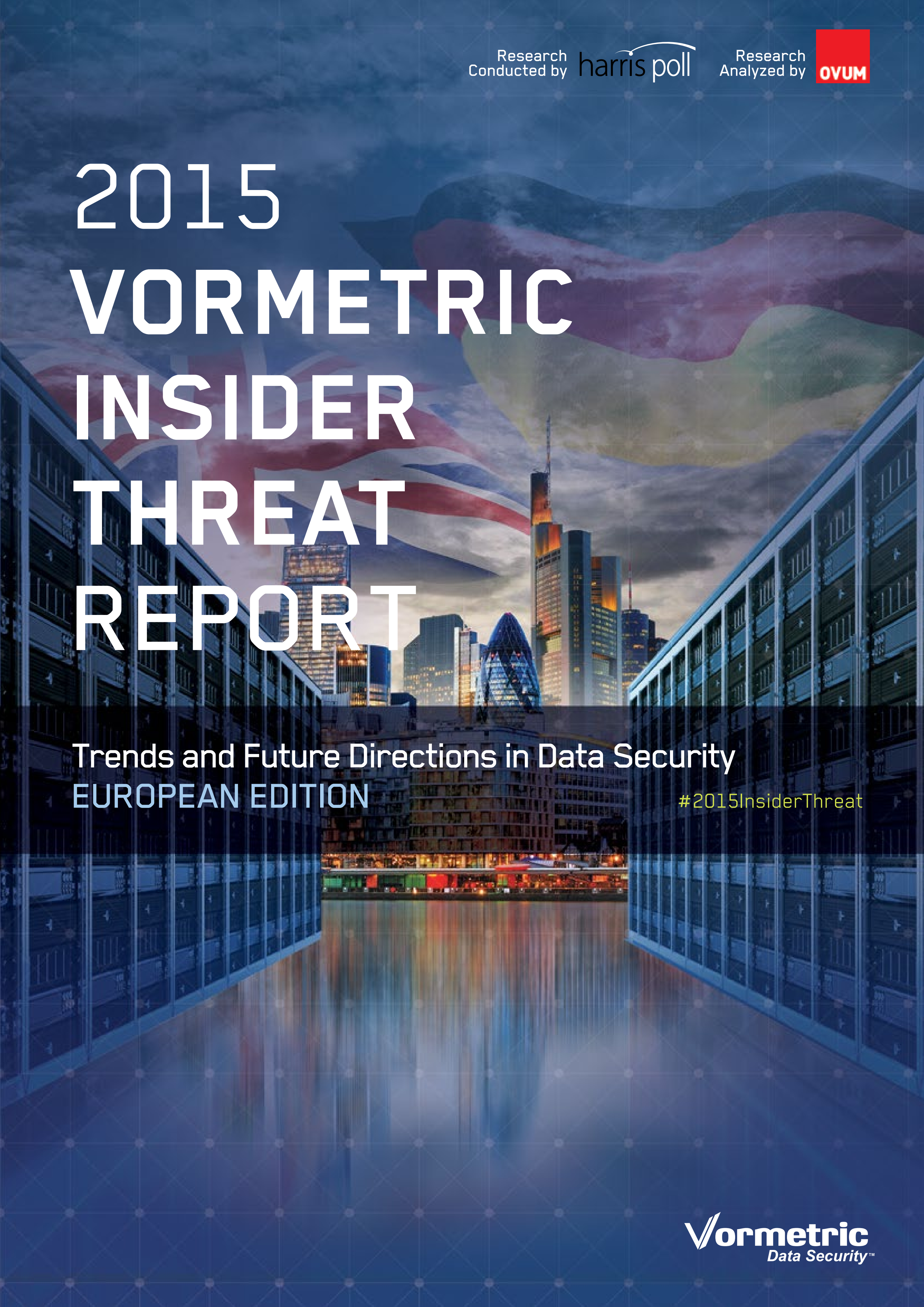


Research Conducted by harris poll

Research Analyzed by OVUM

2015 VORMETRIC INSIDER THREAT REPORT

Trends and Future Directions in Data Security

EUROPEAN 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

KONICA MINOLTA

SUMMARY

Catalyst

The number of reported attacks on business systems and the data breaches that follow continue to rise each year. Whether you accept the recently reported IBM figure of more than 1 billion compromised records during 2014 or the more modest number of 700 million records from Verizon, the negative impact and financial losses for the businesses involved make recovery extremely difficult and costly.

The European edition of the *2015 Vormetric Insider Threat Report* looks into the reasons why so many organizations are being breached, and provides business insight and opinion into the data breach threats that enterprise organizations face on a daily basis. The report is based on an online survey commissioned by Vormetric and conducted by Harris Poll in fall 2014 among 818 IT decision-makers in major global markets. Their views are relevant and often shrewd, as are their opinions on the types of user that put key business information assets most at risk. This version of the *Insider Threat Report* provides the opportunity to analyze the security and risk responses from senior European business and IT experts and compare their feedback to the United States and global position.

> *"Insider threats are caused by a widening range of offenders. The individuals and groups involved have moved beyond everyday employees and IT staff. They now include malicious outsiders with the skills needed to access and then steal valid user credentials."*

Ovum view

Insider threats are caused by a widening range of offenders. The range of individuals and groups involved has moved beyond everyday employees and IT staff. It now includes malicious outsiders with the skills needed to access and then steal valid user credentials. It also has to include business partners, suppliers, contractors and third-party service providers, because some of the most high-profile data breaches in recent times have been initiated from within these groups. Unless properly managed, all these individuals have the opportunity and, in many cases, the skills to reach inside corporate networks and steal business assets.

Alongside the U.S., the mature technology markets of Europe are the most attractive and most targeted for all forms of malware and data theft activity. The vast amount of private and company-sensitive information that is available presents a treasure trove of opportunities for malicious insiders, as well as external attackers with insider knowledge.

> *"Compliance is no longer the gold standard."*

When compared to last year's report, the 2015 version of the *European Insider Threat Report* (ITR) shows that survey respondents have a higher level of insider threat awareness. They have moved to a position where they are focusing on the protection of their most important company assets. They are starting to put the actions of insiders who can cause the most damage—such as systems administrators, contractors and service providers—under the security microscope.

In the 2014 report*, the top issues worrying survey respondents were the amount of data that needed to be protected, the distributed nature of that data and how best to identify and control users who had access. Irrespective of the progress that has been made to identify and deal with high-risk users, a lot more work still needs to be done to protect each organization's most important data assets. This was highlighted by the 87% of IT decision-makers who felt that their organization was still vulnerable to insider attacks and, because of this, were looking to increase or at least maintain existing spending levels on IT security and data protection.

The two major European markets examined in this report are Germany and the U.K. Both are primary data theft targets, and many organizations within both countries have suffered high-profile data breaches. There are, however, measurably different attitudes toward business and technology risk between the two. Survey results show that the U.K. is more open toward the use of new technologies that have a higher risk profile, such as mobile, cloud and big data.

In Germany, usage levels are lower in these areas, and more emphasis is placed on continuing to store corporate assets on-premise. These differing views on the use of technology are highlighted throughout the report. They emphasize approaches to risk and data protection that often separate the two countries, but on other occasions, show a common European bond on issues such as best practices, brand protection and compliance.

Key messages:

- Only 13% of European survey respondents said that their organizations were safe from insider threats. This represented a slight improvement on the 9% that said they felt safe last year, but still leaves 87% feeling vulnerable. Japanese respondents believe that ordinary users (56%) pose the biggest internal threat to corporate data. Privileged users are well down the list, at 37%.

- Maintaining compliance remains an important theme for European organizations, but it is no longer seen as the gold standard. Future spending patterns show that protecting critical intellectual property and preventing data breaches are now the top priorities.

- Over 50% of European organizations placed privileged users as the highest risk group when considering their data protection requirements. Contractors, service providers and business partners were also on the hit list.

> *"Only 13% of European survey respondents said that their organizations were safe from insider threats."*

*The 2014 Vormetric Insider Threat Report *was issued in April of 2014 and focused on Europe's three largest technology and business markets—France, Germany and the United Kingdom (U.K.). Across these three markets, 540 senior IT professionals and business managers, over 80% from midsize to large enterprise organizations, were interviewed by telephone by Ovum on the impact that insider threats have on their organizations and on how prepared they are to deal with insider activity.*

"40% of U.K. survey respondents said that their organizations had experienced a data breach or failed a compliance audit in the last year."

EUROPEAN ORGANIZATIONS FACE AN EVER-EXPANDING RANGE OF INSIDER THREATS

Very few organizations feel safe from insider attacks

The European version of the Vormetric ITR identified that only 13% of respondents said that their organizations were not at all vulnerable from insider threats. This represented a slight improvement on the 9% that said they felt safe in last year's survey, but still leaves 87% of organizations feeling vulnerable to insider threats.

The European numbers, which were mainly gathered from German and U.K. respondents, are close to the global average, where 11% of all respondents said that they were safe from attack and 89% felt vulnerable. Taking into account all the areas that have been included in the various ITR surveys across Europe, Asia-Pacific and North America, the region with the highest reported levels of concern about data theft activity is the U.S., where 93% of respondents said their organizations were vulnerable and only 7% felt safe.

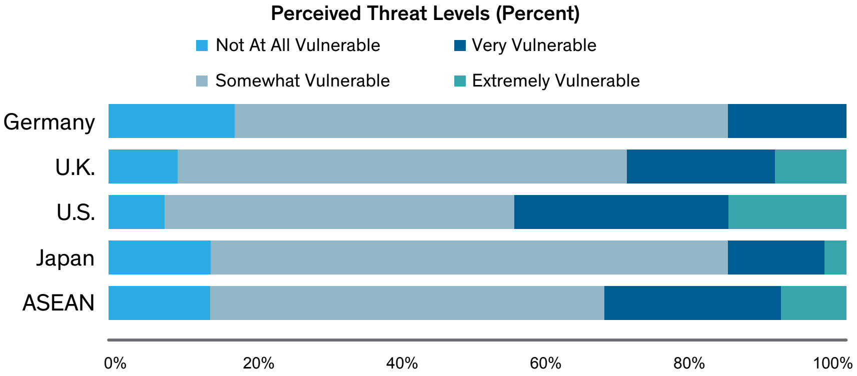


Figure 1: Organizations' perceived vulnerability to insider threats

When evaluating the German and U.K. numbers further, a theme that is repeated at several points during the report begins to emerge. As a group, German respondents felt that their organizations were more secure than their near neighbors in the U.K. Only 9% of U.K. IT decision-makers reported that their organizations were safe from insider attacks. The German figure of 17% was well above the global average, and higher than the "Feeling Safe" position reported by any other country. Confirming this overall position, Germany was the only country with a 0% level response of "Not at all Vulnerable." The equivalent U.K. position had a 10% response, and the U.S. was even higher, at 17%.

While accepting the relative safety and well-being felt by German IT decision-makers when compared to the U.K. and the U.S., it was still the case that four out of every five IT decision-makers in Germany felt that their organizations were vulnerable to insider threats.

A recent study by the European Center for Media, Data and Society (CMDS) revealed that there were significant differences in the data breach volumes between the leading European countries. When comparing the number of compromised records per 100 people caused by data breaches in the European Union (EU), the U.K. tops the list at 220. This brings the German position of relative safety and well-being into perspective. Its reported data breach ratio per 100 people was 68. However, when further reviewing the CMDS figures, the European nation that ought to feel least at risk is the Netherlands, where the reported risk number is just 23.

Unsurprisingly, U.K. organizations were the most pessimistic in Europe about the chances of current and future EU regulations helping to improve things. Very few felt that compliance and regulatory enforcement would help prevent organizations from losing data or having it stolen. This also goes some way to explain why fulfilling compliance with existing regulations is no longer seen as the most important reason for increasing expenditure on security, when compared to more direct and practical approaches to protecting sensitive data and intellectual property.

A worrying factor, and one that has been reported across all geographies and vertical markets, is the actual number of businesses that have suffered a data breach or failed a compliance audit in the last 12 months. As highlighted in Figure 2, 40% of U.K. survey respondents said that their organization had experienced a data breach or failed a compliance audit in the last year. This figure closely matches the global average, but is still slightly lower than the U.S. figure of 44%. In Germany, where only 26% of respondents admitted a problem in the last year, numbers were far closer to that of Japan, where 29% reported a data breach or compliance audit problem.

No organization can afford to position itself as being completely safe from attack; too many remain vulnerable and too many are regularly being breached or failing to meet compliance and security audit requirements. All need to do more to protect data from insider threat activities and from attacks by external sources using valid credentials that have been stolen or acquired from legitimate users.

"In Germany, only 26% of respondents admitted encountering a data breach or failing a compliance audit in the last year."

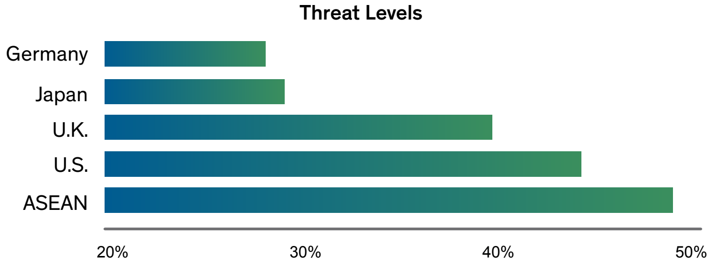


Figure 2: The percentage of IT decision-makers that reported a data breach or failed a compliance audit in the last 12 months

Several well-known European organizations have suffered a data breach in the last 12 months and had their reputations damaged as a result of the unwanted media attention:

- **Deutsche Lufthansa, the largest airline in Germany and Europe**, reported that its website had been hacked and customer records compromised, allowing criminals to steal frequent flyer miles in order to obtain vouchers and redeem awards. The attack approach is believed to have involved matching passwords to valid user credentials to gain access to the airline's online portal.

- **U.K. telephone and broadband provider TalkTalk** was hacked during 2015, and 4 million customer records were stolen. The company blamed a third-party contractor for the data breach that caused customer information (account numbers, addresses and phone numbers) to be put at risk. The initial point of access remains unclear, but it seems that a third-party contractor that had access to TalkTalk customer accounts was compromised.

- **French public TV broadcaster France Télévisions** suffered a data breach and the loss of over 100,000 email records. It appears that little technical knowledge was needed to steal the data, as the records were kept in plain text on a public-facing server with little or no security controls in place.

- **Moonpig, the online greeting card provider**, was found to have major security vulnerabilities within its web facilities. These vulnerabilities put the personal data of 3 million customers at risk. The identified problem involved weak authentication controls that allowed open access to the personal account details of other account users, including name, address and some credit card information.

Compliance remains important but is not the gold standard it used to be

In the global version of the Vormetric ITR, reputation and brand protection, at 51%, replaced compliance as the number-one priority. The same position was found in the U.S., where reputation and brand issues (47%) also outscored compliance. However, this review of the German and U.K. positions shows differences when compared to the global numbers and the U.S. position. As shown in Figure 3, Germany, at 59%, and the U.K., at 53%, continued to see maintaining compliance requirements as the most important reason for securing sensitive data. That does, however, leave the European numbers out of line with global, U.S. and other mainstream markets.

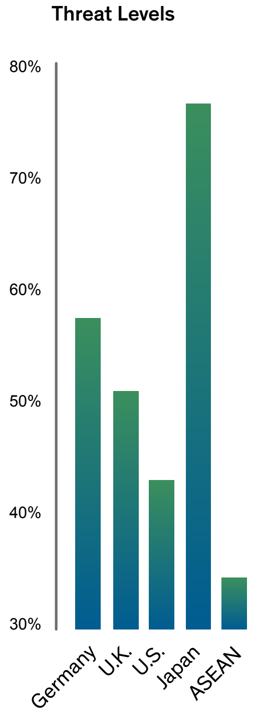


Figure 3: Compliance remains an important issue for German and U.K. organizations.

Nevertheless, this only represents one component of the overall compliance picture. When considering why organizations choose to spend more of their IT budget on security, German and U.K. IT decision-makers fall back in line with the rest of the world. In terms of its importance as a driver for security spending, compliance and audit were well behind key data protection issues such as protecting critical intellectual property, protection of finances and other assets, prevention of data breaches and the pressures exerted by business partners and customers.

> *"The top 2 IT spending priorities in the U.K. and Germany were protecting intellectual property and preventing data breach incidents, with compliance falling to last place in Germany and second to last in the U.K."*

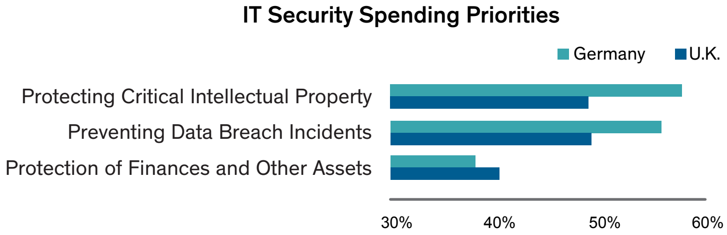


Figure 4: The top 3 IT security spending priorities for German and U.K. organizations

This is an interesting change of position from last year. In the 2014 ITR report, European support for compliance as a security spending driver was the top priority, at 40%. It is now down to 33%. Last year, it was followed on the priority list by business-partner and customer pressures. This year, the tables have turned—compliance has been overtaken by the need to protect critical intellectual property (52%), the need to prevent data breaches (49%) and the protection of financial and other assets (38%).

> "GERMANY, AT 59%, AND THE U.K., AT 53%, CONTINUED TO SEE MAINTAINING COMPLIANCE AS THE MOST IMPORTANT REASON FOR SECURING SENSITIVE DATA."

Europe recognizes that the most dangerous insiders have privileged access—but protection isn't keeping pace

The analysis and survey feedback about which insiders European organizations believe pose the greatest threat to organizations and their data proved to be both astute and, to some extent, contentious. It was astute because organizations said that privileged users—systems administrators and IT specialists—with the best technical skills posed the greatest risk to business systems and the data they hold. It was contentious because the results continue to underestimate the potential data theft opportunities that other internal user groups continue to have.

Realistically, privileged users have always been a high-risk group. Nevertheless, previous survey results have ignored that risk and focused more on accepting the integrity and professionalism of the individuals involved.

However, the damage that this type of technical user can cause has been demonstrated on a number of occasions. For example, it was highlighted in the late 2013 Vodafone Germany breach, where a technically astute attacker with insider knowledge of the company's most sensitive internal systems gained access to and stole the personal data of 2 million of the company's customers.

The survey results presented in Figure 5 show that 54% of European companies (Germany 55% and the U.K. 53%) identified privileged users as the number-one risk group. These numbers provided a comparatively similar result to the global return of 55%, but were still five points below the U.S., where 59% of respondents were worried about privileged users.

> *"Less than 50% of enterprise IT decision-makers report that they have deployed privileged access management (PAM) technology."*

Percentage by User Group

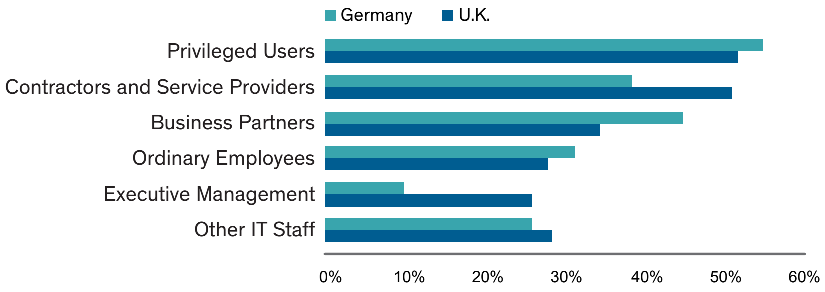


Figure 5: The positions of Germany and the U.K. on insiders who pose the most risk to organizations

But the consistency of the mid- to high-50s responses on privileged users is as far as the geographic agreements go. The global and U.S. numbers show a 9- and 13-point gap, respectively, between privileged-user responses and the next highest risk groups. Globally, these were contractors and service providers (SPs), at 46%, but in the U.S. it was business partners, also at 46%.

In the European markets, there were also differences within the tier-two and tier-three insider threat rankings—the U.K. positions contractors and SPs at a similar threat level to privileged users (53% see privileged users as high risk, and 51% also see contractors and SPs in a similar vein). For German survey respondents, contractors and SPs are positioned as their tier-three option (39%), with business partners seen as posing a higher risk (45%).

All of which represents a significant change of overall positioning from just a year ago. Last year in the 2014 European ITR, when asked who posed the biggest internal threat to corporate data, almost 50% of respondents said everyday users. The next largest group was IT service providers, then third-party contractors—and only after that were privileged users given consideration.

"Ovum recognizes the overwhelming need to control the access rights of systems administrators and other privileged users."

Since then, privileged-user threats have hit the senior management radar across most major global markets—with the notable exception of Japan, where privileged users continue to languish third on the risk list, behind ordinary employees and contractors/SPs.

For IT decision-makers in Germany, the U.K. and the U.S., controlling the activities of privileged users and keeping data safe is now at the top of their wish list. Unfortunately, the actions that have been taken to improve the situation do not match the threats involved. The global total identifies that less than 50% of IT decision-makers say that their enterprises have deployed privileged access management (PAM) technology.

On the subject of deploying privileged protection solutions, the U.K. is by far the worst offender. Only 40% of U.K. IT decision-makers said that their organizations have PAM facilities in place. The U.K. figures look even more dismal when compared to the responses received from IT decision-makers in German organizations, where 59% have deployed PAM technology. Overall, the German response was 10 percentage points above the global average, 12 above the U.S. and a massive 19 percentage points higher than the U.K.

"54% OF IT DECISION-MAKERS IN EUROPEAN ORGANIZATIONS (GERMANY 55% AND THE U.K. 53%) IDENTIFIED PRIVILEGED USERS AS THE NUMBER ONE RISK GROUP."

Many of the threat issues that apply to privileged users, such as a lack of control over their access rights and too little monitoring of the actions they take, also extend to contractors, service providers and business partners. These groups may sit below the radar in many organizations, but more needs to be done to maintain control over the sensitive data resources they have access to.

Ovum recognizes the overwhelming need to control the access rights of systems administrators and other privileged users. We would argue that the necessary security and monitoring controls should be extended to, and consistently applied against, all individuals who have the opportunity to access and make use of company-sensitive information.

In order to achieve these objectives, the list of top security and data protection solutions that European organizations are investing in to safeguard their data assets include database encryption and data access monitoring technology. These are the top two priorities identified by IT decision-makers in German and U.K. organizations, and they also feature strongly in the U.S. results.

Cloud usage is increasing, but the majority of sensitive company information remains on-premise

As has been identified in previous versions of the ITR, the top-three locations, by volume, where company-sensitive data is stored by European organizations and must be protected continue to be databases (49%), file servers (39%) and the cloud (36%). This position is consistent across most major geographies, but there are some specific regional differences.

"Globally, the top-three locations, by volume, where company-sensitive data is stored by European organizations and must be protected continue to be databases (49%), file servers (39%) and the cloud (36%)."

Survey responses show that U.K. organizations now hold as much company-sensitive data in the cloud as they do on-premise in database and server storage facilities. By comparison, German organizations look to be a picture of technology moderation and constraint, as well as exhibiting a determined resistance to change. German database usage rates, at 58%, are a significant 20 percentage points above the U.K. (38%), 9 points above the global average and 11 above the U.S. The server figures for Germany, at 40%, outstrip the U.K. (33%) and the U.S. (35%). They also push the cloud into third, at 31%.

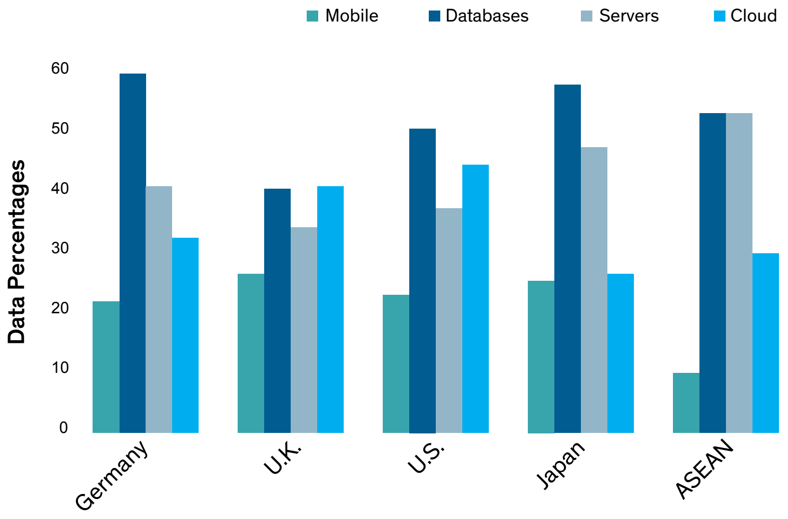


Figure 6: Top-three selections for locations of volumes of sensitive data

Alongside the lower cloud usage levels reported by IT decision-makers in German organizations, it was German respondents that consistently positioned the use of cloud services as providing the greatest risk to company-sensitive data. As shown in Figure 7, the German risk score for cloud and mobile was 49% and, as such, has become a major deterrent when German organizations are considering further cloud and mobile usage opportunities. The global risk score for the cloud is 40%, whereas the U.K., which has high cloud usage rates, only reports a risk score of 37% and, like the U.S., continues to promote the counterargument in favor of the extended use of cloud-based services.

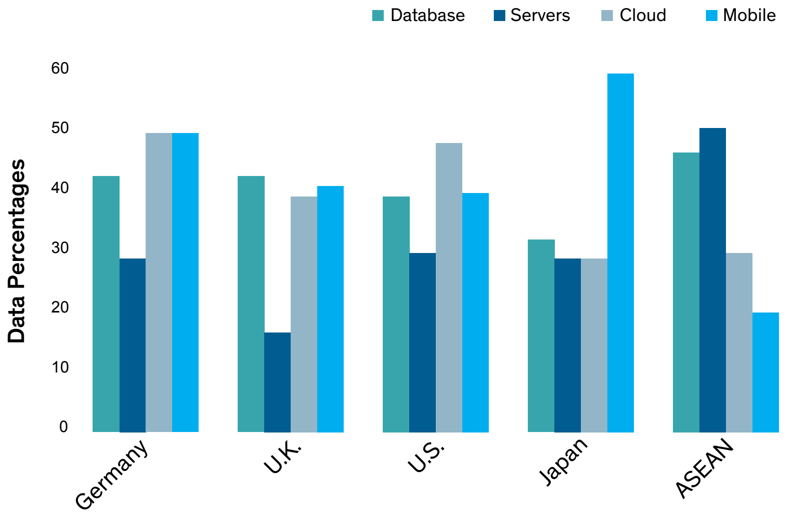


Figure 7: Top-three selections for locations that are at the greatest risk for loss of sensitive data

“German respondents consistently positioned the use of cloud services as providing the greatest risk to company-sensitive data.”

Mobile security issues rank alongside cloud issues when organizations consider data protection requirements

When considering the operational components that cause IT decision-makers most concern, as highlighted in Figure 7, mobile usage and the data stored on mobile devices get close to the top of most lists. Be that as it may, Figure 8 clearly shows that, in comparison to the actual volume of company-sensitive data stored on mobiles devices, the associated risk is far greater than it should be. The actual data volumes reported by German and U.K. organizations are well below those stored in databases, servers, the cloud and even big data environments.

> *"In comparison to the actual volume of company-sensitive data stored on mobile devices, the associated risk measured was far greater than it should be."*

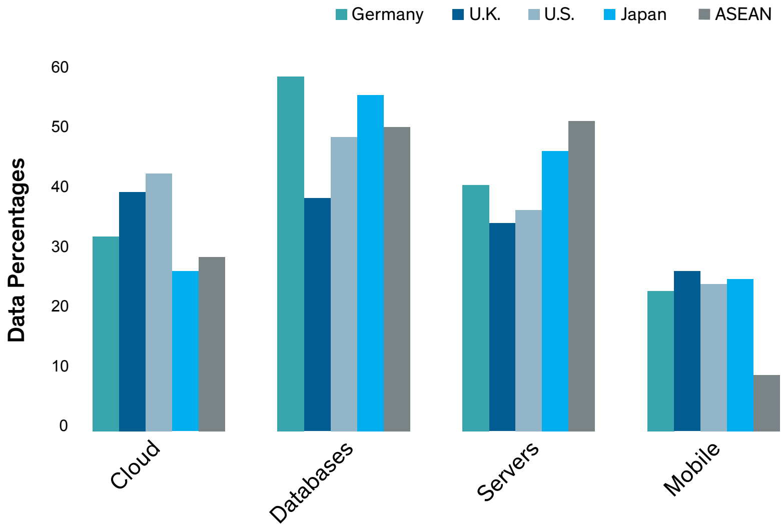


Figure 8: The data volumes stored on mobile devices compared to other mainstream locations

The fear-factor levels are heightened because of the flexibility of use that mobile devices encourage, as well as the lack of control that organizations continue to have over devices that they often do not own but employees choose to use.

The European research shows that mobile usage rates vary between different countries and individual market verticals. U.K. mobile device usage rates when sensitive data is involved are at 25%. This is higher than in Germany (21%), and also higher than both the U.S. and the global average.

For mobile, the U.K. risk level is the same as that of the U.S. and slightly below the global average figure of 39%. Germany holds less sensitive data on mobile than other major markets, but at 49%, also exhibits far higher levels of concern about how mobile devices will be used. In fact, the German market's risk view on mobile is similar to the one it holds on the use of cloud services. Both are seen as high-risk technologies, and usage in both areas is restricted to levels that are well below other mature technology markets.

GERMANY AND U.K. ORGANIZATIONS ARE INCREASING THEIR SPENDING ON DATA PROTECTION TECHNOLOGY

Enterprise concerns remain high as insider threats continue to grow across all markets

The recently published *Global Insider Threat Report* identified that, in the year ahead, 59% of enterprise survey respondents were looking to increase their security spending to deal with insider and external threats to their data. Only 7% believed they were in a secure enough position to spend less on security, and the remaining 37% planned on spending at least as much as they did last year. The figures for Germany and the U.K., by comparison, are similar (see Figure 9), albeit slightly higher on the percentage of organizations that are looking to reduce their security spending (9% in Germany and 11% in the U.K.).

The security spending numbers differ more when comparing Germany and the U.K. to the U.S., where only 5% of IT decision-makers think they are in a position to reduce spending on security. Otherwise, the overall numbers for German and U.K. organizations looking to spend at least the same or more on security follow the global pattern, but with two notable exceptions.

German spending-growth patterns are more conservative than those of the U.K. and the U.S., with a higher percentage of German IT decision-makers reporting that their organizations (47%) are spending the same as last year. The U.S. equivalent is 33%, and the U.K. is 39%. Only 6% of German respondents plan to undertake high increases in spending on security, whereas increases at the highest level among U.S. respondents sit at 17%.

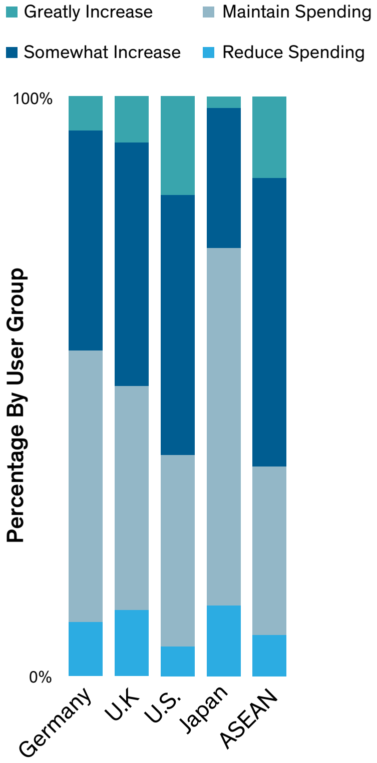


Figure 9: Increased security spending in Germany and the U.K. with comparisons to the U.S.

"51% OF U.K. RESPONDENTS AND 44% OF GERMAN RESPONDENTS WERE INCREASING SPENDING TO OFFSET THREATS TO DATA—VERSUS 62% IN THE U.S."

“Globally only 7% of respondents believed they were in a secure enough position to spend less to offset threats to data.”

“The U.S. sees itself as the number-one malware attack target. The mature technology markets of the U.K. and Germany generally sit close to the top of those same most-targeted lists.”

The typical security spending pattern we see emerging across all major markets—Europe, the U.S. and Asia-Pacific—is one of maintaining existing levels, alongside moderate but generally not massive increases. Drilling down into the detailed numbers, the U.K. very closely mirrors the global position, insofar as only 1% of IT decision-makers say that their organizations will spend much less on security in the year ahead; 8% (global 6%) will spend somewhat less; 39% will spend the same; 42% will spend somewhat more; and 9% (global 12%) will spend significantly more.

Europe, like North America, is a primary target for both internal and external data theft. The U.S. sees itself as the number-one malware attack target, and many of the regularly produced Internet and cybercrime threat reports from organizations such as RSA and Symantec tend to agree with that assessment. The mature technology markets of the U.K. and Germany generally sit close to the top of those same most-targeted lists because of the quality, value and amount of data available.

When reviewing where both German and U.K. organizations are going to be spending their hard-earned security budget increases, the patterns that emerge are very similar. Figure 10 shows that the top area of spending by German (46%) and U.K. (45%) IT decision-makers will be on network defenses, which is likely to have been driven by the increasing levels of DDoS flood attacks against commercial business networks.

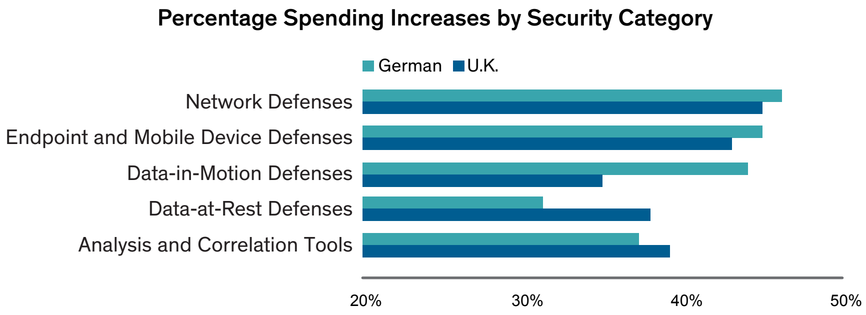


Figure 10: Technology areas where German and U.K. respondents plan to increase security spending in the next 12 months

Other key areas where increases in security and data protection spending are anticipated include endpoint and mobile device protection—Germany 45% and the U.K. 43% (U.S. 56%). There will also be spending increases on data encryption, data masking and data loss prevention (DLP) products to protect data-at-rest and data-in-transit, as well as on the monitoring, analytical and correlation tools needed to maintain control over data access and usage and provide better understanding of the threat environment.

A COMMON STANCE ON CLOUD AND BIG DATA IS NOT ALWAYS SHARED BETWEEN GERMANY AND THE U.K.

> *"At a global level, cloud and big data issues are focused on the need to protect more data assets."*

Both are worried about the protection of enterprise data assets and both have data sovereignty issues

For cloud and big data, the common security issues that German and U.K. IT decision-makers share is an overriding concern about data protection, the increasing volumes of sensitive data that need to be protected, data sovereignty concerns about where data will be held, and third-party and partner access control issues.

At a global level, cloud and big data issues are focused on 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.

European IT decision-makers were expected to have more concerns about data location issues (where data is kept and who has access) than other regions and, as shown in Figure 11, with a 45% response rate, the U.K. numbers to some extent bear this out.

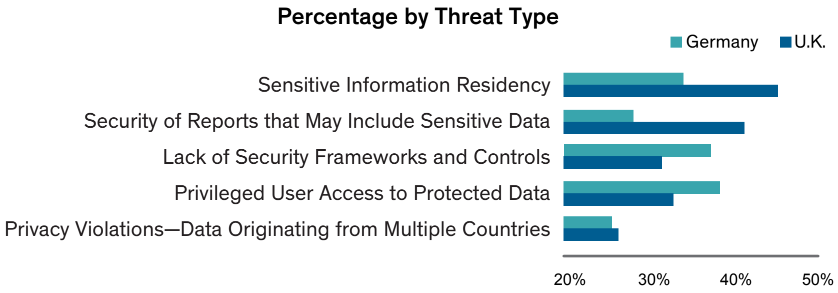
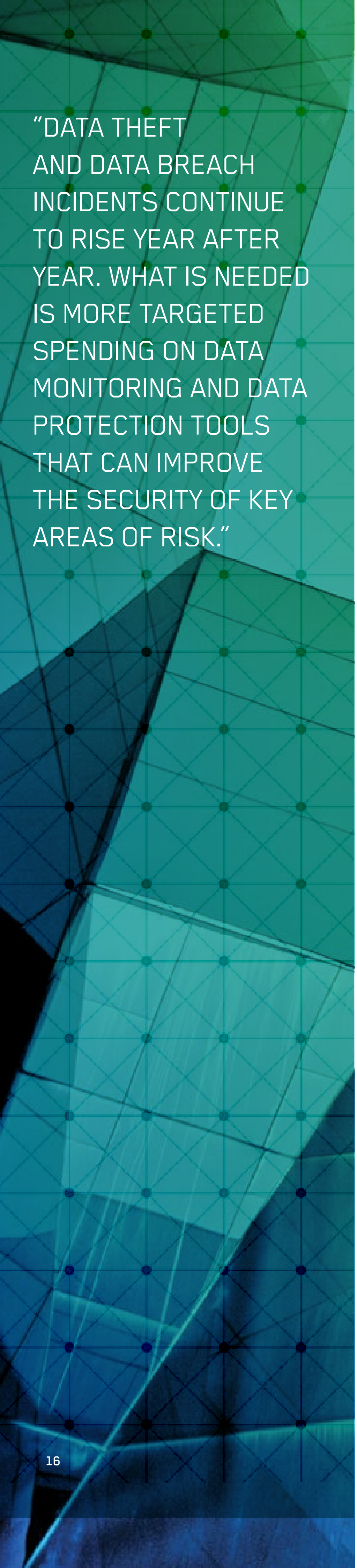


Figure 11: Cloud and big data usage, security and data protection concerns

Germany, where data location and residency was expected to be even more of a key issue than in other countries, only returned a 34% response. This was lower than the global average and significantly lower than both the U.K. and the U.S.

When analyzing this unforeseen lack of concern further, it becomes apparent that the lower-than-expected German numbers are being influenced by lower usage levels for cloud and big data initiatives. Nevertheless, even accepting that that's the case, the response is out of line with other expressions of concern that German managers have expressed on the use of cloud and big data.



"DATA THEFT AND DATA BREACH INCIDENTS CONTINUE TO RISE YEAR AFTER YEAR. WHAT IS NEEDED IS MORE TARGETED SPENDING ON DATA MONITORING AND DATA PROTECTION TOOLS THAT CAN IMPROVE THE SECURITY OF KEY AREAS OF RISK."

MANAGEMENT SUMMARY AND RECOMMENDATIONS FOR ENTERPRISES

The number of European organizations that suffer security breaches and have had company-sensitive data stolen continues to rise. In Germany and the U.K., organizations have quite rightly prioritized the need for better privileged-user controls. There are notable variations in approach to security between the two countries, but both recognize the need to deal with and control privileged users, contractors, service providers and business partners. There is less focus on other groups, such as executive managers, other employees and other IT staff, which is unfortunate because within these groups there will be users with the skills and the inclination to put enterprise data at risk. What organizations need to have in place are access controls that match the business requirements of each user and make use of a least-privilege approach to ensure that access to facilities that are outside their remit are refused.

The report focused on the main insider threat concerns of IT decision-makers from Germany and the U.K. It found that more effort was needed to protect sensitive data and control the access rights of the respective user groups. As such, the increased spending patterns in Germany and the U.K. are welcomed. They are a recognition of the vulnerable position that enterprise organizations continue to find themselves in—and this is important because most organizations currently do not know enough about who has access to their data and what their users are doing once access had been granted.

Data theft and data breach incidents continue to rise year after year. What is needed is more targeted spending on monitoring and protection tools that can improve the security of key areas of risk, such as company-sensitive data, while also providing network and device protection. That spending must recognize that security management and security monitoring have an increasingly important role to play.

The overall security and threat responses from German organizations position the country as conservative in its attitude toward risk, with its lower-than-average usage of mobile applications and its aversion/reluctance to follow the latest cloud and big data usage trends. Its spending patterns on security also reflect this, insofar as increase rates are lower than those reported in the U.K. and the U.S., where organizations look as though they are firefighting a security position that is in danger of overwhelming them. We would continue to argue that organizations need to and can do more to keep their data safe. In all cases, a unified threat and data protection strategy that involves the use of layered security and fits the risk profile of each organization is needed.

"What organizations need to have in place are access controls that match the business requirements of each user."

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 to October 16, 2014, among 818 adults, ages 18 and older, who work full-time as IT professionals and have at least a major influence on IT decision-making in their companies. 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 U.K. (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 1,500 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.

THE *2014 VORMETRIC INSIDER THREAT REPORT—EUROPEAN EDITION*

The *2014 Vormetric Insider Threat Report* was issued in April 2014, and focused on Europe's three largest technology and business markets—France, Germany and the United Kingdom (U.K.). Across these three markets, 540 senior IT professionals and business managers, over 80% from mid-size to large enterprise organizations, were interviewed by telephone by Ovum on the impact that insider threats have on their organizations and on how prepared they are to deal with insider activity.

2015 **VORMETRIC** INSIDER THREAT REPORT–*EUROPEAN EDITION*

Vormetric.com/InsiderThreat/2015

Vormetric
Data Security™