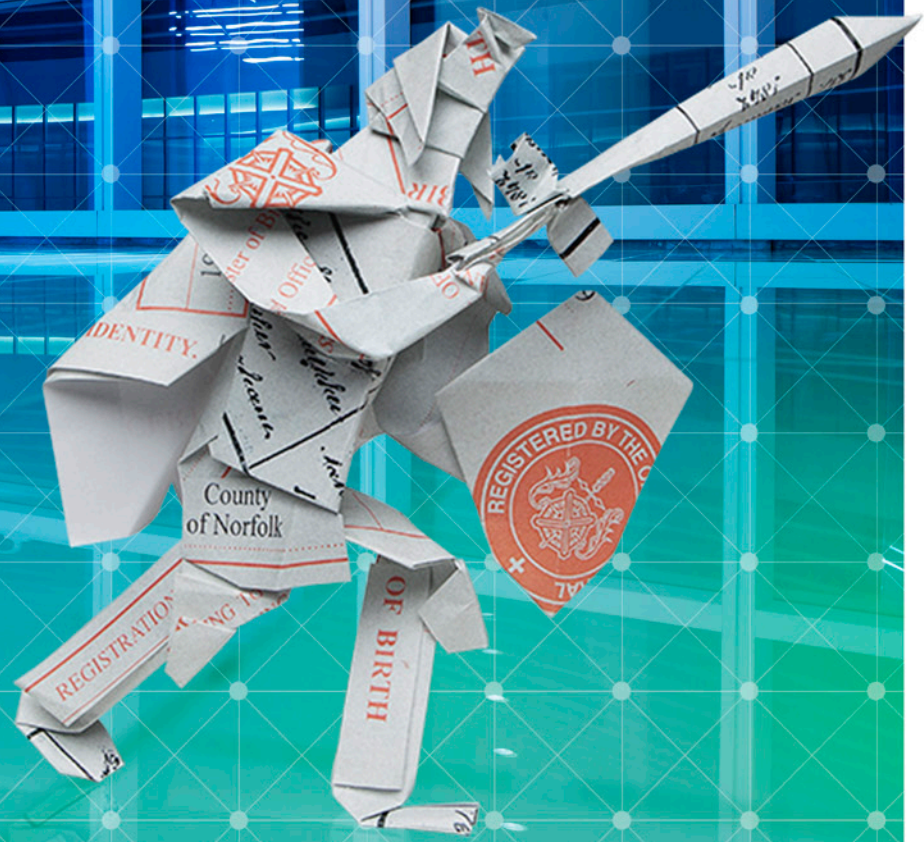
Vormetric
Data Security™

Research Conducted by OVUM

2014 INSIDER THREAT REPORT

European Edition



A European study conducted by Ovum Research on behalf of Vormetric Data Security and with cooperation from:

Field Fisher Waterhouse

SECURITY Innovation Network

OASIS

CSA cloud security alliance℠

Total Device SECURING YOUR DATA

mongoDB

Vormetric Data Security™

TABLE OF CONTENTS

EXECUTIVE SUMMARY

CATALYST

The *2014 Vormetric Insider Threat Report* – European Edition provides insight into the views of senior IT professions and business managers on the realities of keeping corporate systems and the data they hold safe for the people who have the most urgent need for access. Insider threat headlines ebb and flow along with the size of each data breach, the profile of the compromised parties, and the sensitivity of the data involved. Highly publicized insider data theft and compromised user privilege events very forcefully confirm the need for better and more inclusive security solutions.

The insider threat landscape is constantly changing. Threats are caused by employees or associates of an organization who either maliciously or accidentally take action that put their organizations and data at risk. However, that is nowhere near the whole story. Just about every high profile and expensive breach is the result of attack techniques used inside the network, and therefore the threat extends to outsiders who have obtained the legitimate credentials needed to gain access and conduct malicious activities that cause operational harm and steal data.

The insider threat to corporate information systems never goes away. It remains consistently high and is increasing. New technology, including the implementation of cloud and big data projects, adds to data theft and loss opportunities. Regulatory and compliance issues, alongside the requirement for companies to protect themselves from brand damage and revenue losses, drive the requirement to provide better protection against "insiders" and those who comprise trusted employees.

OVERVIEW

The *2014 Vormetric Insider Threat Report* focuses on Europe's three largest technology and business markets – France, Germany, and the United Kingdom (UK). Across these three markets 540 senior IT professionals and business managers, over 80% from mid-to-large enterprise organizations, were interviewed on the impact that insider threats have on their organizations and on how prepared they are to deal with insider activity. The survey results show that despite industry-wide initiatives, detecting and remediating security breaches continues to get harder and very few organizations feel safe from insider attacks.

IT security teams make best use of the tools at their disposal, but need to do more as the number and scale of losses continue unabated. They are invariably hindered by point-based protection solutions, old fragmented security technology and strategies that struggle to keep up with the ever-changing threat landscape.

> "As large-scale breaches, APTs, and Snowden-related discussions dominate the news cycle, it is clear that insider threats are among the most prominent IT security issues facing organizations today, a feeling which is reflected within the findings of our report."

Servers and databases continue to hold the bulk of each organizations structured and unstructured data assets and, as shown in the examples below, are responsible for the vast majority of high-profile data breaches. Controlling mobile devices is a concern because of their ever-growing use within operational environments, but the main issues when related to inside threat activity is how these devices are used as the source of access to data held in corporate servers and data centers.

There are countless examples of insider data thefts and compromised users, ranging from local to international levels. Recent European cases include: March 2014, when the UKs fourth largest Supermarket group Morrisons become the victim of an insider attack. The theft involved the bank account details of around 100,000 staff being published on line. As is often the case, the retailer's own security systems did not find that their sensitive data had been compromised. The company was alerted by a third party, in this case the local newspaper which had anonymously been sent a file containing the sensitive employee information. The leak is described as a serious theft of data, and the company is urgently reviewing its internal data security position. Initial Investigations showed that the theft of sensitive employee data was not the result of an external attack. The company is now working with industry experts and the police, the source of the data breach has been identified, and an employee has been arrested.

BREACHED MORRISONS VODAFONE TARGET

Late 2013, Vodafone Germany confirmed that an attacker with insider knowledge had stolen the personal data of two million of its customers from a server located in Germany. Customer name and address and date-of-birth information and some bank account details were taken. In this case Vodafone identified the perpetrator as an insider with knowledge of its most sensitive internal systems. Vodafone claims to have up-to-date and well maintained security systems, but still fell victim to what the company described as "a highly complex attack that was conducted with inside knowledge of its most secure internal systems." In this case only German customers were affected by the breach and the company took all necessary steps to stop the attack as soon as it was identified and informed the relevant German authorities.

Beyond Europe, the Minneapolis-based US retailer Target's data breach is set to become the worst ever. Latest information suggests that names, postal addresses, phone numbers, and email details for upwards of 70 million people have been stolen. This follows the initial disclosure in December 2013 when Target admitted that the payment card details of 40 million consumers had been put at risk. Industry experts believe that the breach was perpetrated by an external attacker using valid access credentials obtained from a Target business partner/service provider. This in itself shows a lack of adequate access control facilities; third party credentials should not offer the levels of access needed to steal highly sensitive company information.

Target was certified as meeting the standard for payment card industry compliance, but being able to tick the compliance boxes does not guarantee a secure environment. Also, apologies and promises from the CEO that customers will not be financially disadvantaged are no longer acceptable, as is already being proved by the lawsuits filed by customers and business partners. The impact and total costs on the organization will be difficult to bear and long-lasting. Direct costs already exceed $60 million, the organization's profits dropped almost 50% in the immediate aftermath, its public reputation has been severely damaged and there are likely to be longstanding business consequences. This breach, coming as it does so soon after Snowden and other high-profile insider attacks, provides clear justification for organizations to look to improve their user access, monitoring, and data protection controls.

SUMMARY OF FINDINGS

Below are a number of the key findings from the interviews completed:

- A mere 9% of organizations felt safe from attack, whereas more than a quarter - 26% felt vulnerable.
- Close to half the respondents (46%) felt that insider threats are more difficult to detect than they were in 2012. A further 36% felt that things had not become any easier.
- Compliance is the key driver for European organizations to spend more on insider threat protection (40% of respondents), followed by the requirements/expectations of customers (30%), and awareness of advanced persistent threats (30%).
- 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 and then third party contractors, and then IT administrators and other IT staff.
- The main problem areas identified by organizations involve the need to protect more IT assets - the distributed nature of those assets, the use being made of cloud-based services, big data initiatives, and mobile devices, and the growing number of users that need to be monitored and managed.
- Major cloud concerns revolve around lack of visibility into service provider security, the potential for unauthorized third party access, and lack of control over where data is held.
- Nervousness over big data initiatives was apparent, mainly due to security concerns over what is still seen by many as new and unproven technology.
- Data encryption and key management, followed by identity and access management, and then network protection, and traditional anti-malware tools were seen as the most important deterrents against insider threats

> “Organizations remain vulnerable and need to do more to deal with insider threats that range from misuse of resources to targeted and malicious APT threats … what is missing is an integrated platform approach to user and data protection.”

VERY FEW Organizations FEEL SAFE FROM INSIDER ATTACKS

When asked how safe they felt their organizations were to the threat of insider attacks, a mere 9% of European IT managers and security professionals who responded to the 2014 Vormetric Insider Threat Report said that their organizations were safe from attack, whereas 26% said they felt vulnerable.

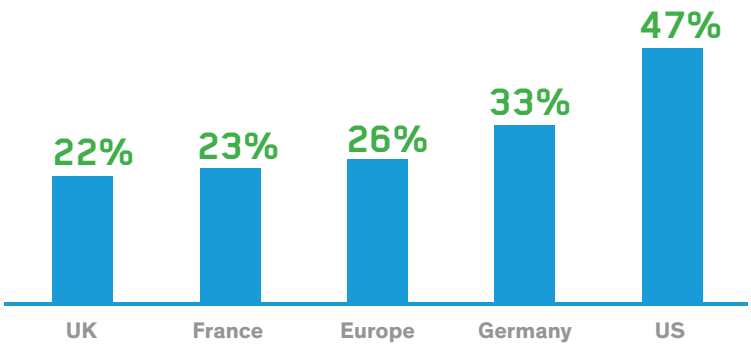
The survey confirmed that a significant proportion of IT security budgets are spent on data protection, access control, and user monitoring technology. Nevertheless, targeted malware attacks – advanced persistent threats (APTs) etc. have the capabilities to compromise user credentials, avoid detection when attacks are launched, and steal data over an extended period without detection. All of which is taking place alongside the more traditional view of insider activity, which continues to be represented by disaffected employees looking to steal corporate information for their own purposes.

Therefore, it is not surprising to find that IT and security professionals feel under pressure from insider threats that emanate from a wide variety of sources including employees, third party business partners, contractors, service providers, and external attackers deploying malicious software that makes use of legitimate credentials to access corporate data.

Figure 1 below identifies the European position on vulnerability to insider attacks. It shows that the European country feeling most vulnerable to the threat was Germany at 33%, with France and the UK both returning figures of 23% and 22% respectively. This contrasted to an earlier US survey from September 2013 which showed that a massive 47% of US respondents felt vulnerable to insider attacks.

> “Almost half of European organizations believe that insider threats are now more difficult to detect, with senior IT managers being very worried about the things their own users can do with corporate data. This risk is compounded by the threat by cyber attacks that are targeting user accounts.”

Figure 1: **The percentage of organizations that felt vulnerable to an insider attack**



INSIDER THREATS

INSIDER THREATS ARE MORE DIFFICULT TO DETECT– SENIOR MANAGEMENT IS RIGHT TO BE WORRIED

Senior IT and business managers are very worried about the things their users can do with corporate data, activities that often do not show up on their security radar and are likely to go undetected. They have significant concerns about, everyday users, third party business partners, contractors, and service providers with their shared access rights. Close to half of European respondents (46%), felt that insider threats are more difficult to detect than in previous times, and significantly, given the extended nature of the insider threat problem, a further 36% felt that things had not become any easier.

A significant proportion of European respondents felt that insider threats were more difficult to detect, with some variations between the different country-level responses. Within the surveyed markets the highest levels of concern were expressed by French respondents at 53%, the middle ground was occupied by the Germans at 47% and the UK had the lowest response rate at 38%

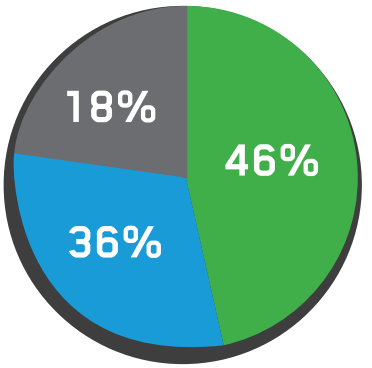
By comparison, the separate US survey had 54% of US organizations saying that insider threats were harder to detect.

Figure 3: **The top 4 reasons why insider threats are more difficult to detect**

1. The growing volume of network activity
2. The growing use of cloud computing
3. There are more employees, contractors, business partners, etc. with access to our network
4. We have more IT assets on the network which makes security more difficult

For European organizations the reasons why security professionals felt insider threats were more difficult to detect were quite widely spread and included the growing number and range of IT assets on their networks that needed to be protected, the associated volumes of network activity and traffic, and the increasing numbers of employees, - contractors, business partners etc. that now demand access. Other important issues included the growing use of cloud computing services and the perceived lack of internal control that cloud-based services bring, plus increasing levels of mobility within the workforce, and the associated growth in mobile device usage and bring your own device (BYOD) issues. Figure 3 above lists the top four reasons why respondents thought insider threats were more difficult to detect.

Figure 2: **How European organizations view the difficulty in identifying insider threats**



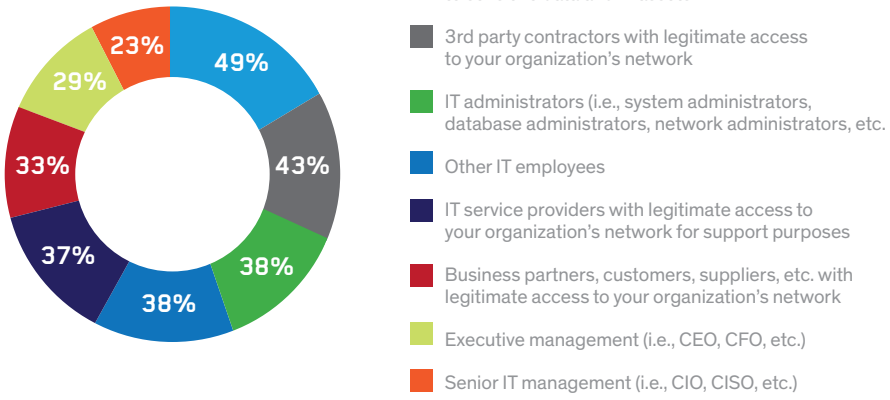
- Insider threats are more difficult to detect/prevent today than they were in 2012
- Insider threats are no easier to detect/prevent than they were in 2012
- Insider threats are easier to detect/prevent today than they were in 2012

EMPLOYEES AND THEIR USE OF OPERATIONAL ASSETS IS BECOMING A MAJOR CONCERN

When European organizations were asked who posed the biggest internal threat to corporate data, almost half of respondents said everyday users; the next largest group was third party service providers, and then IT administrators and other IT staff. The top issues raised (49% of respondents) were about how best to keep tabs on and control users who have legitimate access to sensitive company data and IT assets. A significant level of concern (43% of respondents) was targeted at third party business partners and contractors who also have legitimate access requirements to organizational networks. The third and fourth major groups that came in for scrutiny from more than a third of respondents (38%) was the range of system, database, and network administrators, and other IT staff who have enhanced access rights to operational systems.

> "Only **9%** of organizations feel safe from attack."

Figure 4: **The percentage figure for user groups posing the highest level insider threats**



Country level comparisons showed France and the UK topping the list and reporting the highest levels of concern about everyday users (52%) and Germany showing a significantly lower 46% response rate.

Corporate insider threat evidence confirms that these are legitimate concerns – In the case of Vodafone in Germany and Morrisons in the UK the source of the breach was traced back to employees and in the US the high-profile breach at the retailer Target had a third party supplier/business partner as the source of intrusion from an external attacker.

REGULATORY COMPLIANCE

The main areas of concern identified involved the need to protect more IT assets - the distributed nature of those assets and the people who use them. The use being made by organizations of cloud-based services and mobile devices and the growing number of users who need to be monitored and managed all builds upon the levels of concern over everyday access.

Another area causing worry was that of privileged user management. Whilst in general being positioned as feeling less vulnerable than their US counterparts, Europeans had greater anxieties around the theft of privileged user credentials, compromised credentials, and abuse of access rights. US organizations agreed that privileged user access abuse was important, but were also worried about other employees and physical theft.

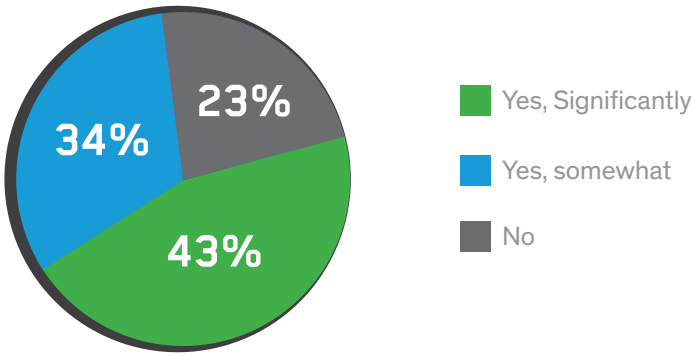
Top European priorities for dealing with privileged users included: the theft of privileged user credentials – 42% of respondents, credentials compromised by cyber-attack - 39%, and abuse of privileged user access rights – also 39%. For the US the top three issues reported were: the abuse of privileged user access rights – 63% of respondents, abuse of access rights by other employees - 61%, and the theft of physical devices containing data – 58%.

In response to known privileged user control issues European organizations are focusing their attention on rule-based separation of duty controls at the privileged user level – 73% of respondents; on maintaining a central point of control over privileged users, their accounts, and their access rights –72%; and protecting hard-coded passwords, embedded credentials, and vulnerable encryption keys – 65%.

REGULATORY COMPLIANCE IS FORCING EUROPEAN Organizations TO SPEND MORE ON INSIDER THREAT PROTECTION

As shown in Figure 5 European organizations are planning to make increases in their information security budgets over the next 12 months because of insider threats. Two thirds plan to increase their security budgets and of the overall respondents 23% were looking to achieve significant budget increases as a direct consequence of insider threats.

Figure 5: **The percentage of organizations planning security budget increases as a result of insider attacks**



Within the headline European markets German respondents - 69%, were the most likely to increase their budgets in the coming year. France came in at 66% and the UK had the lowest response levels at 63%.

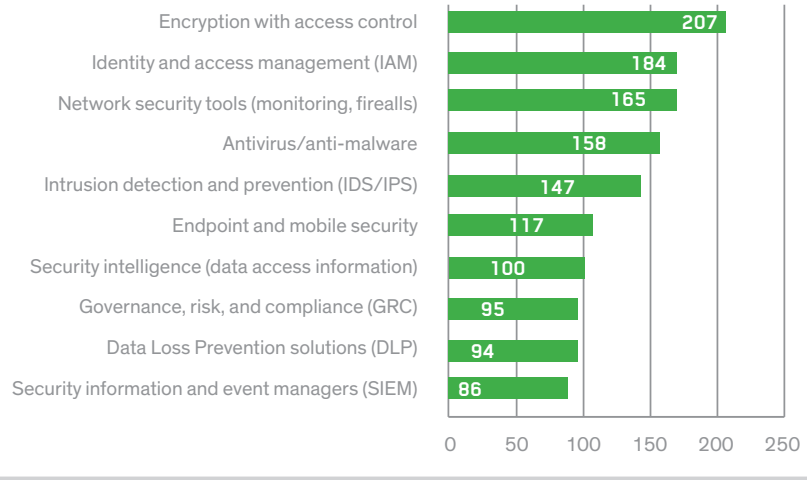
European organizations reported that regulatory compliance was the biggest factor making them inclined to spend more on insider threat protection technology. Key compliance regulations that have an impact on user and data protection issues within

the European Union (EU) include the European data protection act which impacts all member states. In mid-March 2014 European politicians voted overwhelmingly to add further new data protection laws to safeguard citizen data adding further compliance pressure to EU organizations. For France there is the French Data protection Act, in Germany the Federal Data Protection Act, and for the UK the UK Data Protection Act. There are also active Freedom of Information Acts across member states and Audit and Company Reporting Directives, often referred to as EuroSOX. Industry specific regulations are plentiful and include Basel III (or the Third Basel Accord) and the Markets in Financial Instruments Directive (MiFiD) in the banking and financial services sectors. There are also across industry regulations that extend beyond Europe, the most high profile of which is the Payment Card Industry Data Security Standard (PCI DSS). PCI DSS touches a wide range of organizations, industry verticals, and geographies.

The survey identified that regulatory compliance was seen by 40% of respondents as being the key force for change when European organizations are looking to justify spending more on insider threat protection. This far outstripped other drivers for increased spend including the next most common which responded to the requirements and expectations of customers (30%), and the awareness of advanced persistent threats (also 30%).

> “US organizations, at **54%**, were less prepared to spend money to address the problem than Europeans at **66%**.”

Figure 6: **Security controls used to protect against insider attacks by number of respondents**



PROTECTION

MAINTAINING GOOD QUALITY INSIDER THREAT PROTECTION REMAINS A KEY OPERATIONAL IMPERATIVE

The survey results showed that European organizations feel more comfortable with their overall security position than their US counterparts, but still have concerns about doing better. Traditional data protection, including the use of signature-based anti-malware products continue to be thought of as the most effective means of addressing insider threats. Arguably this represents a misalignment between the data protection and user access vulnerabilities that exist within organizations and the security solutions European organizations put in place to provide a broad-brush protection strategy against everyday malware attacks, but without the capability to deal with targeted and advanced attacks that bypass traditional defenses.

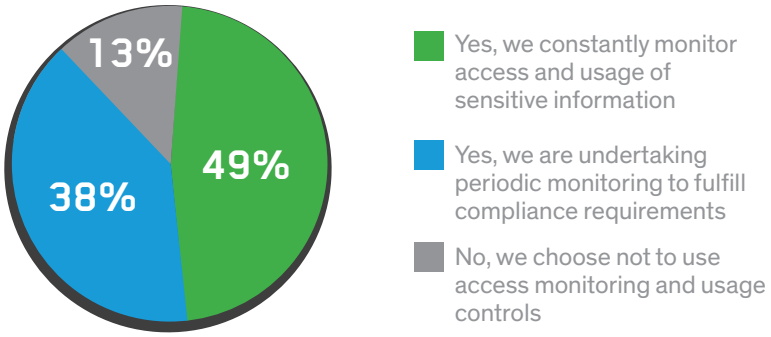
The top four groups of security controls that European organizations describe as being the most important for protecting data against insider attacks were: Encryption and access control – 39%; identity and access management (IAM) at 34%, network security tools, 31%, and antivirus/ anti-malware protection at 30%.

The results suggest that European security spending patterns do not always match their core protection requirements. This is especially the case with insider threat protection because of the constantly changing nature of the threat. It also offers an interesting comparison between the European markets and the seemingly more nervous/cautious US sector.

From a positive perspective the data protection priorities identified by European organizations look to be well directed as there appears to be good levels of usage and confidence in the protection provided. 68% of European organizations encrypt their sensitive data (i.e., company confidential data, regulated data, Intellectual Property (IP), customer data, etc.). US responses from the earlier survey showed very similar levels of usage at 69%.

> “Both US and European organizations admit that compliance is the primary driver for spending increases.”

Figure 7: **Monitoring of sensitive information resources**

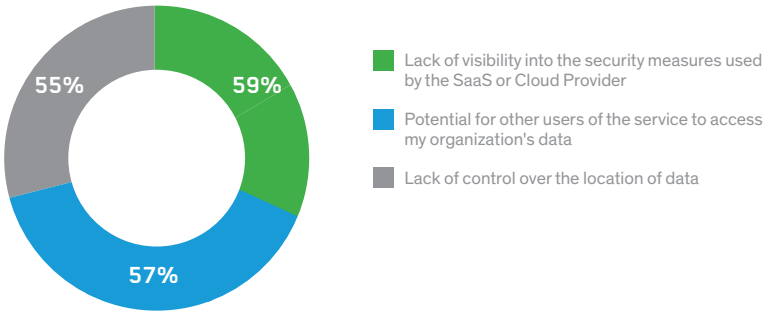


68% of European organizations also claim that they enforce fine-grained access controls by creating usage rules for individual systems, applications, and documents that are intended to protect their most sensitive data. This compared to a 57% response rate for US organizations. One important area that was out of line when comparing Europe with the US was the use of monitoring facilities. Close to 50% of European organizations reported that they constantly monitor access to sensitive information. This compared favorably to the US where only 29% of organizations undertake ongoing monitoring.

Over and above these figures a further 38% of European organizations commit to periodic monitoring. The top reasons stated for not maintaining a constant monitoring approach by European organizations was: it is too costly to fully monitor sensitive data access and usage activities (68%), we don't have enough security staff members to fully monitor and analyse sensitive data access and usage activities (64%), and we limit monitoring to specific sensitive data access and usage in order to meet national and industry regulatory compliance demands (62%).

> "In summary, organizations remain vulnerable and need to do more to deal with insider threats that range from misuse of resources to targeted and malicious APT threats."

Figure 8: **Percentage responses for the top three cloud and SaaS usage concerns**



CLOUD AND BIG DATA

ONGOING CONCERNS FOR USER AND DATA PROTECTION FOCUS ON THE USE OF NEW TECHNOLOGY

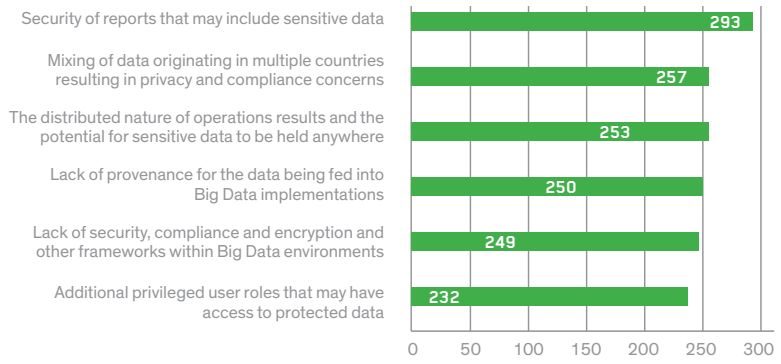
Respondents to the survey said that going forward cloud and big data are major areas of concern with regard to insider threats. Specific issues around cloud and SaaS include a lack of visibility in service provider security facilities – 59% of respondents said this. The potential for unauthorized third party access worried 57%, and lack of control over where data is held; mixing of data from different regions and countries and holding data beyond geographic borders, concerned 55% of European organizations.

Developments that would improve cloud take up included: better service level commitments and liability terms for a data breach caused by the service provider or another customer of the cloud provider – 59%. Encryption of the organization's SaaS/cloud data with local control maintained over encryption keys - 57%, and detailed physical and IT architectural implementation information being made available – also 57%.

For big data initiatives there were a mixture of views expressed which highlighted nervousness about making use of what is still new technology and the overall benefits that can be gained. For example, from a security point of view more than a third of respondents (36%) saw the technology as both a threat and an opportunity. A further 26% recognized only the threat side.

These responses fit in with general industry trends where the most advanced organizations are grabbing the big data opportunity and claiming successful outcomes from its use. This includes the ability to deliver and improve security threat intelligence on insider activities, operate risk-based security controls, and as a result improve the risk profile of their organizations. Others are adopting a wait and see approach as they struggle to see how they can deliver value from using the technology.

Figure 9: **Number of respondents with concerns about big data issues**



As shown in Figure 9 survey respondents were concerned about the protection of big data reports holding sensitive information - 69% of respondents, mixing data from different countries that could result in privacy and compliance violations 60%, and the distributed nature of operations resulting in the potential for sensitive data to be held anywhere across the implementation 59%.

Most respondents recognized the link between big data projects and security, very few, only 2%, did not make the connection. However, a further 10% who recognized the links were struggling to know where the connections lay and the necessary follow up actions that would be needed.

Organizations ARE BEING HINDERED RATHER THAN HELPED BY EXISTING SECURITY PRODUCTS AND STRATEGIES

Only 9% of organizations that responded to the 2014 Vormetric European insider threat survey felt safe from attack, and more than a quarter felt that their organizations were vulnerable. Almost half felt that insider threats are now more difficult to detect than was previously the case. This level of recognition was widespread across all European markets, which confirms the requirement to increase spending on insider protection solutions. It is also a damming indictment of legacy, point-based security products that no longer provide the levels of protection and scalability needed to deliver effective data and insider threat protection.

The theme of ongoing concern continued when industry experts were asked about who posed the biggest internal threat to corporate data. Half of all respondents said that everyday users caused the most problems. There were also serious issues with service providers, third party contractors, and IT administrators and other IT staff. The Insider Treat Survey identifies that European organizations recognize the need for better insider threat protection, but still need to do more to improve their risk position and make improved use of protection solutions.

In summary organizations remain vulnerable and need to do more to deal with insider threats that range from misuse of resources to targeted and malicious APT threats. They are often hindered rather than helped by the fragmented security solutions that have been deployed to protect valuable data assets. What is required and, due to legacy and cost-of-replacement issues, what is often missing is an integrated platform approach to user and data protection.

Rather than spending more time and effort maintaining older security products, better value would be provided through targeted replacement, integration, and control. Areas where improvements ought to be made include: putting in place a central management approach to provide a single-pain-of-glass that offers a concentrated and consistent view of each organizations risk profile and security position. Deliver on the multiple protection requirements for data at rest and data on the move. Provide encryption and integrated key management for sensitive data assets, access control to ensure that only authorized users can get in, and a security intelligence layer that identifies new threats, highlights security deficiencies, monitors user interactions, and operates in line with the risk profile of the organization.

“Rather than spending more time and effort maintaining older security products, better value would be provided through targeted replacement, integration, and control.”

OVUM RESEARCH

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.

In his position as principal analyst, Andrew has worked to promote the delivery of research on business- and user-focused security systems and written papers on a wide range of business- and technology-related areas. Andrew has been the lead author on a number of major security reports on subjects including identity and access management, security management and, most recently, information security, data loss prevention, and web security. He is also a regular speaker at Ovum strategy briefings and master classes, and has undertaken external speaking engagements.

Andrew has worked in the IT industry for over 30 years and, before joining Ovum, was employed as an operations manager and business analyst for an internationally known high street retail service provider. He was responsible for the management and implementation of the company's EPOS systems and for the selection, deployment, management, and operation of its supporting business systems. Prior to this, Andrew worked as a systems analyst and project manager for a large financial services organisation.

ABOUT VORMETRIC

Vormetric (@Vormetric) is the industry leader in data security solutions that span physical, virtual and cloud environments. Vormetric helps over 1300 customers, including 17 of the Fortune 25 and many of the world's most security conscious government organizations, to meet compliance requirements and protect what matters —their sensitive data —from both internal and external threats. The company's scalable solution protects any file, any database and any application — within enterprise data center, cloud, big data environments — with a high performance, market-leading Vormetric Data Security Platform that incorporates application transparent encryption, access controls and security intelligence. Vormetric – because data can't defend itself.

OVUM'S KNOWLEDGE CENTERS

Ovum's Knowledge Centers are new premium services offering the entire suite of Ovum information in fully interactive formats. To find out more about Knowledge Centers and our research, contact us:

Ovum Europe
Mortimer House
37-41 Mortimer Street
London W1T 3JH, UK
+44 20 7551 9000
crmgroup@ovum.com

Ovum Australia
Level 5, 459 Little Collins Street
Melbourne, VIC 3000
Australia
+61 3 9601 6700

Ovum New York
100 Wall Street, 9th Floor
New York
NY 10005, USA
+1 212 686 7400

PUT VORMETRIC TO WORK FOR YOU

To learn more about how Vormetric can protect your valuable data where it matters, visit Vormetric.com or contact us at info@vormetric.com.

Global Headquarters
2545 N. 1st Street, San Jose, CA 95131
Tel: +1.888.267.3732
Fax: +1.408.844.8638
www.vormetric.com

EMEA Headquarters
200 Brook Drive
Green Park, Reading, RG2 6UB
United Kingdom
Tel: +44.118.949.7711
Fax: +44.118.949.7001

APAC Headquarters
27F, Trade Tower, 159-1
Samsung-dong,
Gangnam-gu, Seoul. (135-729)
Tel: +82.2.6007.2662
www.vormetric.co.kr