451 Research®

Vormetric Data Security™

2016 VORMETRIC DATA THREAT REPORT

Trends in Encryption and Data Security

FEDERAL GOVERNMENT EDITION

RESEARCH BRIEF

#2016DataThreat

TABLE OF CONTENTS

INTRODUCTION 3

OLD SECURITY HABITS DIE HARD 4

KEY FINDINGS 5

ABOUT THIS RESEARCH BRIEF 5

THE BIG DISCONNECT 5

Compliance still a driver – but compliance is NOT security 6

SKILL SHORTAGES AND BUDGETARY CONSTRAINTS LOOM LARGER IN US FED 7

RISKY BUSINESS 8

CLOUD, BIG-DATA AND IOT PRESENT NEW CHALLENGES 9

Cloud 9

Big Data 10

ioT 10

RECOMMENDATIONS 10

RECOMMENDATION SUMMARY 11

ANALYST PROFILE 11

ABOUT 451 RESEARCH 12

ABOUT VORMETRIC 12

OUR SPONSORS

INTRODUCTION

The past few years have subjected the U.S. economy to a seemingly endless chain of well-publicized data breaches that have left few Americans confident that U.S. organizations are doing enough to ensure the safety of their digitally stored personal information.

The past few years have subjected the U.S. economy to a seemingly endless chain of well-publicized data breaches that have left few Americans confident that U.S. organizations are doing enough to ensure the safety of their digitally stored personal information. The Cybersecurity National Action Plan (CNAP) recently outlined by President Barack Obama acknowledges some of the current weaknesses in our national digital infrastructure and contains several proposals to help reduce our overall vulnerability to cyber threats, including $3bn in new funding, the creation of a federal CISO role, plans to recruit new cybersecurity talent and increased information sharing with the private sector. Regardless of the timing, appropriateness and ultimate effectiveness of the proposals outlined in CNAP, the plan highlights the growing awareness that as a nation, we need to do more to help increase our overall preparedness to meet the security threats presented by a new world order filled with cyber-criminals, nation-states, hacktivists and cyber-terrorists.

This may be particularly true for federal agencies, many of which are dealing with outdated systems and budget constraints that have limited their state of readiness to meet modern challenges. Unfortunately, there are plenty of examples to illustrate our need for greater attention to cybersecurity within the federal sector. The most recent was the confirmation of yet another cybersecurity incident at the IRS in which hackers used stolen SSN automated malware to produce over 100,000 e-file PINs, which could be used to file fraudulent tax returns.

"President Obama's recent cybersecurity proposals highlight the need to do more to increase our preparedness to combat cyberthreats."

OLD SECURITY HABITS DIE HARD

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

At a high level, our global survey results showed that in many ways, security professionals are like generals fighting the last war. As an example, spending intentions reflected a tendency to stick with what has worked – or not worked - in the past, such as network and endpoint security. This was no less true in the US federal vertical, where the top category for increased spending over the next 12 months among U.S. government respondents (53%) is network defenses, followed by analysis and correlation tools (46)%. Further, 60% of respondents believe network defenses are 'very' effective, more than any other vertical and well above the U.S. average of 53%. Conversely, the US Fed vertical takes a fairly dim view of data-at-rest defenses - only 68% of respondents selected 'very' or 'extremely' effective, the lowest of any vertical and below the U.S. average of 75%. Similarly, data-at-rest defenses were ranked dead last in terms of spending plans, with just 37% planning to increase their spending on data-at-rest defenses, compared to the U.S. average of 45%.

Over time, we are hopeful that the security industry will come around to the fact that perimeter defenses offer little help defending against multi-stage attacks, and that approaches that have proven to be effective at protecting data after attackers have bypassed perimeter defenses – such as file and application encryption and access controls – will gain more attention.

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.

As was the case with our global Data Threat Report, responses from the U.S. Federal vertical contained a mix of good and not-so-good news. On the positive side, 58% of US Fed responded 'somewhat' or 'much' higher, when asked about their overall spending intentions with respect to protecting sensitive data. The bad news is that this was the lowest of all verticals, and well behind financial services at 69%. Worse yet, 61% of US federal respondents indicated they had experienced a breach at some point in the past, higher than the U.S. average of 57% and trailing only healthcare (63%). U.S. federal respondents are also the least likely to increase their spending as a result of data breaches (42% vs. 32%).

"OVER TIME, WE ARE HOPEFUL THAT THE SECURITY INDUSTRY WILL COME AROUND TO THE FACT THAT PERIMETER DEFENSES OFFER LITTLE HELP DEFENDING AGAINST MULTI-STAGE ATTACKS."

To be fair, there are some encouraging takeaways. 37% of U.S. federal respondents plan to invest in data-at-rest defenses this year. Following best practices also appears to be gaining momentum–while compliance remains the primary motivator for securing sensitive data, nearly half (48%) are looking to implement data security to follow industry best practices. And there are increasing signs that respondents are looking to implement 'newer' security tools such as cloud security gateways (40%), application encryption (34%), data masking (31%) and tokenization (27%). In summary, U.S. federal agencies are doing many of the right things–they just need to do more.

KEY FINDINGS:

There's still work to be done

- 58% of U.S. Fed respondents plan to increase data security spending, the lowest of all verticals
- 61% experienced a breach at some point in the past, higher than the U.S. average of 57%
- U.S. Fed respondents are also the least likely to increase their spending as a result of data breaches (42% vs. 32%).

What we're doing right

- 37% of U.S. federal respondents plan to invest in data-at-rest defenses this year.
- Nearly half (48%) are looking to implement data security to follow industry best practices
- 40% plan to implement cloud security gateways
- 34% plan to implement application-layer encryption
- 27% plan to implement tokenization

In the following sections we will highlight several key topics with respect to the US federal vertical, and also point out notable instances where the federal vertical differed from other segments.

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. Federal Government. 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.

THE BIG DISCONNECT

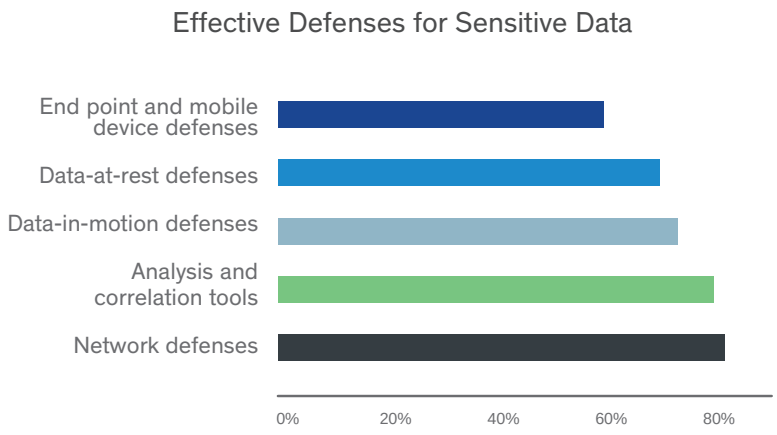


Figure 1: Ratings of Very or Extremely Effective for Defenses in Protecting Sensitive Data

As noted above, overall security 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 truly needed to prevent data theft. For example, with respect to tools that have been shown to be more effective in protecting sensitive data than simple perimeter defenses, only 68% of federal government respondents viewed data-at-rest defenses as 'very' or 'extremely' effective, below the U.S. average of 75% and ranked second to last across all categories. Similar views towards data security are generally reflected in respondents' plans for federal security spending within the next 12 months. The top category for increased spending over the next 12 months among 53% of U.S. government respondents is network defenses, with analysis and correlation tools in second place with 46%. Data-at-rest defenses were ranked dead last in terms of plans to increase security spending at 37%, below the U.S. average of 45%.

"Security 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 truly needed to prevent data theft."

Compliance still a driver – but compliance is NOT security

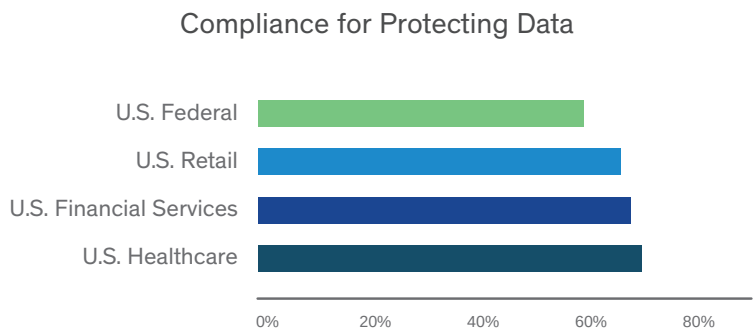


Figure 2: Ratings for Compliance as Very or Extremely Effective at Protecting Data

"Many security executives across the globe still appear to equate compliance with security, 57% of U.S. Federal and nearly two-thirds (64%) of our global respondents, viewed compliance requirements as either 'very effective' or 'extremely effective' in preventing data breaches."

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. Given that the US public sector is one of the more heavily regulated sectors in the U.S., it's no surprise that 57% of U.S. federal respondents also view compliance as 'very' or 'extremely' effective, though it's worth noting this trails other heavily-regulated sectors such as healthcare (68%), financial services (66%) and retail (65%). 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. Yet compliance is still the leading reason for securing sensitive data in the US federal vertical (55%) and top reason for data security spending (57%), higher than global average of 46%, but inline with overall US (54%).

SKILL SHORTAGES AND BUDGETARY CONSTRAINTS LOOM LARGER IN US FED

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 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 51% of federal respondents. Complex deployments also typically require significant staffing requirements, and not surprisingly 'lack of staff to manage' came in as the second highest barrier at 44% of U.S. federal respondents, the highest percentage for this category across all U.S. vertical industries; healthcare was second with 38%. 451 Research has chronicled the imbalance between demand and supply for skilled security personnel, and it's no surprise that this might be felt more acutely in the public sector. In that sense, CNAP's plan to establish scholarships and offer student loan forgiveness as a way to more effectively compete for scarce security personnel with the private sector has merit. It's also not surprising that budgetary constraints received the highest ranking as a data security adoption barrier in the federal government sector (43%), well ahead of more 'wealthy' verticals like financial services (26%).

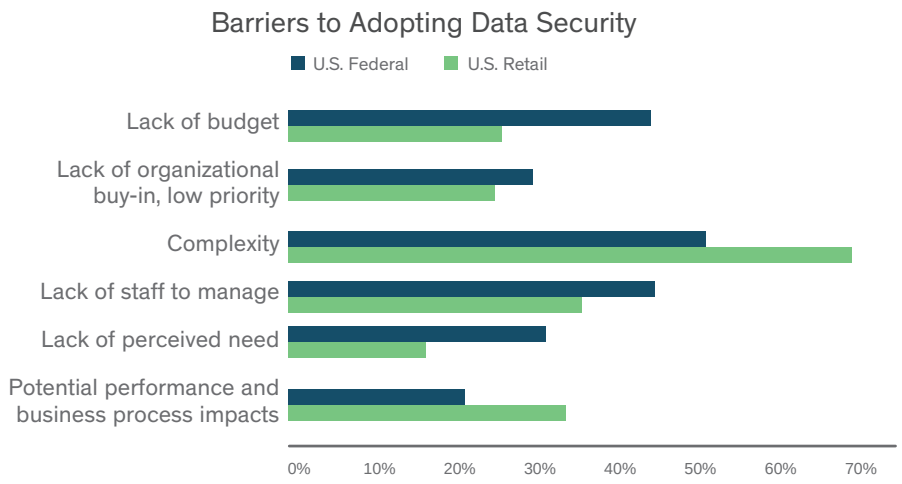


Figure 3: Percentage of Data Security barriers for U.S. Federal versus U.S. Retail

"COMPLEXITY AND LACK OF STAFF WERE THE TOP TWO BARRIERS TO ADOPTING DATA SECURITY."

RISKY BUSINESS

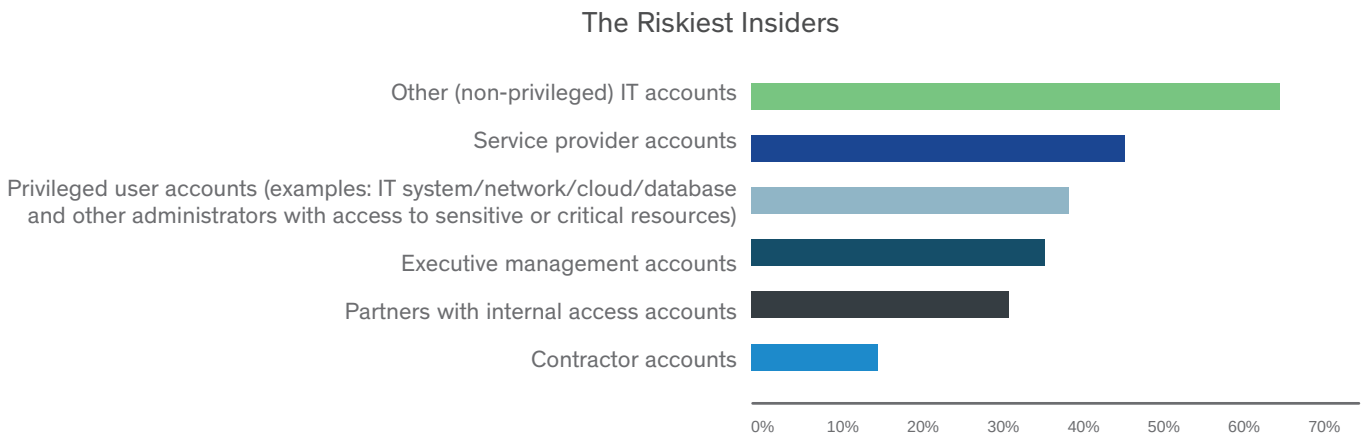


Figure 4: Percentage of riskiest insiders by user type

When it comes to insider risks to sensitive data, 65% of U.S. federal government respondents state that privileged user accounts are the riskiest, with contractor accounts coming in a distant second (43%),. With respect to external threat actors, cyber-criminals held the #1 spot with 76% of federal respondents. Somewhat surprisingly, only 47% of U.S. federal respondents recognize nation-states as a high-risk external threat, despite reports of attacks from Iran, North Korea and China against federal targets such as the Office of Personnel Management (OPM) and the IRS to name a few.

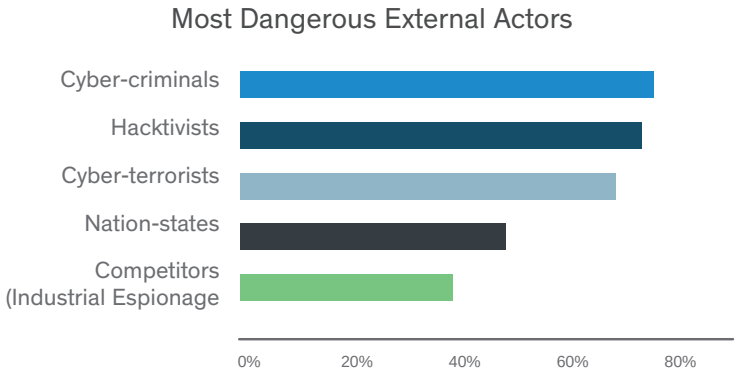


Figure 5: Most dangerous external actors ranked by percentage

"SOMEWHAT SURPRISINGLY, ONLY 47% OF U.S. FEDERAL RESPONDENTS RECOGNIZE NATION-STATES AS A HIGH-RISK EXTERNAL THREAT."

CLOUD, BIG-DATA AND IOT PRESENT NEW CHALLENGES

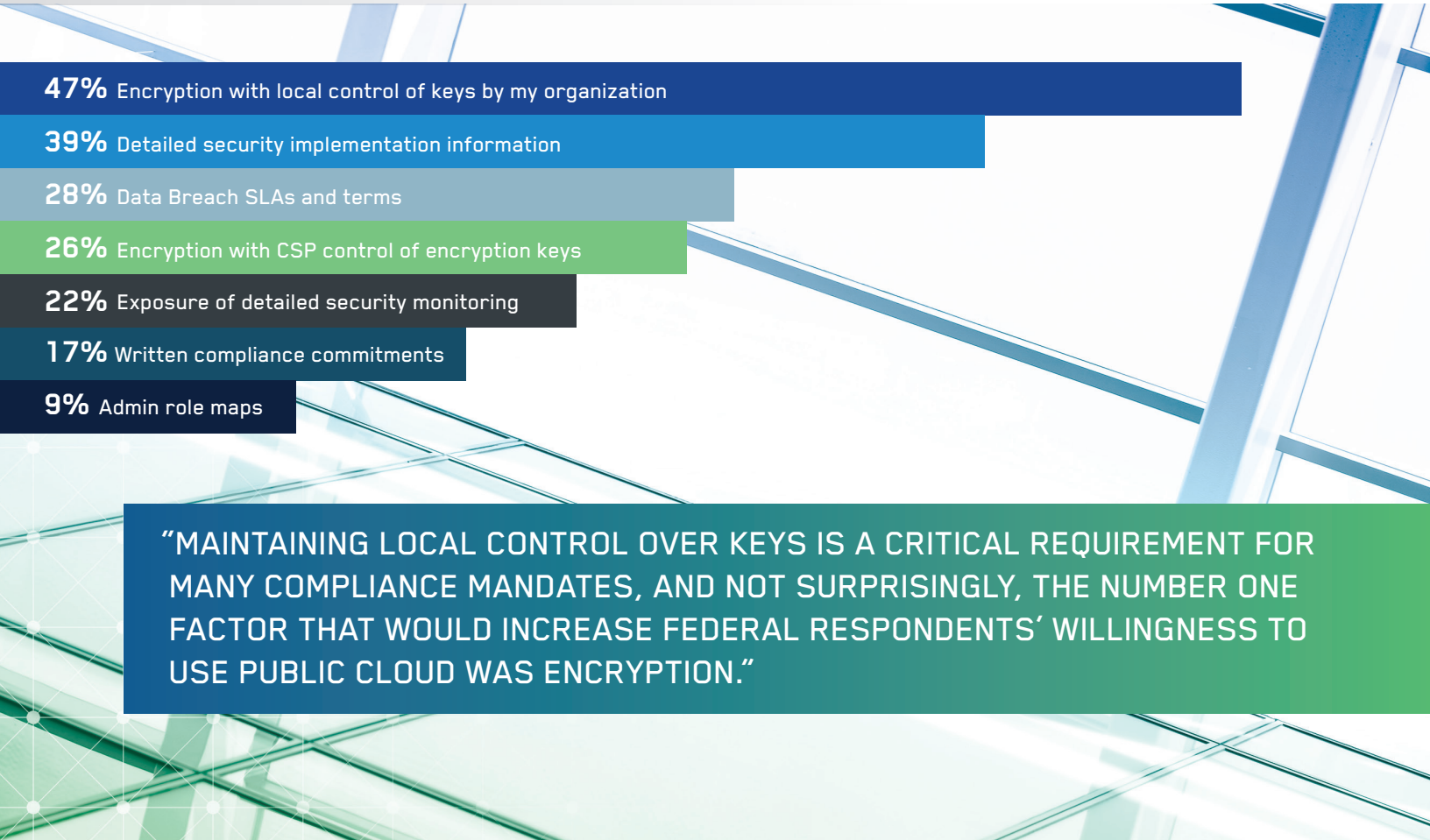
Much has been made of the unique security challenges posed by the triumvirate of big-data, cloud computing and IoT. Since the latter take advantage of resources that largely exist outside of traditional enterprise boundaries, legacy security tools and approaches that rely on a hardened perimeter to enforce 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.

Cloud

U.S. federal concerns regarding public cloud services were generally in line with other U.S. industries. The top concerns included security breaches or attacks at the service provider and increased vulnerabilities from a shared infrastructure, each with 70% of responses. Even so, 84% of U.S. federal respondents are planning on storing sensitive data in some form of public cloud environment (IaaS, PaaS or SaaS) within the next 12 months.

What are the primary ways to ease cloud adoption concerns among public sector respondents? Like most regions, encryption of sensitive data stored in the cloud was a 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 federal respondents' willingness to use public cloud was encryption, at 47% of responses. In comparison, we noticed a much wider disparity with respect to encryption with key management handled by the service provider than in most other regions in the U.S. as well as abroad. Just 26% of respondents indicated they would opt for service provider control of keys, well below the U.S. average of 37%. It's worth noting that the two options elicited nearly identical responses from all U.S. verticals in last year's survey, and we anticipate the gap between the two key management options will continue to widen over time and awareness of the importance of key management continues to grow.

Figure 6: What Would Increase Federal Cloud Usage?



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

Big Data

While federal government trails other verticals in terms of adopting new technologies such as mobile, SaaS and IoT, the sector is surprisingly optimistic with respect to big-data; the latter was the ranked second in terms of the 'new' technology environments federal respondents were most likely to store sensitive data (56% of respondents), trailing only IaaS at 62%. One potential explanation is that the U.S. federal vertical sees big-data as less risky than other verticals – only 15% regard big-data implementations as presenting the greatest risk for loss of sensitive data, compared to 24% overall. With regards to what risks they were most concerned about, the fact that sensitive data may reside anywhere within a big-data environment was the number one answer (57% versus the U.S. average of 45%). The number two and three concerns were securing reports that may contain sensitive data (48%) and privileged access to big-data (39%).

IoT

Though IoT promises to present a security hurdle of epic proportions, security concerns also reflect IoT's early stage of adoption. Given the sheer volume of IoT devices that are anticipated, securing sensitive data generated by IoT devices is not surprisingly the primary concern of most security professionals (35%), followed by the loss or theft of IoT devices (29%). And while most respondents 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 at 27% of respondents.

RECOMMENDATIONS

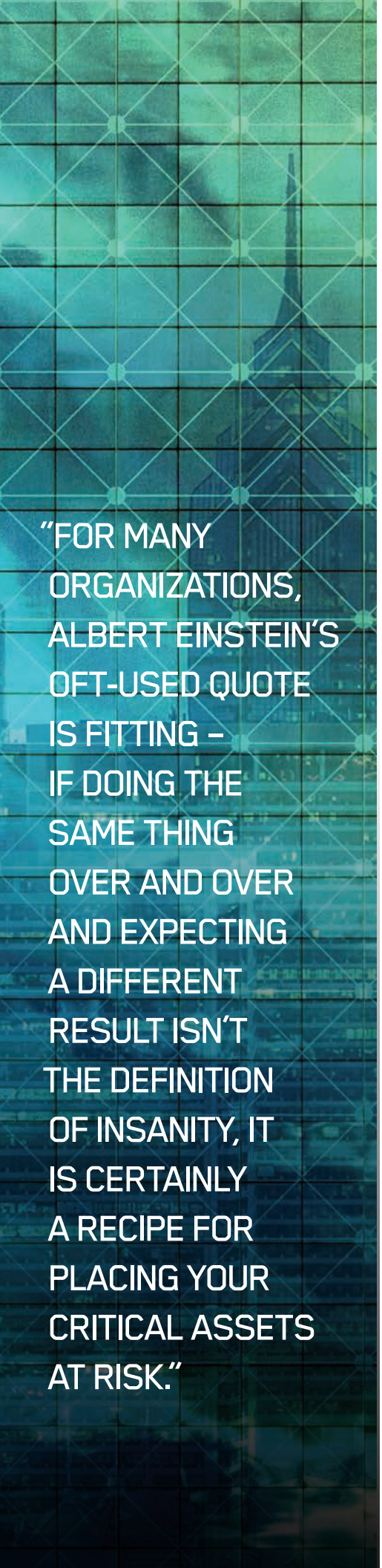
The past few years have been challenging ones for the information security industry as a whole, and nearly everyone has been affected – end users, enterprises and security vendors alike. If we have learned anything in that time, it is that our old ways of doing business and securing our resources are 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, public sector 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 more critical component of any comprehensive security strategy, and enterprises of all sizes need to consider things like data discovery and classification, DLP and encryption for more than just meeting compliance check-boxes and protecting laptops and USB drives from loss or theft. 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 main data security hurdles of complexity, and specifically for US federal customers, lack of staff and budgetary constraints, 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. Federal government customers should thus consider vendors with a broad range of data security options to help reduce both the upfront acquisition cost as well as 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 is following new developments in threat analytics and techniques to monitor data access patterns that can establish baselines of 'normal' activity that can be used to identify potential breaches and provide a greater degree of visibility into potentially compromised resources.



RECOMMENDATION SUMMARY

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.

ENCRYPTION AND ACCESS CONTROL	Use encryption for more than checking compliance boxes. Consider an 'encrypt everything' strategy as a way to pursue industry best practices
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 staffing requirements
SECURITY ANALYTICS	Use data access monitoring and threat indicators to identify new threat patterns

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