Ovum research shows privileged users are highest risk to data for 54 percent of IT Decision Makers (ITDMs) in European organisations

Survey also reveals that 40 percent of ITDMs in UK firms have encountered a data breach or failed a compliance audit in the last 12 months

LONDON – June 17, 2015 – Vormetric, a leader in enterprise data security for physical, virtual, big data, public, private and hybrid cloud environments, today announced the European findings of its 2015 'Insider Threat' survey. The survey was conducted online on their behalf by Harris Poll in fall 2014 among 818 enterprise IT decision makers (ITDMs) in various countries, including 204 in the UK and Germany. Analysis and research into the results was performed by analyst firm Ovum. The research uncovered that 54 percent of the German and UK respondents believe that privileged users (system administrators, database administrators, network administrators, etc.) pose the biggest risk to their organisation – a substantial step up from 38 percent in last year's 2014 Vormetric Insider Threat Report – European Edition. Only 13 percent said that their organisations were not at all vulnerable to insider threats – a slight improvement on the 9 percent that said they felt safe last year, but still leaving 87 percent feeling vulnerable.

ClickToTweet: Most Dangerous Insiders for U.K. and Germany – Privileged Users #2015InsiderThreat http://bit.ly/1S5Z1se

The insider threat is multi-faceted and does not only relate to the deliberate theft of data. If systems are not appropriately secured, employees can also inadvertently put sensitive company information at risk. In addition, modern cyber attacks frequently rely on hijacking log-in credentials of unsuspecting users, often targeting 'privileged users' who have the greatest levels of network access. Cyber criminals then use these credentials to log-in and appear as legitimate users so that they can steal data undetected.

"With the research showing that more than half of European organisations now classify privileged users as posing the highest risk to their data, there is clearly a growing need to manage and secure what these users can do on the corporate network," said Andrew Kellett, Principal Analyst Infrastructure Solutions at Ovum. "Although most organisations will have already realised that this type of user account needs to be implemented and overseen with far greater care than they perhaps once were, there remains a variety of technical challenges to overcoming the risk they pose – not least because this type of user account is usually used to perform essential network maintenance and administration procedures that cannot be interfered with."

The key findings of the Ovum survey include:

- 54 percent of IT decision-makers in European enterprises placed privileged users as the highest risk group when considering their data protection requirements. Contractors, service providers, and business partners were also seen as possible risks.

- Although 51 percent of UK respondents and 44 percent of German respondents are increasing spending to offset threats to data, this lags behind 62 percent in the US
- Only 13 percent of IT decision-makers in European enterprises identified that they were not at all vulnerable to insider threats
- 40 percent of UK respondents reported that their organizations have encountered a data breach or failed a compliance audit in the last 12 months
- Compliance was identified by respondents as still the top reason for securing sensitive data in Europe (56 percent), but reputation and brand protection are close behind (54 percent)
- Top European IT security spending priorities identified by respondents were protection of Intellectual Property (52 percent) and preventing a data breach incident (48 percent)

"With 40 percent of UK firms either being breached or failing a compliance audit in the last year, we are clearly a long way from anything approaching adequate data security," said Alan Kessler, CEO of Vormetric. "Part of the problem is an overemphasis on compliance. With insider related attacks changing by the hour, you can think of today's compliance mandates as requiring organizations to use the weapons of yesterday to fight today's battles. Given this reality, encryption and access controls are increasingly the weapons of choice today to protect organizations critical data."

To find out more about the risks posed by insider threats and for detailed findings from Ovum, visit the Vormetric website: http://www.vormetric.com/campaigns/insiderthreat/2015/eu

Source/Methodology – 2015 Vormetric Insider Threat Report

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.

Source/Methodology - 2014 Vormetric Insider Threat Report

The 2014 Vormetric Insider Threat Report – European Edition research was conducted by telephone by Ovum Research on behalf of Vormetric from 6 January through 7 February of 2014, with analysis also from Ovum. The report focused 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 (180 from each country), over 80% from mid-to-large enterprise organisations, were interviewed on the impact that insider threats have on their organisations and on how prepared they are to deal with insider activity.

About Vormetric

A leader in data security solutions, Vormetric (@Vormetric) protects data-at-rest in physical, virtual, big data and cloud environments. Trusted by businesses and governments for over a decade, Vormetric's Data Security Platform secures the data of more than 1,500 global enterprises—including 17 of the Fortune 30. With Vormetric, a single infrastructure and

management environment protects data wherever it resides with file, volume and cloud storage encryption, tokenization with dynamic data masking, field-level application encryption, sophisticated access control policies, third party and integrated encryption key management.

Media Contacts:

Vormetric UK/EMEA

Jonathan Mathias / Kasia Murphy
Johnson King
+44 (0)20 7401 7968
VormetricTeam@johnsonking.co.uk

# # #