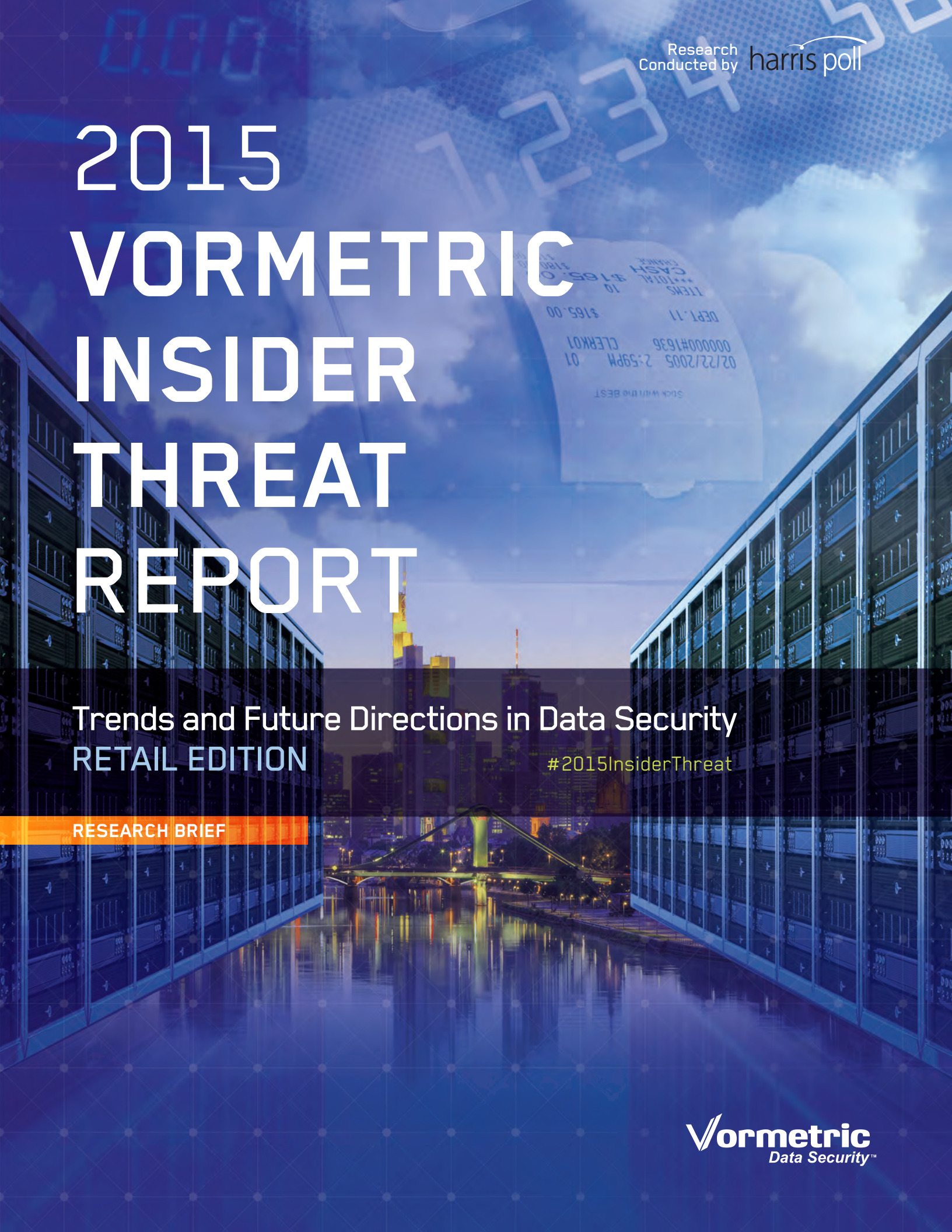


Research Conducted by harris poll

2015 VORMETRIC INSIDER THREAT REPORT

Trends and Future Directions in Data Security

RETAIL EDITION

#2015InsiderThreat

RESEARCH BRIEF

Vormetric Data Security™

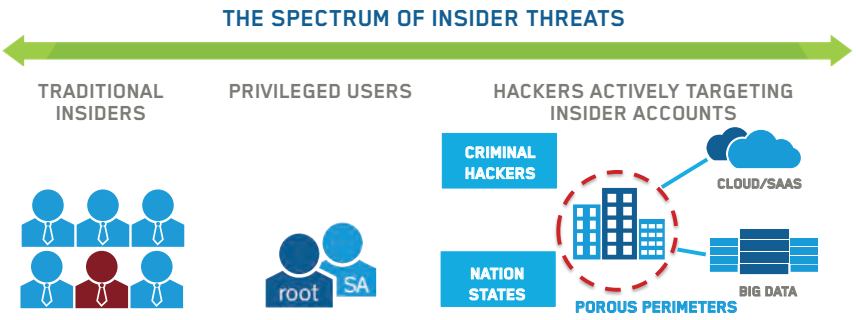
RETAIL CUSTOMERS AT RISK

ABOUT THIS RESEARCH BRIEF

This Research Brief highlights the results collected online by Harris Poll from 102 IT decision makers in U.S. retail enterprises in the Fall of 2014. U.S. results are compared, where applicable, to findings among IT decision makers in other U.S. enterprises, as well as those in other countries.

INSIDER THREATS–NO LONGER JUST TYPICAL EMPLOYEES

In the past, insider threats resulted mainly from employees with access to financial data or other secret and sensitive information. That's no longer the case today. Today, employees with legitimate access, service providers or contractors that maintain infrastructure and privileged users are all possible actors, and potential attack vectors when their credentials are compromised.



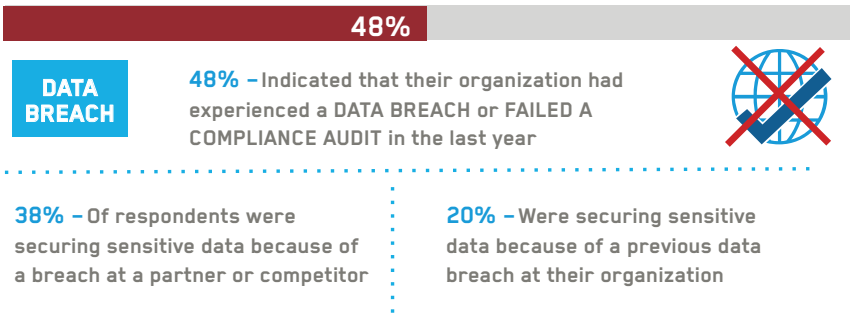
Criminal hackers continue to be retailers' greatest worry, and nearly every retail data breach has included a compromise of a privileged user account or a privileged account at a partner with access to the retailers' network. In the U.S., where less vulnerable "pin and chip" technology for credit card transactions is rarely deployed today, retailers' "Achilles Heel" has been conventional magnetic stripe credit card data.

Since retailers have used magnetic stripe credit card data to help keep track of customer profiles and preferences, the result has been a proliferation of sensitive data sites across retail networks beyond the server environments needed simply for transaction processing—and increased exposure for retailers.

RETAIL CUSTOMERS FEEL THE PAIN

The last two years have seen a continuous stream of U.S. and international retailers that have publicly admitted to significant losses of their customers' personal data. Although the highest profile has been losses of credit card data, thieves often moved on to steal logins and passwords, email IDs and physical addresses. They also target customer profile information about what, where and how people are buying from these retailers. It's a different level of information loss from those in the past, and the results have also been different. Not so long ago, data breach remediation for end users, and shake ups within IT organizations were typically the only results of a retail data breach. But some recent breaches have resulted in bottom line quarterly profit problems and replacements all the way to top executive staff. Home Depot, Target, Nieman Marcus, eBay, Staples and a host of others have been seriously affected.

RETAILERS ARE FAILING TO SECURE THEIR DATA



3x

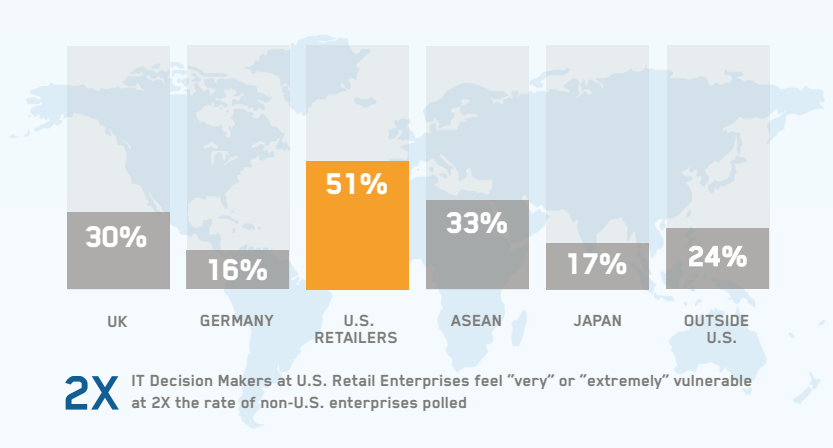
INCREASE IT SECURITY SPENDING PRIORITY FOR DATA BREACH PREVENTION

From 21% in the *2013 Vormetric Insider Threat Report* data to 57% in the *2015 Vormetric Insider Threat Report*.

U.S. RETAILERS–"VERY" OR "EXTREMELY" VULNERABLE

Although the overall rate of U.S. retailers who responded as being "Somewhat" or more vulnerable was the same as the overall U.S. number of 93%, the big differences were in the rate at which respondents at retailers reported being "Very" or "Extremely" vulnerable (51%). The rate was more than twice that of enterprise respondents outside of the U.S. (24%).

U.S. RETAILERS–HIGHEST RATES OF "VERY" OR "EXTREMELY" VULNERABLE



ATTITUDES TO IT SECURITY INVESTMENTS ARE CHANGING

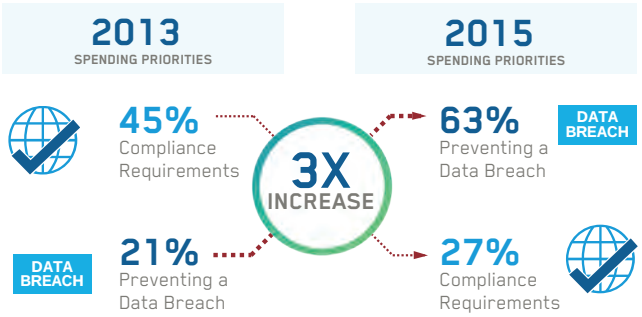
With this level of concern, and with the constantly repeated news of data breaches, U.S. retail organizations appear to be responding with a change in their IT Security spending priorities.

Looking back to the results returned from our *2013 Vormetric Insider Threat Report*, compliance was by far the biggest driver for IT Security spending increases at 45%. Those citing a data breach at their organization as a driver were only 7% of respondents at the time, and 21% of respondents noted that they were setting increased spending priorities because of a data breach at another organization.

Fast forward to today, and the scene has dramatically changed. Preventing a data breach incident is now the top driver for setting IT Security spending priorities at 63%, 3× from 2013, while fulfilling compliance requirements and passing audits has fallen to the bottom of the list at 27%.

In addition, 62% of respondents are planning to increase spending to offset the threats, versus 51% for enterprises outside of the U.S.

DRAMATIC CHANGES IN IT SECURITY SPENDING PRIORITIES



TOP IT SECURITY SPENDING PRIORITIES AMONG IT DECISION MAKERS AT U.S. RETAILERS

59%

PRIVILEGED USERS— THE MOST DANGEROUS INSIDER

With the combination of their often unfettered access to data on systems that they maintain, and the risks from compromise of their credentials, it's no wonder that respondents identified Privileged Users as the insiders that pose the largest risk to their organizations.

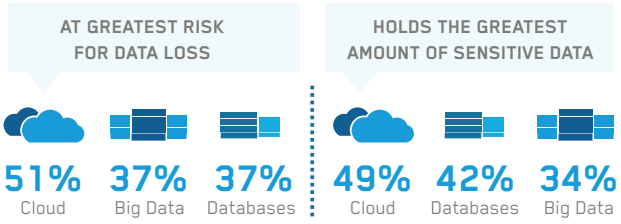
CLOUD, BIG DATA AND DATABASES ARE TOP DATA LOSS RISKS

Continued growth in cloud and big data deployments has introduced new security concerns due to increased volumes of sensitive data, the distributed nature of that data, a lack of control over the data, and the growing number of users who need to access it. This is a new extension of the ongoing balancing act between business efficiency and security.

The result? Both traditional databases and newer cloud and big data environments are top worries for retailers.

With cloud environments both holding the greatest amount of sensitive data (49%), and having a corresponding concern for the risks of loss that this entails (51%), retailers have a clear view of where they are vulnerable. Databases are the traditional location for credit card information and for customer profiles, while big data environments are frequently used to perform deep analysis of customer buying patterns and behavior. As a result, respondents showed great concern for the risks that these environments entail for their organizations.

CLOUD, BIG DATA AND DATABASES ARE HIGH RISKS FOR DATA LOSS



THE MOST SURPRISING FINDING FOR IT DECISION MAKERS AT U.S. RETAILERS–THEY AREN'T SURE HOW TO SOLVE THE PROBLEM

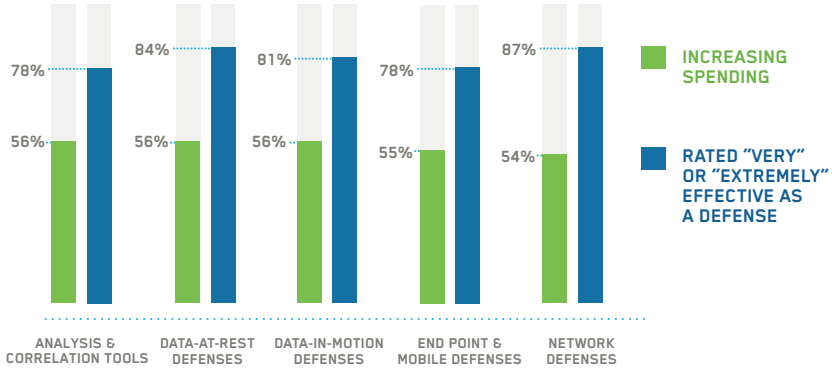
When asked what IT Security solutions organizations were planning to increase spending on, the results show that the respondents reported about the same level of investments in all categories, and also rated all categories of defenses as almost equally effective in defending against the threat. What's more, 77% of retail organizations also responded that compliance requirements were "Very" or "Extremely" effective at offsetting insider threats. We believe that this represents a problem—organizations are not identifying and investing in the solutions that are most effective at solving the problem.

The emphasis on compliance is surprising given that many of the retail data breaches in the last year happened to retailers who were compliant with standards such as PCI DSS. The facts are that compliance requirements evolve slowly, and can't keep up with fast changing threats. They are a good "baseline" to build a security strategy from, but do not represent a full solution.

In the past when threats changed more slowly, compliance requirements were considerably stricter than organizations needed for day-to-day operations, and looked on as a "gold standard." This can no longer be considered to be true.

The lack of focus about which IT Security investments to make, and which defenses are most effective in offsetting insider threats is also disturbing. The data shows that retailers are still planning their spending, and rating as effective, IT security tools that haven't fixed the problem. Both IT analysts and industry experts can frequently be heard to say that it is no longer "if" organizations' external defenses will be penetrated, it is only a question of "when." Endpoint and network defenses are the usual entry points, as the nature of attacks has evolved to bypass these traditional defenses. What is needed is a data first security strategy to offset these threats.

U.S. RETAILERS– ARE NOT SURE HOW TO SOLVE THE PROBLEM

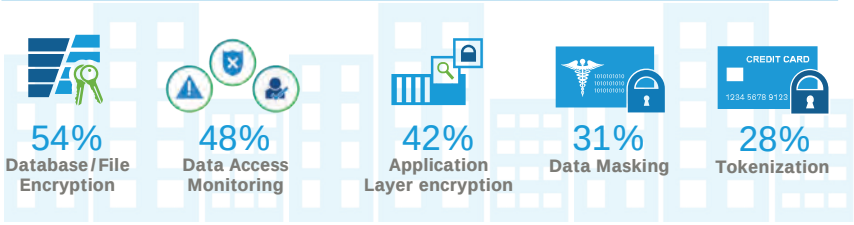


Organizations both plan to invest in, and also rate as effective end-point and network defenses that are consistently penetrated in insider attacks.

IMPLEMENT A DATA FIRST SECURITY STRATEGY TO OFFSET THESE THREATS:

- Because point-based security solutions are already failing to detect advanced attacks using employee credentials and data theft by legitimate users, a layered defense combining traditional as well as advanced data protection techniques is the path forward.
- Data protection initiatives need to concentrate on *protecting data at the source*. For most organizations, this will involve protecting a mix of on-premise databases and servers, and remote cloud and big data applications.
- Companies should integrate new encryption technology that minimizes operational impact and works with strong access controls and key management for all important data sources.
- Implementing integrated data monitoring and technologies such as security information and event management (SIEM) systems to identify data usage and unusual and malicious access patterns is critical to maximizing security.
- To keep the whole organization safe, companies must develop an *integrated data security strategy* that includes monitoring, relevant access control, and levels of data protection, and leaves security to the CISO, not the boardroom.

RETAILERS' EXISTING PROTECTIONS FOR DATA-AT-REST



With insider threats to data security on the rise, organizations that focus their security spending on protecting data at the source, implementing data access monitoring technologies, and developing an integrated security strategy that includes the latest encryption technologies will have greater success protecting their most valuable asset.

To read the full *2015 Vormetric Insider Threat Report—Global Edition*, please visit www.vormetric.com/InsiderThreat/2015.

HARRIS POLL—SOURCE AND 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.

THE 2013 VORMETRIC INSIDER THREAT REPORT

On the behalf of Vormetric, Enterprise Strategy Group conducted research around insider threats, privileged users, and advanced persistent threats (APTs). The survey targeted primarily Fortune 1,000 industries and was responded to by 707 IT executives and managers with knowledge of IT security and insider threats.

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

RESEARCH BRIEF

Vormetric.com/InsiderThreat/2015

Vormetric
Data Security™