

2016 VORMETRIC DATA THREAT REPORT

Trends in Encryption
and Data Security

EUROPEAN EDITION

#2016DataThreat



TABLE OF CONTENTS

INTRODUCTION	3	THE U.K. AND GERMANY MOST WARY OF PRIVILEGED INSIDERS, BUT DIFFER SHARPLY ON OTHER INSIDER THREATS	11
OLD SECURITY HABITS DIE HARD	4		
GERMANS FEELING MORE VULNERABLE THAN MOST	5	CLOUD, BIG-DATA AND IOT PRESENT NEW CHALLENGES	11
KEY FINDINGS	6	Cloud	12
ABOUT THIS RESEARCH BRIEF	7	Big Data	13
Compliance is NOT security, though Germany and the U.K. differ	7	IoT	13
PENDING DATA SOVEREIGNTY REGULATIONS COULD BOOST DATA SECURITY, PARTICULARLY ENCRYPTION, MASKING AND TOKENISATION	8	RECOMMENDATIONS	13
COMPLEXITY THE TOP BARRIER TO DATA SECURITY, IN GERMANY AND THE UK TOO	10	RECOMMENDATION SUMMARY	15
		ANALYST PROFILE	15
		ABOUT 451 RESEARCH	15
		ABOUT VORMETRIC, A THALES COMPANY	15

OUR SPONSORS



INTRODUCTION

The past few years have subjected organisations across the globe to a seemingly endless chain of well-publicised data breaches. The latter have elevated concerns about protecting sensitive data beyond the technical realm and into the mainstream public consciousness, and left few individuals confident that organisations are doing enough to ensure the safety of their digitally stored personal information.

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, organisations are spending billions each year on various forms of cybersecurity and venture capitalists continue to spend princely sums on startups touting the latest and greatest new security offerings.

“The number of records breached in 2015 was more than twice that of 2014.”

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. 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. Thus as the line between ‘insider’ and ‘outsider’ continues to blur, the scope of the 2016 edition of the Vormetric Data Threat report has been expanded to encompass all manner of threats to sensitive data, and to get a better sense of what the most relevant threats organisations 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 is targeted to the European market, specifically the U.K. and Germany, and will address both the similarities to our global report, and also key distinctions with respect to the U.S. and other regions such as Australia, Brazil, Mexico and Japan.

“AS THE LINE BETWEEN ‘INSIDER’ AND ‘OUTSIDER’ CONTINUES TO BLUR, THE SCOPE OF THE 2016 EDITION OF THE VORMETRIC DATA THREAT REPORT HAS BEEN EXPANDED TO ENCOMPASS ALL MANNER OF THREATS TO SENSITIVE DATA.”

OLD SECURITY HABITS DIE HARD

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 €35 billion is spent annually on information security products, and the lion’s share 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.

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

As an example, results from our 2016 global report showed that spending intentions reflected a tendency to stick with what has worked - or not worked - in the past, such as network and endpoint security. This also held true in the U.K., where network security was once again the top category for increased spending over the next 12 months (42%). In terms of effectiveness, however, network security fell into a tie for third place in terms of effectiveness with data-in-motion defences (69%), while data-at-rest gained the top spot at 75% - the only nation that ranked data-at-rest security as the most effective at securing sensitive data. Unfortunately some of the optimism towards data security in the U.K., is not yet translating into spending - data-at-rest defences were ranked near the bottom in terms of spending priorities for the next 12 months (34%) ahead of only data-in-motion defenses (30%). As in most regions, complexity, lack of staff and performance concerns are among the top concerns with respect to adopting data security in the U.K., which will be discussed in more detail below.

“Network security was once again the top category for increased spending over the next 12 months in the U.K., though data-at-rest defenses were ranked highest in terms of overall effectiveness.”

In Germany, by contrast, network security was ranked at the top in terms of effectiveness: 81% of German respondents rated network defenses as either ‘very’ or ‘extremely’ effective at protecting sensitive data, while data-at-rest security fell to third place at 68%. In terms of spending, however, network security fell to a distant fourth-place ranking, with just 35% of German respondents planning to increase their spending in the next 12 months - one of the lowest rankings for network security spending of any region. The outlook for data security spending was much brighter in Germany, however. While many regions ranked data-at-rest security at or near the bottom in terms of spending priorities, the category slipped into second spot in Germany at 37%.

Defenses Rated as Very or Extremely Effective at Protecting Sensitive Data

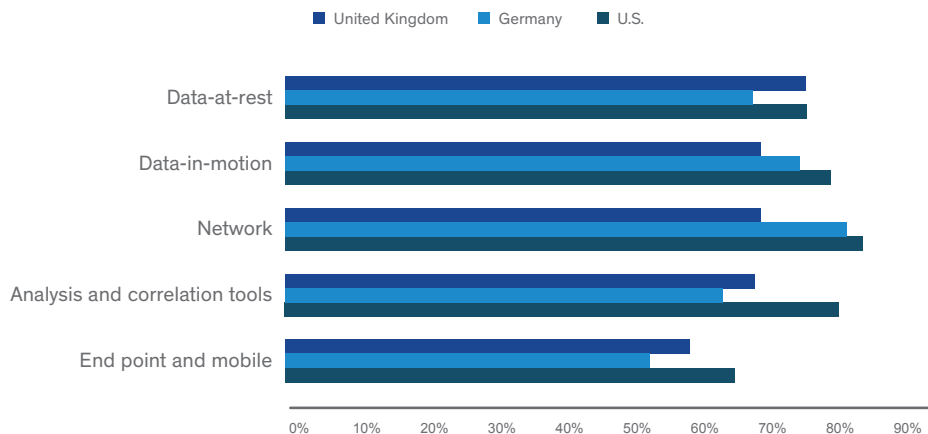


Figure 1: Ratings of Very or Extremely Effective for Defenses in Protecting Sensitive Data

IT Security Spending Plans By Type of Defense

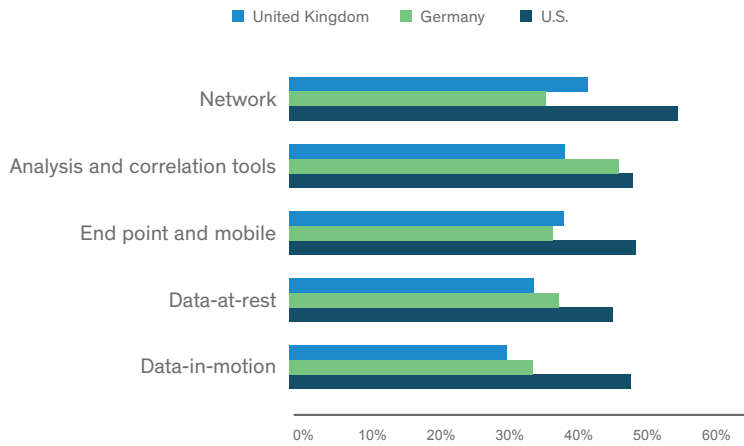


Figure 2: IT Security spending plans by type of defence

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

GERMANS FEELING MORE VULNERABLE THAN MOST

Germany and the U.K. also differed sharply in terms of past breaches and vulnerability levels. In Germany, 72% of respondents claim to have been breached at some point, second only to Australia at 85%. Further, 37% of German enterprises claim to have been breached in the past year alone – more than any other region and well ahead of the 22% global average. Not surprisingly, German respondents are also feeling quite vulnerable – 40% responded either ‘very’ or ‘extremely’ vulnerable to both internal and external data threats.

In the U.K., however, while 64% claim to have been breached at some point in the past (slightly ahead of the 61% global average), the nation came in at the low end of the spectrum in terms of feelings of vulnerability – just 23% indicated they feel ‘very’ or ‘extremely’ vulnerable to data threats, below the global average of 30%. Further, despite recent incidents like the Talk Talk breach in 2015, U.K. respondents were among the least likely to increase spending on encryption and data security as a result of a high-profile breach (46%, compared to 49% in Germany, 64% in the U.S. and 53% globally).

Data Breach and Compliance Audit Failures

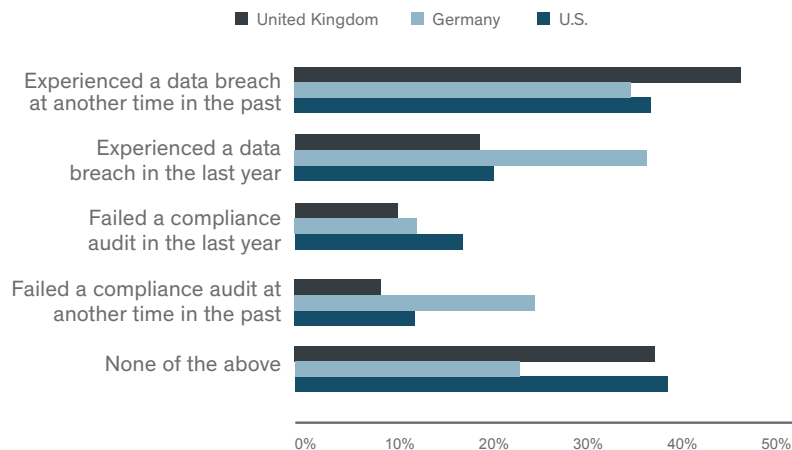


Figure 3: Comparative rates of data breach and compliance audit failures

KEY FINDINGS:

There's still work to be done

- In the U.K., network security was ranked at the top in terms of spending priorities for the next 12 months (42%), while data-at-rest defences were ranked near the bottom (34%).
- In Germany, 81% of German respondents rated network defences as either 'very' or 'extremely' effective at protecting sensitive data, the top selection.
- 72% in Germany and 63% in the U.K. experienced a breach at some point in the past, higher than the global average of 61%. 37% of Germans claim to have been breached in the past year alone - more than any other region and well ahead of the 22% global average.
- 40% in Germany indicated they felt either 'very' or 'extremely' vulnerable to both internal and external data threats.
- 67% of German respondents viewed compliance requirements as either 'very' or 'extremely' effective in preventing data breaches, ahead of the global average of 64%.

To be fair, there are some encouraging takeaways. For example, the U.K. had the highest percentage of respondents (59%) that selected implementing best practices as a strategic reason for utilising encryption (vs. 53% globally). U.K. respondents also identified data-at-rest security as the most effective at protecting against sensitive data (75%), the top selection in that country.

And there are increasing signs that respondents in both regions are looking to implement 'newer' security tools. Specific categories with the biggest planned increases for data security spending in Germany include multi-factor authentication (54%), privileged identity management (47%) and SIEM and analytics tools (45%), while the top choices for the U.K. include application layer encryption (52%), tokenisation (49%) and multi-factor authentication (44%). In summary, both the U.K. and Germany are doing many of the right things – they just need to do more of them.

What we're doing right

- In the U.K., data-at-rest was ranked first in terms of effectiveness of protecting sensitive data at 75%.
- The top reason in Germany to use encryption was to follow best practices (48% vs. 53% globally).
- 53% in the U.K. and 42% in Germany plan to implement application layer encryption (vs 40% globally).
- 49% in the U.K. plan to implement tokenisation, the highest of any region and ahead of the global average of 39%.
- The U.K. (41%) and Germany (40%) had among the highest spending intentions for cloud encryption gateways (38% global average).

In the following sections we will highlight several key topics with respect to both the U.K. and Germany and also point out notable instances where the latter differed from other regions.

“U.K. RESPONDENTS ALSO IDENTIFIED DATA-AT-REST SECURITY AS THE MOST EFFECTIVE AT PROTECTING AGAINST SENSITIVE DATA (75%), THE TOP SELECTION IN THAT COUNTRY.”

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 over 100 senior security executives in each region. These results will be compared, where applicable, to findings in other key regions such as the U.S., Latin America and APAC.

Compliance is NOT security, though Germany and the U.K. differ

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 programme, the steadily growing volume of data breaches should serve as a strong reminder that we need to do more than just tick the compliance box if we want to make sure our data remains safe.

Yet compliance was another notable area where we see a divergence in attitudes between the two nations. Germany, for example, had one of the most sanguine views of compliance – 67% of German respondents viewed compliance requirements as either 'very' or 'extremely' effective in preventing data breaches, ahead of the global average of 64% and trailing only Brazil (83%) and Australia (68%). Yet German organisations were also more likely than most regions to have failed a compliance audit at some point in the past (36%), trailing only Australia (a notable outlier at 61%) and ahead of the global average of 32%.

It's not surprising then that compliance was ranked the number one reason in Germany for securing sensitive data (47%), in line with the global average of 47%. What was surprising was that only 39% of respondents from Germany selected compliance as a cloud security concern, making it the lowest-ranked cloud concern in Germany and well below the global average of 62%. It's also worth noting that requirements from business partners, customers and prospects was tied with compliance at 47%, well ahead of the global average of 37% and trailing only Japan (50%). Part of this may be attributed to the growing concern in Europe of being publicly exposed for not exercising adequate precautions with customer data. Implementing best practices was the third-highest ranked reason to secure sensitive data in Germany, (39%), slightly lower than the 44% global average). Germany also had the lowest concern for reputation and brand protection of any region (33%), which was the number one-ranked global response at 51%, and was also less likely than any nation other than Japan to select protecting brand or reputation as a strategic driver for deploying encryption.

The U.K. came in at the opposite end of the spectrum with respect to the effectiveness of compliance mandates – just 61% responded 'very' or 'extremely' effective, ahead of only Japan at 33% and Mexico (57%). Yet compliance is still one of the leading reasons for securing sensitive data for UK respondents (47%), in line with the global average. The number one reason for securing sensitive data in the U.K. was reputation and brand (50% vs. the 51% global average).

"Many security executives across the globe still appear to equate compliance with security, though Germany and the U.K. have divergent views; 67% of Germans viewed compliance requirements as either 'very effective' or 'extremely effective' in preventing data breaches, compared to just 61% in the U.K."

"The number one reason for securing sensitive data in the U.K. was reputation and brand."

Effectiveness of Compliance Requirements for Preventing Data Breaches

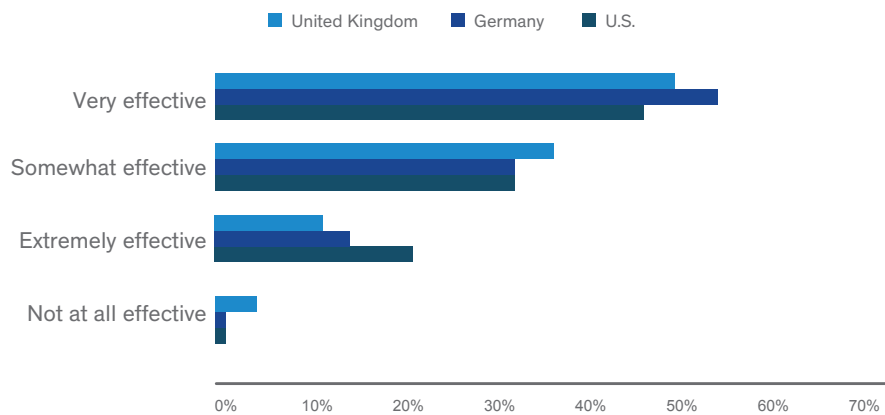


Figure 4: Ratings for effectiveness of compliance requirements for preventing data breaches

PENDING DATA SOVEREIGNTY REGULATIONS COULD BOOST DATA SECURITY, PARTICULARLY ENCRYPTION, MASKING AND TOKENISATION

While compliance mandates can serve as an effective baseline, many suffer from a lack of specificity, while those that lay out detailed security requirements often fall out of date quickly as technology and attack methods evolve. That said, the upcoming General Data Protection Regulation (GDPR) that was recently passed in Europe promises to set a higher bar for enterprises and security practitioners to meet. While there are many nuances to GDPR, the new legislation promises to have more ‘teeth’ than many other compliance mandates, with hefty fines for organisations that fail to take steps to protect the privacy of data in their custody. Additionally, GDPR also identifies certain security controls that companies that are bound by GDPR can use to mitigate their overall risk exposure, including encryption and data masking, as well as tokenisation.

In addition to GDPR, there are perhaps as many as 100 national and regional laws that mandate protection of personal data in privacy-sensitive countries like Canada, Australia, as well as in Asia and Latin America. In that spirit, we asked several questions in this year’s survey that attempted to shine some light on the importance of data privacy and sovereignty.

When it came to reasons for encrypting data, meeting local data sovereignty requirements was the fourth-ranked global response (38%), trailing best practices, compliance requirements (PCI, HIPAA, etc.) and adverse reputational damage. Interestingly, data sovereignty fared even lower in the U.K. and Germany, who along with Japan (33% each) had the lowest responses of any region, though it could be argued that GDPR is directed as much – if not more so – at non-EU nations such as the U.S.

However, data sovereignty concerns were more apparent with respect to cloud resources. When we asked respondents what their top security concerns were regarding the use of public cloud, data sovereignty was the number three response globally (65%), trailing cloud provider breaches and concerns from shared infrastructure, but was the number one response in the U.K. (66%) and the number two response in Germany (60%). Similarly, with respect to Big Data concerns, privacy violations resulting from data originating in multiple countries was the number three global concern (40%), but the number one response in the U.K. (43%) and number two in Germany (44%).

“DATA SOVEREIGNTY WAS AMONG THE TOP TWO SECURITY CONCERNS IN BOTH GERMANY AND THE U.K REGARDING THE USE OF PUBLIC CLOUD AND BIG DATA RESOURCES.”

Encryption Strategies

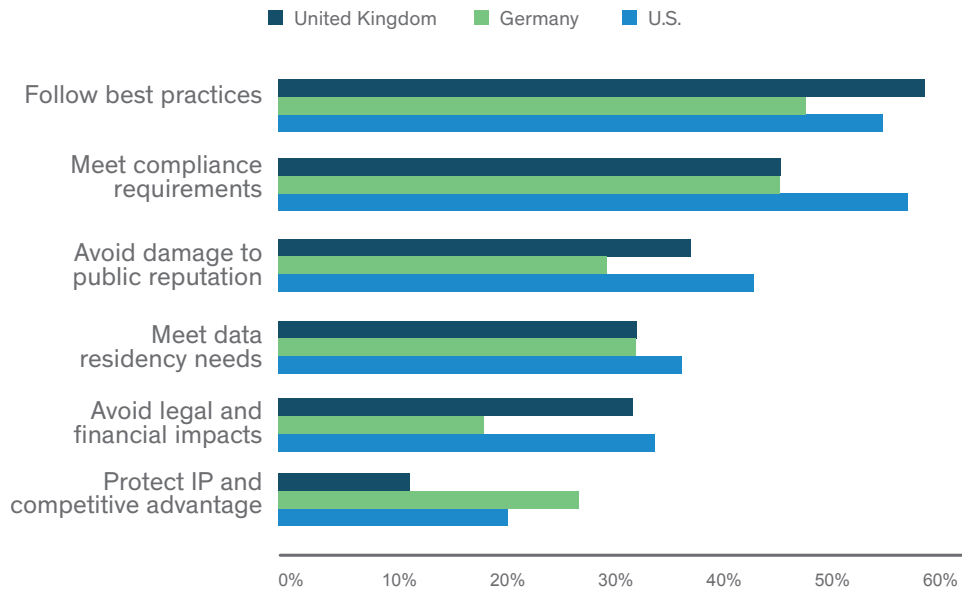


Figure 5: Encryption strategies

Top Cloud Security Concerns

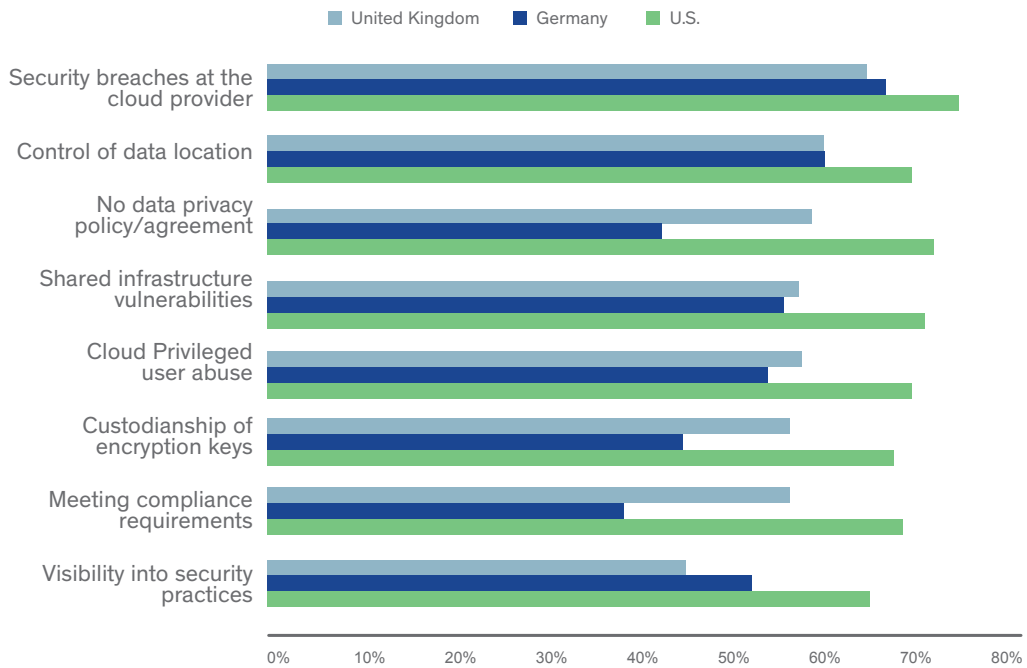


Figure 6: Top Cloud Security Concerns



Figure 7: Top Big Data Security Concerns

COMPLEXITY THE TOP BARRIER TO DATA SECURITY, IN GERMANY AND THE UK TOO

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 being protected, 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 for both nations, though by a much wider margin for Germany (71%) compared to the UK (56%) and the global average (57%). Complex deployments also typically require significant staffing requirements, and not surprisingly 'lack of staff to manage' came in as the second highest barrier globally (38%) and in Germany (35%). The UK, however, had the lowest concerns about staffing requirements (29%) of any region, and were more concerned about the potential impact of data security on performance and business processes (33%) relative to other adoption barriers.

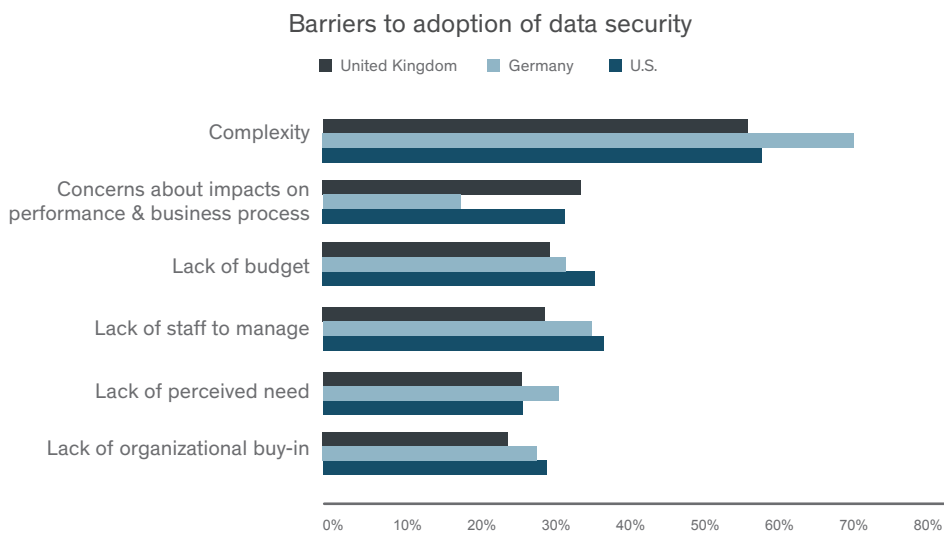


Figure 8: Barriers to adoption of data security

THE U.K. AND GERMANY MOST WARY OF PRIVILEGED INSIDERS, BUT DIFFER SHARPLY ON OTHER INSIDER THREATS

When it comes to insider risks to sensitive data, attitudes between Germany and the UK again differed sharply, particularly with respect to ordinary employees and executive management. Like most regions, both Germany (58%) and the UK (59%) identified privileged insiders as the number one threat, in line with the global average of 58%. The U.K. also conformed to the global results with its second (executive management; 39%) and third (contractor accounts; 38%) most common responses.

Germany, however, is more concerned about ordinary employees (45% vs. 33% globally) than any other nation except Japan (also 45%). Germany is also much less concerned with executive management than any other region (30% vs. 45% global average) – only Japan was close at 36%.

With respect to external threat actors, cyber-criminals held the number one spot in both Germany and the U.K., with 84% and 81% of respondents, respectively, slightly ahead of the global average (79%). ‘Hacktivists’ were the number two choice in both regions, though the U.K. (72%) showed slightly more concerns than Germany (64%) and the global average (66%).

“Like most regions, both Germany and the U.K. view privileged users as the top insider threat. However, Germans are also more concerned than other regions about ordinary employees – but not executive management.”

The Most Dangerous Insiders

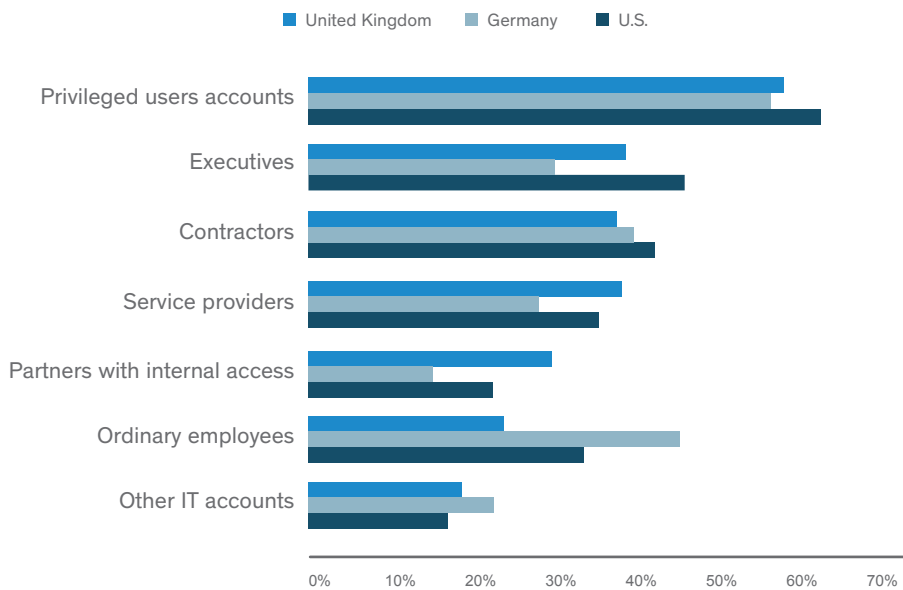


Figure 9: Ratings for the most dangerous insiders (selection as a top three risk)

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

The U.K. and Germany also had widely divergent attitudes with respect to cloud resources. For the most part, U.K. responses reveal a generally more conservative stance towards public cloud resources than the rest of the world, particularly when compared to nations such as Brazil and Mexico that are among the most aggressive with their public cloud plans. For example, U.K. respondents signaled lower plans to store sensitive data than the global average in each of three major public cloud deployment models: SaaS (U.K. 44%; global 53%); IaaS (U.K. 50%; global 53%); and PaaS (U.K. 44%; global 49%). Germany, however, has higher plans for public cloud, and was ahead of the global average for both SaaS (56% vs. 53% globally) and PaaS (56% vs. 49% globally) and only trailed for IaaS environments (46% vs. 53%).

With respect to the top security concerns from using public cloud resources, responses from both Germany and the U.K. generally reflected a lower degree of concerns across the board. When it came to specific security concerns, however, both nations were generally in line with other regions: breaches at the cloud provider, vulnerabilities from shared infrastructure and data sovereignty were the main concerns. Breaches at the cloud provider, the number one global response at 70%, was also identified by 66% of respondents from Germany as the top response, and was the second-ranked response in the U.K. at 65%. Data sovereignty issues, the number three global response at 65%, were the second-ranked (60%) and top-ranked (66%) responses in Germany and the U.K., respectively.

Aside from a slight re-ordering of the top cloud security concerns, the two nations differed in a few areas such as custodianship of encryption keys, compliance and service-level agreements (SLAs). Only 39% of respondents from Germany, for example, selected compliance as a cloud security concern, making it the lowest-ranked concern and well below the global average of 62%. Similarly, only 43% of German respondents viewed the lack of policies or SLAs relating to privacy as a concern, compared to the global average of 65%.

What are the primary ways to ease cloud adoption concerns among German and U.K. respondents? Like most regions, encryption of sensitive data stored in the cloud was the top choice for both Germany and the U.K. 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 (48% globally). Both Germany and the U.K. expressed a strong preference for encryption with local control over encryption keys – with Germany's 62% and the U.K.'s 55% the top two global responses. The U.K. also had the lowest percentage response of any nation for encryption with keys controlled by the service provider (29% vs. 35% globally).

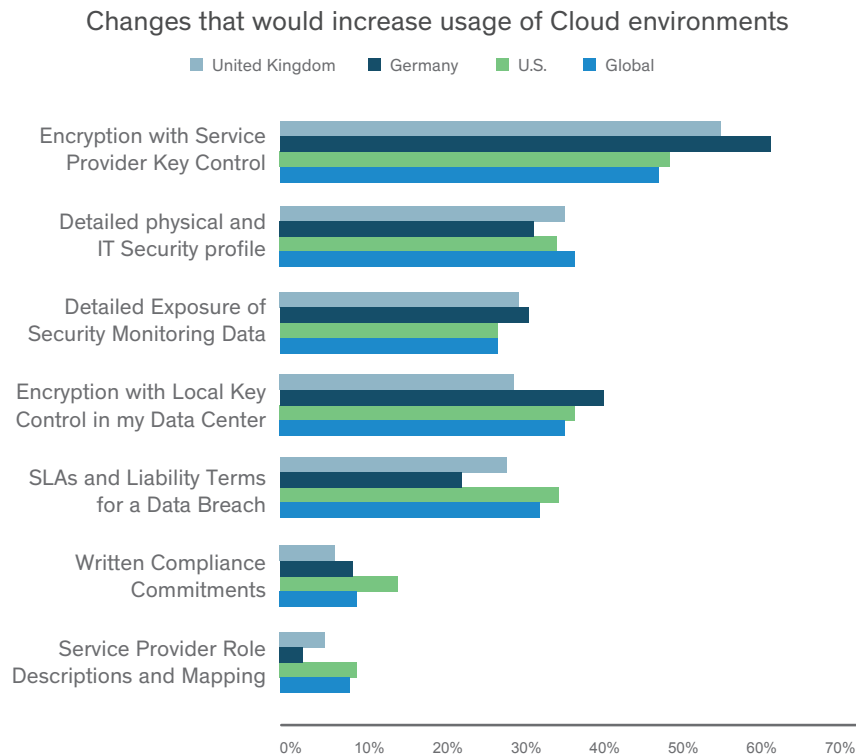


Figure 10: Changes that would increase usage of Cloud environments

Big Data

In terms of plans to store sensitive data in Big Data environments, Germany and the U.K. diverged once again. While German respondents have higher plans to store sensitive data in Big Data environments than the global average (56% vs. 50%), the U.K. falls towards the bottom of the range (45%). With respect to the risks of Big Data, both nations are relatively in line with global responses - 23% of German respondents and 26% in the U.K. view Big Data as one of the most risky locations to store sensitive data, compared to 21% overall. With respect to what risks they were most concerned about, the security of Big Data reports that may include sensitive data were the top Big Data security globally at 42%, though slightly less of an issue for both Germany (34%) and the U.K. (36%). Given the heightened global concerns about data sovereignty, particularly in Europe, privacy issues related to data originating in multiple countries were top answers for both nations (44% Germany; 43% U.K.; 40% global). The top concern in Germany, however, was that sensitive data can reside anywhere within a distributed Big Data environment (51% vs. global average of 41%).

“Germany and the U.K. also diverge when it comes to Big Data. German respondents have higher plans to store sensitive data in Big Data environments than the global average (56% vs. 50%), the U.K. falls towards the bottom of the range (45%).”

IoT

Though the Internet of Things (IoT) promises to present a security hurdle of epic proportions once it achieves mainstream acceptance levels, current IoT security concerns largely reflect IoT’s early stage of adoption. This was true across both our global results and also within both Germany and the U.K. Aside from Japan (17%), the U.K. has among the lowest plans to store sensitive data in IoT environments (25% vs. 33% global average), while Germany is only slightly less conservative (30%). Similarly, when it comes to the most risky locations for storing sensitive data, IoT was well down the list for both nations, ranking seventh in Germany and tenth in the U.K..

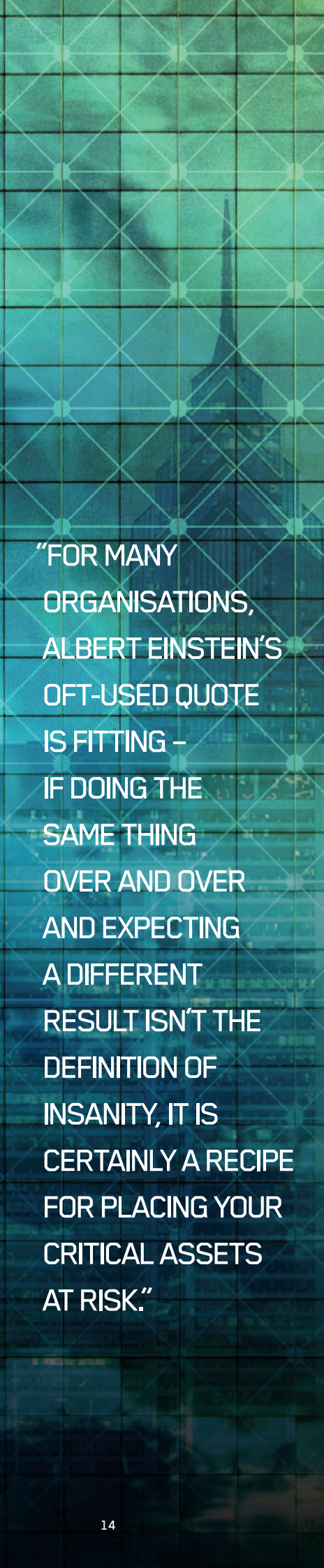
“Aside from Japan, the U.K. has the lowest plans to store sensitive data in IoT environments, while Germany is only slightly less conservative.”

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 certainly held true for the U.K. (42%). IoT devices were less of a concern for Germany, however (27%), where the top response by a slim margin was the lack of industry standards for securing IoT devices (30%). A close second for both nations was privacy violations resulting from IoT devices (29% for both Germany and the U.K., 30% for the global average).

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 organisations, 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, European organisations must recognise that doing more of the same won’t help us achieve an improved security posture. As an industry, and as a region, 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.



“FOR MANY ORGANISATIONS, 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.”

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. Organisations 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. And regions like Germany and the U.K. that are increasingly concerned with data sovereignty issues and bound by new regulatory mandates like GDPR, gateway encryption and tokenisation could also be valuable additions to the security toolkit.

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 data security hurdles of complexity and lack of staff - for the U.K. as well but particularly for Germany - 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. For the U.K. specifically, vendors and enterprises need to consider the potential impact of data security on performance and business processes.

European organisations 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 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.

RECOMMENDATION SUMMARY

DISCOVER AND CLASSIFY	Get a better handle on location of sensitive data, particularly for Cloud, Big Data and IoT
ENCRYPTION AND ACCESS CONTROL	Data centre: Consider an 'encrypt everything' strategy Cloud: encrypt and manage keys locally Big Data: employ discovery as a complement to encryption IoT: consider device authentication and encryption, as well as encryption in transit
DATA SOVEREIGNTY	Consider adopting encryption as well as tokenisation to meet growing data sovereignty compliance demands like GDPR
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

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.

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 organisations 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.



Garrett Bekker
Senior Analyst
451 Research

ABOUT VORMETRIC, A THALES COMPANY

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 centralised key management let organisations 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.CO.UK and find us on Twitter [@VORMETRIC](https://twitter.com/VORMETRIC).

