

2016
**VORMETRIC
DATA THREAT
REPORT**

Trends in Encryption
and Data Security

GLOBAL EDITION

#2016DataThreat



TABLE OF CONTENTS

INTRODUCTION	3	ENCRYPTION USE CASE DRIVERS	13
EXECUTIVE SUMMARY	4	BARRIERS TO ADOPTION OF DATA SECURITY	15
Lies, Damn Lies and Statistics	4	SECURING SAAS, BIG DATA AND IOT	16
Compliance Does Not Ensure Security	5	TOP REGIONAL DIFFERENCES	20
Times Have Changed. Security Strategies, Not So Much	5	TOP DIFFERENCES BY INDUSTRY SEGMENT	21
Mobile, Cloud and Big Data: Driving Change, Creating Complexity	6	ADDITIONAL FINDINGS	21
SPENDING INTENTIONS	7	RECOMMENDATIONS	22
REASONS FOR PROTECTING DATA	8	METHODOLOGY	23
DATA SOVEREIGNTY	10	ANALYST PROFILE	23
THREAT ACTORS	11	ABOUT 451 RESEARCH	23
SENSITIVE DATA LOCATIONS	12	ABOUT VORMETRIC	23

OUR SPONSORS



INTRODUCTION

The previous three editions of the *Vormetric Insider Threat Report* provided insights into the growing threat to corporate data from insider attacks, motivated in part by the numerous concerns raised by the Edward Snowden incident and revelations of widespread surveillance efforts by the NSA.

Since the publication of that report, we have been exposed to an ongoing and seemingly endless string of data breaches that have elevated concerns about protecting sensitive data beyond the technical realm and into the mainstream public consciousness. Hardly a week goes by without news of another damaging data breach incident—according to the Privacy Rights Clearinghouse, the number of records breached in 2015 was more than twice that of 2014—despite the fact that, collectively, we are spending billions each year on various forms of cybersecurity and venture capitalists are spending princely sums on startups touting the latest and greatest new security offerings.

Yet, as we have been painfully reminded in the past twelve months, threats to data no longer come from insiders alone, whether malicious or inadvertent. Indeed, many of the most pernicious attacks we've seen in the recent past have come, not just from insiders, but from an assortment of external actors—including cybercriminals, nation-states, hacktivists and cyberterrorists—that frequently masquerade as insiders by using stolen or compromised credentials to access all types of valuable data, including personally identifiable information (PII), personal health information (PHI), financial data and intellectual property.

In addition to “bad guys” acting like insiders, firms are also relying on a growing list of third-parties to handle both non-core and increasingly core business functions. In addition to traditional outsourcing relationships, public cloud services, big-data applications and the emerging Internet of Things (IoT) have collectively expanded the data supply chain and contributed to an exponential increase in the number of external parties with some level of access to our networks and sensitive data. Prior work by 451 Research has indicated that, in the case of some large global firms, the number of third-party data relationships can easily number in the tens of thousands. Thus, as the line between insider and outsider continues to blur, we have accordingly expanded the scope of our study to include external actors in an effort to encompass all manner of threats to sensitive data.

The *2016 Vormetric Data Threat Report* is based on a survey conducted by 451 Research during October and November of 2015. We surveyed 1,100+ senior security executives from across the globe, including from key regional markets in the U.S., U.K., Germany, Japan, Australia, Brazil and Mexico, and key segments such as federal government, retail, finance and healthcare.



“91% IMPLEMENTING SECURITY BEST PRACTICES SHOWED THE LARGEST YEAR-OVER-YEAR INCREASE OF ANY CATEGORY.”

EXECUTIVE SUMMARY

At a high level, this year's survey contained a mix of encouraging and not-so-encouraging results. On the positive side, the number of respondents (39%) who indicated that their organization has either experienced a data breach or failed a compliance audit due to data security issues in the past year has held steady from our two prior surveys, despite the increased volume of data breaches. We're also seeing encouraging signs that data security is moving beyond serving as merely a compliance checkbox. Though compliance remains a top reason for both securing sensitive data and spending on data security products and services, implementing security best practices posted the largest gain across all regions. Another encouraging sign is that the majority of respondents expect their spending on data security to increase: 58% said their spending to protect against data threats would be either "somewhat higher" (46%) or "much higher" (12%), up slightly from 56% last year.

On a more somber note, however, more respondents (91%) were feeling some degree of vulnerability to both internal and external threats to data than last year (87%), and nearly one-third were feeling either "very vulnerable" or "extremely vulnerable" (Figure 1). It's also worth pointing out that nearly two-thirds (60%) of our respondents indicated that their organization had been subject to a data breach at some point in the past, up slightly from last year's survey at 58% (although energy firms represented a small part of our sample, the sector registered the highest increase in breaches in the past year at 41%, versus 22% overall). Thus, while the results don't necessarily indicate things have gotten markedly worse, they certainly haven't gotten better, and in most cases our exposure to data theft remains alarmingly high and may still be undetected.

"Though compliance remains a top reason for both securing sensitive data and spending on data security products and services, implementing security best practices posted the largest gain across all regions."

Vulnerability of Sensitive Data

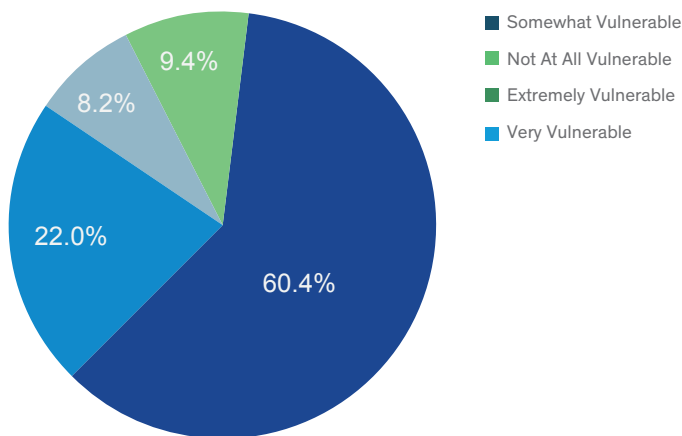


Figure 1: Percentage of organizations that feel their sensitive data is vulnerable to internal and external threats

Lies, Damn Lies and Statistics

As the saying goes, "data doesn't lie," and both the size of our sample and relative stability and year-to-year continuity of our previous surveys suggest the results of this study are statistically valid. But statistics can also reflect prior misconceptions and prejudices that have persisted throughout the industry. Overall, our 2016 survey results shine a light on lingering questions that suggest many companies remain in denial about the threats posed to their data by both insiders and outsiders, as well as the most effective ways to combat them.

Compliance Does Not Ensure Security

For example, though 61% had experienced a breach in the past, only 21% cited a past data breach as a reason for securing sensitive data, and only 26.8% cited breaches at competitors like Sony, Home Depot or Target as a motivator for increased attention to data security. And while we were encouraged to see the shift toward implementing security best practices, many security executives across the globe still appear to equate compliance with security—nearly two-thirds (64%) of our respondents viewed compliance requirements as either “very effective” or “extremely effective” in preventing data breaches, up from 58% last year. It’s no surprise that the most regulated industries—IT, healthcare, financial services and retail—have the most sanguine views on the effectiveness of compliance requirements, particularly IT (27% selected “very effective”). But as we have learned from data theft incidents at companies that had reportedly met compliance mandates (such as Target), being compliant doesn’t necessarily mean you won’t be breached and have your sensitive data stolen.

Times Have Changed. Security Strategies, Not So Much

Spending intentions also reflected a tendency to stick with what has worked—or not worked—in the past. While the majority of respondents plan to increase spending to protect their sensitive data, the category leading the charge in terms of increased spending intentions was once again network security at 48%, followed by security incident and event management (SIEM) and endpoint security at 43% each. Over time, we suspect that the security industry as a whole will come to grips with the fact that perimeter defenses offer little help defending against multi-stage attacks: Once our adversaries pass the first line of defense, there is little standing in their way.

While new tools and techniques in threat detection and analytics that can help provide visibility into anomalous behavior and prevent escalation of attacks are currently being developed, none of these emerging techniques can offer a silver bullet. As we’ve learned, determined attackers will eventually find a way in. Yet data-at-rest approaches that have proven to be effective at protecting the data itself once attackers bypass perimeter defenses—such as file and application encryption and access controls—are not seeing the same acceleration in spending intentions.

Clearly, there’s still a big disconnect between what we are spending the most of our security budget on and what’s needed to ensure that our sensitive data remains secure. 451 Research estimates that nearly \$40 billion is spent annually on information security products, and the vast majority of that sum is spent on legacy security technologies like firewalls, anti-virus software and intrusion prevention—yet data breaches continue to increase in both frequency and severity. To a large degree, it can be argued that security professionals are like old generals fighting the last war, and our old standby tools are no longer sufficient on their own.

“NEARLY TWO-THIRDS OF OUR RESPONDENTS VIEWED COMPLIANCE REQUIREMENTS AS EITHER ‘VERY EFFECTIVE’ OR ‘EXTREMELY EFFECTIVE’ IN PREVENTING DATA BREACHES.”

Mobile, Cloud and Big Data: Driving Change, Creating Complexity

With the rapid adoption of mobile, cloud and big data, it's no longer enough just to secure our networks and endpoints. A lot of work needs to be done by both vendors and their enterprise customers before we can genuinely feel confident we are doing the right things. That said, 57% of respondents to this year's survey cited "complexity" as the main barrier to adoption for data security, with "lack of staff to manage" (38%) a distant second. If data security hopes to emerge from the shadow of its network and endpoint security peers, the implicit message for data security vendors is to make products that are simpler to use and require less manpower to implement and maintain. This could point the way to greater acceptance of platform approaches as an alternative to point products, more automation and potentially more services-based delivery options for various forms of data security, such as encryption, key management and data loss prevention (DLP), to name a few obvious candidates.

KEY FINDINGS:

- Roughly 39% of respondents indicated their organization has either experienced a data breach or failed a compliance audit due to data security issues in the past year—in line with prior surveys—and nearly two-thirds (61%) have been breached at some point in the past (although energy firms represented a small part of our sample, the sector experienced nearly twice the level of breach activity as the overall sample: 41% versus 22% overall).
- Overall, respondents are feeling slightly more vulnerable to data threats—90% felt at least "somewhat vulnerable" to both internal and external threats to data, up from 87% last year.
- Interestingly, two-thirds (64%) viewed compliance as either "very effective" (47%) or "extremely effective" (17%) for protecting sensitive data, compared to 58% last year.
- Though compliance remains a key driver of data security spending, implementing best security practices has gained in importance as a top reason for both securing sensitive data and spending on data security products and services, posting the largest gain across all regions.
- Lack of knowledge of where sensitive data is located is frequently noted as a barrier to effective data security, particularly as data is increasingly distributed across mobile, cloud and big-data environments. Yet nearly half (47%) of all respondents claimed they had "some idea" where their sensitive data is located, and a surprising 43% claimed to have "complete knowledge" of their sensitive data, which suggests respondents may be in denial about their sensitive data awareness.
- Only 21% cited a past data breach as a reason for securing sensitive data, and only 26.8% cited breaches at competitors like Home Depot or Target.
- Across nearly all geographies, "complexity" was the number-one barrier to adopting data security tools and techniques more widely, selected by 57% of respondents.
- Complex deployments also typically require significant staffing requirements, and the "lack of staff to manage" came in as the second highest barrier, albeit a distant second at 38% of respondents.

SPENDING INTENTIONS

As noted above, overall spending intentions suggest a focus on business as usual and highlight a growing disconnect between what we are spending the bulk of our security budgets on and what's needed to prevent data theft. Network defenses (firewalls, intrusion protection systems [IPS], DLP, etc.) had the most "increase" responses for spending intentions at 48% (Figure 2). For many security professionals, it's fairly straightforward to plug another appliance in the rack, sprinkle on some rules and voila! Box checked, move on to the next fire. Another old staple of most firms' security arsenals, endpoint security, had the second highest intended increase at 44%, tied with security analytics and correlation tools (SIEM, log management, etc.).

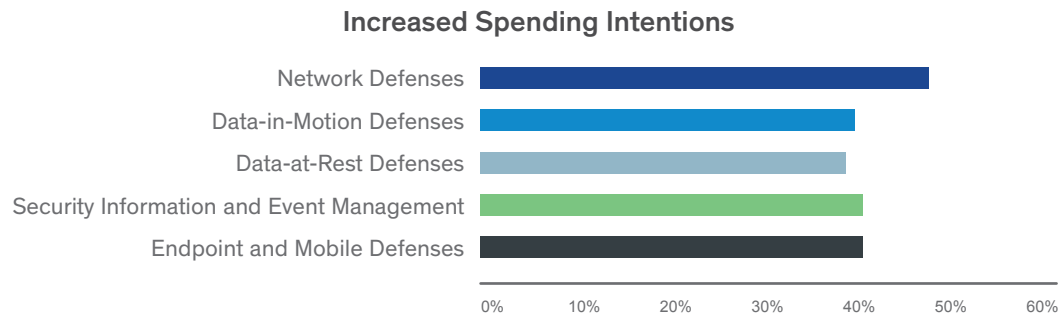
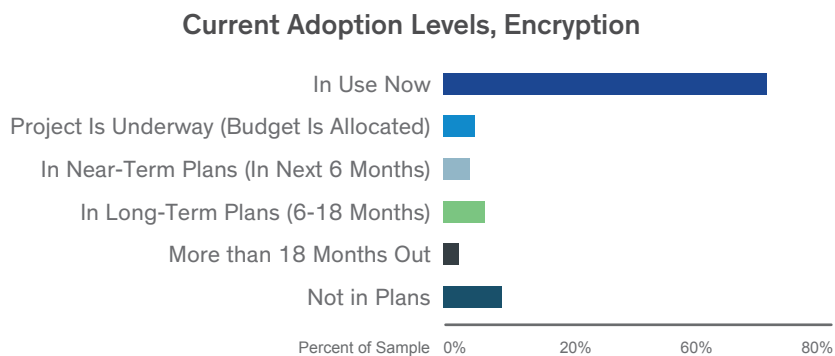


Figure 2: Planned spending increases, by product category

Conversely, products that can directly help mitigate data theft—data-in-motion and data-at-rest defenses such as encryption—were near the bottom of the list at 40% and 39%, respectively. We suspect that part of the reason is that data-at-rest protections have typically been most widely applied to legacy resources, such as PCs, laptops, mobile devices, email messages and databases and file servers, and thus are already widely deployed (Figure 3).



Source: 451 Research Information Security Voice of the Enterprise Survey, Q3, 2015

Figure 3: Current adoption levels, encryption

REASONS FOR PROTECTING DATA

Still a Lot of Faith in Compliance Mandates, Though Best Practices Gaining Steam

As we have been made painfully aware over the past few years, being compliant with existing regulatory requirements doesn't necessarily mean you won't be breached and your sensitive data won't be stolen. Many of the victims of recent well-known breaches had reportedly been certified as PCI compliant, and some had gone above and beyond what was required by their respective standard. This is not to suggest that compliance mandates have no value in helping companies improve their security posture; indeed, compliance mandates can help firms establish a baseline of what may be needed to secure data. But one of the limitations of compliance mandates is that they can't possibly adapt fast enough to the constantly changing threat environment or be specific enough to provide detailed guidance on what is needed. It's also not necessarily reflective of a problem with the standards themselves, but often of the way those standards are implemented by IT professionals and interpreted by standards assessors and auditors.

Nonetheless, many security professionals still equate compliance with security, and globally, nearly two-thirds (64%) viewed compliance requirements as either "very effective" or "extremely effective" in preventing data breaches. Brazil was the most naively optimistic with 82% placing a high degree of confidence in regulatory mandates helping to protect data. Compliance also scored high in terms of the most important reasons for securing sensitive data and was still the second-ranked response globally—it was highly ranked by countries such as the U.S. (55%), Australia (51%) and Germany (47%), as well as industries that face strict regulatory compliance or data residency/privacy mandates, such as healthcare (61%) and financial services (55%).

However, there are some signs that other motives for securing data are gaining momentum. Reputation and brand protection retained its top spot and was selected by nearly 50% of respondents—it was also the top response in the U.S., U.K. and Mexico (Germany and Japan ranked requirements from business partners and customers as their top choice). Implementing security best practices remained in third place but showed the largest year-over-year increase of any category, increasing from 39% to 44% (Figure 4).

Most Important Reasons for Securing Sensitive Data

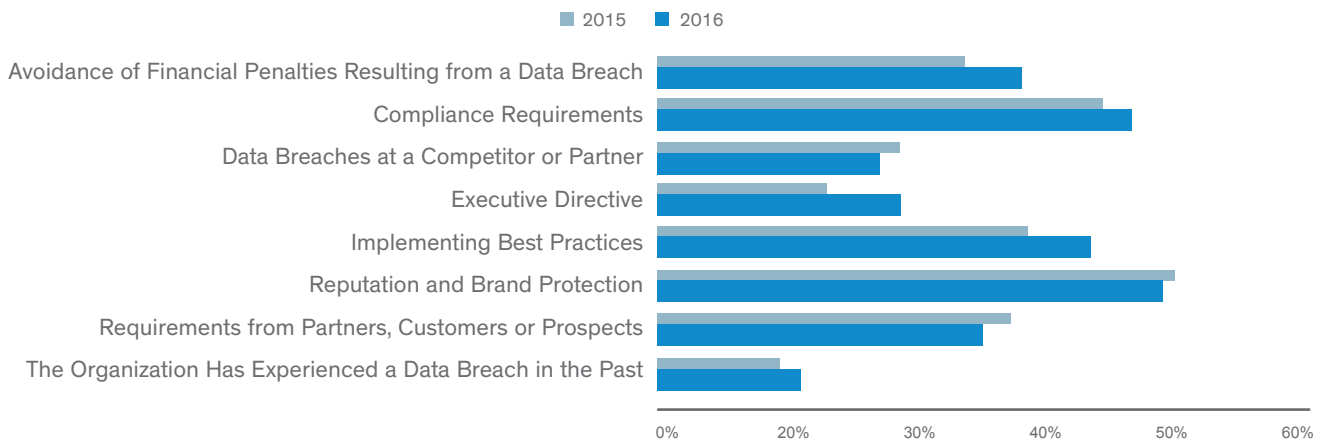


Figure 4: Most important reasons for securing sensitive data, 2015 versus 2016

“IMPLEMENTING SECURITY BEST PRACTICES SHOWED THE LARGEST YEAR-OVER-YEAR INCREASE OF ANY CATEGORY.”

However, when it comes to the main motivators for spending on overall IT security, compliance jumped back into the top spot with a slight edge over protecting brand/reputation, and implementing security best practices held steady in third place (Figure 5).

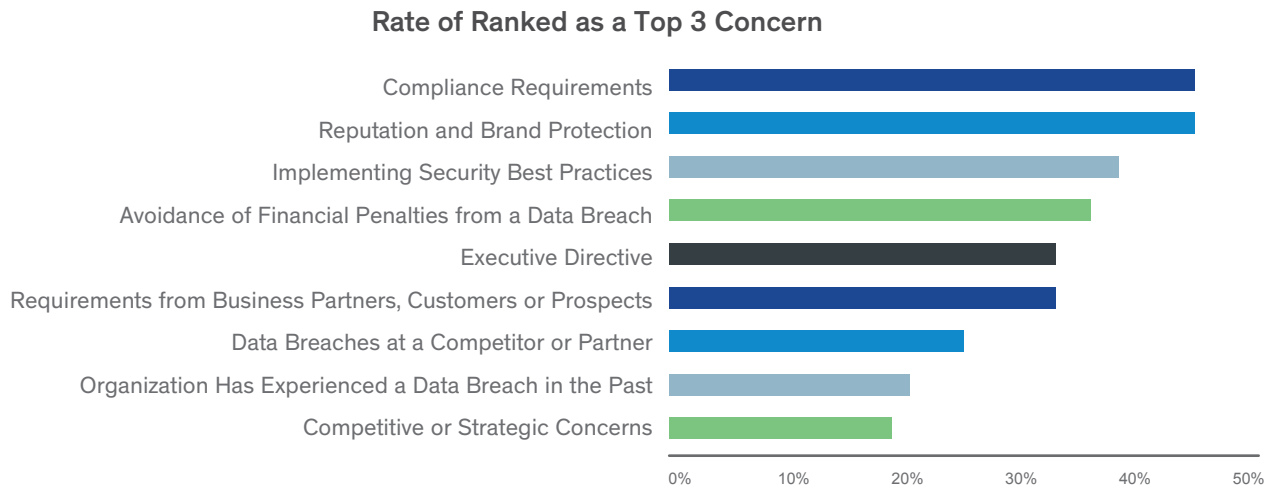


Figure 5: Ranked impact on security spending, highest to lowest

Interestingly, though 61% of respondents admitted to being hacked in the past, data breaches at competitors or partners appear to have had less of an impact on companies’ plans for securing sensitive data and spending intentions than other factors such as compliance, security best practices and brand protection, ranking seventh overall. On the positive side, when asked specifically how high-profile and potentially embarrassing incidents—like the Sony breach, Hilary Clinton’s email conundrum, Snowden’s embarrassment of the CIA/NSA and the recent Ashley Madison hack—would impact spending, 53% indicated they planned to increase their spending on data security, with the retail (65%) and healthcare (64%) verticals leading the charge.

DATA SOVEREIGNTY

Despite Safe Harbor Concerns and Pending Regulations, Data Sovereignty is Not Yet a Top Driver For Data Security

We also asked respondents a new question about the types of data firms are most concerned with protecting, and once again, we see the strong pull of regulatory compliance exerting its influence. Overall, respondents were most concerned with protecting PII (personally identifiable information such as Social Security numbers), financial data and classified data, in that order. Data subject to data residency/ data sovereignty laws came in near the bottom of the list, which is highly surprising given the fallout from the Snowden/NSA revelations and recent concerns about the expiration of Safe Harbor protections with the U.S. A related and somewhat equally surprising result was that protecting customer or business partner data was ranked dead last (Figure 6).

“Despite the Snowden/NSA revelations and concerns about the expiration of Safe Harbor protections, data sovereignty is not yet a top driver for data security.”

Ranked as a Top 3 IT Security Spending Concern

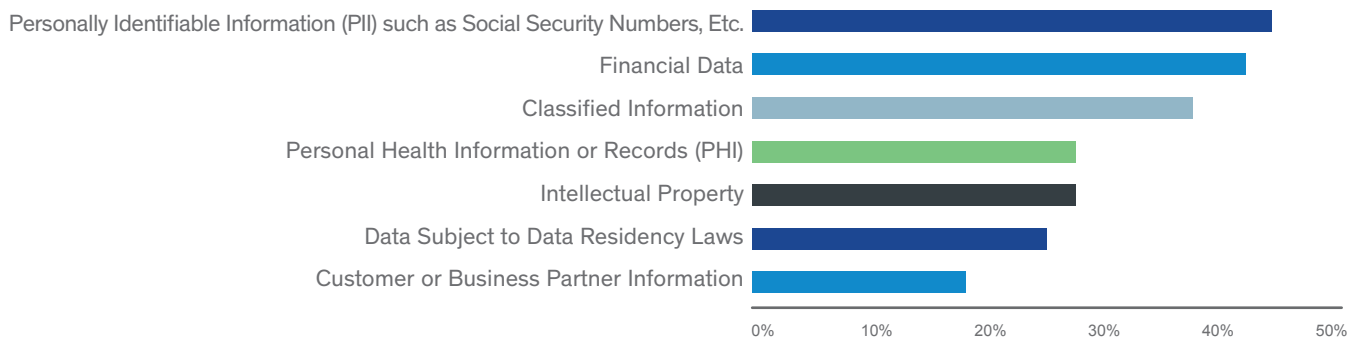


Figure 6: Data concerns, ranked highest to lowest, all responses

The results were a bit more encouraging when respondents were asked this year about their encryption strategy. While meeting compliance requirements and protecting brand and reputation were still near the top of the list, the top choice was to use encryption to follow best practices, regardless of compliance mandates, most notably among financial services firms. And while many data security vendors have recently made large efforts to position themselves as protectors of intellectual property, only 18% selected protecting IP as a key piece of their encryption strategy.

Pending Data Sovereignty Regulations Could Push Data Security into the Boardroom

Though much has been made recently of the invalidation of Safe Harbor protections between the European Union (EU) and the U.S., the reality is that Safe Harbor has been on life support since the Snowden affair several years ago, in large part since it relied on self-certification as a primary enforcement mechanism and was thereby generally ineffective. What may well have more of an impact, however, are the more than 100 national and regional laws that mandate protection of personal data, particularly the General Data Protection Regulation (GDPR) currently being drafted by the EU. Unlike the EU's Directive 95/46/EC (the "Directive") it is intended to replace, GDPR will be universally enforceable in law across all EU member nations and will provide oversight and apply specific penalties for non-compliance. GDPR could be enacted as

early as the end of 2015 and will provide a two-year window for companies doing business within the EU or processing data pertaining to EU citizens to comply with its provisions. Regardless of its final form, however, GDPR will clearly have “more teeth” than its predecessor and for many enterprises will require substantial changes to the way they do business. Beyond GDPR, global firms operating outside the EU may also have to comply with different regional and national data privacy laws in privacy-sensitive countries like Canada and Australia, as well as in Asia and Latin America.

Though the exact form of many of these laws has yet to take shape, we suspect many global firms will take steps to get ahead of the curve. For example, we are seeing growing evidence of cloud and Internet providers like Microsoft® and Salesforce® building local data centers to avoid running afoul of data sovereignty laws. We also anticipate that data sovereignty will provide an added boost for the application of data encryption and tokenization, both of which are frequently specified as a primary control for existing data privacy regulations. In the case of GDPR specifically, firms will need to, not only provide for protection of data, but also be able to prove it via detailed audit logs and forensics.

“Privileged users remain the primary insider threat concern, though concerns about executive management increased sharply.”

“Despite concerns about cyber-warfare from China, Russia, Iran and North Korea, cybercriminals are seen as the number-one external threat.”

THREAT ACTORS

Privileged Users, Executives and Cybercriminals Head the List of Risky Threat Actors

In terms of threat actors, privileged users (admins, DBAs, etc.) were identified once again as presenting the largest risk to an organization’s sensitive data by 58% of respondents, a slight increase from our prior survey (Figure 7). The potential for abuse by privileged users has been in the spotlight since the fallout from the Snowden incident, and privileged account management has received substantial interest as a result. Privileged access has also been boosted in the public consciousness by malicious threats and malware that compromise privileged credentials as a primary way of escalating their ability to access critical data. The results were true across most geographies, although notably Japanese respondents overwhelmingly view ordinary employees as the number-one risk, while energy companies view ordinary employees with greater suspicion than other verticals (53% of energy companies versus 34% overall).

IT Insiders Posing Greatest Risk

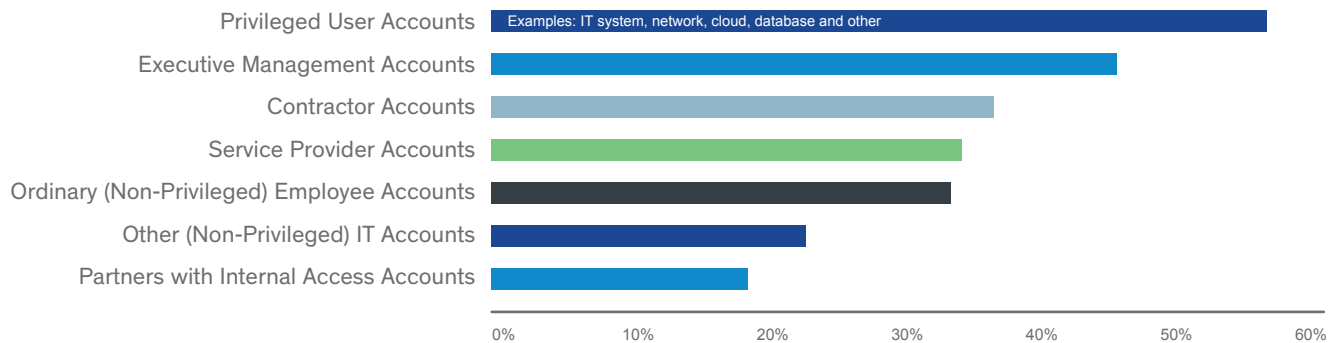


Figure 7: Insiders posing the greatest risk

The most notable change in this year’s report was a large increase in executive management as a potential threat vector, rising to the second spot (45% of respondents) from the fifth spot last year (28%). Though we are not aware of any major breach incidents involving executive management, the logic is straightforward—along with privileged IT staff, executives typically have access to nearly anything they desire, largely because they can. Executives also typically tend to follow lax security practices and are often the main source of requests for “exceptions” to existing security policies. Given the prevalence of using stolen credentials as a key component of most data breaches, executive credentials are also a ripe target for attackers.

In accordance with the expanded scope of this year’s report, respondents were also asked which external threat actors they were most concerned about. Cybercriminals headed the list, followed closely by hacktivists and cyberterrorists. Despite all the discussions about China’s, Russia’s, Iran’s and North Korea’s alleged involvement in recent data breaches, we were somewhat surprised that respondents were least concerned with nation-states (Figure 8).

Greatest External Risks

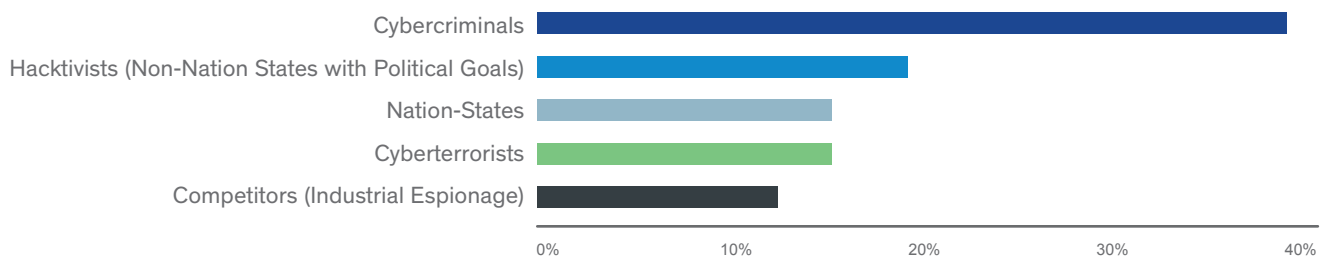


Figure 8: Greatest external risks ranked lowest-highest

SENSITIVE DATA LOCATIONS

Many Organizations Know Where Their Sensitive Data Is Located—at Least They Think They Do

It’s a common refrain that you can’t secure what you don’t know about, and knowing where your sensitive data is located has been trumpeted as a necessary starting point for any comprehensive data security program (Figure 9). As the growth of cloud computing and big data has led to an explosion of both structured and unstructured data that is more distributed than ever, there has been a corresponding interest in tools for performing data discovery and classification. And the looming specter of IoT should increase the number of devices and data they generate by orders of magnitude.

“Though our frequent conversations suggest otherwise, most security professionals claim at least some knowledge of where their sensitive data is located. 43% claim ‘complete knowledge.’”

Do You Know the Location of Your Sensitive Data?

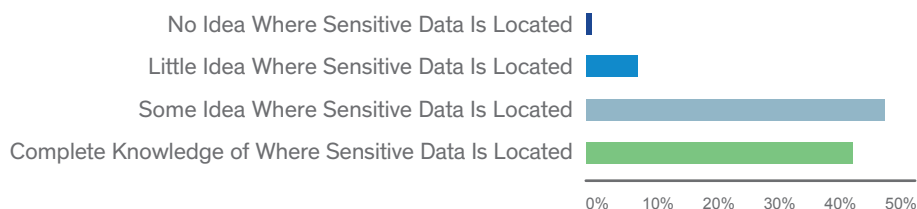


Figure 9: Location of sensitive data

This year, we decided to test this hypothesis to see if firms truly do know where their sensitive data is located, and the results were a bit surprising. Only 10% claimed little or no knowledge of the location of their sensitive data, while nearly half (47%) of all respondents claimed they had “some idea” where their sensitive data is located and a shocking 43% claimed to have “complete knowledge” of the location of their sensitive data. IT (52%) and financial services (50%) were among the most confident, while those with the least complete knowledge were transportation (19%), government (37%), retail (38%)

and manufacturing (38%). At the very least, the results are highly counterintuitive and could suggest that our prior conceptions about the need for data discovery and classification were actually misconceptions. At worst, the results suggest many firms are in denial about how much sensitive data they have and where it’s located, which could be a harbinger of continued damaging data breaches.

Plans for Security Spending Increase in 2016

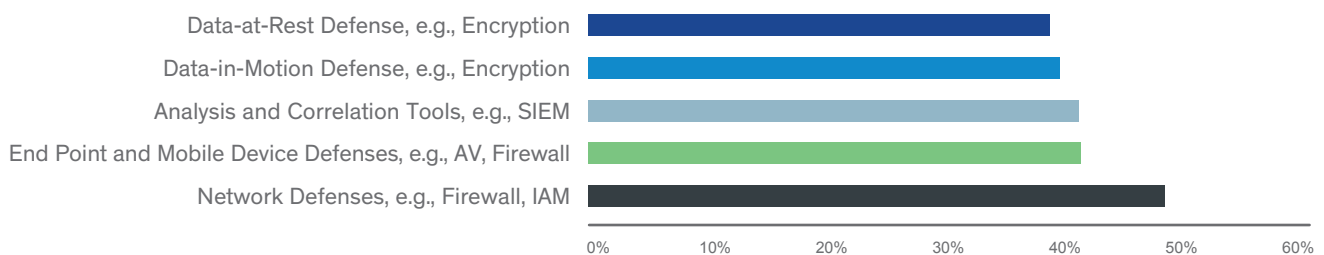


Figure 10: Spending increases for 2016

ENCRYPTION USE CASE DRIVERS

Cloud, Big Data and Data Sovereignty Driving Broader Potential Use Cases for Encryption

As noted above, products that can directly help mitigate data theft—data-in-motion and data-at-rest defenses such as encryption—were near the bottom of the list in terms of spending intentions at 40% and 39%, respectively (Figure 10). Additionally, prior survey work by both 451 Research and Vormetric has documented that historically encryption has been most frequently applied to things like PCs, laptops, hard drives and emails. These stats beg the following questions: Why isn’t encryption a higher priority, and why hasn’t it been deployed more broadly through most enterprises?

As we will discuss in more detail, one of the barriers to more widespread adoption of encryption has been existing perceptions about complexity, as well as costs and potential staffing requirements. As with most areas of security, a tradeoff applies with encryption—the greater the degree of protection, the greater the added cost and complexity. And as we will discuss, a related issue is the sheer number of varieties of encryption and potential use cases that may call for encryption, adding more complexity to the mix.

Broadly speaking, encryption has traditionally been broken down into two high-level groups: data-in-motion and data-at-rest. Data-in-motion defenses are used to protect the transmission of data between networks and include virtual private networks (VPNs)—a longtime staple of most firms’ security arsenals—that rely on either Internet Protocol Security (IPSec) or Secure Sockets Layer (SSL) encryption, as well as Secure Shell (SSH) and the embedded web security protocol HTTPS. Data-at-rest defenses include an even broader variety of technologies and use cases that can range from full disk encryption for protecting laptops and hard drives from loss or theft, to file-level encryption and access controls to address system-level attacks and insider privilege abuse, and finally to application layer controls such as encryption, tokenization and data masking to protect against higher-level attacks such as Structured Query Language (SQL) injection and rogue database administrators.

Additionally, many of the aforementioned products currently available are also designed for specific platforms or operating systems. To illustrate, certain data security vendors focus on providing functionality that is optimized for a select group of operating systems, device platforms or software as a service (SaaS) applications. The end result is that many firms that would like to adopt a more

comprehensive encryption strategy have been forced to deal with a growing assortment of point products and vendors.

Still, several factors suggest the sands are slowly shifting toward more widespread use of encryption and related techniques. For one, as we've argued earlier, traditional security tools are no longer doing a good enough job, and across the industry, there is growing recognition that multi-layer attacks will eventually succeed at penetrating even the most hardened networks. Second, as we noted earlier, further adoption of public cloud resources and big data will provide data-at-rest encryption with a higher place of prominence, given the limitations of legacy security tools in environments where enterprises no longer control the underlying resources upon which they are built.

With respect to big data specifically, though it may be hard enough to know where your sensitive data is located, it's even harder to classify it and determine its level of sensitivity, particularly when it is constantly changing. As an example, data that might not normally be considered sensitive might become so once it has been applied to a big-data experiment and yields results that may be highly proprietary. Thus it's not surprising to us that the data security technologies with the largest plans to implement were application layer encryption (40%), tokenization and multi-factor authentication (39%) and cloud encryption gateways (38%), each of which is particularly suitable for addressing cloud, big-data and data residency/sovereignty use cases (Figure 11).

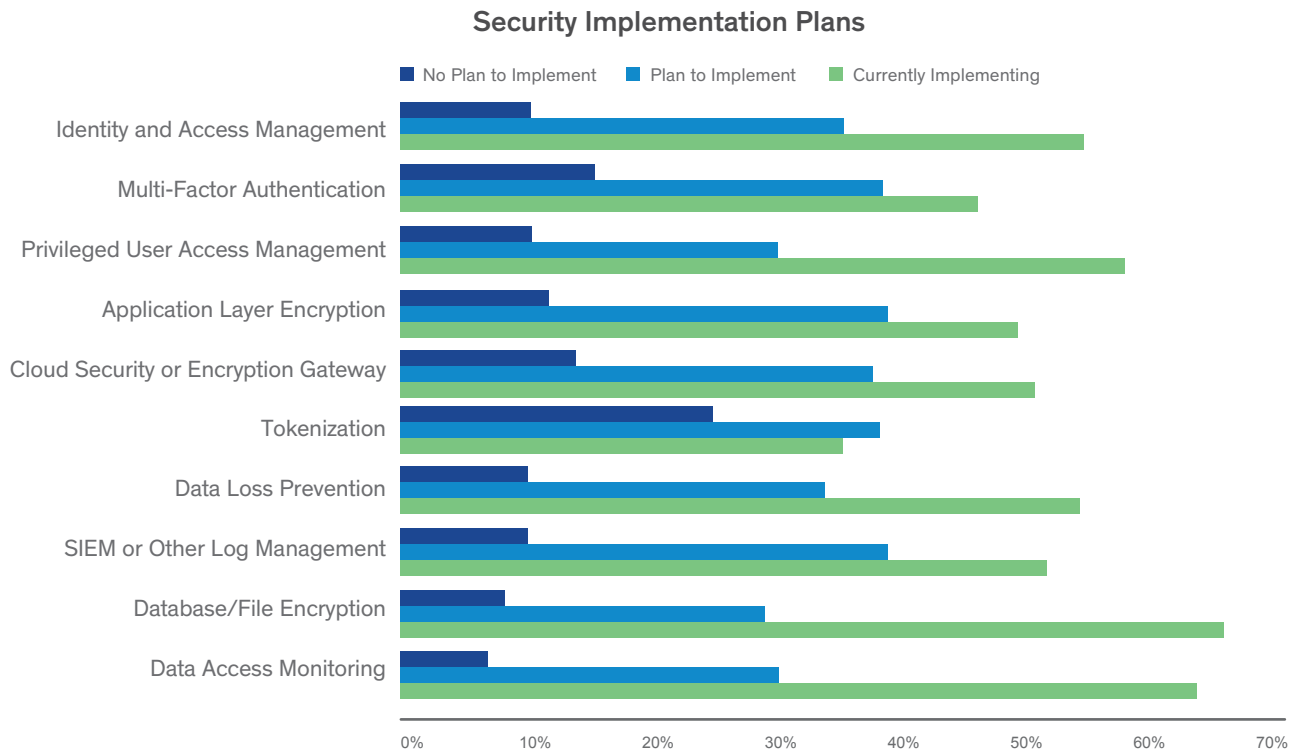


Figure 11: Plans to implement

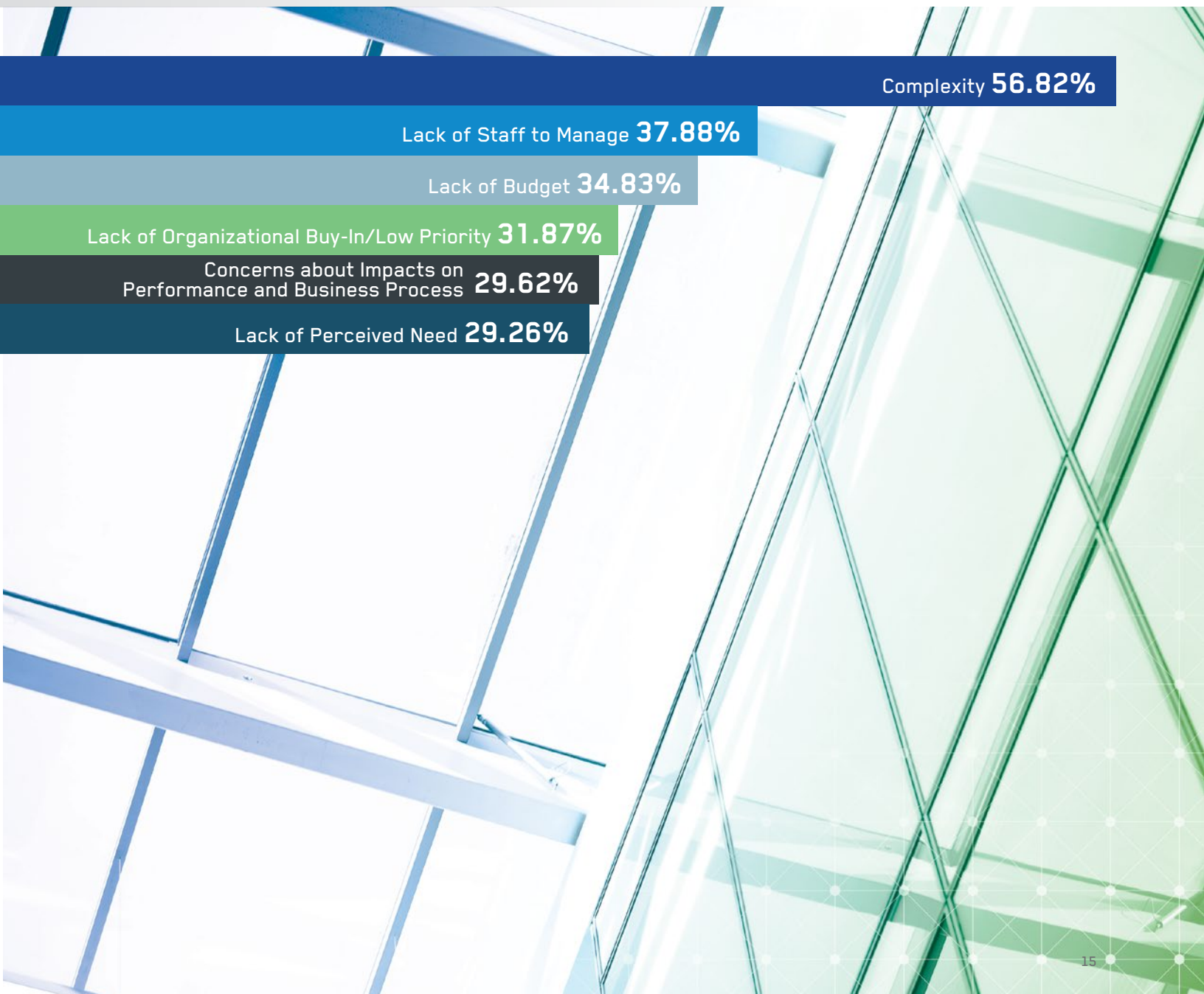
BARRIERS TO ADOPTION OF DATA SECURITY

Complexity and Lack of Skilled Staff Holding Back Data Security Adoption

Data security has had a reputation for being difficult to install and maintain, though deployment challenges can vary greatly in terms of the type of data security selected and where in the IT stack it is deployed, i.e., at the disk level, file level or application layer. To some extent, our results reflected that perception, and across nearly all geographies and industry verticals, “complexity” was the number-one barrier to adopting data security tools and techniques more widely, selected by 57% of respondents (Figure 12). We also hear frequent complaints about the potential adverse impacts of encryption and data security on network and application performance and business processes, though this was a fairly low priority in most regions aside from the U.K.

“Across nearly all geographies, ‘complexity’ was the number-one barrier to adopting data security, followed by lack of staff.”

Figure 12: Barriers to adoption of data security



Complex deployments also typically require significant staffing requirements, so “lack of staff to manage” came in as the second highest barrier, albeit a distant second at 38% of respondents. Staff shortage was particularly acute in the education, automotive and government sectors. The clear message for data security vendors is that, to achieve broader adoption of data security products, particularly those for small and medium-sized businesses (SMBs), they need to be simpler to use and require less manpower to deploy, operate and maintain on an ongoing basis.

“Combined with a chronic shortage of security personnel, data security offered as a service could be a growth area.”

Complexity and concerns about staffing requirements dovetail neatly with an emerging problem afflicting the entire information security landscape—a chronic and growing shortage of skilled security personnel. Vendors, enterprises and service providers alike lament the challenges of finding and retaining skilled security staff, and some estimates have cited the gap at over one million current job openings. And thanks to the proliferation of mobility, cloud and big data, firms are faced with a growing assortment of point security products to manage. In short, firms are tasked with doing much more with the same—or less—resources.

This combination of complexity and staff shortages creates a ripe opportunity for complex security products like data security and encryption that can be managed as a service. Not surprisingly, we have seen the emergence of service-based offerings of DLP, encryption key management and digital certificate management. We anticipate more service-based data security offerings to emerge in coming years.

SECURING SAAS, BIG DATA AND IOT

Much has been made of the unique security challenges posed by the triumvirate of big data, cloud computing and IoT. Since the latter two take advantage of resources that largely exist outside of traditional enterprise boundaries, legacy security tools and approaches that rely on a hardened perimeter to enforce existing notions of “internal” versus “external” have limited applicability in the new world order. At the same time, security concerns repeatedly show up as one of the leading barriers to more broad adoption of these new computing models.

Among the various next-generation architectures, SaaS applications and big data lead the pack in terms of security concerns. When asked which locations would experience the greatest amount of data loss in the event of a breach, databases and file servers were still the top choices, though SaaS apps and big data were both ranked third overall, well ahead of infrastructure as a service (IaaS) in eighth place. Although there is a burgeoning cottage industry devoted to securing SaaS applications, big data’s showing was a bit of a surprise but is mainly due to the dominance of respondents from the U.S. in the sample, particularly from financial services firms—most other countries have been slower to adopt big data and ranked it much lower.

One of the primary concerns about public cloud services remains breaches or attacks at the cloud service provider. Though attacks on cloud providers are rare and most of the latter arguably do a better job of securing their infrastructure than most enterprises, over 70% of respondents were either very concerned or extremely concerned about the potential for such attacks. To a somewhat lesser degree, respondents were also concerned about the risk of using shared cloud infrastructure, visibility into the cloud provider’s security measures, lack of control over the location of data, privacy policies and privileged users at the cloud provider.

“Attacks or breaches at cloud providers remain a top concern for cloud adoption.”

Concerns with Service Provider Security

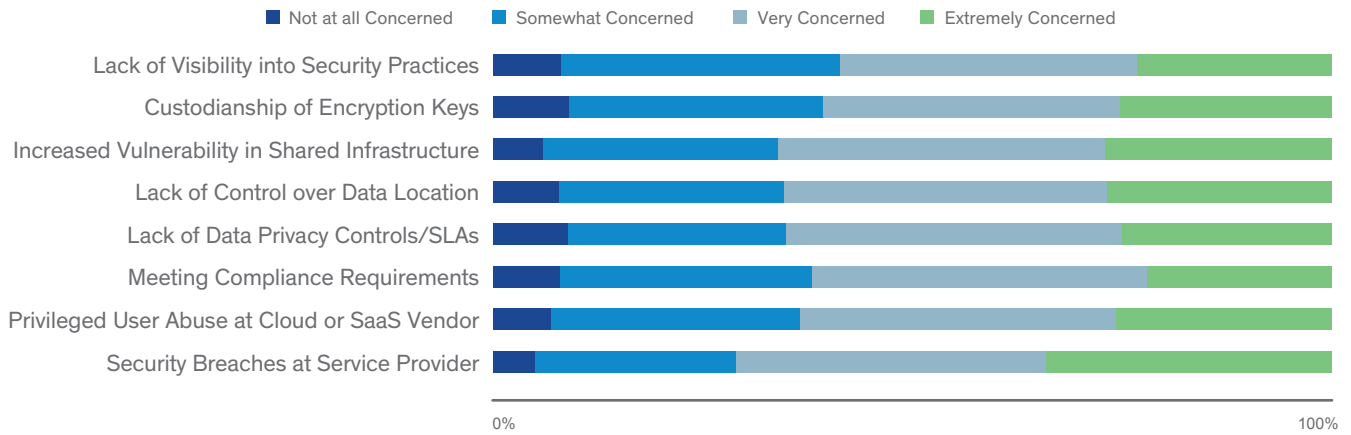


Figure 13: How concerned are you about the following data security issues as they relate to public cloud services?

Encrypting sensitive data stored at cloud providers is a sound way to address many of the above concerns, and 451 Research expects that over the coming years all SaaS providers housing sensitive enterprise data will have to offer encryption services to be considered viable options.

However, one key issue that is shaping up to be critical in terms of security for SaaS applications is encryption key management, more specifically, whether the service provider or the customer maintains control over the keys. The initial industry response was to deploy third-party encryption gateways that encrypted data en route to cloud applications and allowed customers to control the keys, albeit often with adverse impacts on the application. Interesting test cases were presented earlier this year as both Salesforce and Box® launched their own native encryption solutions. The Box solution, for example, provides customers with the ability to maintain administrative control over encryption keys, while Salesforce Shield offers only a vendor-controlled option.

“ONE KEY ISSUE THAT IS SHAPING UP TO BE CRITICAL IN TERMS OF SECURITY FOR SAAS APPLICATIONS IS ENCRYPTION KEY MANAGEMENT.”

Maintaining local control over keys is a critical requirement for many compliance mandates, and so not surprisingly, the number-one factor that would increase willingness to use the public cloud was encryption, at 48% of responses (Figure 14). While deploying encryption with service provider control over keys was the third-ranked option at 35%, the gap between the two deployment options for key management is widening in favor of local control, which elicited nearly identical responses in last year's survey. We anticipate the gap between the two key management options will continue to widen over time. We also anticipate that we'll see an increased role for more granular access controls as some of the emerging vendors—which 451 refers to as cloud application control (CAC) vendors and others refer to as cloud access security brokers (CASB)—continue to evolve their offerings.

Removing Barriers to Public Cloud

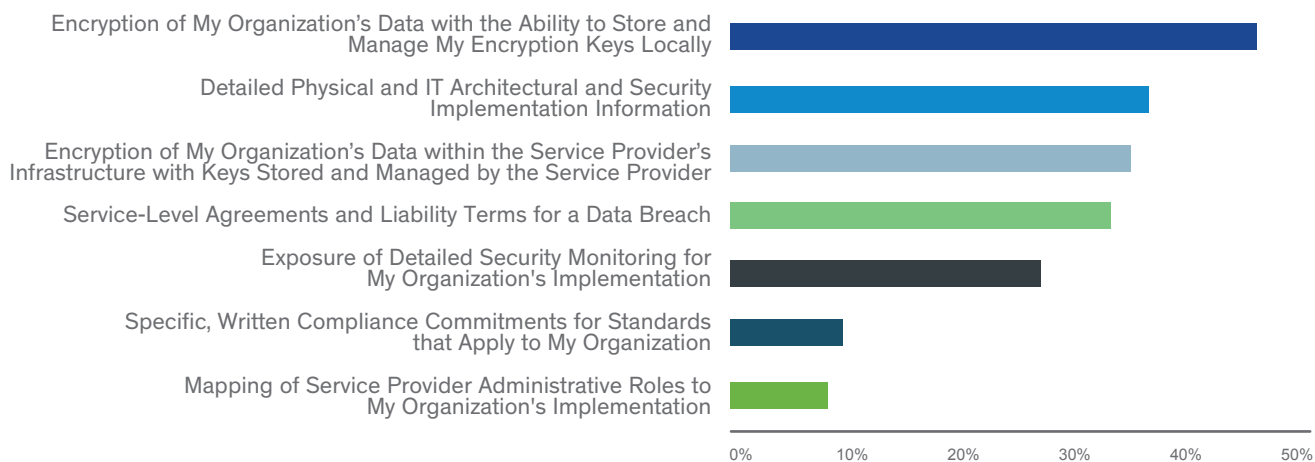


Figure 14: What would increase your willingness to move SaaS applications to the public cloud?

Though IoT promises to present a security hurdle of epic proportions, security concerns for IoT remain low. With the exception of Australia, most regions currently see little risk from data generated by IoT devices, which suggests IoT's early stage of adoption and reflects adoption patterns with cloud and big data. Given the sheer volume of devices that are anticipated, securing sensitive data generated by IoT devices is the primary concern of most security professionals (36%), followed closely by privacy violations related to data generated by IoT devices (30%). And while most recipients expressed overall confidence in their ability to locate their sensitive data, with respect to IoT specifically, discovering sensitive data generated by IoT devices is a top concern and only slightly trails the prior concerns at 29% of respondents. We suspect the greater concerns about data discovery reflect both the novelty of IoT, as well as the sheer volume of data generated by a variety of devices.



“THOUGH IOT PROMISES TO PRESENT A SECURITY HURDLE OF EPIC PROPORTIONS, SECURITY CONCERNS FOR IOT REMAIN LOW.”

TOP REGIONAL DIFFERENCES

In many cases, regional results closely tracked global results, with several notable exceptions. We will touch on the regional variances briefly in this section and explore them more in depth in upcoming regional editions. As an example, responses from countries such as Australia and Germany appear to be shaped by cultural biases and regulatory environments that are more skewed toward compliance and privacy than other regions like Scandinavia (not included in the scope of this study), where local norms accept the online posting of data that is considered highly sensitive elsewhere, such as salary information and tax returns.

Germany ranked compliance as the number-one reason for securing sensitive data, though requirements from business partners and customers were tied with compliance. Reputation and brand protection, the number-one reason on a global basis, was ranked sixth overall by German respondents. Germany also led the way in favoring local encryption key storage, which was cited by 62% of respondents and ranked as the number-one reason to increase use of public cloud resources.

Results from Australia suggested something of a “siege mentality”—85% of Australians claim to have been breached at some point in the past, versus 61% overall, and 61% had failed a compliance audit in the past, nearly double the 32% global average. 54% of Australian respondents saw themselves as either “extremely” or “very” vulnerable, notably higher than the 30% global average. Australia also led the way in terms of using encryption to meet data residency requirements at 49%, versus the 38% global average.

Brazil was the most sanguine about the effectiveness of regulatory compliance for preventing data breaches, with 83% rating compliance mandates as either “extremely” or “very” effective, versus the 64% global average. Brazil also had the highest plans for placing sensitive data in SaaS, IaaS, platform as a service (PaaS) and big-data environments and had the highest data security spending plans, with nearly 74% of respondents planning to increase spending on data security in the next 12 months.

Results from Japan show a lot of work remains to be done in terms of improving data security. Japan scored the lowest in terms of having complete knowledge of where sensitive data is located (22% versus 43% overall), and was also at the top of list for firms with no encryption strategy at 17%, versus the 5% global average. Part of the challenge is financial—Japan ranked lack of budget as the number-one barrier to adopting data security and encryption and had the lowest plans to increase spending on data security in general (31% versus 59% overall) and in response to recent high-profile breaches (22% versus 53% overall)

The following data points were also noteworthy and will be areas for further analysis in upcoming regional reports:

- In most regions, privileged insiders such as IT personnel and database administrators are viewed as the biggest internal threat. However, Germany and Japan place a nearly equal importance on the potential threat from ordinary employees.
- While reputation and brand protection, compliance and best practices were the top three reasons for securing sensitive data globally, Germany ranked brand near the bottom of the list, and both Germany and Japan rated requirements from business partners or customers as the number-one reason.
- Databases, file servers and mobile devices were identified by most regions as the locations most at risk for loss of sensitive data, though Australians were most concerned with data stored on mobile devices and respondents from Brazil identified IoT devices among the top three concerns.
- With respect to locations that actually stored the most sensitive data, SaaS apps and big data jumped into third place overall, in part due to increased adoption of big data in the U.S.
- In Japan, only 20% plan to store sensitive data in big-data environments, below the global average of 50%, and only 17% plan to store data in IoT devices, versus 33% globally.

TOP DIFFERENCES BY INDUSTRY SEGMENT

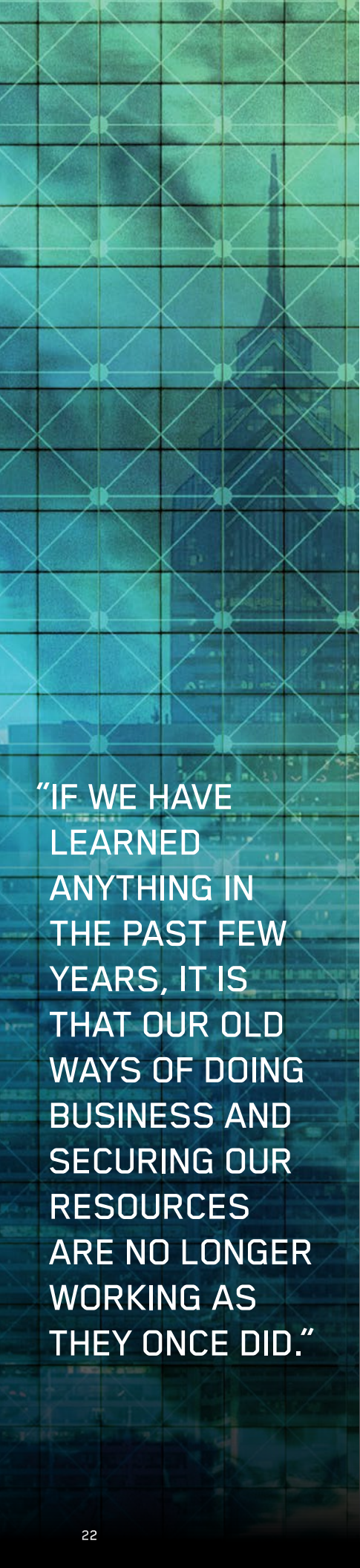
In terms of industry segments, results once again often tracked global results, though with nearly 40 industry verticals represented, there are greater opportunities for separation from the overall results. For sake of brevity, we will restrict our following comments to the eight or ten industry segments with the largest sample sizes, and will reserve deeper analysis for upcoming vertical market reports.

Similar to nations with a cultural or regulatory bias in favor of privacy, segment results also followed expected patterns and attitudes toward data security, compliance and overall security. As an example, two of the most highly regulated verticals, healthcare (61%) and financial services (55%), also had the highest ratings of compliance as a main reason for securing sensitive data relative to the overall average of 47%. Healthcare was also one of the verticals with the most faith in compliance mandates to prevent data breaches (21%), trailing only IT (27%). Predictably, the retail segment was most concerned with protecting brand and reputation, selected by 57% of respondents.

Energy respondents were nearly twice as likely to have experienced a data breach in the past year at 41%, versus 22% overall. Thus it isn't surprising that energy also scored the highest in terms of feeling most vulnerable to data threats, with 56% feeling either "very" or "extremely" vulnerable, again nearly twice the overall average of 30%. Historically, energy has not been one of the core verticals for security vendors, which typically derive the bulk of their sales from the "big four" of healthcare, government, financial services and retail. However, there are signs this is beginning to change, in part due to growing concerns about attacks on critical infrastructure by both nation-states and cyberterrorists. Energy was also most concerned with privileged insiders (88% versus 58%) and ordinary employees (53% versus 34%). Energy was near the pack in terms of data security spending intentions—66% of respondents expect their spending on data security to increase over the next 12 months, second only to IT (73%).

ADDITIONAL FINDINGS

- In terms of locations most at risk for loss of sensitive data, financial services seemed to be the most concerned about big data, while the two most concerned with SaaS applications were IT (36%) and retail (33%), versus 26% overall.
- For spending intentions, IT had the most respondents expecting to increase data security spending over the next 12 months (73%), followed by energy (66%). The sectors with the most respondents expecting to lower their data security spending were computer hardware and software and telecommunications, at 21%, respectively.
- Healthcare and retail, two of the sectors most impacted by high-profile breaches recently, were also the most likely to increase data security efforts as a result of those breaches, at 64% and 65%, respectively.
- With respect to adoption barriers for data security, "lack of staff to manage" was cited as the number-two overall reason (38%) and appears to be a particular problem for education (53%), automotive (53%) and government, engineering and telecommunications (44% each).



**“IF WE HAVE
LEARNED
ANYTHING IN
THE PAST FEW
YEARS, IT IS
THAT OUR OLD
WAYS OF DOING
BUSINESS AND
SECURING OUR
RESOURCES
ARE NO LONGER
WORKING AS
THEY ONCE DID.”**

RECOMMENDATIONS

The past few years have been challenging ones for the information security industry as a whole, and nearly everyone has been affected—end users, enterprises and security vendors alike. If we have learned anything in that time, it is that our old ways of doing business and securing our resources are no longer working as they once did. For many organizations, Albert Einstein’s oft-used quote is fitting—if doing the same thing over and over and expecting a different result isn’t the definition of insanity, it is certainly a recipe for placing your critical assets at risk.

So where do we go from here? There is a considerable amount of innovation taking place in the security industry, and 451 Research is tracking a lengthy list of vendors that are applying new techniques to prevent attacks as well as detect potential threats and narrow the window of exposure. That said, none of these emerging techniques can offer a silver bullet, and as we’ve learned, determined attackers will eventually find a way in.

As firms grow to accept the limitations of traditional security approaches, data security is likely to become a more critical component of a comprehensive security strategy. But as we have discussed, data security is not without its own challenges. For starters, we believe firms need to get a better handle on where their sensitive data is located and what its level of sensitivity might be so that the appropriate protections can be put in place. Thus we see the ability to discover and classify data growing in importance as data is increasingly distributed beyond the enterprise network confines and across cloud, mobile, big-data and IoT environments.

Additionally, as data breaches are gradually accepted as an artifact of modern corporate life, enterprises of all sizes need to consider encryption for more than just meeting compliance checkboxes and protecting laptops and USB drives from loss or theft. Of course, more liberal use of encryption also raises the potential for introducing an array of single-function products that are needed to address an increasingly diverse set of use cases, which in turn can increase overall complexity and staffing requirements. To minimize the drag on internal resources, data security-conscious firms should look to vendors that can address a broad variety of use cases and reduce complexity through automation and multiple deployment options, to help reduce both the acquisition cost as well as ongoing operational costs that have traditionally been associated with data security.

Lastly, we suggest customers explore, in addition to encryption, new security analytics techniques that can offer an extra layer of protection above and beyond what encryption alone can provide. For example, 451 is following new developments in threat analytics and techniques that can monitor data access patterns to establish baselines of normal activity, which can help identify potential breaches and provide a greater degree of visibility into potentially compromised resources.

METHODOLOGY

- The data in this study (with the exception of Figure 3) is based on web and phone surveys of 1,114 senior IT executives with influence on or responsibility for IT security purchases in their organizations.
- Respondents represented a representative range of company sizes, from \$50 million U.S. to \$2 billion-plus U.S.
- There was also a representative sample of vertical industries.
- 451 Research conducted the surveys in October and November of 2015.

ANALYST PROFILE

Garrett Bekker is a Senior Analyst in the Enterprise Security Practice at 451 Research. He brings a unique and diverse background, having viewed enterprise security from a variety of perspectives over the past 15 years. Garrett spent more than 10 years as an equity research analyst at several investment banking firms, including Merrill Lynch, where he was the lead enterprise security analyst, as an investment banker, and also in sales and marketing roles with early-stage enterprise security vendors. Throughout his career, Garrett has focused on a wide variety of subsectors within enterprise security and is now focusing primarily on identity and access management (IAM) and data security, with a special interest in applying the former to cloud-based resources.



Garrett Bekker
Senior Analyst
451 Research

ABOUT 451 RESEARCH

451 Research is a preeminent information technology research and advisory company. With a core focus on technology innovation and market disruption, we provide essential insight for leaders of the digital economy. More than 100 analysts and consultants deliver that insight via syndicated research, advisory services and live events to over 1,000 client organizations in North America, Europe and around the world. Founded in 2000 and headquartered in New York, 451 Research is a division of The 451 Group.

ABOUT VORMETRIC

Vormetric's comprehensive high-performance data security platform helps companies move confidently and quickly. Our seamless and scalable platform is the most effective way to protect data wherever it resides—any file, database and application in any server environment. Advanced transparent encryption, powerful access controls and centralized key management let organizations encrypt everything efficiently, with minimal disruption. Regardless of content, database or application—whether physical, virtual or in the cloud—Vormetric Data Security enables confidence, speed and trust by encrypting the data that builds business.

Please visit WWW.VORMETRIC.COM and find us on Twitter [@VORMETRIC](https://twitter.com/VORMETRIC).

