Vormetric's 2015 Insider Threat Report: 93% of U.S. Organizations Polled Vulnerable to Insider Threats

Report Follows Record Year of Data Breaches; Reveals Spending Priorities, Security Risks

SAN JOSE, Calif. – Jan. 21, 2015 –Vormetric, a leader in enterprise data security for physical, big data, public, private and hybrid cloud environments, today announced the results of its 2015 Insider Threat Report (ITR), conducted online on their behalf by Harris Poll and in conjunction with analyst firm Ovum in fall 2014 among 818 IT decision makers in various countries, including 408 in the United States. The report details striking findings around how U.S. and international enterprises perceive security threats, the types of employees considered most dangerous, environments at the greatest risk for data loss and the steps organizations are taking to secure data.

Click to Tweet: 93% of U.S. organizations polled respond to being vulnerable to insider threats. See the #2015InsiderThreat report http://bit.ly/1HBvHVg

In the past few years, rapid growth in the volume of sensitive information combined with new technologies has chipped away at the effectiveness of traditional endpoint protections and network perimeter security. In tandem come warranted concerns about the number and types of employees who have access to sensitive data. While Edward Snowden may be viewed as the "insider threat" poster child, not all employees have malicious intentions. Simply by having access, privileged insiders may unwittingly put data at risk – or be used by an outside actor as a conduit for siphoning data.

The 2015 ITR statistics from U.S. organizations polled are sobering:

- 93% of U.S. respondents said their organizations were somewhat or more vulnerable to insider threats
- 59% of U.S. respondents believe privileged users pose the most threat to their organization
- Preventing a data breach is the highest or second highest priority for IT security spending for 54% of respondents' organizations
- 46% of U.S. respondents believe cloud environments are at the greatest risk for loss of sensitive data in their organization, yet 47% believe databases have the greatest amount of sensitive data at risk
- 44% of U.S. respondents say their organization had experienced a data breach or failed a compliance audit in the last year
- 34% of U.S. respondents say their organizations are protecting sensitive data because of a breach at a partner or a competitor

"Vormetric's 2015 Insider Threat report indicates nearly all of U.S. organizations polled perceive a security vacuum and feel quite threatened," said Andrew Kellett, lead analyst for Ovum and one of the architects behind the report. "As much as we may have hoped to believe it, the Edward Snowden affair was not our data security pinnacle. According to the report, almost half of the U.S. organizations polled experienced a data breach or failed a compliance audit in the past year – which tells us the situation has probably gotten more complicated."

In 2014, the U.S. saw some of the worst data breaches in recent memory with household names Sony, Home Depot, J.P. Morgan Chase and Supervalu experiencing massive financial and reputational blows due to cyberattacks. According to the Identity Theft Resource Center, over 700 data breaches occurred in 2014 alone, up from 614 in 2013. With these breaches have also come associated legal ramifications and public soul-searching by senior management and board level executives about where to place the blame.

"As the past year demonstrates, these threats are real and need to be addressed," said Alan Kessler, CEO for Vormetric. "Organizations wishing to protect themselves must do more than take a data-centric approach; they must take a data-first approach. Although we are heartened that 92% of organizations plan to maintain or increase their security spending in the coming year, our larger concern is about how they plan to spend that money. The results indicate there is still disagreement about where corporate data which is most at risk actually resides. Our experience, observations and conversations with customers have taught us that even if the situation isn't entirely black and white, organizations' use of encryption, access controls and data access monitoring greatly reduce their risk and exposure."

Click to Tweet: 44% of U.S. enterprises polled had a data breach or failed a compliance audit in the last year #2015InsiderThreat http://bit.ly/1HBvHVg

U.S. attacks have received the lion's share of attention due to their size and high profiles, but worries about data security are not limited to America. According to the report:

- Despite a rash of data breaches among organizations that were considered compliant, 59% of global respondents found compliance standards to be "very" to "extremely" effective
- 55% of global respondents believe privileged users are the biggest threat. In the U.S., that number is slightly higher, with 59% citing privileged users. And while 46% of U.S. respondents believe partners with internal access pose the second-highest threat, global results point the finger at contractors and service providers
- The top 3 reasons for protecting sensitive data among those polled globally are as follows:
    - Implementing best practices (38%)
    - Reputation and brand protection (51%)
    - Compliance requirements (50%)
- 54% of global respondents will increase security spending to offset the threat in the coming year

The current global reality is that more and more data is being stored in various repositories all over the world and more and more players– such as third party service providers and contractors – are being thrown into the mix. Although respondents generally believe compliance standards to be effective, these standards run the gamut from weak to very stringent. Companies can and should go above and beyond compliance and take common sense measures to protect themselves, including:

- Implementing encryption and access controls
- Taking careful stock of which employees should have access to data
- Diligently monitoring data access activities to get ahead of infiltrations before they snowball

The survey results and research report are available from Vormetric and can be found here.

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.

Quote Sheet: 2015 Vormetric Insider Threat Report Partners

Rackspace

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

Couchbase

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

Financial Services Information Sharing and Analysis Center (FS-ISAC)

"As part of its mission to provide cyber and physical threat intelligence, analysis and sharing, FS-ISAC also partners with respected thought leaders to pro-actively deliver compelling research and trend reports," said Eric Guerrino, with the FS-ISAC. "The topic of insider threats has long been an area of focus and concern. Cyber threats that compromise insider credentials and traditional insider risks have played a part in many of the recent data breaches around the world. This report highlights how organizations are recognizing the need to protect data from this threat, and provides relevant information that can be immediately useful to our members and to the financial sector overall."

FishNet Security

"At FishNet Security we help organizations deliver information security excellence," said Rich Fennessy, CEO of FishNet Security. "The report outlines how vulnerable enterprises feel today, and emphasizes the need for trusted partners that can help them safely take advantage of cloud, big data, IoT and mobile technologies while protecting their organizations from both traditional insider threats, and the compromise of the insider accounts that are so often targeted by hackers today."

AZM

"As a leader in IT security for servers, thin clients systems and cloud environments, we see this report as a strong resource for global enterprises, highlighting the vulnerabilities of their infrastructure and providing guidance on how to keep their organizations secure and reduce the load of their internal staffs involved in security, by securing their own data, as well as their client's data" said Shumon Okada, CEO, AZM.

Carahsoft

"The latest wave of cyber attacks is consistently compromising insider accounts to gain access to data, and malicious insiders like Edward Snowden and Bradley Manning also continue to present a threat to government," said Michael Shrader, Vice President of Intelligence and Innovative Solutions at Carahsoft, which serves as Vormetric's master government aggregator. "Cloud computing, mobile, and big data

environments only add to the risks. The 2015 Vormetric Insider Threat Report consistently highlights the vulnerability of organizations to these threats as well as the need for trusted partners that can help federal, state, and local government agencies implement the latest technologies to best serve their constituents and protect confidential data as they do so."

Cloud Security Alliance

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

FieldFisher

"Privacy concerns and the legal consequences of loss of protected data are clearly increasing globally," said Phil Lee with Fieldfisher. "This report finds that all organizations are at risk, with 40% of respondents having suffered a data breach or failed a privacy and security compliance audit in the last year. Organizations that haven't already done so need to make sure they achieve the minimum compliance standards that apply across the jurisdictions in which they operate, and even look beyond those in order to prevent the same kind of high profile breaches that Sony, Target and other organizations have suffered."

M.Tech

"As a best-of-breed security, network and performance solutions provider, the evidence in the report highlights what we see every day with our customers – Enterprises are struggling to adapt to enhanced threats and new technologies alike," said James Wong, Regional Director of M.Tech. "The report highlights that the ASEAN region had the highest rate of organizations that reported they had encountered a data breach or failed a compliance audit in the last year worldwide (48%). With this in mind, the guidance it includes about how organizations can improve data security to prevent breaches and meet compliance requirements is very timely."

OASIS

"As a non-profit consortium dedicated to driving the development and adoption of open standards, we are deeply interested in supporting the safe adoption of cloud, IoT, big data and other new technologies," said Laurent Liscia, CEO at OASIS. "The 2015 Vormetric Insider Threat Report clearly shows the need for organizations to feel secure in their use of sensitive data within these environments, as well as their everyday operations, and suggests the need for standards that support this goal."

Raber+Märcker

"As a leader in IT Security for Germany-based enterprises, our customers depend on us to help secure their IT environments, and to help them use new technologies like cloud computing both safely and in compliance with regulations," said Harry Zorn with Raber-Märcker. "The 2015 Vormetric Insider Threat Report clearly identifies the level of vulnerability that enterprises feel both globally and here in Germany, as well as providing strong guidance on creating the controls that will safeguard data regardless of where it is stored."