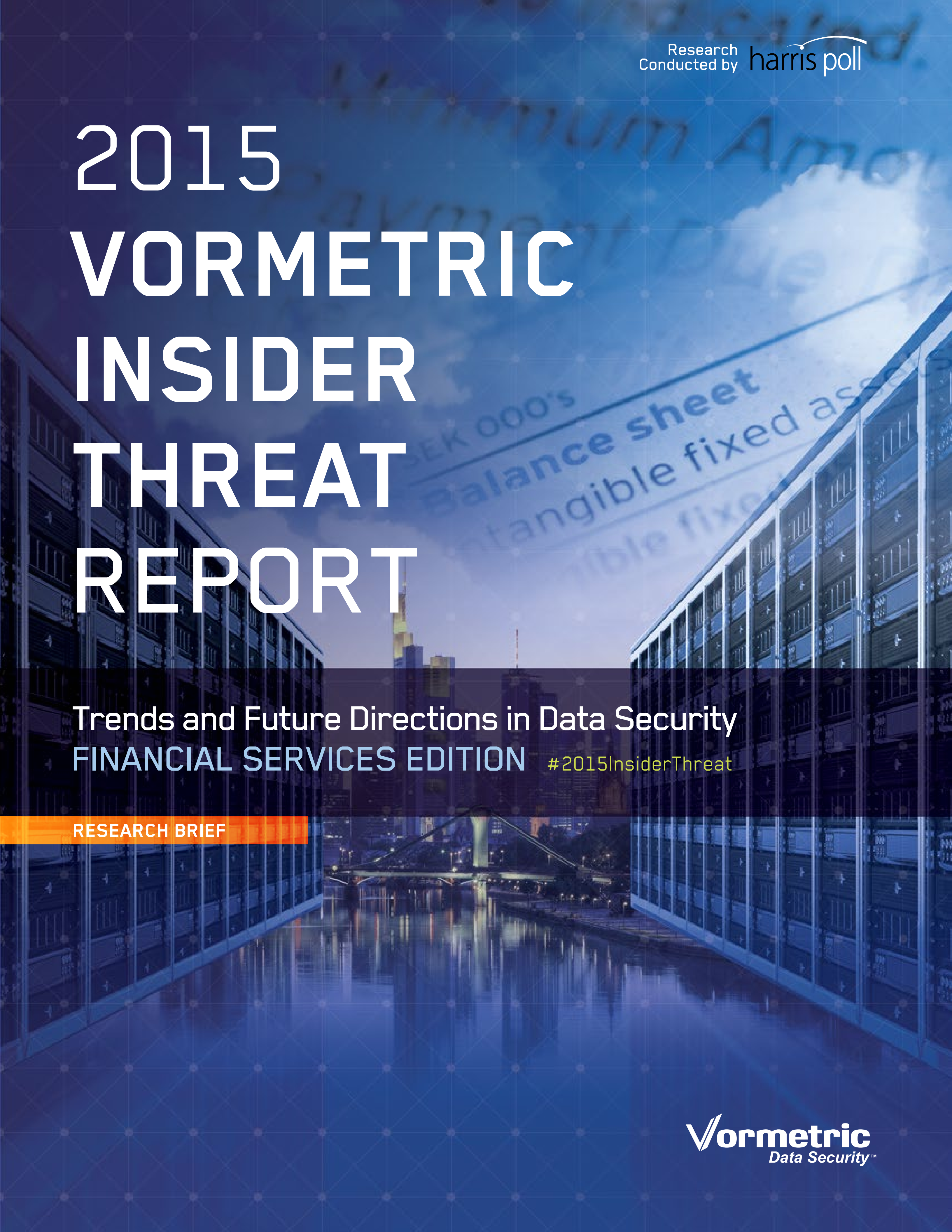
Research Conducted by harris poll

2015 VORMETRIC INSIDER THREAT REPORT



Trends and Future Directions in Data Security

FINANCIAL SERVICES EDITION #2015InsiderThreat

RESEARCH BRIEF

Vormetric Data Security™

US FINANCIAL SERVICES SPOTLIGHT

ABOUT THIS RESEARCH BRIEF

This Research Brief highlights the results collected online by Harris Poll from 102 IT decision makers in U.S. financial services 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.

FINANCIAL SERVICES ARE A PRIMARY TARGET

Financial services enterprises have always known that they are a primary target for both traditional employee theft, and criminal hackers trying to steal assets. Insider thefts and inside jobs have been around as long as banks and brokerages have existed. Today, employees with legitimate access, service providers or contractors that maintain infrastructure and privileged users (both internal and at cloud and SaaS providers) are all possible actors, and potential attack vectors when their credentials are compromised.

Criminal hackers continue to be a top worry for financial services organizations, and nearly every financial sector breach has included a compromise of a privileged user account or a privileged account at a partner. Nation state hackers attempting to commit acts of cyber terrorism, destabilize financial infrastructure, embarrass opponents or gain competitive advantage are another major concern.

WHERE DO INSIDER THREATS COME FROM?
NOT JUST FROM YOUR TYPICAL EMPLOYEE

root
SA
CRIMINAL HACKERS
NATION STATES
TRADITIONAL INSIDERS
PRIVILEGED USERS
SERVICE PROVIDERS & CONTRACTORS
HACKERS TARGETING INSIDER ACCOUNTS

THE MOST VULNERABLE SECTOR—US FINANCIAL SERVICES

We asked a crucial question of all survey respondents—"How vulnerable is your organization to insider threats?" Although U.S. financial services did not have the highest rates of feeling very or extremely vulnerable (they responded at 44%, well below the level for U.S. retailers at 51%), overall they responded with the highest rate of somewhat or more vulnerable (97%). This was a common theme for U.S. organizations, who felt consistently more vulnerable than their international counterparts (84%). Our belief is that this sense of vulnerability is driven by multiple factors:

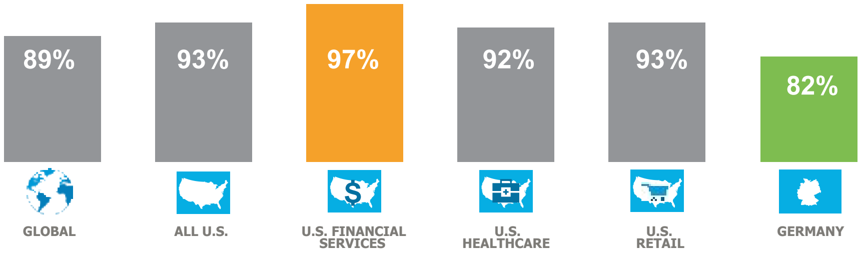
- Their knowledge of their own shortcomings, having failed compliance audits or encountered data breaches themselves in the last year (41%).
- The significant level at which they've seen breaches at partners and competitors (34%) as well as in the media.
- And the awareness that they are always a prime target, given the treasure trove that their financial assets and corporate data represent.

97%

SOMEWHAT OR MORE VULNERABLE

We asked a crucial question of all survey respondents—"How vulnerable is your organization to insider threats?"

LEVELS OF "SOMEWHAT" OR MORE VULNERABLE TO INSIDER THREATS BY SEGMENT



FAILING TO SECURE THEIR DATA

U.S. financial services organizations are encountering real difficulty in securing their assets. Since 2009, there has been a cadence of large and small breaches at these institutions making news headlines—starting with Heartland payments, moving on to Global Payments and concluding this year with JPMorgan Chase. These attacks most often include a strong element of compromised insider credentials.

It is troubling to find that 41% of financial services respondents reported that they encountered a data breach or failed a compliance audit in the last year. With their responsibility to protect financial assets, this sector has always tended to invest more heavily in IT Security controls than others. A second statistic adds to this picture with 27% of respondents protecting sensitive data in response to a past data breach (the highest rate of major sectors that were polled).

The implied high rate of failure to meet compliance audits is especially telling. Compliance requirements do not evolve as fast as threats in this sector, and as a result have become only a good "baseline" to build from for a full data security strategy. Failure at this baseline level is not a good sign for the security of their customers' information.

2.5x

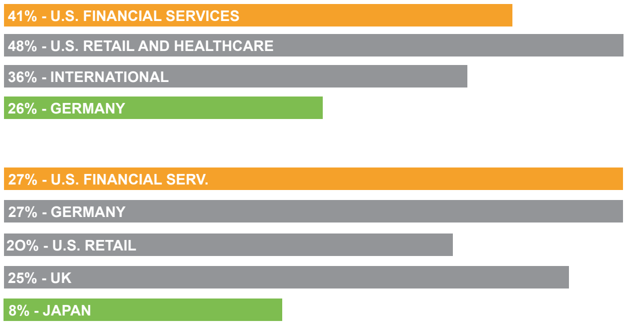
INCREASE IT SECURITY SPENDING PRIORITY FOR DATA BREACH PREVENTION

From 21% in 2013 to 57% in 2015.

FINANCIAL SERVICES ORGANIZATIONS– FAILING TO SECURE THEIR DATA

41% ENCOUNTERED A DATA BREACH OR FAILED A COMPLIANCE AUDIT IN THE LAST 12 MONTHS

27% ARE PROTECTING DATA BECAUSE OF A PAST DATA BREACH



THE TOP DRIVERS FOR PROTECTING DATA AT U.S. FINANCIAL SERVICES ENTERPRISES

From the responses to the poll, it appears that U.S. financial services organizations have reputation and brand protection as a top priority for securing sensitive data (50%). Their IT security spending priorities also seem to be a good match for this. Preventing a data breach is now their top priority (57%), even above protecting finances and other assets (43%). With the recent exposure that data breaches are garnering in the press, as well as the bottom line and leadership changes that have become part of the results, it seems that these organizations have their priorities in the right place.

It is also important to note that this priority set is different from just a few years ago. In our *2013 Vormetric Insider Threat Report* data set, we found that compliance was by far the biggest driver for IT Security spending increases by all respondents at 45%. In the polling results from U.S. financial services organizations used to create this brief, compliance dropped to third, polling at 39%. However, the most radical change comes from those citing a data breach at their organization as a driver for IT security spending, this changed from 7% in 2013 for all respondents, to a much higher result of 57% from financial services respondents in our polling.

TOP DRIVERS FOR U.S. FINANCIAL SERVICES ORGANIZATIONS

TOP 3 REASONS FOR SECURING SENSITIVE DATA

50%	REPUTATION AND BRAND PROTECTION
43%	COMPLIANCE REQUIREMENTS
42%	AVOIDING DATA BREACH PENALTIES

TOP 3 IT SECURITY SPENDING PRIORITIES

57%	PREVENTING A DATA BREACH INCIDENT
43%	PROTECTION OF FINANCES & OTHER ASSETS
39%	FULFILLING COMPLIANCE REQUIREMENTS AND PASSING AUDITS

THE MOST DANGEROUS INSIDERS

As a result of their roles, and the architecture of the systems they manage and maintain, systems administrators and business users with privileged access have had access to the most sensitive corporate data, with few controls placed around this access. For the U.S. financial services sector today, it is clear that concerns over privileged user access have reached the top of their security agendas.

Rogue users with admin rights (such as Edward Snowden) as well as service providers that provide and maintain internal and cloud infrastructure for the organization are clearly shown as sources of risk. As noted earlier, this risk is not solely from their roles and work for the organization, but also by the potential for damage when these insider credentials have been compromised by an outside attack. At 63%—a full 20 percentage points above the rate for the next category—their concerns are very clear. Partners with internal access comprise that next category at 43%.

THE MOST DANGEROUS INSIDERS ADMINISTER AND MANAGE INFRASTRUCTURE

63% Privileged Users

Privileged Users include System Administrators, Network Administrators, Linux/Unix Root Users, Domain Administrators and other IT roles.

43% Partners with Internal Access

40% Contractors/Service Provider Employees

(Snowden was a contractor)

Respondents from U.S. financial services organizations top three selections for insiders that pose the largest risk to their organization.

DATABASES, FILE SERVERS AND CLOUD ENVIRONMENTS HOLD FINANCIAL SERVICES SENSITIVE DATA

A transition is clearly underway in the U.S. Financial Services sector to use sensitive data within newer cloud environments (36%) while still keeping much of their critical data within local databases (48%) and file servers (41%). Internationally, cloud adoption lags that of the U.S. and the results for the financial sector follows the same pattern. For U.S. financial services organizations, cloud was rated as the third highest ranked environment for storing volumes of sensitive data (36%), big data environments were a close follower (31%), while for all respondents polled outside of the U.S. these numbers were cloud (31%) and big data environments (26%).

It is no surprise then to see cloud rated as one of the locations at greatest risk for loss (42%), but somewhat surprising to see mobile rated as their top risk (47%), given the low volumes of data that might be exposed. Perhaps the specter of a single multi-million dollar loss because of a mobile compromise is the primary reason for this.

Cloud and big data environments come with their own unique set of concerns for insider threats to sensitive data. For cloud environments, the infrastructure is out of the enterprises' control, resulting in concerns that include the lack of visibility into where the data resides and moves, as well as who is able to access it. This is true unless the enterprise is able to obtained commitments specifically governed by contracts, SLAs and controls that are not commonly available in the industry. At the end of the day, the financial services company is liable to customers and regulators, regardless of the commitments by the cloud provider.

WORRIES AND THE GREATEST VOLUMES OF SENSITIVE DATA

HIGHEST VOLUMES OF SENSITIVE DATA	48% DATABASES	41% FILE SERVERS	36% CLOUD
ORGANIZATIONS ARE MOST WORRIED ABOUT DATA ON	47% MOBILE	45% DATABASES	42% CLOUD

U.S. financial services organizations greatest volumes of data-at-risk are in databases, on file servers and in cloud environments. Mobile devices are their area of biggest concern for greatest risk of loss.

IMPLEMENT A DATA FIRST SECURITY STRATEGY TO OFFSET THESE THREATS:

- Because endpoint, firewall and network IT security controls are failing to keep attackers out, or halt malicious insiders, 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 leverage a range of data-centric security techniques that protect where the data is stored, and can move with the data. Use data encryption, tokenization, data masking and other techniques that can de-identify data, that include access controls, and that increase data access visibility.

- 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.

- Select data-centric solutions that cover a broad set of use cases, environments, and data types with minimal infrastructure sets for the best total cost of ownership. Scalability and performance are also key attributes.

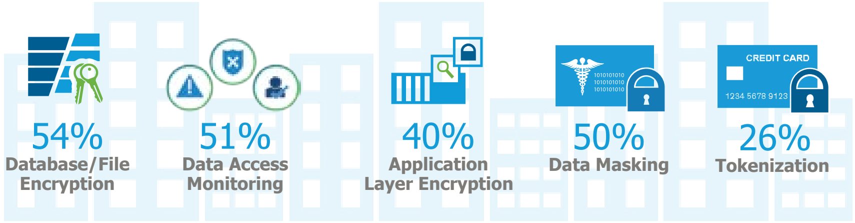
- To keep the whole organization safe, companies must develop an *integrated data security strategy* that includes monitoring, relevant access control, and levels of data protection, and leaves security to the CISO, not the boardroom.

63%

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 is no wonder that respondents identified Privileged Users as the insiders that pose the largest risk to their organizations.

U.S. FINANCIAL SERVICES 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.

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.

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

2015 **VORMETRIC** INSIDER THREAT REPORT—*FINANCIAL SERVICES EDITION*

RESEARCH BRIEF

Vormetric.com/InsiderThreat/2015

Vormetric
Data Security™

©2015 Vormetric, Inc. All rights reserved.