451 Research®

Vormetric
A Thales company

2016 VORMETRIC DATA THREAT REPORT

Trends in Encryption and Data Security

FINANCIAL SERVICES EDITION

RESEARCH BRIEF

#2016DataThreat

TABLE OF CONTENTS

OUR SPONSORS

rackspace the #1 managed cloud company

Couchbase

GTRA

NUTANIX

informatica

OASIS

Adistec

QTS

CSA cloud security alliance

ZM

kyos embedded security

FUSIONSTORM

intellect security intelligent security solutions

FINANCIAL SERVICES ISAC

EMI Executive Mosaic

INTRODUCTION

According to the legend of Willie Sutton, the oft-misquoted bandit robbed banks because 'that's where the money is'. Thus it's no surprise that the U.S. financial industry is among those that are most heavily targeted by cyber attacks, and like the broader global economy, has been subject to numerous and well-publicized data threats.

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.

"88% of U.S. financial respondents chose cybercriminals as the number risk to sensitive data. "

Previous editions of the Vormetric Data 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. 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 'cyber-terrorists' – that frequently masquerade as insiders by using stolen or compromised credentials to steal all types of valuable data, including Personally Identifiable Information (PII), Personal Health Information (PHI), financial data and intellectual property. As an example, 88% of U.S. financial respondents chose cybercriminals as the number risk to sensitive data.

Thus as the line between 'insider' and 'outsider' continues to blur, we have accordingly expanded the scope of the 2016 edition of the Vormetric Data Threat report to include to encompass all manner of threats to sensitive data, and get a better sense of what the most relevant threats organizations are facing today, how they are addressing those threats, and what we can do better to prepare ourselves against a growing chorus of adversaries. This special version of the 2016 data threat report focuses specifically on responses from the U.S. financial services industry, and will address both the similarities to the global report, and also key distinctions with respect to other high-profile verticals like healthcare, retail and the U.S. federal government.

ABOUT THIS RESEARCH BRIEF

The 2016 Vormetric Data Threat Report is based on a survey conducted by 451 Research during October and November of 2015. In this research brief, we'll highlight the results collected from 100 senior security executives within the U.S. financial services sector. These results will be compared, where applicable, to findings in other key U.S. verticals such as financial services, healthcare, and retail, as well as those in other countries.

"Our global survey results showed that in many ways, security professionals are like generals fighting the last war. "

THE BIG DISCONNECT

At a high level, our global survey results contained a mix of both good and not-so-good results that showed that in many ways, security professionals are like generals fighting the last war. 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 and intrusion prevention - yet data breaches continue to increase in both frequency and severity. 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.

"70% of financial services respondents indicated that their overall spending levels for protecting sensitive data will either be 'somewhat' or 'much' higher in the next 12 months, by far the highest of any vertical."

OLD SECURITY HABITS DIE HARD

For the financial services sector specifically, the results and conclusions were similar to many of those obtained in the Global Data Threat Report, and likewise contained a mix of good and not-so-good views. On the positive side, the U.S. financial market is still spending - a lot. In fact, 70% of financial services respondents indicated that their overall spending levels for protecting sensitive data will either be 'somewhat' or 'much' higher in the next 12 months, by far the highest of any vertical and significantly higher than both the U.S. and global averages of 62% and 59%. Further, U.S. financial services has the highest percentage of respondents planning to increase spending across the various types of security defenses compared to any other vertical or region with a 56% average increase, compared to the U.S. and global averages of 49% and 43%.

In terms of breach activity, the financial sector results also offer a ray of optimism. While 44% of U.S. financial respondents indicated they have experienced a data breach in the past, this figure is notably lower than other U.S. verticals such as healthcare (63%), government (62%) and retail (52%). Similarly, 52% of financial services respondents claimed they have never been breached or failed a compliance audit in the past, well above the U.S. average of 39% and industries like healthcare (27%) and government (30%). However, financial services firms were not surprisingly less likely to increase spending on data security as a result of a breach (60%) than other sectors such as healthcare (71%) and retail (70%) and the U.S. average (64%).

"44% OF U.S. FINANCIAL RESPONDENTS HAVE EXPERIENCED A DATA BREACH IN THE PAST, NOTABLY LOWER THAN OTHER U.S. VERTICALS SUCH AS HEALTHCARE (63%), GOVERNMENT (62%) AND RETAIL (52%)."

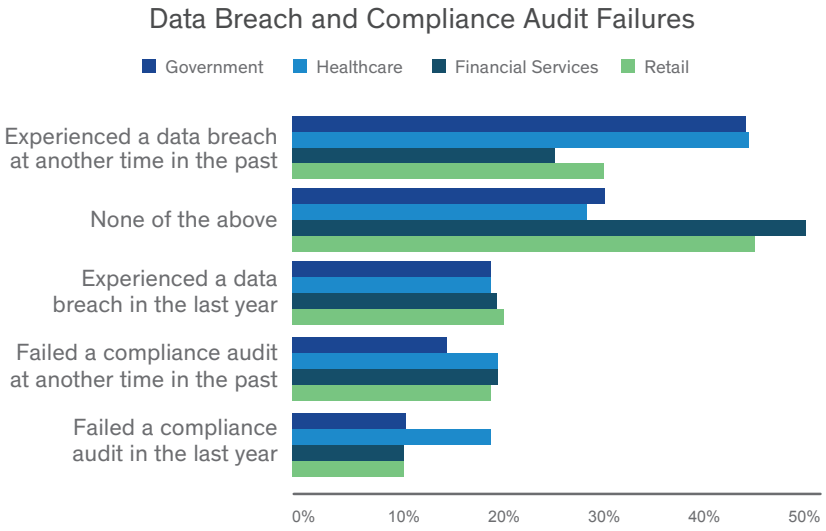


Figure 1: Comparative rates of data breach and compliance audit failures

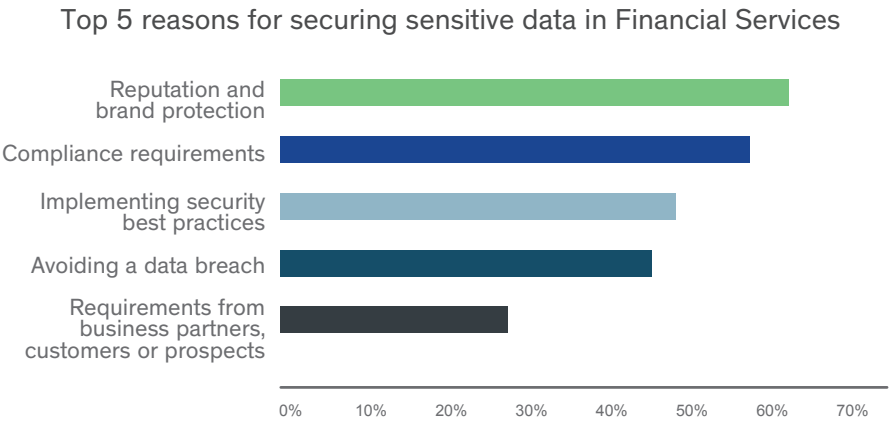


Figure 2: Top 5 reasons for securing sensitive data in Financial Services

While there are encouraging signs that the financial services industry is taking steps to increase their overall security preparedness, like other sectors, spending remains skewed towards traditional areas such as network (65%) and end point defenses (58%), which have the highest expectations for increased spending. Network security was also ranked near the top in terms of effectiveness: 84% of respondents rated network defenses as either 'very' or 'extremely' effective at protecting sensitive data - the #1 ranked security category among financial respondents, and also the highest response of any vertical in our sample.

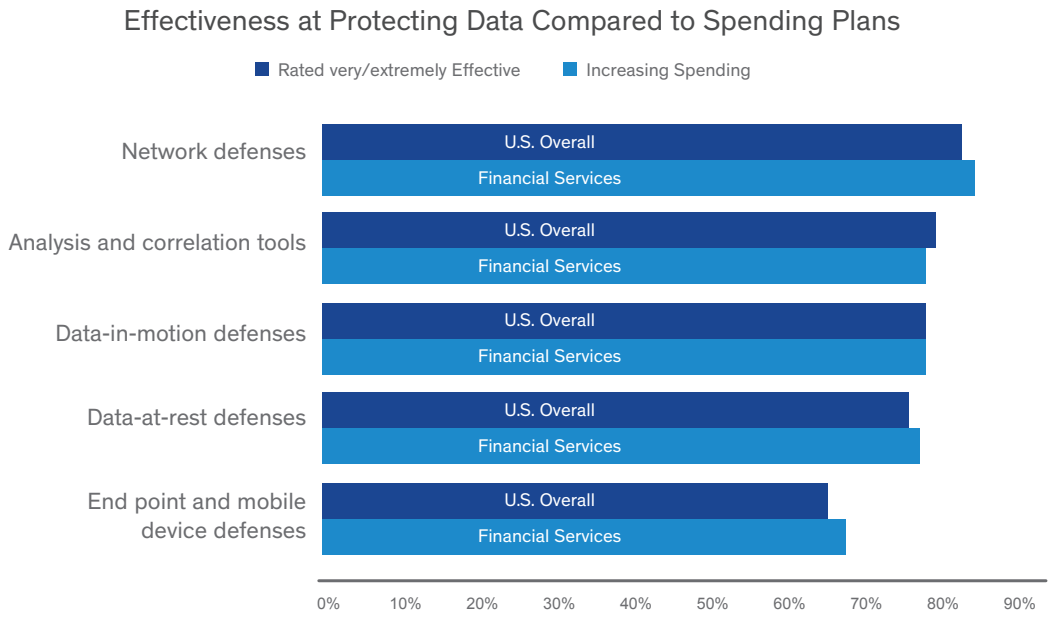


Figure 3: Ratings for effectiveness at protecting data compared to spending plans

Conversely, the financial services industry has a somewhat less optimistic view of data security, particularly data-at-rest defenses. Like many other regions and verticals, the latter was ranked second-to-last in terms of overall effectiveness - 77% selected data-at-rest defenses as either 'very' or 'extremely' effective - ahead of only endpoint security at 67%. It's worth noting, however, that financial services had the highest effectiveness response for data-at-rest security than any other sector, and only trailed network security (84%) by a small margin. When it comes to spending intentions, however, the outlook for data-at-rest defenses is less rosy. While 48% plan to increase their spending on data-at-rest defenses, this is well below network defenses (65%) and at the bottom of the list for spending priorities across all security categories. Notably, endpoint security has the second-highest percentage for spending intentions, despite having the lowest effectiveness rating.

"ENDPOINT SECURITY HAS THE SECOND-HIGHEST SPENDING INTENTIONS, DESPITE HAVING THE LOWEST EFFECTIVENESS RATING."

KEY FINDINGS:

There's still work to be done

- 84% of respondents rated network defenses as either 'very' or 'extremely' effective at protecting sensitive data
- 44% experienced a breach at some point in the past.
- Endpoint security has the second-highest spending intentions, but the lowest effectiveness rating
- Spending on data-at-rest defenses is at the bottom of the list across all security categories

To be fair, there are other encouraging takeaways. While reputation and brand protection (62%) and compliance (58%) are still primary motivators for security spending, the need to implement security best practices (48%) is also gaining momentum. Financial services respondents were also more likely to use encryption to follow best practices than other verticals (65% vs. 57% U.S. average).

Survey responses also indicate that financial respondents are also looking to implement 'newer' security tools. Specific categories with the biggest planned increases for data security spending for financial services include as tokenization (42%), DLP (34%) and application layer encryption (33%). In summary, the financial services industry is doing many of the right things – they just need to do more of them.

What we're doing right

- 70% of U.S. Financial respondents plan to increase data security spending, the second highest of all verticals
- 77% selected data-at-rest defenses as either 'very' or 'extremely' effective
- 48% of U.S. Financial respondents plan to invest in data-at-rest defenses this year.
- 42% plan to implement tokenization
- 33% plan to implement application layer encryption

In the following sections we will highlight several key topics with respect to the U.S. Financial vertical, and also point out notable instances where financial services differed from other segments.

Compliance still a driver – but compliance is NOT security

Many security executives across the globe still appear to equate compliance with security, and nearly two-thirds (64%) of our global respondents viewed compliance requirements as either 'very effective' or 'extremely effective' in preventing data breaches, up from 59% last year. However, while compliance can serve as an effective starting point or baseline for any information security program, the steadily growing volume of data breaches should serve as a strong reminder that we need to do more than just check off compliance boxes if we want to make sure our data remains safe.

Yet many security professionals in the financial services industry share a similar view of compliance with their peers in other industries - 66% of respondents view compliance requirements as either 'very' or 'extremely' effective in preventing data breaches, in line with the U.S. average of 67%, and second only to U.S. Healthcare (68%). The U.S financial vertical is also still spending heavily to meet those compliance requirements - 56% of financial services respondents indicated that compliance requirements had the highest impact on spending (compared to US total - 52% and Global - 46%).

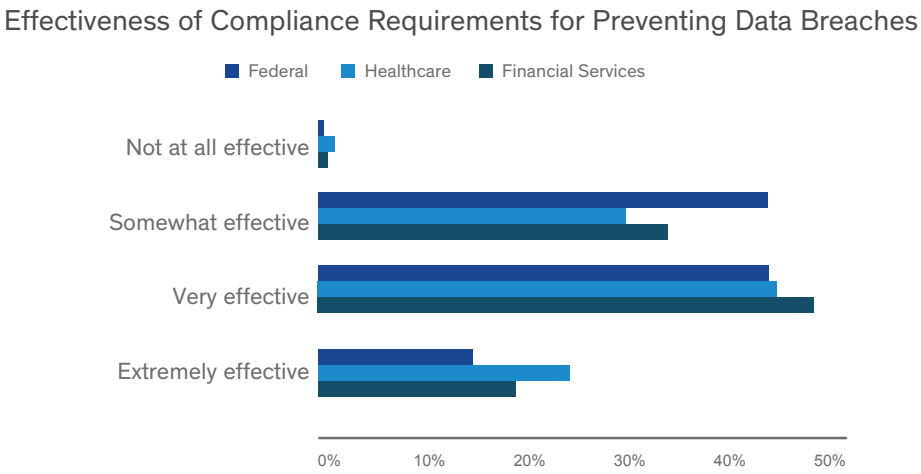


Figure 4: Ratings for effectiveness of compliance requirements for preventing data breaches

MANY FINANCIAL 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. Yet only 5% of financial respondents claimed little or no knowledge of the location of their sensitive data, while exactly half (50%) claimed they had ''complete knowledge' of the location of their sensitive data, more than healthcare (44%), retail (39%) or U.S. federal government (38%). At the very least, the results run counter to our own experiences with enterprise customers, and at worst, suggest that many financial 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.

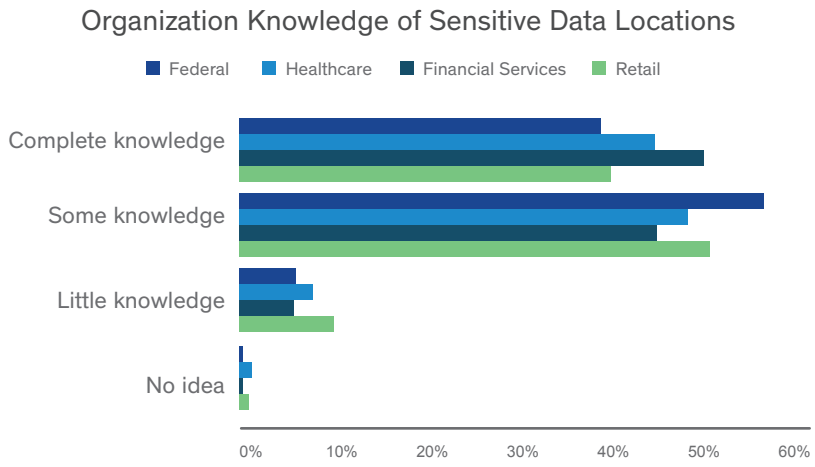


Figure 5: Ratings for organization knowledge of sensitive data locations

COMPLEXITY AND STAFFING SHORTAGES TOP BARRIERS TO DATA SECURITY ADOPTION

Data security has often been perceived as being difficult to install and maintain, though deployment challenges can vary greatly in terms of the specific type of data security selected, and also where in the IT stack it is deployed, i.e. at the disk level, file level or application layer. Not surprisingly, our results reflected that same perception - 'complexity' was identified as the number one barrier to adopting data security more widely, selected by 68% of respondents, compared to the U.S and global averages of 58% and 57%. Complex deployments also typically require significant staffing requirements, and not surprisingly 'lack of staff to manage' came in as the second highest barrier (35%), in line with the U.S. average of 37%.

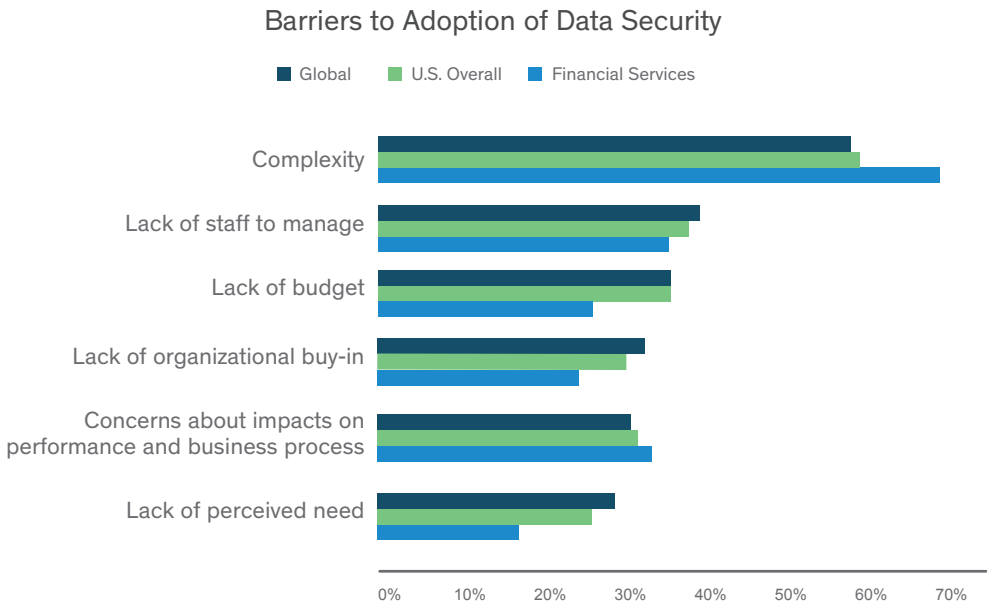


Figure 6: Barriers to adoption of data security

RISKY BUSINESSES

Similar to other verticals and regions, privileged user accounts were identified as the top insider threat, chosen by 59% of U.S. financial respondents, slightly below the U.S. average of 63%. Executive management accounts and contractor accounts were tied for the next two top insider threats, at 43% each. With respect to external threats, U.S. financial respondents chose cyber criminals as the overwhelming number one risk to sensitive data, selected by 88% of respondents versus the U.S and global averages of 80% and 79%; 'hacktivists' came in second with a 71% response. Perhaps not surprisingly, financial data was the main area of focus for data security spending (58%) among financial respondents.

"PRIVILEGED USER ACCOUNTS WERE IDENTIFIED AS THE TOP INSIDER THREAT, CHOSEN BY 59% OF U.S. FINANCIAL RESPONDENTS, SLIGHTLY BELOW THE U.S. AVERAGE OF 63%."

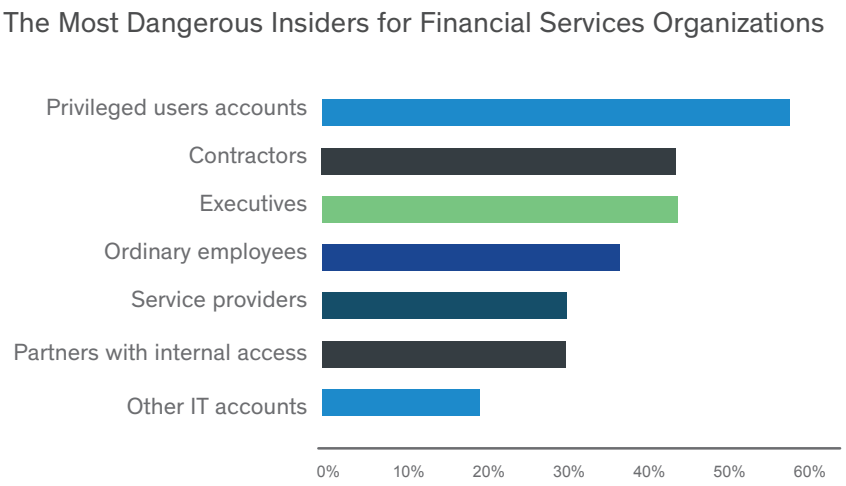


Figure 7: Ratings for the most dangerous insiders for financial services organizations

CLOUD, BIG-DATA AND IOT PRESENT NEW CHALLENGES

Much has been made of the unique security challenges posed by the triumvirate of big-data, cloud computing and IoT. Since the latter 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' vs. 'external' have limited applicability. At the same time, security concerns repeatedly show up as one of the leading barriers to more broad adoption of these emerging computing models, despite the fact that the most regions and industry verticals plan to store increasingly more sensitive data in non-legacy environments.

Cloud

Financial respondents indicated a higher degree of comfort with cloud resources - 91% indicated they planned to store sensitive data in some public cloud environments (either SaaS, IaaS or PaaS), compared to the global average of 85%. With respect to the cloud security, financial industry responses regarding public cloud services were generally similar to other regions: breaches at the cloud provider and vulnerabilities from shared infrastructure were identified as the top two concerns, with 75% either 'very' or 'extremely' concerned with the former (in line with the U.S. average), while 72% identified the latter as the number concern (vs. 73% U.S. average).

What are the primary ways to ease cloud adoption concerns among healthcare sector respondents? Like most regions, encryption of sensitive data stored in the cloud was the top choice. However, who manages the keys and where they keys are stored is shaping up to be critical issue for the cloud security. Maintaining local control over keys is a critical requirement for many compliance mandates, and not surprisingly was the number one factor that would increase respondents' willingness to use public cloud globally, at 48% of responses. The same held true for financial services, where 51% identified encryption with local control as the top way to alleviate cloud security concerns. It's also worth noting that encryption with cloud provider control over encryption keys was selected by 15% fewer respondents (36%) – a wider gap than most verticals or regions.

"MAINTAINING LOCAL CONTROL OVER KEYS IS A CRITICAL REQUIREMENT FOR MANY COMPLIANCE MANDATES, AND NOT SURPRISINGLY WAS THE NUMBER ONE FACTOR THAT WOULD INCREASE HEALTHCARE RESPONDENTS' WILLINGNESS TO USE PUBLIC CLOUD WAS ENCRYPTION."

"ENCRYPTION WITH CLOUD PROVIDER CONTROL OVER ENCRYPTION KEYS WAS SELECTED BY 15% FEWER RESPONDENTS (36%) – A WIDER GAP THAN MOST VERTICALS OR REGIONS. "

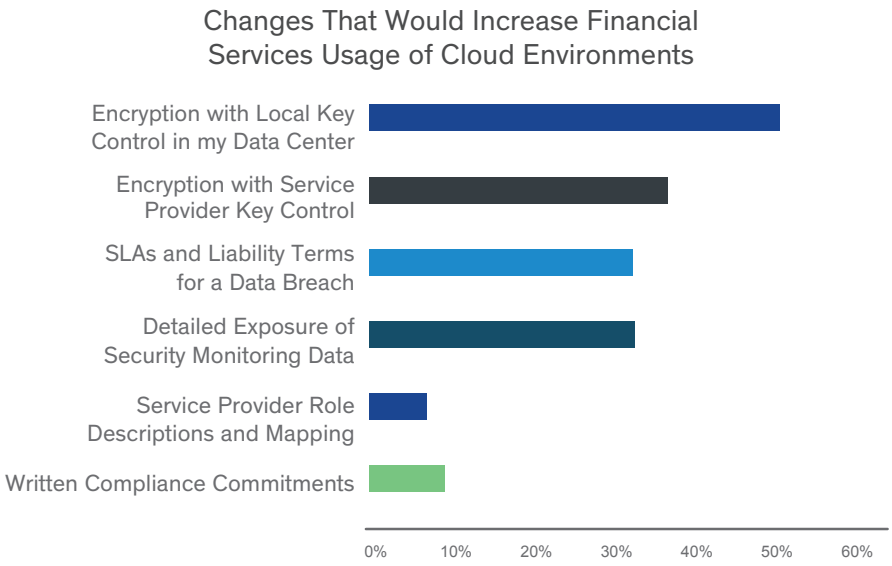


Figure 8: Changes that would increase financial services usage of Cloud environments

Big Data: a Big Deal in Financial Services

U.S. financial services showed more concern about big-data environments than most other regions/industries. 'Big Data environments' were selected as the third-highest risk for data loss (33% vs. 24% U.S. and 21% global), trailing only databases (56%) and file servers (42%). Financial services also had the highest percentage of respondents identifying big-data as a risky location for storing sensitive data (33%) than other verticals like healthcare (22%), retail (20%) or government (15%). The biggest concern regarding big-data security is the fact that sensitive information may reside anywhere within the environment (48% vs. 45% U.S. average and 41% global average), followed by the generation of reports that may include sensitive data (43%). Despite these concerns, however, 59% of U.S. financial services respondents are planning on storing sensitive data in big-data environments in the next 12 months, compared to the U.S. and global averages of 54% and 50%, and ahead of government (56%), healthcare (51%) and retail (46%).

"U.S. financial services showed more concern about big-data environments than most other regions/ industries. "

Internet of Things (IoT)

Though the Internet of Things (IoT) promises to present a security hurdle of epic proportions, security concerns also reflect IoT's early stage of adoption, and this was true across both our global results and within the financial sector. Just 12% of financial respondents identified IoT devices as at the greatest risk of loss for sensitive data, compared to the U.S. average of 16% and healthcare at 21%. Additionally, only one-third of respondents plan to store sensitive data in IoT implementations, in line with the U.S. average of 33%. Given the sheer volume of connected devices that are expected to be deployed in the coming years, securing sensitive data generated by IoT devices is not surprisingly a primary global concern of most security professionals (35% globally), and this was also the top concern for financial services(31%). Similar to most other industries and regions, privacy violations from data generated by IoT devices was the second most popular response (31%), while attacks on IoT devices that may impact critical operations rounded off the top three (29%).

"Just 12% of financial respondents identified IoT devices as at the greatest risk of loss for sensitive data, compared to the U.S. average of 16%"

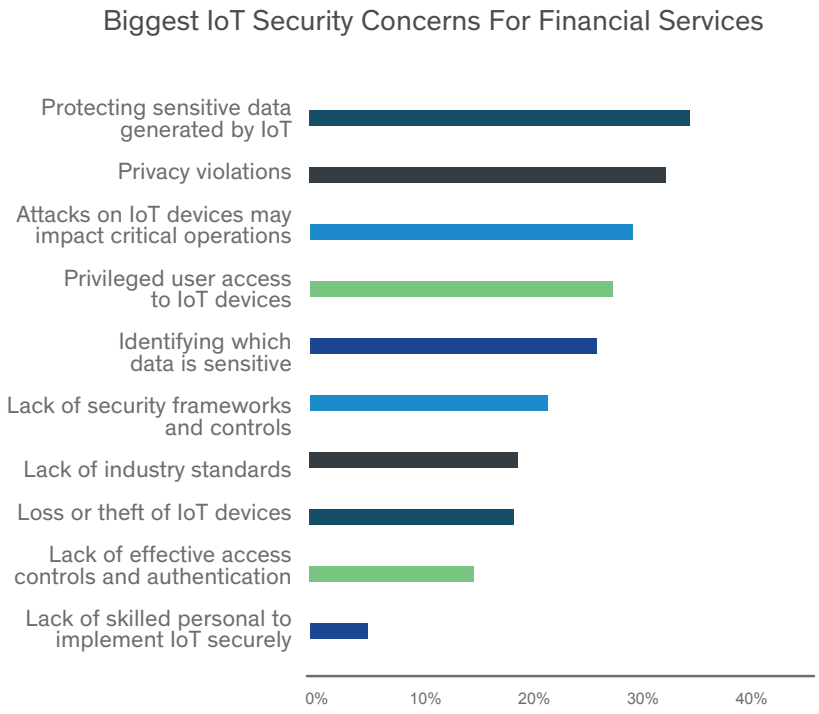


Figure 9: Biggest IoT security concerns for financial services

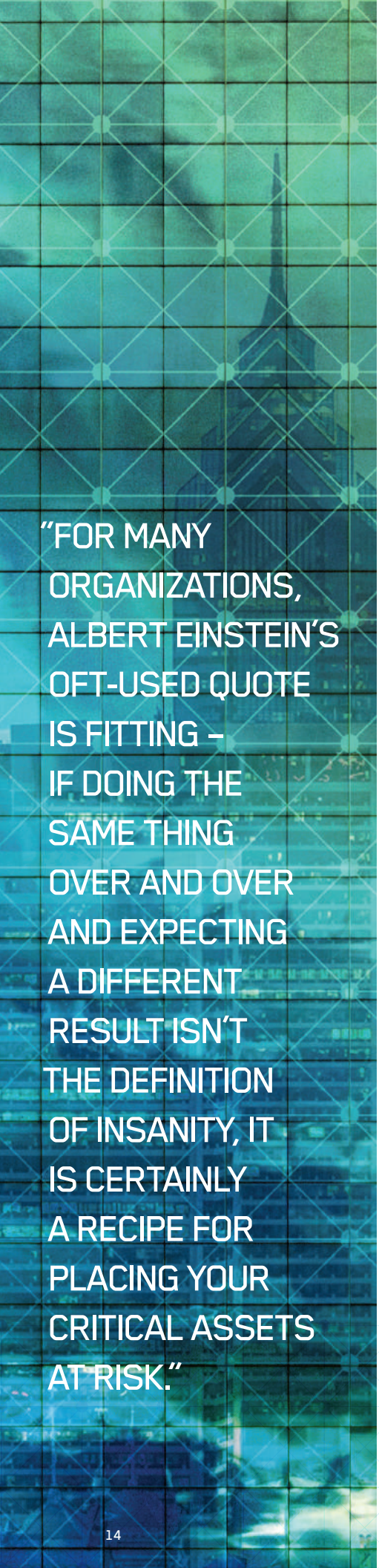
RECOMMENDATIONS

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? Like most regions and verticals, financial organizations must recognize that doing more of the same won't help us achieve an improved security posture. As an industry, we need to pay more attention to new techniques for preventing attacks as well as detecting potential threats more rapidly and narrowing the window of exposure.

As firms grow to accept the limitations of traditional security approaches, data security is likely to become a critical component of any comprehensive security strategy. Organizations of all sizes and in all regions need to consider things like data discovery and classification, DLP and encryption, particularly as cloud, big-data and IoT create greater volumes of sensitive data distributed across an exponentially larger array of devices. This is particularly true of financial services, which has the highest proportion of respondents that claim superior knowledge of the location of sensitive data in their organization.

But as we have discussed, data security is not without its own challenges. More liberal use of encryption and other data security techniques 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. Given the top two data security hurdles for financial services – namely, complexity and lack of staff - the message for enterprises and data security vendors is clear. In order to achieve broader adoption of data security products, the latter must be more cost effective, simpler to use and require less manpower to deploy, operate and maintain on an ongoing basis.



While financial services organizations have the luxury of more available budget than most other verticals, the latter should still consider vendors with a broad range of data security options to help reduce not only the upfront acquisition cost, but also vendor proliferation, integration challenges as well as the ongoing operational costs that have traditionally been associated with data security. We have also seen the emergence of service-based offerings for a variety of data security tools such as DLP, encryption key management and digital certificate management, to name a few, and we anticipate more service-based data security offerings to emerge in coming years.

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

DISCOVER AND CLASSIFY	Get a better handle on location of sensitive data, particularly for early Big Data adopters like financial services
ENCRYPTION AND ACCESS CONTROL	**Data center**: Consider an 'encrypt everything' strategy **Cloud**: encrypt and manage keys **Big Data**: employ discovery as a complement to encryption **IoT**: consider device authentication and encryption, as well as encryption in transit
DATA SECURITY PLATFORMS	Use platform solutions to avoid a tangle of point products and keep costs down
SERVICES-BASED DELIVERY	Look for services- based offerings or partnership programs to reduce complexity and staffing requirements

ANALYST PROFILE

Garrett Bekker is a Senior Analyst in the Information 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

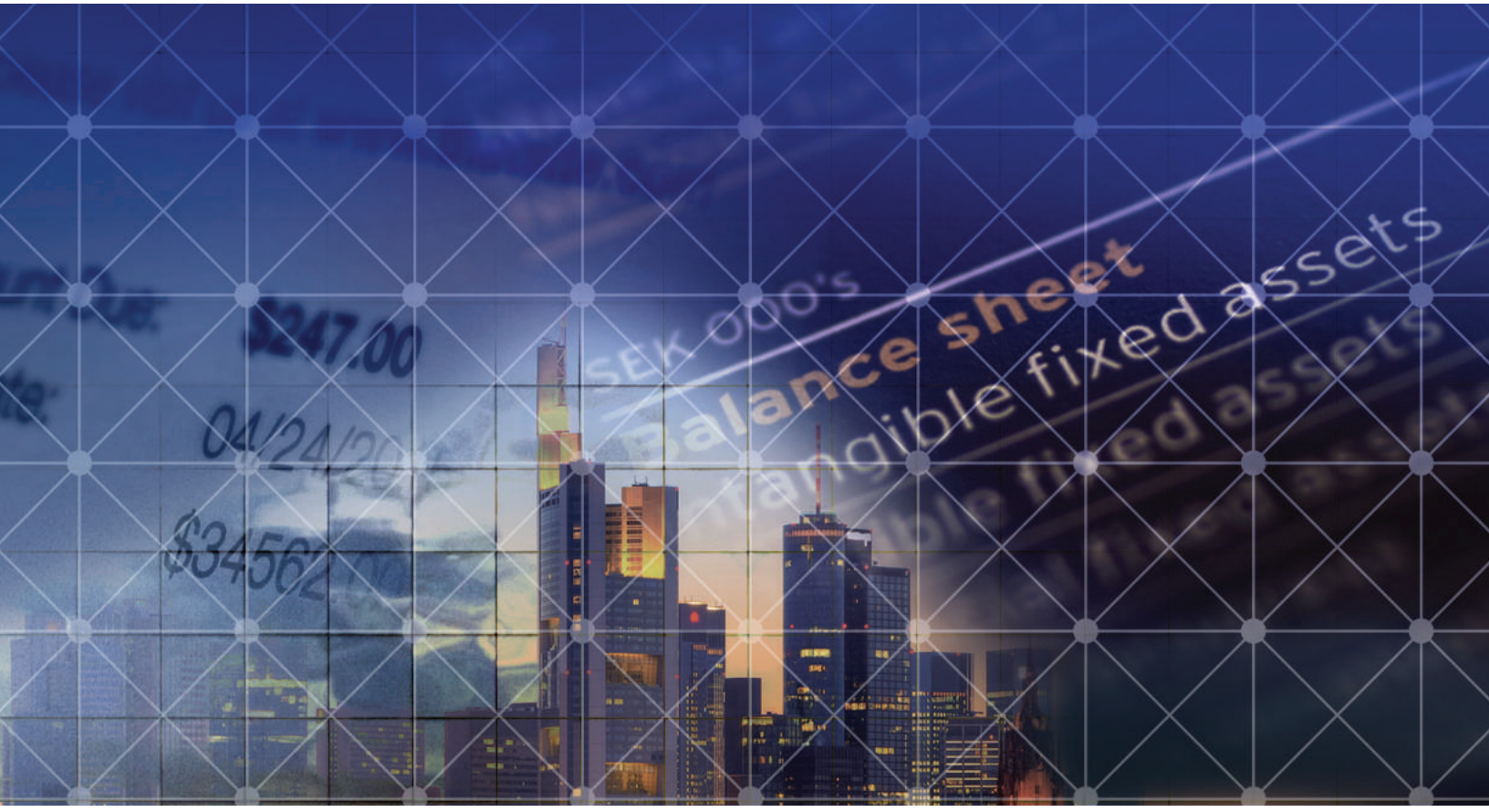
ABOUT 451 RESEARCH

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**.



Vormetric Data Security™

Vormetric.com/DataThreat/2016