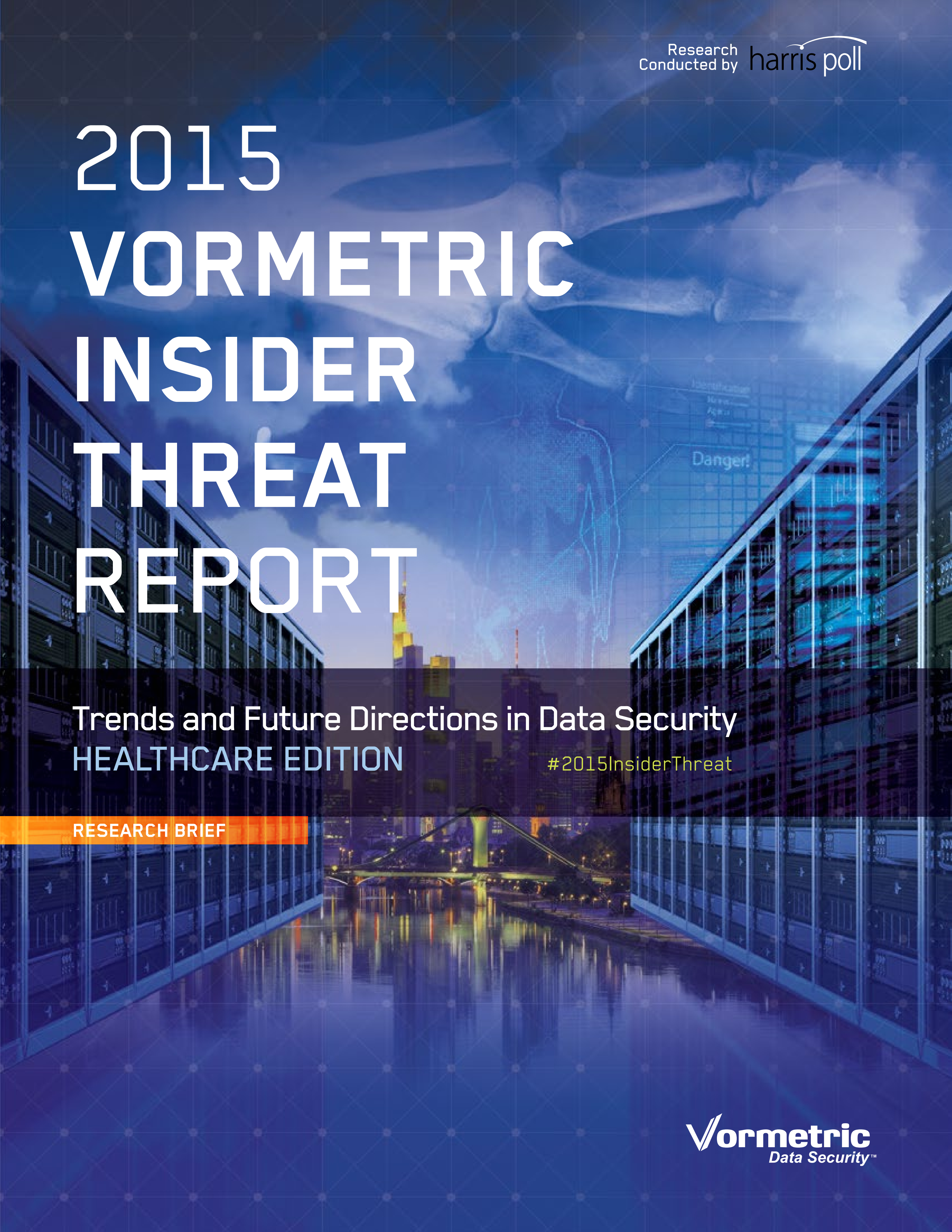
Research Conducted by harris poll

2015 VORMETRIC INSIDER THREAT REPORT



Trends and Future Directions in Data Security

HEALTHCARE EDITION

#2015InsiderThreat

RESEARCH BRIEF

Vormetric
Data Security™

U.S. HEALTHCARE SPOTLIGHT

ABOUT THIS RESEARCH BRIEF

This Research Brief highlights the results of an online survey conducted on behalf of Vormetric by Harris Poll in fall 2014 that included responses from 102 IT decision makers in U.S. healthcare organizations, as well as 818 total IT decision makers in the U.S., U.K., Germany, Japan and the ASEAN region. Where applicable, U.S. Healthcare results are compared against the findings for IT decision makers in U.S. Retail and Financial Services, as well as global results.

HEALTHCARE'S MISSION NEEDS TO INCLUDE MORE THAN PATIENTS' PHYSICAL HEALTH

Healthcare data (Personal Health Information [PHI] and other personal data held by healthcare organizations) has become one of the most desirable commodities for sale on "black" Internet sites, and for good reason. Healthcare records typically contain enough detail to not only apply for credit cards or loans, but can also be used to generate large sums from fraudulent medical charges, or even to compromise patients' existing financial accounts. As a result, stolen healthcare records command a large premium versus more mundane stolen information, such as credit card data.

OUR SPONSORS

Couchbase

CSA

FINANCIAL SERVICES ISAC

rackspace. the #1 managed cloud company

fishnet™ SECURITY

OASIS

carahsoft.

PREVENTIA

AZM

M.TECH Your Preferred I-Security Partner

fieldfisher

Raber+Märcker Prinzip Partnerschaft

The environment for healthcare insider threats has also grown more complex. Ordinary employees are no longer the primary threats, but only an element of a broader problem. Now included in the wider problem set are:

- Privileged users who manage IT infrastructure and have full access to the data on the systems that they manage
- Employees such as doctors, nurses, billing departments, administrators and other skilled health professionals
- Service providers and contractors with access to enterprise networks, such as IT, HVAC and SaaS providers, as well as healthcare-specific organizations, such as postsecondary care facilities and insurance companies
- Criminals who compromise any of these accounts

Note that in the recent Anthem breach, the compromise of an IT administrator's credentials was the initial entry point that caused the breach and exposure of 13.5 million patient records.

There can also be potential longer-term problems for individuals whose healthcare data has been compromised. Detailed patient and care records can not only destroy credit results in cases of identity theft, but can further haunt individuals' futures if health information becomes public, exposing information that can result in personal tragedy, loss of work and failure to be hired.

Historically, healthcare has also been slower to prioritize data protection. Patient care has always been the priority—with IT in place primarily to serve technical and business needs. With the required move to ePCRs and to share patient information across healthcare providers, it is time for that to change. Healthcare organizations are now required to not only prioritize the protection of patients' physical health, but also the protection of the healthcare data that can compromise their personal and financial futures if exposed.

HEALTHCARE ORGANIZATIONS DATA SECURITY FAILURES

The results clearly point to systemic failures within healthcare organizations when it comes to protecting sensitive data. Among IT decision makers in the organizations surveyed, 48 percent report either encountering a data breach or failing a compliance audit in the last year (tying with U.S. Retailers as the highest of any category surveyed). The data breach rate in the last year is likely to be the smallest portion of this—our survey found that 26 percent are protecting data because of a data-breach at an undefined time in the past. Many of these breaches, then, will have occurred in previous years, leaving the majority of the 48 percent as compliance audit failures.

U.S. Healthcare organizations are now required to meet a complex web of government and industry regulations around sensitive data—failure to meet these standards in a required audit leads to compliance audit failure:

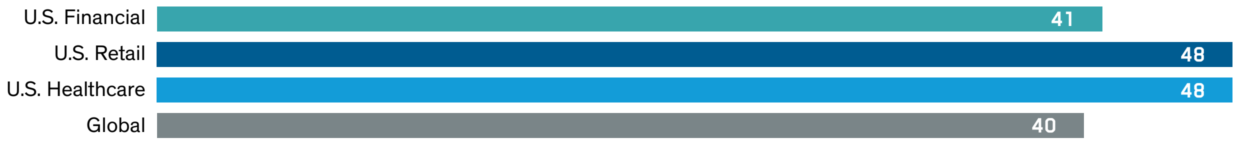
- HIPAA/HITECH: U.S. Health Insurance Portability and Accountability Act (HIPAA), as well as Health Information Technology for Economic and Clinical Health Act (HITECH) requirements for safeguarding electronic Personal Healthcare Information (ePHI)
- EPCS: U.S. Drug Enforcement Agency's (DEA) requirements for Electronic Prescriptions of Controlled Substances (EPCS)
- PCI DSS: Security of credit card transactions as required under the Payment Card Industry Data Security Standard (PCI DSS)
- FDA: U.S. Food and Drug Administration (FDA) requirements for ensuring the trustworthiness and reliability of electronic records and signatures

Note that healthcare organizations are also subject to U.S. state, federal and local data breach statutes, but that there is no compliance audit requirement for this set of mandates.

The problem with compliance regimes is that they typically evolve over time, with years passing between standards revisions, and even longer periods for legislation. It is important that healthcare organizations take to heart the fact that this results in compliance requirements becoming a baseline for data protection, not a best practice. Threats can rapidly grow and change, leaving slow-moving compliance requirements behind as new threats emerge.

With this in mind, the high rate of compliance audit failure takes on new importance. With failure to reach even baseline protection comes increased vulnerability and a concomitant increase in incidents of breaches.

Healthcare Organizations Are Failing to Secure Their Data (Percentage of Breaches/Failures)

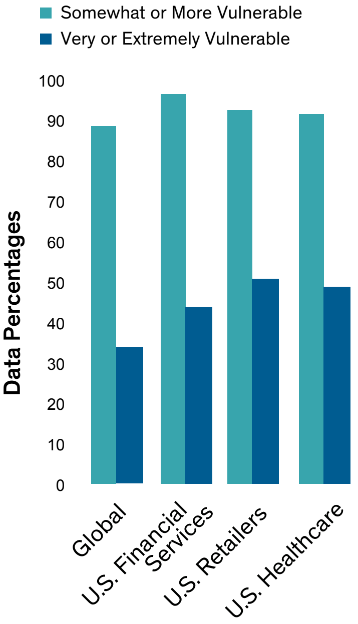


48% of U.S. Healthcare organizations reported either encountering a data breach or failing a compliance audit in the last year.

U.S. HEALTHCARE–HIGHLY VULNERABLE

Given the high rate of data breaches and compliance audit failures reported, it should be no surprise that IT decision makers in U.S. Healthcare organizations polled feel that their organizations are highly vulnerable. Of those polled, 92 percent responded to being somewhat or more vulnerable, with 49 percent of those—nearly half—responding to being very or extremely vulnerable. Two other U.S. vertical segments with high risks for data—financial services (44 percent) and retail (51 percent)—responded at similar levels. The global average, however, is substantially lower, at 34 percent very or extremely vulnerable. U.S. healthcare and retail segments were the two highest levels measured of any region or category globally.

U.S. Healthcare—One of the Top Two Rates Globally of High or Extreme Vulnerability

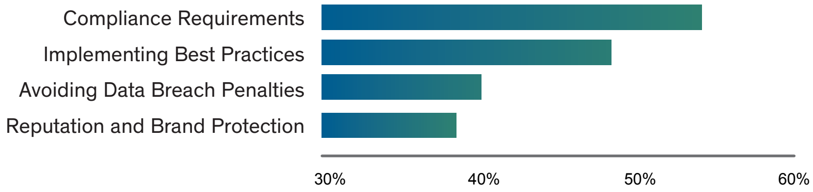


HEALTHCARE'S DATA PROTECTION PRIORITIES

The priority that IT decision makers in healthcare organizations place on protecting data to meet compliance requirements is another telling factor. Respondents by far selected compliance requirements as the largest driver for securing sensitive data, at 54 percent. With this focus on compliance as a top priority, it can be hard to pay attention to the wider threats to data security that now need equivalent priority.

Responses from IT decision makers in U.S. Healthcare and Retail have already made this change—with compliance dropping to the second or even third selected driver for protecting data. For example, compliance for U.S. financial services organizations has dropped to second, at 43 percent, behind reputation and brand protection, at 50 percent.

Top Reasons For Securing Sensitive Data For U.S. Healthcare



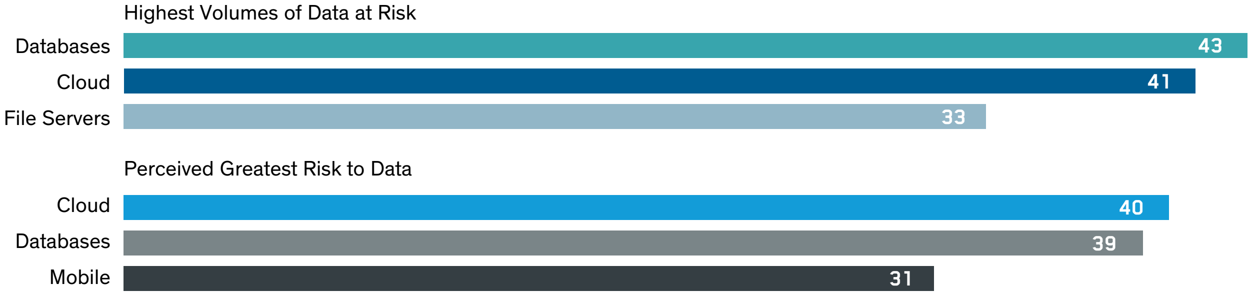
“IT decision makers in U.S. Healthcare organizations rate cloud environments as the highest risk for loss of sensitive data, at 40%—but are still deploying sensitive data there.”

BIG DATA AND CLOUD DEPLOYMENTS IN HEALTHCARE ARE GROWING—DESPITE THE ADDITIONAL RISK

Enterprise adoption of cloud and Big Data environments has always been slowed by concerns about security. However, response for IT decision makers in U.S. healthcare organizations show that use of these environments is already above 50 percent for all cloud deployment categories—including SaaS, IaaS, PaaS (Software, Infrastructure and Platform as a Service, respectively). With the additional security risks that organizations encounter in cloud deployments, it’s troubling to find such a high percentage of respondents using sensitive data within them.

Principal concerns for cloud environments include the lack of visibility into the physical and IT security stances at the cloud provider, the lack of data protection and encryption services, and a paucity of commitments to compliance requirements and data breach incident responses. See the Cloud and Big Data editions of this report for more detail.

Cloud and Databases Represent the Greatest Risks to Healthcare Data (Percent)

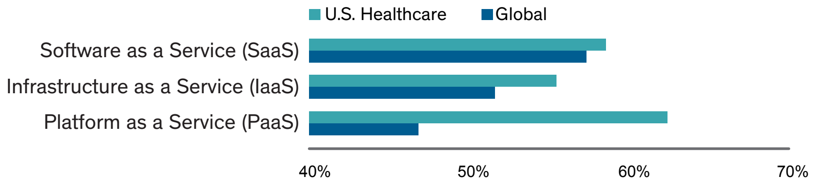


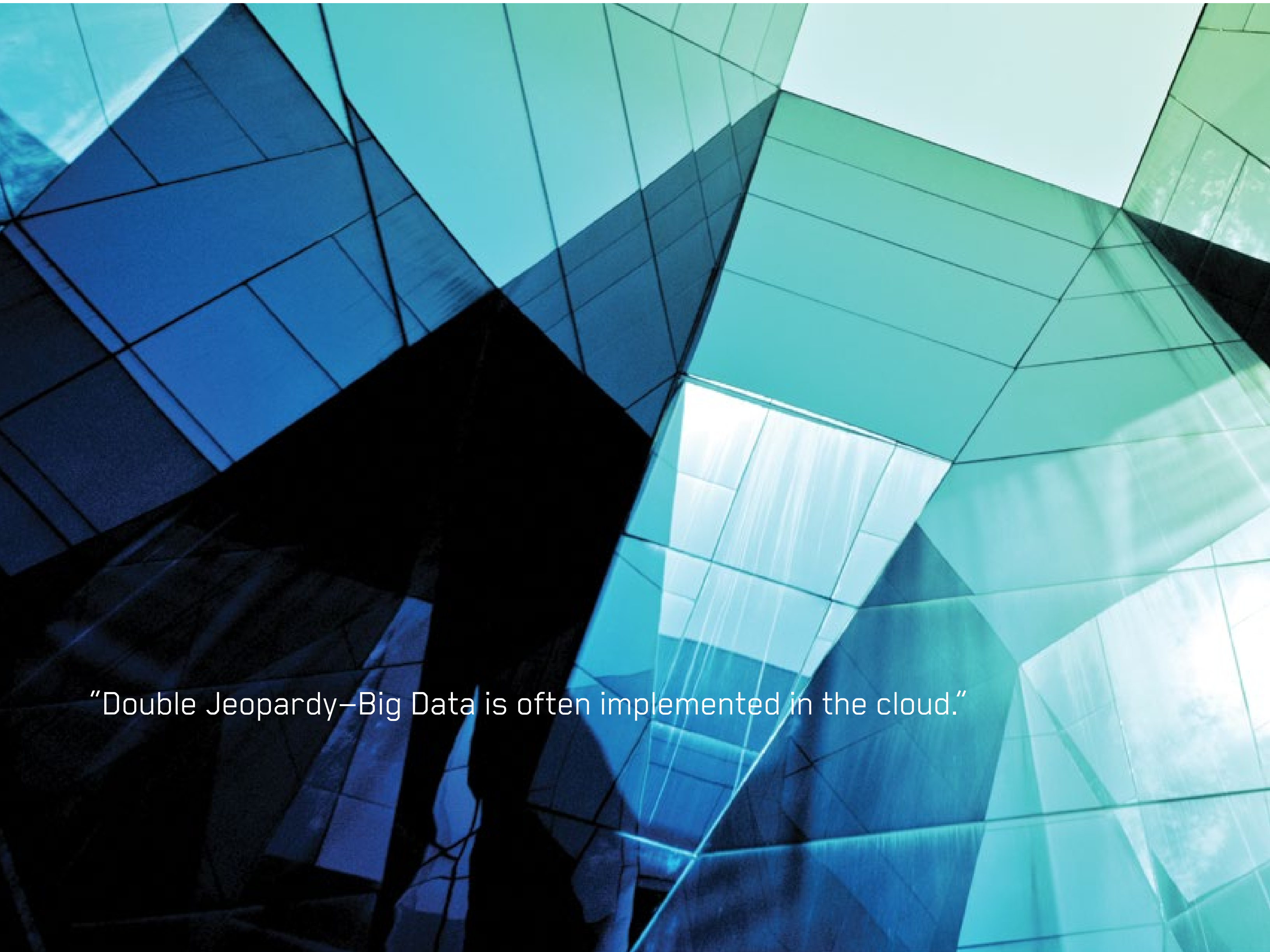
Respondents identified environments that represented their largest perceived risks to data, and also identified locations where the largest volumes of data could be compromised.

In the ongoing need to balance business efficiency and security, healthcare providers have already deployed sensitive information to cloud environments, and are now realizing that they have created a large additional risk to their organizations. At 40 percent, cloud environments are rated highest as a location for volumes of data at risk, with deployments of sensitive data in these environments as high as 62 percent of organizations for PaaS, 58 percent for SaaS and 55 percent for IaaS.

The high level of sensitive data use within SaaS environments poses a unique problem. Enterprise can add data-protection controls to mitigate risks on their own within IaaS and PaaS environments (especially file and application encryption, enterprise management of encryption keys, access controls to encrypted data, and tokenization). Within SaaS environments, security implementations are almost entirely under control of the SaaS vendor. Few of these vendors will disclose their security stances and access capabilities—or give enterprises direct control of the protection of their data.

High Rates of Sensitive Data Use in the Cloud





“Double Jeopardy—Big Data is often implemented in the cloud.”

Big Data implementations represent another set of additional risks. Their highly distributed nature and diversity of data sources often result in large volumes of sensitive data being present within the environment. Among U.S. healthcare respondents, 26 percent found Big Data environments to be a top-three selection for volume of sensitive data at risk. Further concerns included:

- A lack of security frameworks within the environment (45 percent)
- The security of reports including sensitive data (38 percent)
- Privacy violations from data originating in multiple countries (36 percent)
- The presence of sensitive data anywhere within the environment (34 percent)
- Privileged user access to protected data within the implementation (21 percent)

> “62%–IDENTIFY PRIVILEGED USERS AS THE MOST DANGEROUS INSIDERS.”

In addition, with Big Data’s requirement for copious computing and storage, organizations will frequently opt to deploy in cloud environments, where resources can be quickly brought online. The result is to add Big Data environment risks to that of cloud environments for a still higher level of vulnerability.

THE MOST DANGEROUS INSIDERS IN HEALTHCARE

Privileged users traditionally have access to all resources available from systems that they manage, and credentials for their accounts are a top focus of outside attackers. With this in mind, it is no surprise that privileged users were identified as the most dangerous inside threat, at 62 percent. It is worth mentioning that when this survey was performed, the Anthem data breach had not yet occurred. The Anthem breach featured the compromise of a privileged user account as the entry point. We might expect even higher numbers if we performed this poll today.

The second- and third-most dangerous insiders were partners with internal access, at 46 percent, and contractor/service-provider employees, at 45 percent. Recall that the Target data breach was initiated through the compromise of a contractor’s credentials—an HVAC provider who had access to Target’s network.

ATTITUDES TO IT SECURITY INVESTMENTS HAVE CHANGED

The results showed that healthcare respondents' reasons for securing sensitive data are in direct contrast to their present priorities for IT security spending. When reporting their IT security spending priorities, data breach prevention was the top selection, with 53 percent of respondents reporting it as a top driver. But when asked about their reasons for securing sensitive data (rather than spending), the focus changed back to compliance as the top priority, at 54 percent, with data breach prevention in third place, at 40 percent. To us, this supports the conclusion that healthcare organizations have not fully absorbed the need to change their priority set.

The IT security spending focus has also changed dramatically in the last 2 years, with the importance of data breach prevention increasing 2.5× in 2015 over 2013. In our *2013 Vormetric Insider Threat Report*, compliance was by far the biggest driver for IT security spending increases, at 45 percent.* Fast forward to today, and the scene has dramatically changed.

> "WITH A 2.5X INCREASE SINCE 2013, DATA BREACH PREVENTION IS NOW THE BIGGEST IT SECURITY SPENDING DRIVER FOR U.S. HEALTHCARE RESPONDENTS."

Preventing a data breach incident is now the top driver for setting IT Security spending priorities at 53 percent, 2.5× up from the 2013 overall number, while fulfilling compliance requirements and passing audits has fallen to 39 percent.

HEALTHCARE ORGANIZATIONS IT SECURITY INVESTMENTS TO SOLVE THE PROBLEM

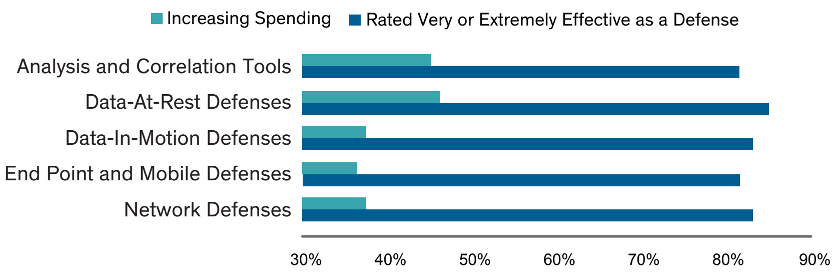
Healthcare organizations are showing the greatest planned investments in data-at-rest defenses (46 percent) and analysis/correlation tools (45 percent), with slightly lower levels planned for data-in-motion (37 percent), end point and mobile (36 percent), and network defenses (37 percent). Ratings for the perceived effectiveness of these tools to prevent insider threats was 83 percent or higher in all cases—See figure 6. In addition, 58 percent of Healthcare respondents believed that compliance requirements were "Very" or "Extremely" effective at neutralizing insider threats.

*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.

These responses are symptomatic of a potential risk. While it is a positive to see slightly higher investment in data-at-rest defenses and analysis and correlation tools (SEIM), organizations are still heavily investing in traditional perimeter defenses, which are not effective at stopping the new generation of threats facing the healthcare vertical.

With compliance requirements now more of a good baseline from which to build more effective data security, the high rate of trust in compliance as an effective defense is another part of the problem. As noted earlier, compliance requirements evolve slowly and cannot keep up with fast-changing threats.

What is needed is a data-first security strategy.



U.S. Healthcare Spending Increases and Defense Effectiveness Ratings

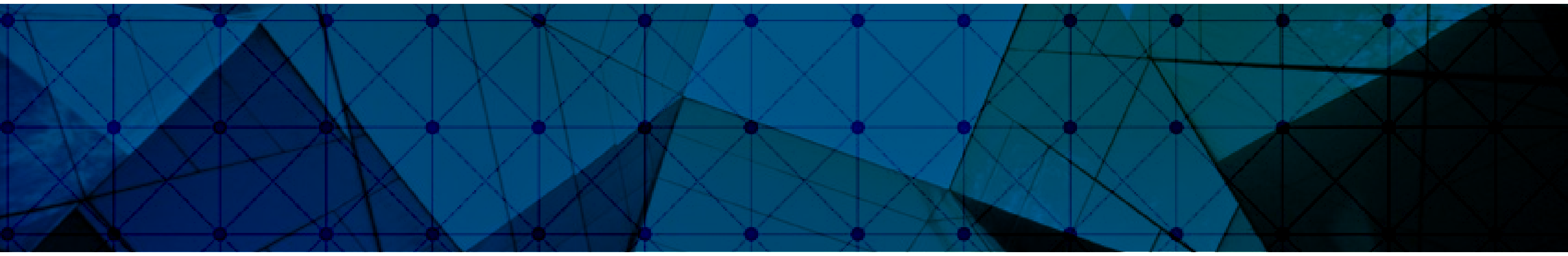
Respondents report investing more in data-at-rest and analysis/correlation tools that help solve the problem, but are still heavily investing in defenses that have failed.

IMPLEMENT A DATA-FIRST SECURITY STRATEGY

- With network and endpoint security solutions failing to stop or even detect attacks by employee insiders, and advanced attacks using employee credentials, 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 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.

HARRIS POLL—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 IT professionals 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 healthcare 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 1,500 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.

FURTHER READING

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

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

Vormetric.com/InsiderThreat/2015