Research
Conducted by harris poll

2015 VORMETRIC INSIDER THREAT REPORT

Trends and Future Directions in Data Security

MEXICO AND BRAZIL EDITION

#2015InsiderThreat

Vormetric
Data Security™

TABLE OF CONTENTS

OUR SPONSORS

Couchbase

FINANCIAL SERVICES ISAC

PREVENTIA

carahsoft.

fishnet™ SECURITY

AZM

CSA

Adistec

OASIS

M.TECH Your Preferred i-Security Partner

fieldfisher

KONICA MINOLTA

rackspace. the #1 managed cloud company

ABOUT THIS REPORT

The Mexico and Brazil edition of the *2015 Insider Threat Report* provides current insights and analysis of the threats confronting organizations across these regions, as well as the approaches being taken in response. This report features the results of an online survey conducted on behalf of Vormetric by Harris Poll in spring 2015. The survey collected responses from 204 IT decision-makers, with 102 respondents from Mexico and 102 from Brazil. All respondents reported being from organizations with revenues of $100 million USD and over. Of respondents from Mexico, 88% represented organizations with revenues of $500 million and above. In Brazil, 78% were from organizations with revenues of $480 million and above.

This report focuses on findings from the respondents based in Mexico and Brazil. These results are also compared with data from our global survey, which captured information from respondents in the U.S., U.K., Germany, Japan and the ASEAN region (countries surveyed in ASEAN included Singapore, Malaysia, Indonesia, Thailand and the Philippines). Conducted in the fall of 2014, this global survey was also conducted by Harris Poll and used the same question set and methodology.

> *“87% of respondents in Mexico and 69% of respondents in Brazil rated their organizations as somewhat or more vulnerable to insider threats.”*

Understanding the Nature and Sources of Insider Threats

When it comes to assessing and addressing insider threats, the environment continues to grow more complex. And as the threat landscape grows more complex, so does the scope of the challenges. It may seem like a contradiction in terms, but insider threats are posed by an ever-widening range of offenders. Today, threats come from individuals or groups who maliciously or accidentally do things that put an organization and its data at risk. Security teams looking to contend with insider threats have to consider the following groups:

- Privileged users who manage IT infrastructure and have full access to the data on the systems that they manage.
- Employees, including staff, management and top-level executives.
- External service providers and contractors with access to enterprise networks and assets. This includes such entities as external development organizations, cloud service providers and others.
- Criminals who compromise the credentials of any of these groups.

Mexico and Brazil at Risk, Like the Rest of the World

The reach of cyberattacks is truly global, and organizations in Latin America are not immune. Enterprises in these regions are equally in need of data security solutions that help meet compliance requirements and prevent the loss of critical financial and intellectual property. For example, according to a study on cybercrime by the Latin American and Caribbean Internet Addresses Registry, phishing alone affects about 2,500 regional banks and accounts for $93 billion USD in annual losses within the region.

The survey results make clear that, both in Mexico and Brazil and across the globe, respondents are seeing the effect of data breaches and are concerned about their vulnerability to attacks. Of respondents polled, 87% in Mexico and 69% in Brazil rated their organizations as somewhat or more vulnerable to insider threats. Further, 48% in Mexico and 26% in Brazil indicated that their organizations had encountered a data breach or failed a compliance audit in the last year. These failures to protect data were also echoed worldwide as organizations struggle with how to protect their critical information from compromise.

> *"49% of respondents in Mexico and 39% in Brazil indicated that their organizations were protecting data because of a previous data breach or one at a partner or competitor."*

Threats Evolving Too Quickly for Compliance Standards and Many Security Teams

Threats continue to grow more advanced, with new attacks and tactics arising on a daily, if not hourly, basis. The pace of evolving threats continues to put IT and security teams in an all-too-familiar position of playing catch up. And if these groups lag behind, those responsible for establishing security policies, compliance mandates and guidelines for entire regions and industries understandably find it an even bigger struggle to keep pace. The result is that the number and severity of breaches continue to grow.

This makes the reliance on compliance found in the survey results a real concern: 52% of Mexican respondents and 59% of Brazilian respondents identified compliance as very or extremely effective in protecting data. These numbers raise fears about an unrealistic sense of security that is being bred by compliance initiatives.

Breaches: Escalating Costs and Increasing Concern in the Boardroom

It is clear that security breaches continue to grow more prevalent and costly. While the reports of breaches packing news channels have been a recurring theme for years, in recent months, the massive scale, escalating costs and devastating nature of breaches have led to the escalation of security as a concern for the boardroom. This has been hastened by the highly publicized departures of top CIOs and CEOs after organizations have been hit by large-scale breaches.

“53% of respondents from Mexico and 52% from Brazil are making preventing data breaches a top IT security spending priority.”

“Required: Data-centric security capabilities for encryption, access control, tokenization, data access monitoring and data access analysis.”

The Bottom Line

IT decision-makers in Mexico and Brazil are struggling with the same threats to data that those in other regions are confronting. In addition, these respondents are also facing growing compliance and regulatory requirements in their local markets. It should come as no surprise that the majority of survey respondents reported that their organizations are making preventing data breaches their top IT security spending priority, with 53% of respondents from Mexico and 52% from Brazil falling into that category.

How should IT decision-makers address this priority? Not by maintaining the current approaches. Planned IT security investments reported by respondents point to a scattershot approach, with increased spending spread across the entire gamut of IT security and a focus on endpoint security and network defenses—the very defenses that continue to be proven fallible by determined attackers.

Instead, IT decision-makers need to place a much stronger focus on protecting data. Security teams throughout the region need to take a hard look at what will have the biggest impact on data protection. They need to determine how to establish vital defenses that can stop attackers after perimeters and networks have been breached. This requires data-centric security capabilities for encryption, access control, tokenization, data access monitoring and data access analysis. These tools reduce an organization’s vulnerabilities, and they enable identification of suspicious activities while they’re in process, so breaches can be stopped before major damage results.

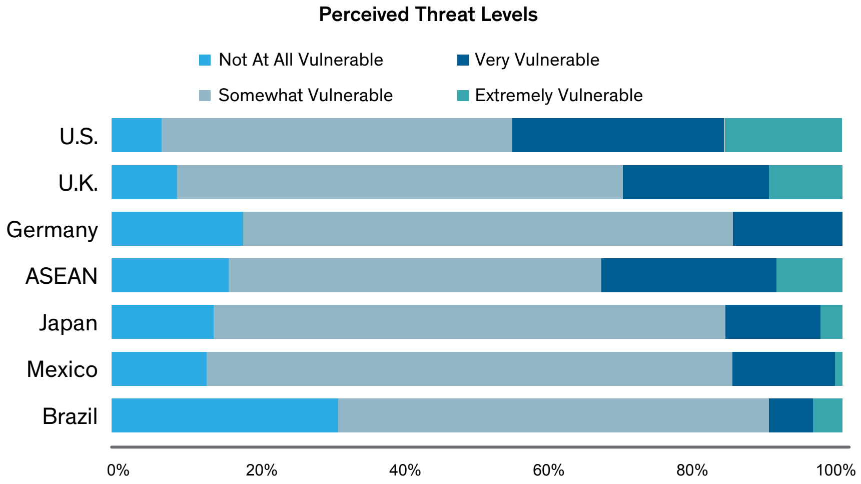


Figure 1: Perceived rates of vulnerability to insider threats

RESPONDENTS REPORTING WIDESPREAD VULNERABILITY

Respondents in both Mexico and Brazil are clear on the risks and their exposure to insider threats. A substantial majority of respondents—69% in Brazil and 87% in Mexico—indicated their organizations were at least "somewhat vulnerable." About 30% of Brazilians felt they weren't vulnerable, which was the highest response rate of any region worldwide. However, that still leaves seven out of 10 in the region that report feeling some degree of vulnerability.

In addition, respondents in both Mexico and Brazil pointed to high rates of failure in protecting data. Respondents were asked the following questions:

- Whether they'd encountered a data breach or failed a compliance audit in the last year
- Whether they were protecting data because of a breach at a partner or competitor
- Whether they were protecting data because they had previously encountered a data breach

> *"Respondents from Brazil reported the highest level of 'not at all vulnerable' to insider threats of all organizations globally (31%), but still showed 69% of organizations as feeling somewhat or more vulnerable."*

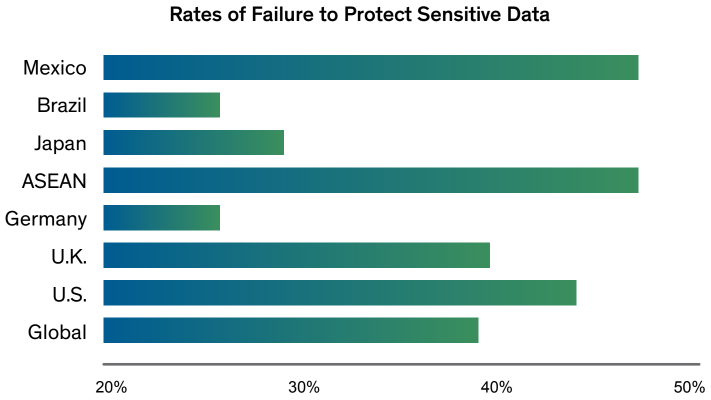


Figure 2: Rates of encountering a data breach or failing a compliance audit in the last 12 months

Mexico and Brazil are at opposite ends of the spectrum when it comes to the percentages of respondents that indicated their organizations had encountered a breach. Brazil was among the countries with the lowest rate of breaches or compliance failures, with only 26% of respondents indicating they'd experienced this form of breach or failure. On the other hand, Mexico was ranked among the highest, with 48% of respondents reporting they had encountered a breach or failed audit.

In particular, compliance failures represent a bigger problem than they may seem. Compliance mandates move at a gradual pace, with new or updated standards often only coming out every couple of years. On the other hand, security threats continue to evolve on a daily, and even hourly, basis. Industry compliance rules may have represented a gold standard for security best practices in the past, but this isn't the case any longer. While remaining compliant is a key requirement, this effort is now really only a starting point upon which effective security frameworks need to be built.

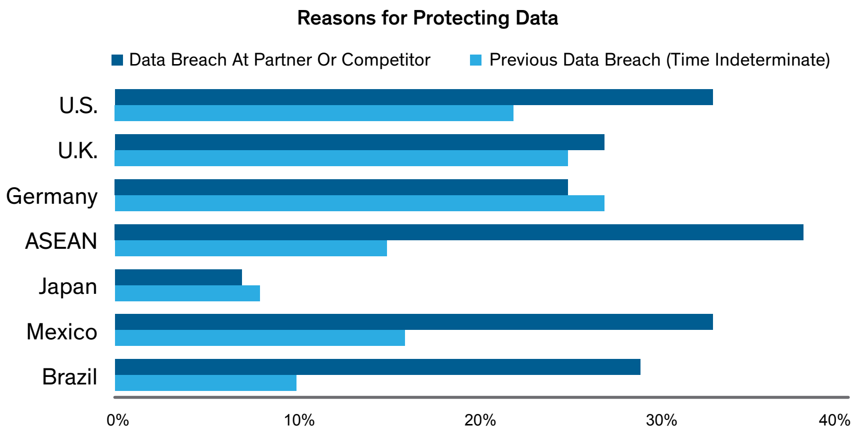


Figure 3: Protecting data because of a previous data breach or a data breach at a partner or competitor

> *"Responses from Mexico and Brazil showed that they were at opposite ends of the spectrum for previously encountering a data breach—Brazil the lowest at 26% and Mexico the highest at 48%."*

Rates of Compromise

Both around the world generally and in Mexico and Brazil in particular, the rates of compromise are high. Respondents were queried about whether breaches occurred in their organization at some time in the past and whether a partner or competitor had encountered a breach. In Mexico, just about half of respondents indicated yes to one of these questions, and almost 40% of respondents from Brazil said yes to at least one.

Perhaps most distressing is the following statistic: In spite of the frequency of breaches, respondents largely pointed to compliance as being effective. More than half of respondents said they viewed compliance as very or extremely effective: 52% of Mexican respondents and 59% of Brazilian respondents fell into one of these categories. These numbers raise concerns about an unrealistic sense of security that is being bred by compliance. If security leadership views their organization as being compliant, they shouldn't be complacent—particularly as threats continue to evolve and grow more sophisticated.

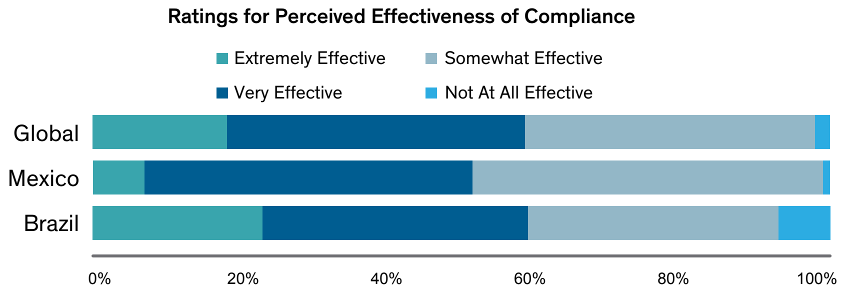


Figure 4: Respondents' ratings for the perceived effectiveness of compliance in protecting data

Summary

Similar to the rest of the world, these numbers for Mexico and Brazil paint a grim picture when looked at in aggregate. Respondents are feeling increasingly vulnerable in the wake of breaches and failed audits. In spite of these realities, however, many are placing a somewhat misguided faith in compliance as an effective route to security—even as evidence to the contrary continues to mount. Data breaches worldwide make clear that compliance does not equal security, and analysts openly express the opinion that "it isn't a matter of if you'll be breached, but when."

RESPONDENTS' BIGGEST CONCERNS

Insiders that Pose the Biggest Risk

It is interesting to review the perspectives of respondents in terms of who the most dangerous internal users are, and also to see how those perspectives have changed. Over the course of the past few decades, computing architectures, security approaches and security threats have all changed radically. During that time, a single internal group has emerged as the most potentially damaging: privileged users.

In order to carry out their responsibilities, these administrators need the permissions required to execute such tasks as software installation, system configuration, user permission management, resource allocation and more. Through this access, administrators in most organizations are almost always able to access the data and services that run on the systems they manage.

While this security gap posed by these privileged users is nothing new, it is one that has grown increasingly critical to address. In recent years, it has been privileged users behind some of the most high-profile compromises, including Edward Snowden, responsible for the well-publicized NSA leaks, and HSBC whistle-blower Herve Falciani. With the rising adoption of virtualization, cloud services and big-data implementations, new layers of administration—and of administrative privileges—that potentially expand the risk are also added.

Many respondents in this most recent survey seem to be well aware of the risks posed by privileged insiders. In the 2015 report, privileged users were the top-rated category for most dangerous insiders, receiving a 57% response globally and 68% in Mexico. It is important to see how this group has risen in prominence in recent years. For example, in our *2013 Vormetric Insider Threat Report*, privileged users were only selected by 34% of respondents, making it the third-ranked category, well behind "ordinary employees," which was selected by 51% of respondents (for more details, see the description of the 2013 report at the end of this document).

"The most dangerous Insiders —privileged users. Just as found in responses elsewhere, respondents from Mexico and Brazil reported that privileged users were their highest-risk employees, at 54% for Brazil and 68% for Mexico."

"Across the global pool of respondents, databases (50%), file servers (38%) and the cloud (36%) are the top-ranked areas where data is at risk."

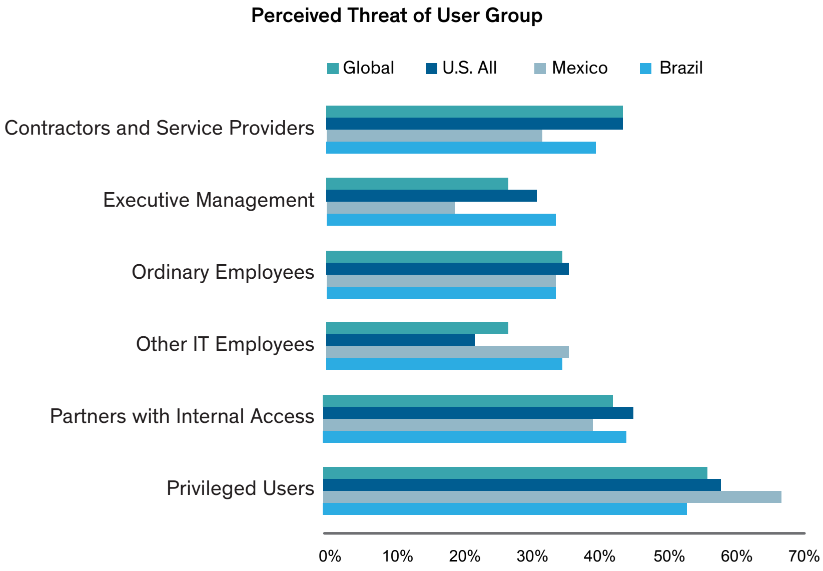


Figure 5: The most dangerous insiders are privileged users

Where Sensitive Data Resides and Where It's at Risk

Across the global pool of respondents, databases (50%), file servers (38%) and the cloud (36%) are the three locations that present the most risk in relation to the amount of sensitive data being housed. Mexico follows a similar pattern of responses: databases, 54%; file servers, 39%; and the cloud, 41%. However, in Mexico, PCs and workstations are a close fourth place, with a 36% response. In Brazil, PCs and workstations are tied for second place with file servers (35%), with only databases (53%) ranking higher.

For mobile devices, it seems clear that, while actual risks are currently low, there are significant concerns about how secure sensitive data is on these devices. In terms of the actual risk by volume of data, mobile devices only netted a 21% response globally, a 20% response among respondents from Mexico and a 23% response in Brazil. However, when it comes to the perception of risk, mobile devices rated highly, receiving a third-highest response of 37% globally and a 31% response in Mexico.

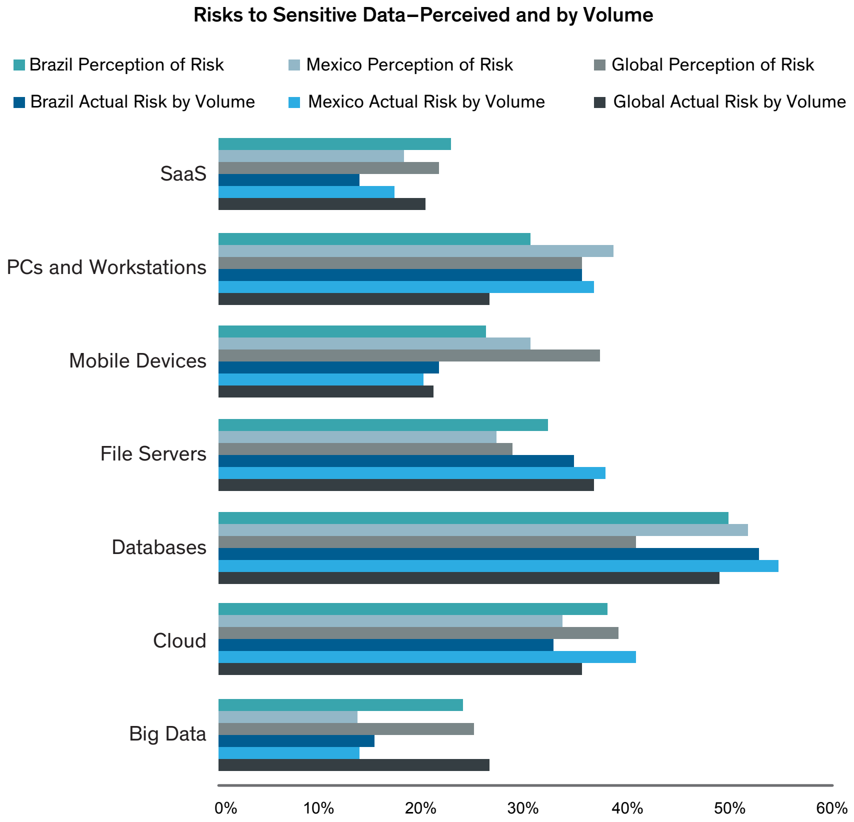


Figure 6: Respondents' perception of risk to sensitive data by category, and the volumes of sensitive data within those environments

> *"In Brazil, 63% of respondents reported housing sensitive data in IaaS cloud environments, compared to Mexico at 43%."*

EMERGING RISKS AND CONCERNS POSED BY CLOUD AND BIG-DATA ISSUES

Cloud Services

This survey and many others show that enterprise reliance on cloud services is continuing to grow more pervasive and that these services are housing more sensitive data. In Brazil, 63% of respondents are housing sensitive data in infrastructure-as-a-service (IaaS) environments, making it the highest-rated country in this regard. On the other hand, Mexico, at 43%, was the country with the lowest response rate in this category.

While it's clear the cloud is housing sensitive data, it's also clear that sensitive data residing in these environments is subject to risks that aren't in play for the assets housed within the traditional enterprise data center. For example, data may be exposed to other tenants in these multi-tenant environments. In addition, if an administrator working for the cloud service provider has their credentials compromised, sensitive data may be exposed. Further, many service providers continue to be the subject of government subpoenas in which customer data is being demanded by government authorities.

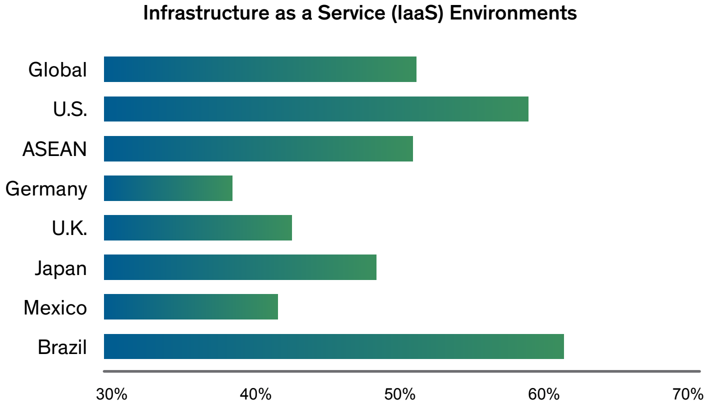


Figure 7: Reported rates of housing sensitive data in IaaS environments

All security-as-a-service (SaaS) environments covered in the survey had a high perception of risk. Beyond the risks confronting other cloud services, security teams have to contend with even more limited visibility and control in SaaS environments. For example, in IaaS environments, administrators can track resources at the operating system, storage and application level—while organizations running in SaaS environments lack this level of visibility. While SaaS categories all received fairly high levels of concern, both globally and in Mexico and Brazil, online backup and cloud storage were ranked number one and two respectively.

To address the risks posed by managing sensitive data in IaaS environments, data-centric controls will grow increasingly vital. By leveraging capabilities like encryption and access control and retaining ownership of keys used to encrypt and decrypt data, security teams can establish auditable, persistent controls over access to sensitive assets. Depending on their technical requirements and objectives, security teams can often choose whether to keep keys stored on the enterprise premises or in the cloud, while still retaining the control required.

Security teams can also mitigate the risks of housing sensitive data in SaaS-based cloud storage environments. In this case, they can leverage cloud encryption gateways that enable files to be encrypted before they are posted to the cloud. As a result, by retaining control over the encryption keys, security teams can also establish and sustain strong controls over who can access data, even when it is stored in these external cloud environments.

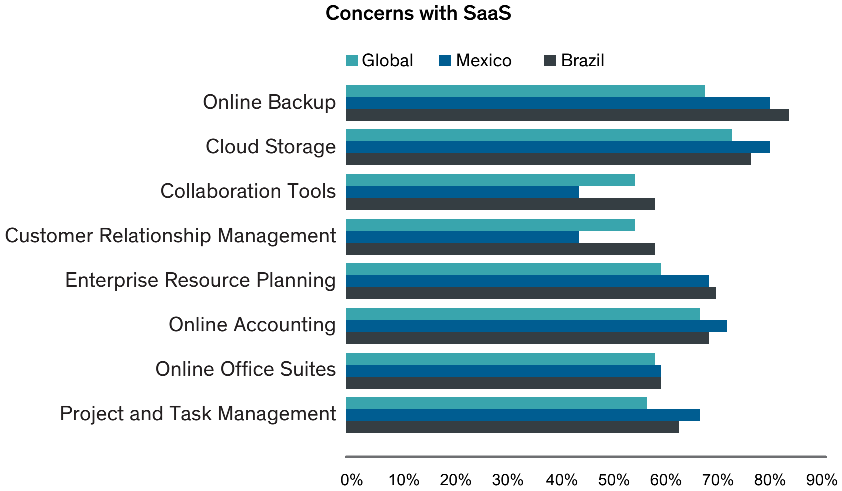
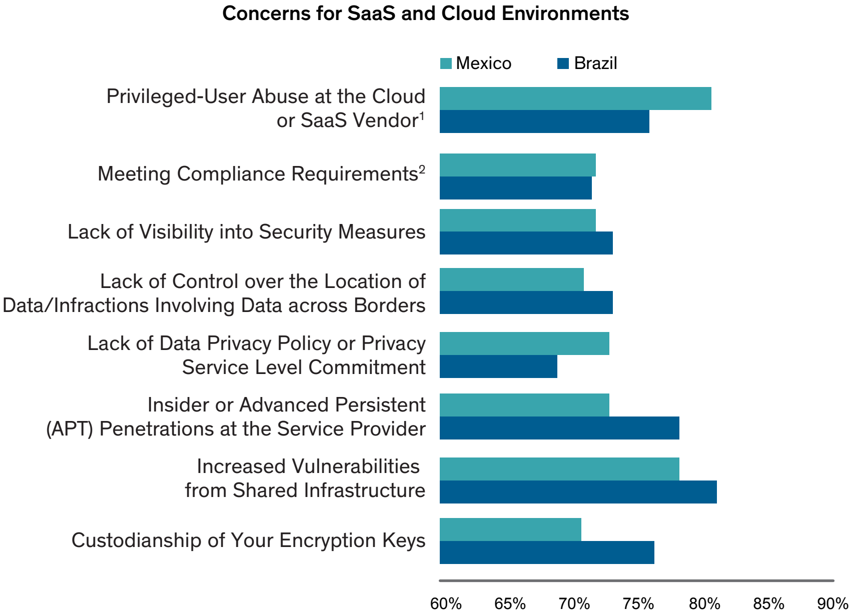


Figure 8: Reported rates of concern about data protection by SaaS environment type

How Should Cloud Providers Respond?

When asked about the concerns surrounding the cloud, respondents effectively said, “all of the above.” In both Mexico and Brazil, each category of concerns netted a response of 70% or higher.

What should cloud providers, including SaaS vendors, do to offset this problem? It will be vital to invest in the technologies that provide customers with the visibility and controls they need. Increasingly, it will be the cloud vendors offering these capabilities that will see their market share and customer lists expand.



[1] Includes system administrators, cloud administrators, storage administrators, virtualization administrators

[2] Examples: PCIDSS, national data protection laws

Figure 9: Levels of concern about data security issues in SaaS environments

Big Data: Adoption Rates and Concerns

Based on the relative responses, it appears big-data adoption rates in Mexico and Brazil are not as high as in other countries. It follows then that percentages, both in terms of actual risk and the perception of risk, are relatively low in both regions.

When looking at specific concerns relating to big data, the highest percentage of respondents in both Mexico and Brazil cited “privacy violations from data originating in other countries.” In contrast, while 49% of respondents in Brazil and 50% of respondents in Mexico selected this concern, on average this was a concern for only 32% of respondents globally.

Mexico and Brazil: Big-Data Concerns

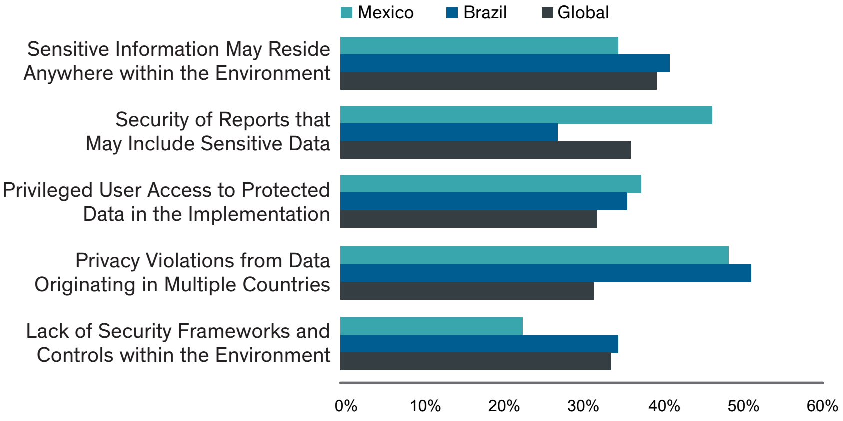


Figure 10: Biggest concerns for data security with big data

How Organizations Are Responding to Threats

Across the world generally, and within Mexico and Brazil, many respondents appear to be upping their IT security spending in order to contend with increasing threats.

Almost one-quarter, 24%, of respondents in Brazil indicated spending levels are going to be "much higher," a percentage that outstrips all other regions. When you consider that a total of 72% of respondents indicated spending will be somewhat or much higher, it seems clear that decision-makers in Brazil view security threats as serious. In Mexico, a smaller percentage, but still a solid majority (55%), indicated spending will be somewhat or much higher.

"DATA-AT-REST DEFENSES WERE VIEWED AS EFFECTIVE AT PREVENTING INSIDER THREATS BY 69% OF RESPONDENTS IN BRAZIL AND 74% IN MEXICO."

Where are respondents making security investments, and how effective do they think these investments are? Just as in other regions around the world, respondents in Mexico and Brazil seemed uncertain about which investments will yield the biggest dividends. These results also seem to be at odds with the news that has surrounded breaches in recent years. For example, network and endpoint defenses are proving to be vulnerable, yet respondents viewed these mechanisms as highly effective, receiving responses of 77% and 70% from global participants, respectively.

Data-at-rest technologies were also viewed as effective by a substantial percentage, receiving a three-quarters response rate globally, 69% in Brazil and 74% in Mexico. It is also interesting to note an apparent discrepancy in perceptions and investments in Mexico. While 74% viewed data-at-rest defenses as most effective, less than one-half have invested in these solutions.

At a high level, it appears many respondents are taking an "all-of-the-above" approach when making security investments. These numbers indicate respondents' organizations continue to pursue many strategies that they've employed for some time. While traditional perimeter and network-based defenses may have sufficed in prior years, those days have passed.

To contend with evolving and ever more advanced cyberattacks—and to align with the changing realities created by cloud-based services, big data and other trends—IT and security teams have a clear mandate to adapt their approaches. While employing a sound defense-in-depth strategy that leverages multiple technologies will continue to be critical, it is growing clear that an increased focus on data-at-rest defenses will be required moving forward.

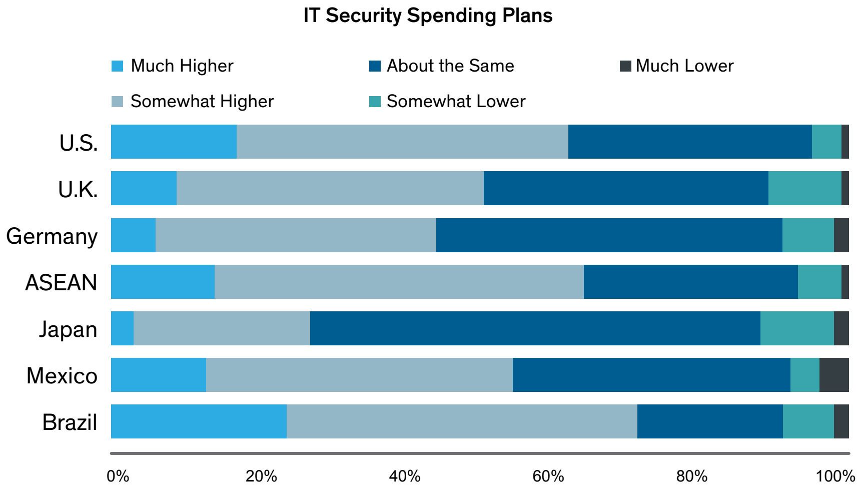


Figure 11: Respondents' reported rates of spending changes to offset threats to data over the next 12 months

How are security spending priorities changing? Recent years have seen a clear shift in priorities. In our 2013 report, we discussed how compliance was the number-one driver for IT security spending (for more details, see the description of the 2013 report at the end of this document). Globally, and in Mexico and Brazil, there's been a shift to focus squarely on preventing a data breach, which was the top-rated category across these regions. Protection of critical intellectual property and protection of finances and other assets were rated second and third, both globally and in Mexico and Brazil. Globally, fulfilling compliance requirements has dropped into fourth place out of five categories.

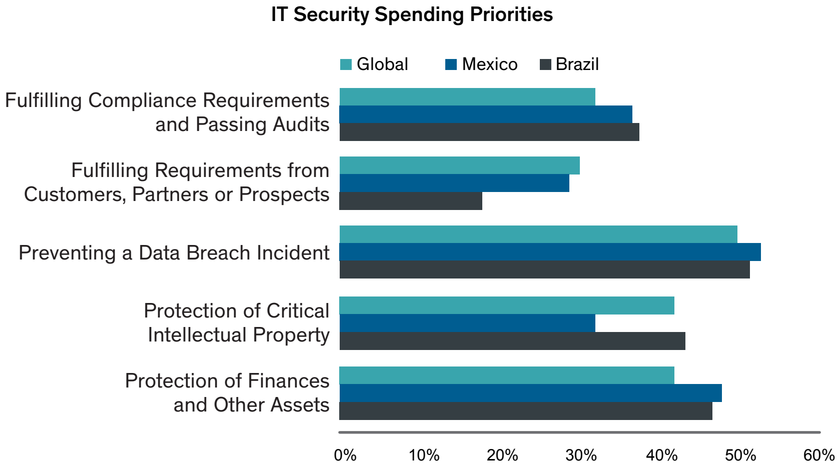


Figure 12: Top or second-level IT security spending priorities for respondents' organizations

"Many respondents are taking an 'all-of-the-above' approach when making security investments… While in prior years perimeter, endpoint and network defenses may have sufficed, those days have passed."

FOCUS ON MEXICO

Representatives polled from organizations in Mexico showed responses that are close reflections of those polled in other parts of the world. Enterprises are feeling vulnerable to threats from insiders and from the compromise of their credentials by outside threats (87% felt somewhat or more vulnerable). They seem to have good reason to feel vulnerable:

- 48% reported that their organizations had encountered a data breach or failed a compliance audit in the last year (the highest level measured in the survey).
- 16% were protecting data because of a previous data breach at their organization at some time in the past.
- 33% were protecting data because of a breach at a partner or competitor.

The level of these responses represents a systematic failure to protect the affected organization's data. In addition, with compliance no longer representing a best practice for data protection, the response rate from Mexico citing compliance as very to extremely effective (52%) represents yet another concern. Compliance requirements are rapidly falling behind the latest cyberattacks, and they now represent much less than even a good baseline for data protection—they represent the best practice for protecting against yesterday's attacks. As a result, compliance regimes have rapidly become less effective, while still draining an organization's IT security funding to meet what are often outdated requirements.

There are good signs that indicate respondents' organizations in Mexico are taking threats to data seriously:

- Recognition that privileged users represent the greatest threat to sensitive data is strong, with respondents selecting them as the insiders that pose the greatest risk. At 68%, responses were 28% higher than the next category—partners with internal access at 40%.
- 55% of respondents said that their IT security spending would be somewhat to much higher to offset these threats.

However, responses identified the same patterns as were found worldwide in how this spending will be applied. With minor variation, there are plans to increase all categories of security spending at approximately the same level (50% to 70%). This represents a failure to understand where to increase investment to best prevent the loss of data.

Respondents also reported usage of sensitive data within the cloud (41%) and SaaS (18%) environments comparable to global averages, but also reported lower usage of sensitive data in big-data environments than other regions (15% in Mexico versus a global average of 27%). When it comes to IaaS environments, however, Mexico had the lowest level of sensitive data use within this cloud environment (43%).

Overall, the responses from Mexico indicate that the respondents feel their enterprises are at high risk of insider attacks—whether from compromise of an insider's credentials or from a malicious insider, contractor or partner. Many organizations also appear to be taking action by increasing spending, but are encountering the same confusion as other organizations across the globe about what needs should be prioritized.

At this point, the best additions to most organizations' layered IT defense set are enhancements that can protect data-at-rest from compromise, while keeping that data available for safe business use. The most effective controls for this are encryption with access controls, data access monitoring and data access profiling—both at the system level and within applications. This combination reduces attack surfaces by limiting access to only users and applications that need it, and then allowing that usage to be tracked to indicate when a compromise is in process.

> *"48% of respondents in Mexico reported that their organizations had encountered a data breach or failed a compliance audit in the last year—the highest level measured in the survey."*

FOCUS ON BRAZIL

Responses from IT decision-makers in Brazil indicated that organizations are feeling somewhat less vulnerable than their global counterparts. Reports of protecting data because of a previous data breach (either their own or that of a partner or competitor) or because of encountering a data breach in the last 12 months were among the lowest levels reported globally.

- 69% of respondents felt vulnerable to insider threats, which is the lowest level measured of all those surveyed.
- 26% of respondents said they had previously encountered a data breach; this ties Brazil with Germany for the lowest level.
- 39% said they were protecting data because of their own data breach or a breach at a partner or competitor, which is the lowest reported rate, except for that of Japan.

Even so, these are fairly high numbers indicating that Brazil is being exposed to the same kinds of attacks and pressures as are felt elsewhere in the world, albeit at a somewhat lower rate than many other regions.

> “RESPONDENTS IN BRAZIL REPORTED THAT THEY WERE INCREASING SPENDING TO OFFSET THREATS AT THE HIGHEST RATE MEASURED—72%.”

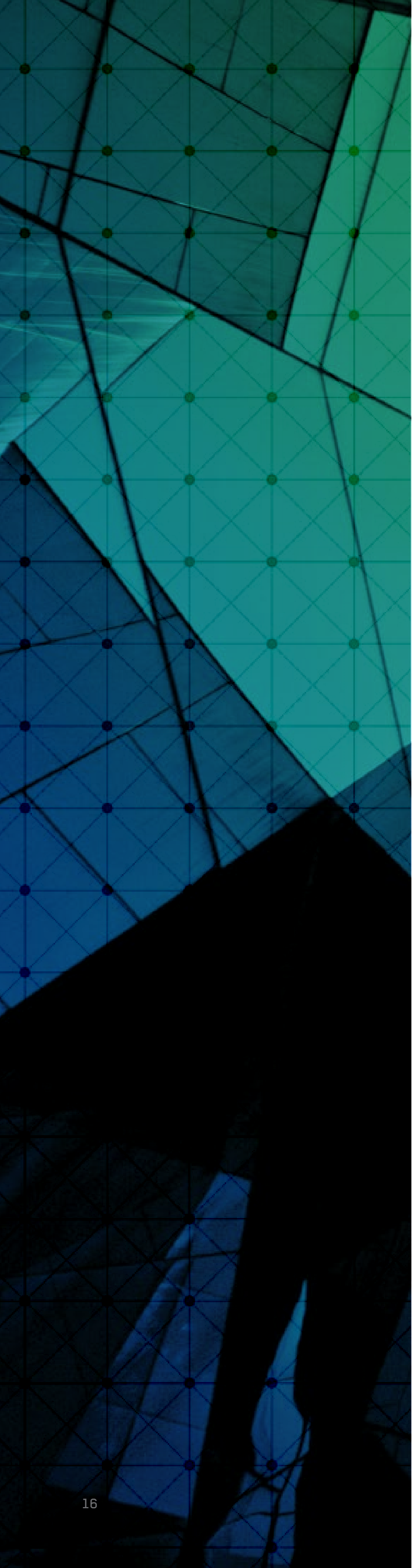
Usage of sensitive data in new technology environments such as the cloud, big data and SaaS doesn’t appear to be the reason for this perception of lower risk, as respondents reported usage of sensitive information within these environments similar to global averages:

- Cloud: 41%, Brazil; 36%, global
- SaaS: 18%, Brazil; 21%, global
- Big data: 17%, Brazil; 27%, global

Respondents from Brazil also had comparable response rates as the global average about the perceived effectiveness of compliance (rate of compliance as very or extremely effective at protecting data: Brazil, 59%; global, 58%). As noted earlier, and as evidence to the contrary continues to mount, this represents a misguided faith in compliance as an effective route to security.

At the same time, Brazilian respondents reported that their organizations were increasing spending “much higher” in the next year to offset these threats; this was the highest rate we measured globally (24%). They were also increasing spending overall at the highest rates of any region that we measured (72%). These investments, however, are scattered across all areas of investment fairly evenly (network, endpoint/mobile, data-in-motion, data-at-rest and analysis/correlation tools), just as with every region that we measured.

This data set clearly illustrates that respondents from Brazil understand that their organizations are under threat, but just as with organizations elsewhere, they still haven’t absorbed that their first priority should be to lock down sensitive data. Many IT organizations have focused for years on protecting networks, endpoints and transactions as the best way to safeguard their organizations, but analysts today consistently point out that peripheral, network and endpoint defenses are no longer effective at keeping out attackers or stopping malicious insiders. A belief that compliance standards are a good way to achieve security is probably a factor here as well. Just as with their global peers, enterprises in Brazil need an added emphasis on protecting data as a first step, in order to protect sensitive data assets even when accounts have been compromised and systems and networks penetrated.



KEY RECOMMENDATIONS FOR ADDRESSING INSIDER THREATS

The following are some key guiding principles security and IT leadership should consider as they seek to strengthen their defenses to guard against insider threats:

- **Establish multi-layered defenses.** Network and endpoint security solutions consistently fail to stop or even detect attacks by insiders or advanced attacks that exploit compromised user credentials. As a result, moving forward, it will be incumbent upon security teams to establish a layered defense that combines traditional approaches as well as advanced data protection techniques, such as database or file encryption with access controls, tokenization, data masking, application-layer encryption and cloud encryption gateways.

- **Secure data at the source.** Increasingly, IT and security teams will need a layered IT security architecture that is focused on protecting data at the source—wherever it resides. For most organizations, this will require establishing controls over servers and databases on premises, as well as in big-data applications and remote cloud environments. Encryption with policy-based access controls is a critical starting point for this approach.

- **Leverage platforms.** To address security demands while maximizing staff and cost efficiency, IT and security organizations will be well served by moving away from point tools and starting to leverage security platforms that offer comprehensive, unified capabilities that address all critical enterprise data protection demands.

- **Institute effective data access monitoring.** To maximize security, it is vital to implement integrated data monitoring and technologies such as security information and event management (SIEM) systems. This represents a critical means to effectively track data usage and identify unusual and malicious access patterns.

- **Go beyond compliance.** To keep the whole organization safe, companies must realize that compliance mandates represent protections for the attacks of yesterday, and go beyond compliance regimes to develop an integrated, holistic data security strategy that includes monitoring, relevant access controls and high levels of data protection. Through this approach, security can be left to the chief information security officer's team—and kept out of the boardroom.

ABOUT THE *2013 VORMETRIC INSIDER THREAT REPORT*

The 2013 Vormetric Insider Threat Report was a collaborative research project conducted by Vormetric and the Enterprise Strategy Group (ESG). The report was based upon a survey of 707 IT professionals responsible for evaluating, purchasing or managing information security technologies and services for their organizations. Respondents came from companies representing numerous industry and government segments. Company sizes varied widely, with revenues ranging from less than $250 million to more than $20 billion. The survey was completed in July 2013, and the report was released in September 2013.

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.

HARRIS POLL—SOURCE/METHODOLOGY

Vormetric's *2015 Insider Threat Report* was conducted online by Harris Poll on behalf of Vormetric from September 22 to October 16, 2014, among 818 adults, ages 18 and older, who work full-time as IT professionals and have at least a major influence on IT decision-making in their companies. 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 U.K. (103), Germany (102), Japan (102) and ASEAN (103), with an additional 102 each from Brazil and Mexico between March 20 and April 2, 2015. Outside of the U.S., companies had 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.

FURTHER READING

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

2015 **VORMETRIC** INSIDER THREAT REPORT–*MEXICO AND BRAZIL EDITION*

Vormetric.com/InsiderThreat/2015

Vormetric
Data Security™