a security breach. The 34% response from US companies was 5% above the global average.

As well as the US, other nationalities differ on their priorities for protecting sensitive data, and in these particular cases local conditions have a strong influence. Legal costs and regulatory fines are high in the US, therefore protecting against data breach penalties was a higher priority for US organizations at 46%—the US top three were data breach protection (46%), brand reputation (45%), and compliance (44%).

When compared to the global average of 39% for data breach protection and a national low of 18% in Germany, the US was significantly out of line. In contrast, Japan retains its focus on compliance as the number one priority for 79% of respondents, with brand reputation at number two and partner and customer requirements in third position.

The US expresses greater levels of concern than other regions

Risk responses and associated concerns over insider threats from US Risk responses and associated concerns over insider threats from US organizations were significantly higher than those reported in other leading markets. The reasons are a combination of strong regulatory and legal controls that come into effect as soon as a data breach is detected and the realities of a situation, which has seen 44% of North American organizations suffer a serious security breach or fail a compliance audit during the last 12 months.

The evidence is both public and compelling. For example, the fallout and legal impact of the Target breach rumbles on as the costs continue to mount. The latest high-profile incidents include Home Depot, the world's largest home improvement retailer where investigations into its more recent payment data systems breach are ongoing. So far it is known that the perpetrators used a third-party vendor's access credentials to break in to the Home Depot network, and these credentials were used to acquire additional rights that allowed them to navigate the network and deploy custom-built malware on the company's self-checkout systems. Payment card data and customer email information appears to have been disclosed, therefore customers will need to keep a look out for unexpected credit and debit card transactions and be on their guard for phishing scams.

Sony Pictures got itself back into the data breach limelight recently after a group calling itself the Guardians of Peace leaked elements of its intellectual property. JP Morgan, the biggest US bank, has admitted that a previously disclosed data breach affected 76 million households and 7 million small businesses, and of course there are many others that have been forced to go on the record during the last twelve months.

As a result of these, and other highly public data breaches, 93% of US organizations said that they felt vulnerable to insider attacks, only 7% felt safe. These figures are above the global average, but the level of difference is most apparent when the US is compared to Germany (where 18% of organizations felt that they had taken sufficient precautions to be safe from insider data theft) and the ASEAN region and Japan, which reported that 16% and 14% of organizations respectively felt safe.

"93% OF US ORGANIZATIONS SAID THAT THEY FELT VULNERABLE TO INSIDER ATTACKS, ONLY 7% FELT SAFE."

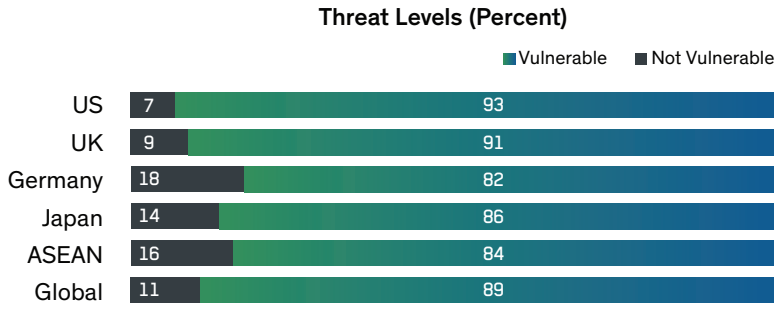


Figure 8: The vulnerability of US organizations to insider threats when compared to other regions

Japan sees insider threats differently

The global report identifies privileged users as the group that poses the highest levels of risk to enterprise organizations. However, while this position is consistent across most countries and regions, there are notable exceptions and Japan is one of those. As shown in Figure 9 ordinary employees (56%) are considered to be the biggest risk, contractors and services providers came second (53%), while privileged users (38%) were positioned as a much lower risk. The reasons behind the differences are not particularly obvious, but could have a lot to do with how insider theft is dealt with and reported within US and European markets when compared to Japan.

There is no evidence to suggest that Japanese organizations have spent more on privileged management technology than organizations in other countries and therefore addressed the problem through the use of technology. It is however worth bearing in mind, when considering the Japanese stance on the security risks posed by ordinary employees, that half of employees who leave their job will keep corporate data from their old employer, and more than half of all insider breaches are caused by well-meaning employees who make mistakes and/or share their access credentials with third parties.

Overall, the vulnerability position of Japanese organizations was close to the global average. Eighty-six percent reported that their companies were vulnerable to insider threats, with the global average set at 89%. Another area where there were clear variations from the global norm was in the most important reasons for securing sensitive data. In the majority of markets brand protection and compliance achieved a similar 50% response, but in Japan compliance was the clear winner supported by 79% of respondents and 28 points above the second category. By comparison the compliance figure was almost double that of the US (44%) and more than double the figure reported by other

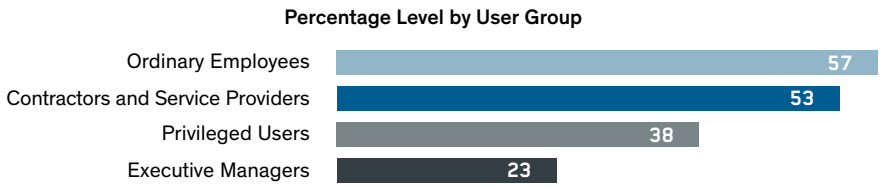


Figure 9: Japanese position for insiders who pose the largest risk to an organization

countries in the ASEAN region (34%). It appears that the value of compliance, which has been a cornerstone of the Japanese approach, remains strong. Whereas other markets have seen the compliance advantage diluted by other important data protection drivers, Japan has mainly stayed with compliance and reputation/brand protection as its two most important requirements.

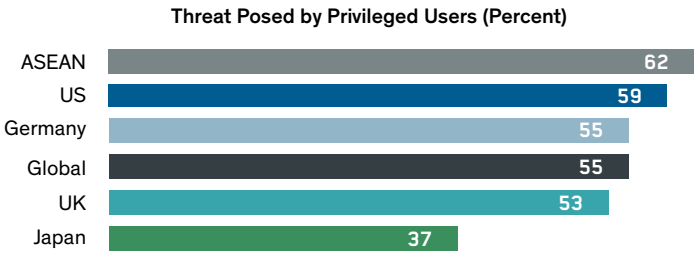


Figure 10: The threat posed by privileged users by individual market

In Japan ordinary employees are considered the greatest risk (56%) while global, the greatest risks are privileged users (55%).

ASEAN HAS ITS OWN UNIQUE CHARACTERISTICS

The ASEAN sector, which includes the key business markets of Indonesia, Malaysia, the Philippines, Singapore, and Thailand have specific data protection and insider threat protection issues that differentiate it from the US, EMEA, and near neighbor Japan. For example, at 48% it had the highest number of organizations that reported that they had succumbed to a serious data breach or had failed a compliance audit in the last year.

"At 48% ASEAN had the highest number of organizations that reported that they had succumbed to a serious data breach or had failed a compliance audit in the last year."

Another significant difference from Japan, which is the most powerful and the most visible technology market within the region, is the ASEAN view on the type of user that is likely to cause the biggest threat. Japanese respondents placed ordinary employees (56%) at the top of their hit list. ASEAN companies at 14% decided that ordinary employees were the safest group and placed them at the bottom. ASEAN took the global position by placing privileged users in the top position of their at-risk list, but they also achieved a response level that was well above the global average. At 62% the ASEAN focus on privileged users was higher than in any other market including the US at 59%. Overall this doesn't look like a balanced position. As well as the higher than average response rates against privileged users, partners with internal access at 60% received an equally negative response within the ASEAN region; whereas other equally deserving threat groups were being almost completely ignored.

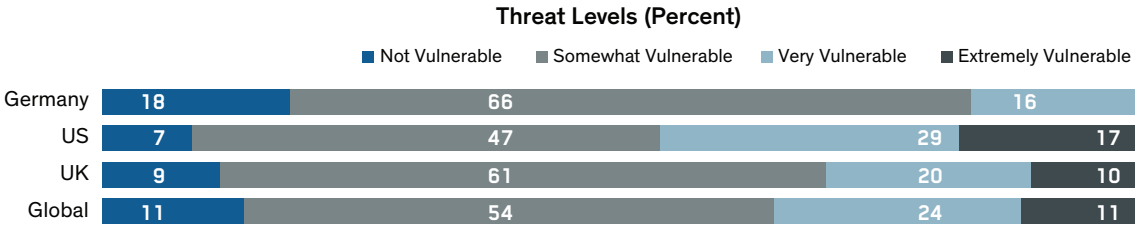


Figure 11: The comparative vulnerabilities of German organizations to insider threats when compared to the global market

EMEA IS A REGION OF CONTRASTS

Germany positions itself as the safest location

The German approach to data protection is proactive. 44% of German organizations are looking to increase their spending on data protection, with the top priority for 55% being the protection of intellectual property (IP). As a group, German organizations generally appear to feel safer than those in any other geographic region. They sit well above the global average and when compared to the US and in particular by direct comparison to European near neighbor the UK, the German numbers are significantly lower when the issues of security concerns arise.

As highlighted in Figure 11, no single German organization said that it was extremely vulnerable to insider attacks. The UK figure was 10%, close to the global average, and the US was a massive 17% above Germany.

However, the highest profile data breach in Europe last year happened in Germany when Vodafone's German operation confirmed that an attacker with insider knowledge had stolen the personal data of 2 million customers. Customer name, address, date-of-birth, and some bank account details were taken. Vodafone identified the perpetrator as a privileged user with knowledge of its most sensitive internal systems. The company described it as a highly complex attack and once identified it took the steps necessary to protect customer data and informed the relevant authorities.

German organizations continue to take a proactive position on data protection and the need to keep sensitive data within geographic boundaries. This along with a more restrictive view on the use of cloud-based services combines to build their stance on business and data protection and their comparative "feel safe" perspective.

"The highest profile data breach in Europe last year happened in Germany when Vodafone's German operation confirmed that an attacker with insider knowledge had stolen the personal data of two million customers."

The UK exhibits high insider threat concerns and has cloud at the center of its agenda

UK insider threat concerns are far higher than those expressed by its European neighbor Germany. Without suffering from the same levels of public exposure when a data breach occurs as the US, the UK's breach numbers are very similar. Forty percent of UK companies said they had suffered a significant data breach or failed a compliance audit in the last year. As a result 51% of UK organizations reported that they were looking to increase spending on security and data protection in the year ahead.

Another significantly different data protection issue that the UK has when compared to Germany and other countries within this report is the location of sensitive data. Fifty-eight percent of German enterprise respondents said that if a breach were to occur databases would be the location most at risk, 40% then said file servers and third on the list was cloud. For the UK the server response was only 38%, a massive 20% below Germany and significantly below the US figure of 47%. In fact, as shown in Figure 12, the UK is the only market where cloud environments are seen as the most at risk when based on the volumes of sensitive data held. This has to be seen as recognition of the growing use of cloud-services within the UK and the volumes of company data now held in the cloud. But even accepting the strong direction of travel towards cloud-based services, at this stage of the journey the UK result was unexpected.

"THE UK IS THE ONLY MARKET WHERE CLOUD ENVIRONMENTS ARE SEEN AS THE MOST AT RISK."

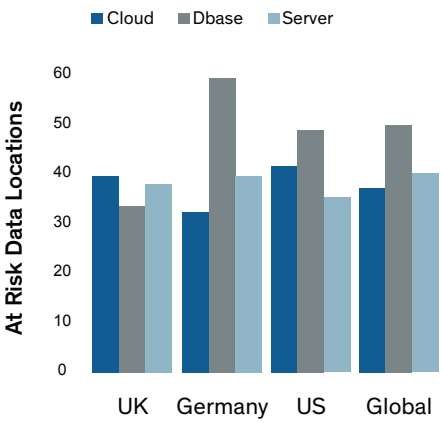


Figure 12: The data risks based on actual volumes of sensitive data stored

THE INDUSTRY PERSPECTIVE ON CLOUD AND BIG DATA INITIATIVES

Data protection remains the top priority across cloud and big data operations

The protection of corporate data is the number one priority for enterprise organizations. Data protection problems have achieved this level of priority because of the continuing explosion in the amount of data that needs to be protected, and allied to the fact that new technology such as cloud and big data adds significantly to the data volumes involved.

"The protection of corporate data is the number one priority for enterprise organizations …. cloud and big data add significantly to the data volumes involved."

However, concern is not solely limited to the amount of data that needs to be protected. There are additional worries about services and facilities that are often maintained away from the control of the company IT department, causing senior management to have additional data theft and loss concerns.

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 will not come as a surprise to business managers and senior IT staff. As shown in Figure 13, cloud environments with 42% 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 and, at 27%, big data operations were not too far behind.

When asked if a data breach did occur, which locations held and would therefore lose the greatest amount of sensitive data and as a result put organizations at most risk, cloud environments had moved up to third place on the "most at risk list" and were only beaten by file servers and databases, which still hold a major albeit reducing proportion of company-sensitive data.

The main issue for both cloud and big data is the continuing growth in their use across enterprise operations, and with it the volumes of sensitive data they are likely to hold in the near future. The direction of travel for new and replacement applications is predominantly towards choosing a cloud-based

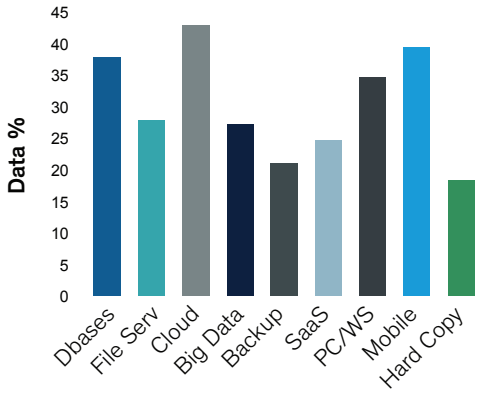


Figure 13: The perception of risk for cloud and big data environments

alternative rather than upgrading previous-generation, on-premise options. Big data strategies are increasingly being introduced whenever there is a requirement to gather analytical intelligence from previously untapped enterprise data sources. Concerns arise because of the data volumes involved and general lack of control over origins, provenance, and whether, for regulatory reasons, data should or can be mixed and shared.

Cloud and big data concerns are genuine and deep rooted

For cloud-based operations the requirement is to ensure that service delivery is secure enough to satisfy the business and guarantee that regulations and controls that have been put in place to keep personally identifiable data safe are maintained. Moving security closer to the assets that need to be protected is beneficial when providing cloud and big data services. A classic example of the type of protection technology that provides benefits using this type of approach is data encryption and key management.

Big data initiatives enable organizations to analyze and extract business intelligence from huge volumes of data, but come with significant usage and processing overheads. The need to keep sensitive data safe implies additional security requirements and brings with it further debate about performance versus security.

This is because the most consistent method of keeping large volumes of data safe involves the use of data encryption technology, but software-based cryptography is known to slow application response times and place heavy workloads on databases and servers. Therefore, better and increased processing efficiencies are needed to persuade business decision makers to make more inclusive use of encryption services.

These improvements are likely to come from a combination of increased processing power and CPU efficiencies from new generation processors, more efficient encryption technology using the advanced encryption standard new instructions (AES-NI) and software solutions that are capable of supporting a new generation approach to mass data encryption. In this context, the issue of non-disruptive encryption services is an important one. Performance continues to be seen as the key factor and in some cases the main barrier to adoption. However, so too is the ability to operate business environments safely and with minimal or zero downtime due to data theft and the loss of unprotected data.

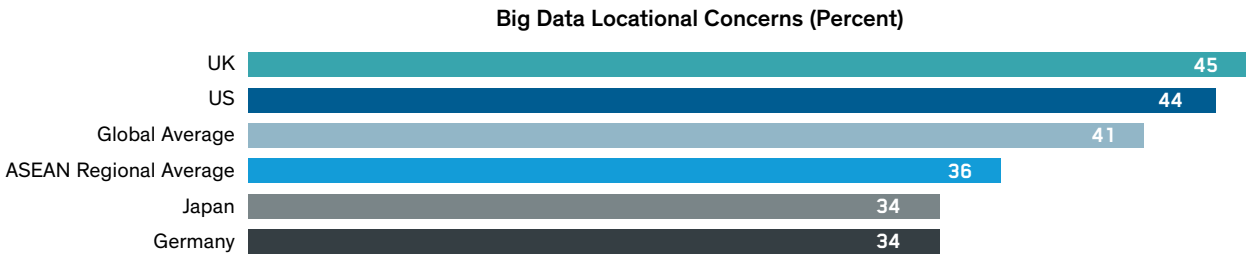


Figure 14: Big data concerns that sensitive information may reside anywhere within the environment

These are important data protection issues when considered against the main concerns that senior managers have about big data projects and the requirement to make information available. Forty-one percent of survey respondents were worried about
data protection and where data is allowed to reside
within the operational environment to support such projects. The figures for the UK and the US were even higher at 45% and 44% respectively.

In summary, the main security concerns for cloud and big data projects involve the protection of sensitive data, unnecessary third-party access, and locational issues over where the data is being held.

"MOVING SECURITY CLOSER TO THE ASSETS THAT NEED TO BE PROTECTED IS BENEFICIAL WHEN PROVIDING CLOUD AND BIG DATA SERVICES."

Spending by financial services organizations on new generation management information systems is on the rise

The market size of management information systems (MIS) in 2013—including data collation, analytics, and reporting systems—to support banks in areas such as distribution, risk, finance, and compliance is estimated at $6.9bn globally. This represents around 5.7% of technology spending in the retail banking industry. Ovum estimates that by the end of 2018, overall technology spending on MIS will reach $9.3bn, representing 6.1% of overall technology spending within the industry.

Financial services and retail are driving big data usage

Big data management information systems have industry-specific relevance when considering the type of business sensitive data analysis projects they are used to support. In the financial services sector big data initiatives are regularly being used by banks to provide fraud analytics, in retail and financial services for customer and web usage analytics. The technology is not replacing current analytical infrastructures, but is extending their scope through its inherent ability to conduct analyses based on all available data, rather than previous generation data sampling approaches.

"In the financial services sector big data initiatives are regularly being used by banks to provide fraud analytics, in retail and financial services for customer and web usage analytics."

"Greater adoption is occurring due to concerted activity from vendors, regulators, and the healthcare industry…supporting security services that monitor and control accessibility and protect sensitive data have an important role to play."

Big data initiatives are being used to look beyond transactional data and text to provide the power and tools to digest digital and physical channel interactions and various types of data such as customer data, graphical data, and geo-locational data.

This is not just a matter of the data being available, or of security encryption technology seeking a problem to solve. Data from customers, banking channels, back-office systems, and third-party sources can yield significant insights that are useful for many activities such as customer marketing, risk management, and infrastructure optimization. All of this can involve highly sensitive data that must remain protected at all times.

The financial services sector, healthcare, and retail face many data and information management challenges. They are investing in big data technology to enable them to address these issues. From a security perspective the global survey results identified that 93% of organizations recognize the need to protect their data and will be looking to increase or at least maintain their security and data protection budgets during the coming year. The figures for the financial services and healthcare sectors exceed this at 94%, with retail lagging behind slightly at 92%.

Healthcare will increasingly turn to cloud services and big data technology

There are multiple drivers for growth in healthcare adoption of cloud and big data-based analytics in areas ranging from electronic health records (EHRs) to workflow management and clinical decision support systems (CDSS) as the healthcare sector moves towards a greater "data liquidity" position and cost pressures force technology efficiencies.

Cloud and big data environments have matured and capabilities have evolved, particularly in terms of security, which is critical for highly regulated industries such as healthcare. The growing uptake of cloud and big data services is also indicative of a wider move to open up and create a more connected healthcare ecosystem including infrastructure-as-a-service (IaaS), platform-as-a-service (PaaS), and software-as-a-service (SaaS) operations.

The current and future challenges facing the healthcare industry require next-generation IT resources and strategies to support significant care delivery and management change. Cloud and big data offers significant potential in addressing basic requirements, such as

cheaper and more flexible infrastructure at lower costs, and more complex requirements, such as delivering richer clinical applications to many more users on different devices and in different locations.

A growing number of cloud and big data service providers and vendors are now healthcare-compliant; many healthcare vendors have worked hard to deliver new cloud computing and big data service functionality. Greater adoption is occurring due to concerted activity from vendors, regulators, and the healthcare industry; supporting security services that monitor and control accessibility and protect sensitive data have an important role to play. When asked about the most important reasons for securing sensitive data, the top three responses from the healthcare sector were compliance (55%), implementing best practices (44%) and reputational protection (41%). In comparison to other business sectors the compliance response was 5% above other industry averages.

Healthcare currently lags behind other industry verticals

The size and urgency of the information management challenges facing healthcare organizations, many of which lag significantly behind other verticals in terms of infrastructure modernization and overall levels of digitization, means that they could benefit more from the opportunities provided by cloud and big data than more advanced industry verticals.

Cloud and big data aligns well with the structural and service changes in healthcare, such as the shift to integrated care delivered in more locations. This requires more flexible public and private platforms that are able to deal with and share much larger data sets, handle greater variations in demand, and support the use of various mobile devices.

The danger lies in growing cloud and big data complexity, particularly in light of the significant legacy infrastructure and application burden. Cloud and big data computing must be deployed and used judiciously along with other business and IT improvement tools and processes. This will require more cloud and data management, both internally and from suppliers, to implement security, governance, and compliance in operationally complex environments.

Big data is helping retailers move away from silo-based decision-making

Historically, retail strategies have generally been product and category specific. Category managers would only have visibility into what products sold the most and which ones had the highest margins etc. Decisions regarding which products to increase and decrease, or add to promotions, were based on partial views of the business.

Although some retailers still plan their strategies around these partial views, others are making the transition to more customer-focused approaches. Decision-making is moving from cut off business silos to centralized and analytical strategies that identify and reward the most regular customers and improve loyalty.

Leading retailers have access to an abundance of very granular data, particularly from loyalty schemes that track the what, where, and when of each customer's purchasing habits. Using big data initiatives this data can be augmented with other business data, such as demographics, credit ratings, weather, and product promotions. A retailer with that level of analytical insight can create personalized promotions to help build loyalty, or use it to improve innovation and support new product launches.

MOST IMPORTANT REASONS FOR SECURING SENSITIVE DATA IN HEALTHCARE:

- *Compliance (55%)*
- *Best Practices (44%)*
- *Reputation Protection (41%)*

PROTECTING YOUR DATA:

- *Concentrate on protecting data at the source*
- *Make encryption with access controls the default*
- *Monitor and analyze data access patterns*
- *Replace point solutions with data security platforms*

RECOMMENDATIONS FOR DEALING WITH INSIDER THREAT ACTIVITY

The last 12 months have seen a continuous flow of organizations being forced to announce that their security has been breached and sensitive data lost due to an insider attack or the illegitimate use of an employee's access credentials.

The number and different types of user who need to be considered when putting together an insider threat protection strategy are diverse and continue to grow. Apart from employees, business partners, suppliers, service providers, and contractors it includes malicious outsiders who have stolen valid user credentials. All of these individuals and groups have the opportunity and in many cases the skills needed to put corporate data at risk.

The majority of company-sensitive data still continues to be stored on-premise on corporate databases and servers. The newer growth areas are cloud and big data where an increasing amount of data is being maintained. Therefore, accepting the current direction of travel for new applications and services, this is where higher volumes of data will be stored in the future and where more inclusive forms of data protection will be needed.

Encryption technology allied to strong access controls and key management is needed for all important data sources and includes the use of database or server, file, and data encryption, tokenization, data masking, application encryption and data on the move encryption.

While accepting that there continue to be performance versus security concerns from IT and business users when considering the deployment of data protection solutions, the requirement to keep company data safe remains the overriding factor. Furthermore, the properly implemented use of hardware-driven encryption, when aligned with the latest generation of CPU-driven processors, helps keep the impact on everyday business operations to a minimum.

Data monitoring and the use of technologies such as security information and event management (SIEM) to identify unusual or malicious data usage and access patterns is also a mainstream requirement.

Controls that maintain the right levels of accessibility and no more are relevant as enterprise organizations strive to maintain control over the various groups who need access. In this context data protection is the key driver. Achieving and maintain compliance is good to see, but far too many compliant organizations have been breached during the last 12 months. What is required to keep the whole organization safe is a unified IT security strategy, incorporating a layered protection approach that adds a new emphasis on data protection as a key element in keeping organizations safe; a strategy that leaves security to the CISO and avoids it becoming a boardroom issue.

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.

Andrew Kellett
Principal Analyst Software
IT Solutions, Ovum

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 protect 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.

2015 **VORMETRIC** INSIDER THREAT REPORT—*GLOBAL EDITION*

Vormetric.com/InsiderThreat/2015

Vormetric
Data Security™