CPL.thalesgroup.com #2020DataThreat

THALES

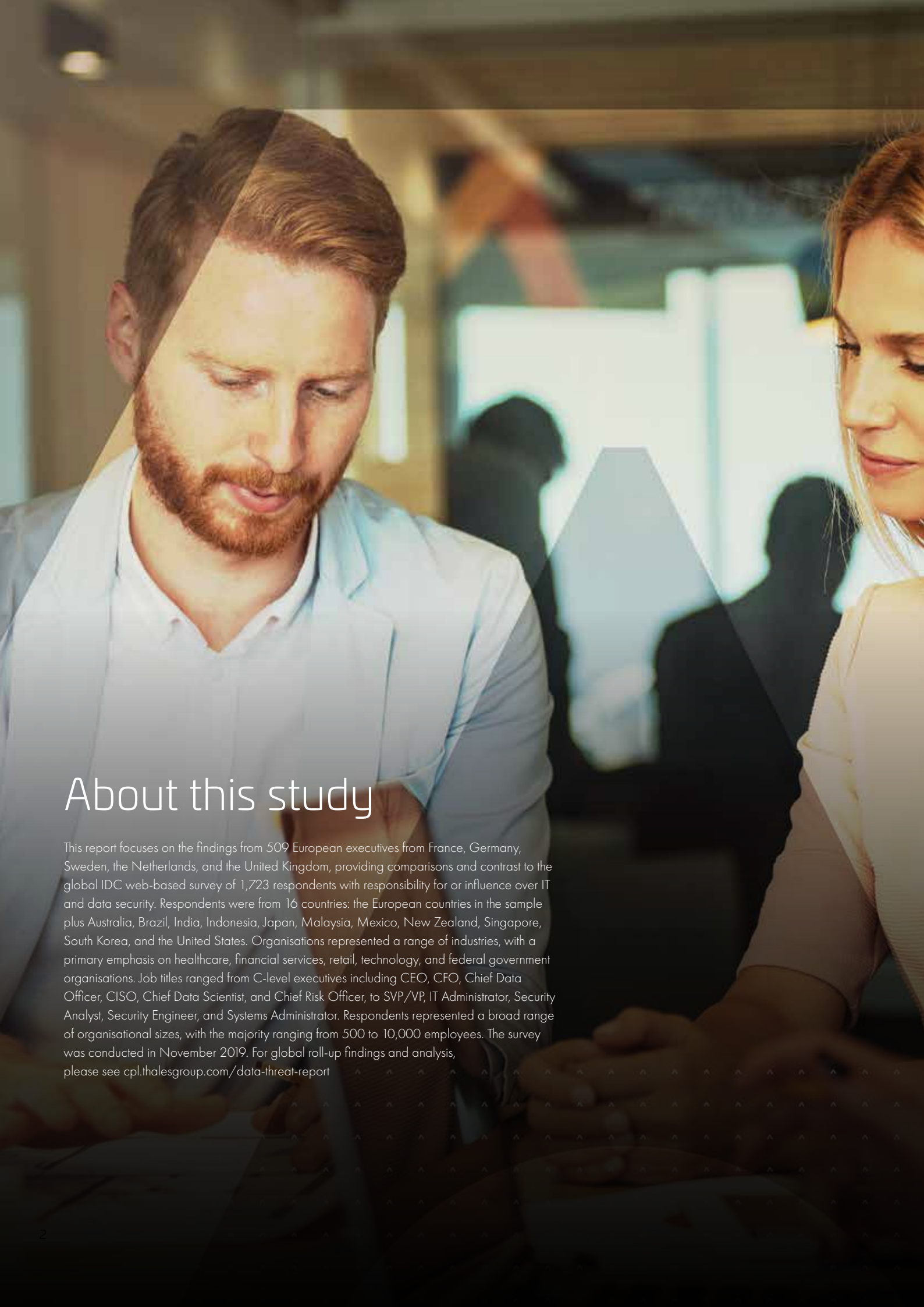
European Data Security Requires a Zero Trust Approach

2020 Thales Data Threat Report

European Edition

RESEARCH AND ANALYSIS FROM:

IDC ANALYZE THE FUTURE



About this study

This report focuses on the findings from 509 European executives from France, Germany, Sweden, the Netherlands, and the United Kingdom, providing comparisons and contrast to the global IDC web-based survey of 1,723 respondents with responsibility for or influence over IT and data security. Respondents were from 16 countries: the European countries in the sample plus Australia, Brazil, India, Indonesia, Japan, Malaysia, Mexico, New Zealand, Singapore, South Korea, and the United States. Organisations represented a range of industries, with a primary emphasis on healthcare, financial services, retail, technology, and federal government organisations. Job titles ranged from C-level executives including CEO, CFO, Chief Data Officer, CISO, Chief Data Scientist, and Chief Risk Officer, to SVP/VP, IT Administrator, Security Analyst, Security Engineer, and Systems Administrator. Respondents represented a broad range of organisational sizes, with the majority ranging from 500 to 10,000 employees. The survey was conducted in November 2019. For global roll-up findings and analysis, please see cpl.thalesgroup.com/data-threat-report

Contents

Our sponsors are:

Executive Summary

European companies and organisations continue to increase their use of a wide variety of digital transformation technologies to improve customer experience, find new sources of revenue, and reduce costs. IDC research shows that this digital transformation (DX) is well underway. Thirty-seven percent of European organisations in our study say they are either aggressively disrupting the markets they participate in or embedding digital capabilities that enable greater enterprise agility.

While DX can provide tremendous value, it also makes data security more complex. Companies are increasingly dependent on, and increasing, the amount of data stored in the cloud. As a result, security teams need to focus on aspects beyond traditional network perimeters. We have reached a point at which nearly half of all data is stored in the cloud (46% of all data), and 43% of that data is sensitive. Additionally, most European organisations are multicloud. All of this adds up to today's data environments becoming increasingly complex, and this complexity is a top barrier to data security.

However, European companies are cognitively dissonant to data security. Nearly two-thirds believe they are not at all vulnerable, resulting in a continued freeze of their security budgets. Without additional funding, European companies will be challenged to implement processes and invest in technologies required to appropriately protect their data. Simultaneously, more than half have been breached or experienced failed security audits in the past year. And when it comes to securing data in the cloud, most European companies rely heavily on their cloud providers' SLAs for responsibility shared, instead of executing on the elements outside of the shared responsibility model by adding adequate controls.

When it comes to investment, data security still represents a small share of overall security budget. Thirty eight percent of European organisations plan to increase data security spending in the next 12 months, a slightly lower amount than last year but significantly lower than the 49% of global respondents who expect spending to increase. In fact, prioritising reputation and brand protection, organisations in Europe focus their effort on reducing complexity, rationalisation, and operationalisation of security controls in line with business priorities.

Compliance-driven spending in the past two to three years inflated security budgets as standards such as GDPR motivated organisations to increase overall expenditures on security. European organisations though still focus a disproportionate amount of spend on network security. One-third of European respondents' focus is on data security, yet data security averages just 14% of overall IT security budget.

46%

of all data is stored in the cloud, and **43% of that data is sensitive.**

In the wake of the COVID-19 global pandemic, organisations must remain vigilant and be prepared for the post-COVID-19 data risk reality. This point is especially relevant today more than ever as the work from home migration has increasingly forced corporate data to be accessed remotely, sometimes on BYO devices. Even if an organisations lose visibility as to where data resides, data security technologies such as encryption and access management will become more crucial to protecting corporate data in a location agnostic manner.

Lower budget allocation for data security in Europe compared to the rest of the world is counterintuitive, considering that trust and security are at the core of the EU's Digital Single Market Strategy. Main regulations include, but are not limited to:

- **GDPR** – rules for the collection and processing of personal information of EU residents
- **ePrivacy Directive** – the regulation to govern privacy in electronic communications, cookies and direct marketing communications
- **eIDAS** – the legal framework for the cross-border recognition of electronic ID and consistent rules on trust services
- **EU Cybersecurity Act** – the framework for business to achieve cybersecurity certification for information and communications technology.

Industry-specific compliance complexity grows with baseline standards set in NIS Regulations (telecommunications), PSD2 (finance), and the like, which sometimes overlap national regulations.

In terms of emerging threats, quantum computing is looming and promises to further complicate data security. Cryptography requirements will fundamentally change when quantum computing comes online, and 69% of European respondents see quantum cryptography affecting their organisation in the next five years.

As organisations face expanding and more complex data security challenges, they need smarter, better ways to approach data security. European companies need to take a multilayered approach to data security by embracing cloud shared security responsibilities and adopting access management technologies that authenticate and validate users and devices accessing applications and networks, while also employing more robust data discovery, hardening, data loss prevention and encryption solutions. Importantly, data security should not undermine business efforts to pursue digital transformation by applying flexible frameworks leading to discretionary trust model implementation.

69%

of European respondents see **quantum cryptography affecting their organisation** in the next five years.

01
Key Findings

Digital Transformation Is Complicating Data Security

Companies and organisations are fundamentally reimagining their business and taking advantage of digital technologies like cloud, mobile, and IoT to transform their operations. Even "traditional companies" will drive more revenue from digital products, services, and experiences. Thirty-seven percent of European organisations in our study say they are either aggressively disrupting the markets they participate in or embedding digital capabilities that enable greater enterprise agility, compared to 43% of global respondents (see Figures 1a and 1b). The U.K. leads all European countries surveyed by far with 51% identifying as either aggressively disrupting their markets or embedding digital capabilities, followed by Germany at 42%.

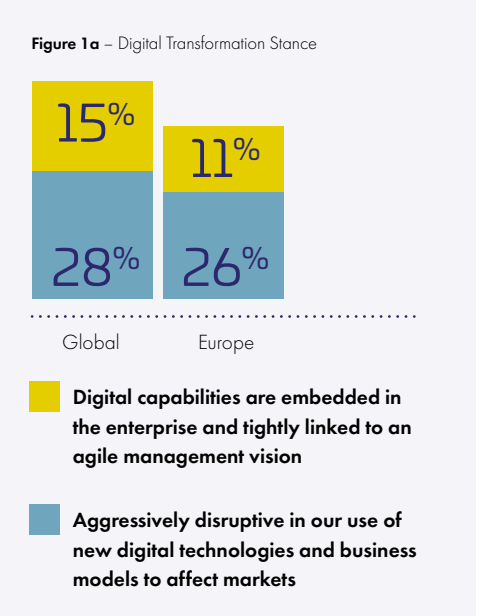


Figure 1a – Digital Transformation Stance

Source: 2020 Thales Data Threat Report Survey, IDC, November 2019

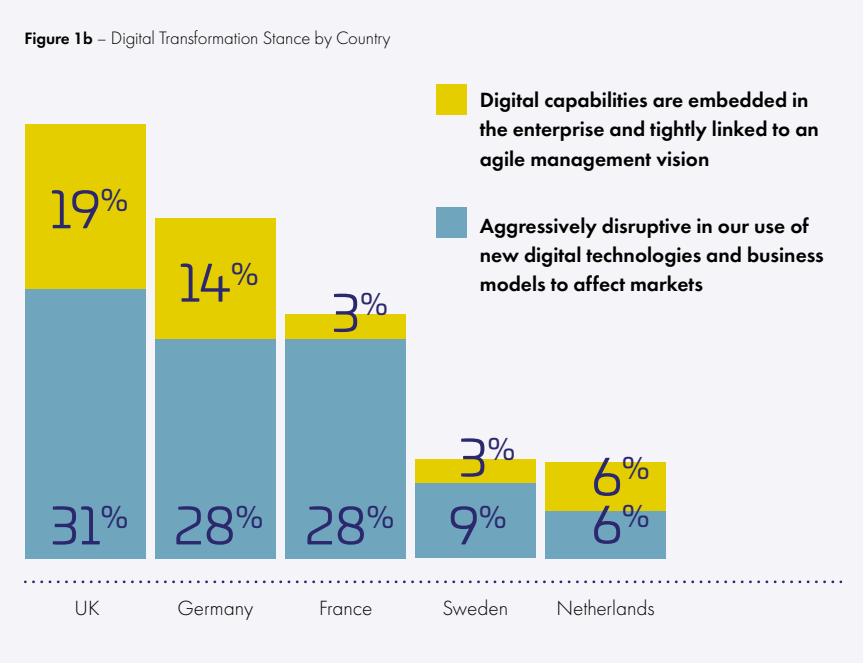


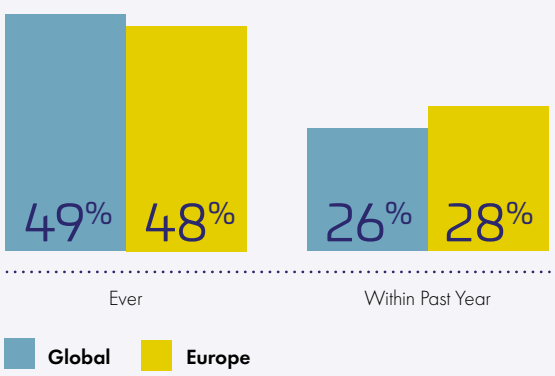
Figure 1b – Digital Transformation Stance by Country

Source: 2020 Thales Data Threat Report Survey, IDC, November 2019

> "Thirty-seven percent of European organisations say they are either aggressively disrupting the markets they participate in or embedding digital capabilities that enable greater enterprise agility."

But no organisation is immune from data security threats, with 48% of European respondents experiencing a breach ever and 28% having been breached in the past year (see Figures 2a and 2b). Another 24% of European organisations report that they have failed a compliance audit in the past year.

Figure 2a – Breach Incident Rates



> "Forty-eight percent of European respondents have experienced a breach and 28% have been breached in the past year."

Figure 2a – Breach Incident Rates

Source: 2020 Thales Data Threat Report Survey, IDC, November 2019

Figure 2b – Breach Incident Rates by Country

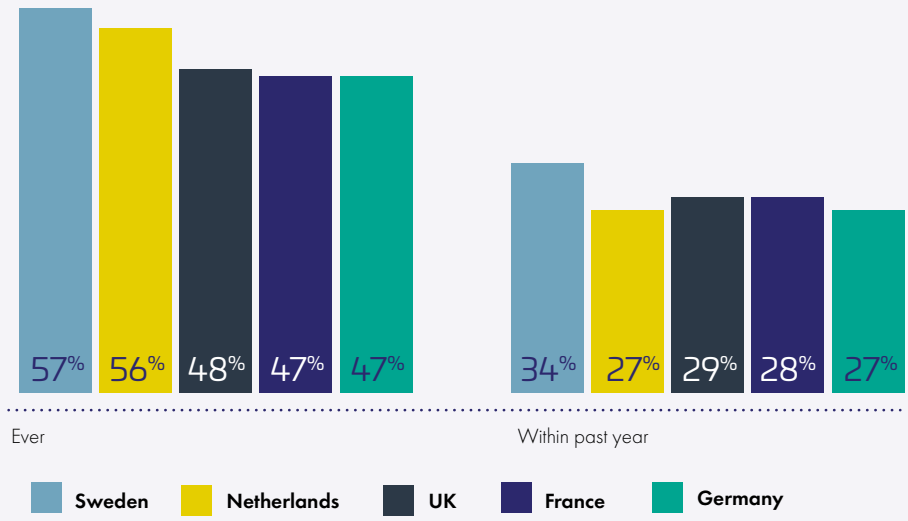


Figure 2b – Breach Incident Rates by Country

Source: 2020 Thales Data Threat Report Survey, IDC, November 2019

While organisations that digitally transform are realising new sources of competitive advantage, these companies face new data security challenges presented by DX. DX positively correlates to vulnerability: the more digitally transformed an organisation is, the more likely that it has experienced a data breach. Digitally determined organisations (those organisations making the strategic, organisational, technological, and financial decisions that will set them up to digitally transform in the next several years) may also have greater data threat exposure. Their greater level of sophistication may also mean they are more likely to be aware that they have been breached. Less sophisticated companies may have less exposure, or they just may have been breached without knowing it.

> "Twenty-four percent of European organisations report that they have failed a compliance audit in the past year."

Clouds Are the Leading Data Environment, Creating Significant Risk

All European organisations surveyed have some sensitive data in the cloud. Data stored in the cloud is nearing an inflection point with our study respondents who say that an estimated 46% of data is in the cloud, slightly lower than the global sample at 50%. More importantly, European respondents say that an estimated 43% of that data in the cloud is sensitive (see Figure 3).

> "100% of European respondents say at least some of their sensitive data in the cloud is not encrypted."

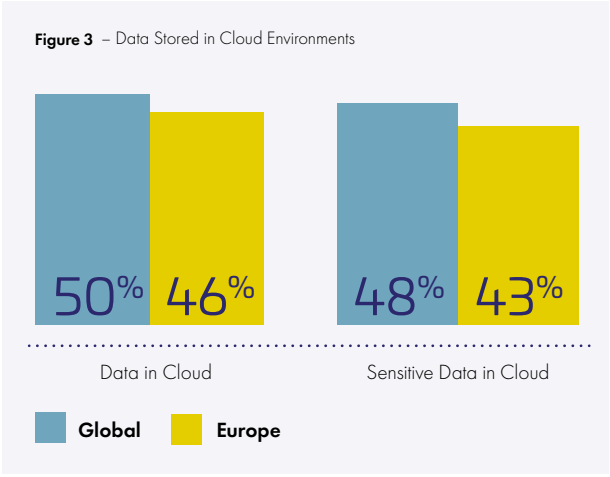


Figure 3 – Data Stored in Cloud Environments

Source: 2020 Thales Data Threat Report Survey, IDC, November 2019

As more sensitive data is stored in cloud environments, data security risks increase. Yet, despite this significant sensitive data exposure, rates of data encryption and tokenisation are low. In fact, 100% of European respondents say at least some of their sensitive data in the cloud is not encrypted. Only 54% of sensitive data stored in cloud environments is protected by encryption and less than half – 44% – is protected by tokenisation (see Figure 4).

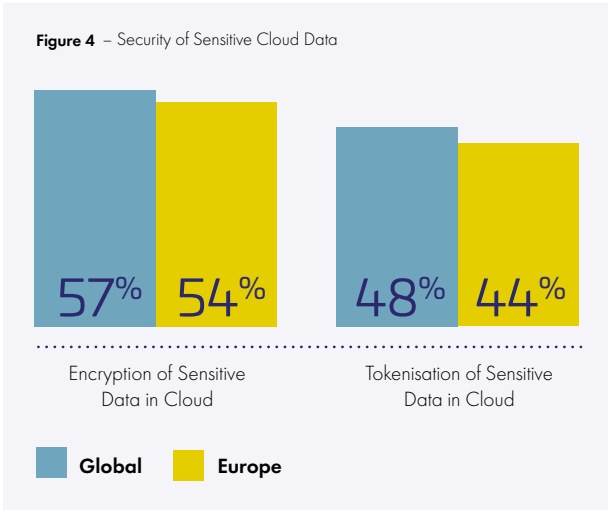


Figure 4 – Security of Sensitive Cloud Data

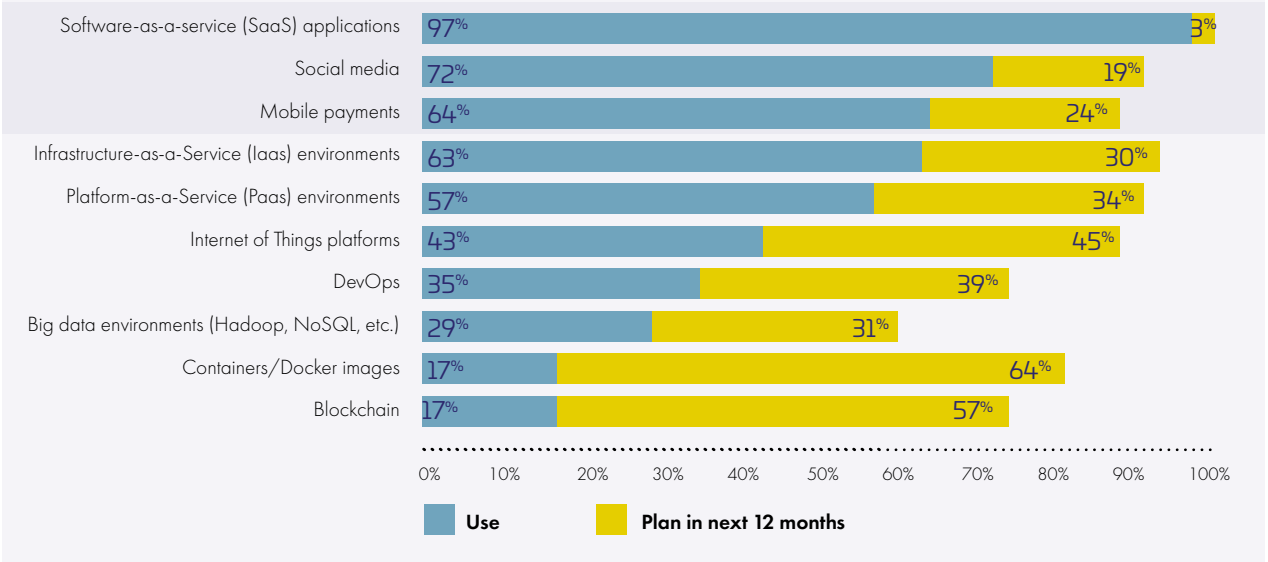
Source: 2020 Thales Data Threat Report Survey, IDC, November 2019

Organisations Are Housing Sensitive Data Across a Broad Range of Technologies

European organisations are adopting a wide range of 3rd Platform technologies, which include cloud, mobile, social, big data, and Internet of Things. SaaS applications have the widest adoption by European enterprises at 97%, up from 65% in 2018 (see Figure 5). Social media, mobile payments, and IaaS and PaaS cloud environments also lead planned adoption. Note that many of these technologies, such as IoT and mobile, are edge technologies, which reinforces the message that data exposure is expanding well beyond the traditional network perimeter.

Figure 5 – Technology Adoption Levels – European Organisations

Figure 5 – Technology Adoption Levels – European Organisations



Source: 2020 Thales Data Threat Report Survey, IDC, November 2019

Likewise, many European organisations are housing sensitive or regulated data in a similarly broad set of technologies. Seventy-nine percent store sensitive data in SaaS applications, 34% store data in IaaS, and 28% store data in PaaS environments. Ninety-nine percent of European organisations in the survey are storing data in at least one of these environments (see Figure 6).

Figure 6 – Technology Environments Used to Store Sensitive/Regulated Data

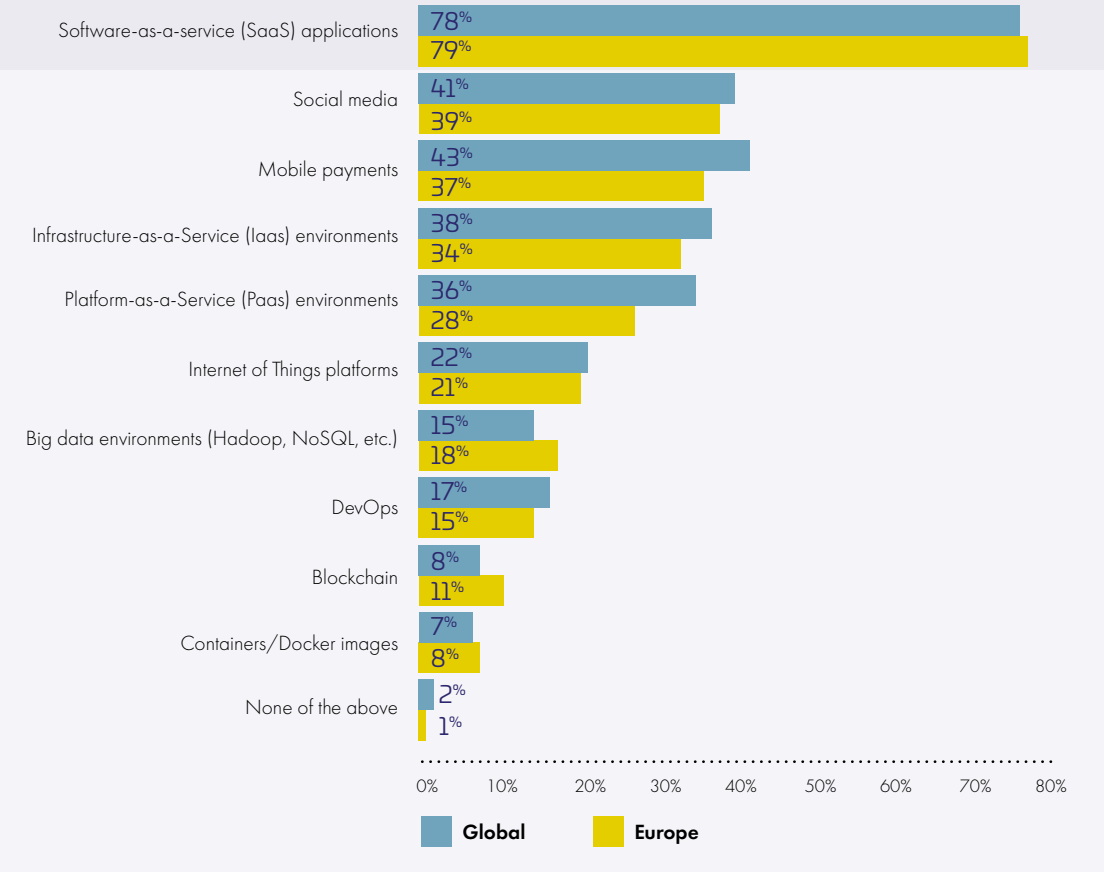


Figure 6 – Technology Environments Used to Store Sensitive/Regulated Data
Source: 2020 Thales Data Threat Report Survey, IDC, November 2019

As companies expand their usage of cloud, mobile, social, big data and IoT technologies from outsourced vendors, sensitive data potentially becomes increasingly vulnerable as a result. Thus, securing the perimeter does little to protect off-premise data, which speaks to the need to take a least privileged access and data protection approach to security. This secure least privileged approach eliminates the binary trust/don't trust approach of yesterday's on-premise, perimeter-centric reality and instead requires an identity-centric continuous validation and verification approach, providing both network and application access protections. Likewise, technologies like encryption and tokenisation assure that if least privileged measures fail and the data is hacked or leaked, or physical devices are stolen, data is also appropriately protected.

> "Seventy-nine percent of European organisations store sensitive data in SaaS applications, 34% store data in IaaS, and 28% store data in PaaS environments."

Complexity of Data Environments Is a Top Barrier to Data Security as Multicloud Becomes the Norm

As more data migrates to the cloud, security becomes more complex. But much of this complexity is self-inflicted, as multicloud has become increasingly common. European companies are using multiple IaaS and PaaS environments, as well as hundreds of SaaS applications. Eighty percent of European organisations are using more than one IaaS vendor, 81% have more than one PaaS vendor, and 29% have more than 50 SaaS applications to manage (see Figure 7).

> "Nearly 1/3 of European organsiations have more than 50 SaaS vendors."

Figure 7 – Number of IaaS/PaaS Vendors in European Organisations

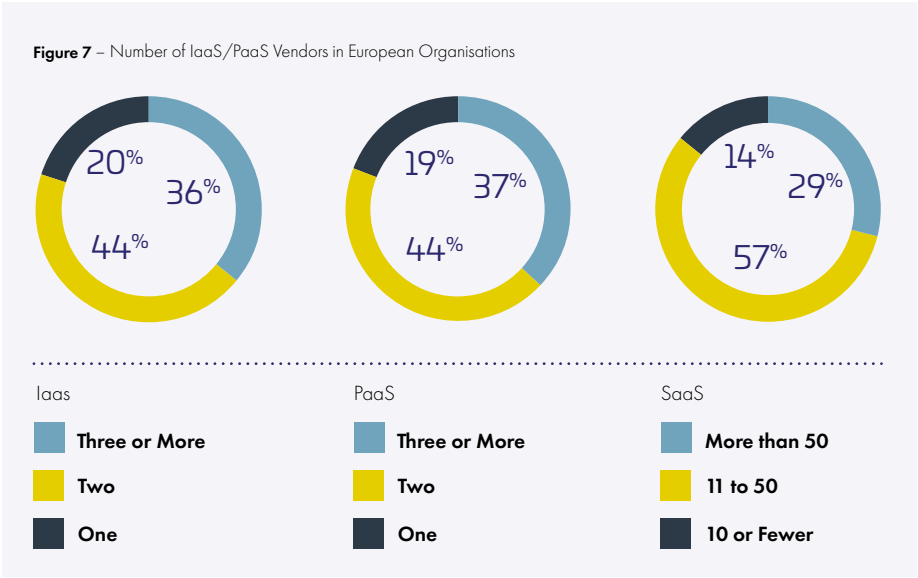


Figure 7 – Number of IaaS/PaaS Vendors in European Organisations

Source: 2020 Thales Data Threat Report Survey, IDC, November 2019

The resulting complexity, including orchestrating key management solutions from each cloud provider across a multicloud environment, is making life more difficult for security professionals. By far, European respondents rate complexity as their top perceived barrier to implementing data security at 40%. Budget concerns and pressure to avoid impact to business performance and process are seen as other barriers (see Figure 8).

Figure 8 – Barriers to Implementing Data Security

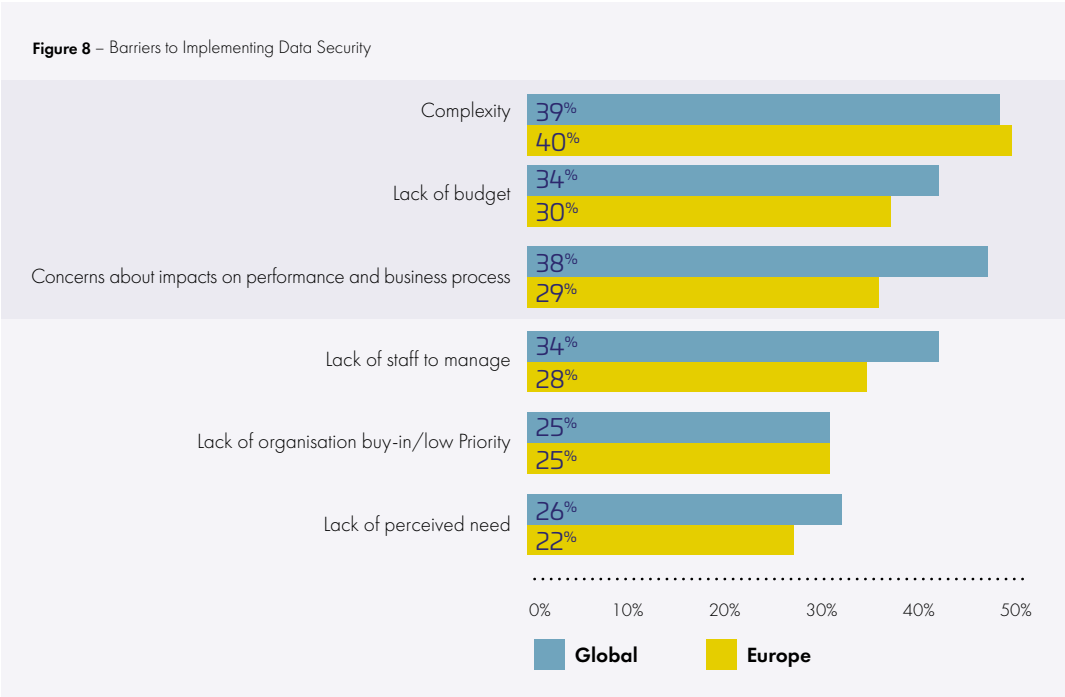


Figure 8 – Barriers to Implementing Data Security

Source: 2020 Thales Data Threat Report Survey, IDC, November 2019

Interestingly, the propensity to deploy encryption solutions for cloud implementations is three times the propensity to spend on additional on-premise implementations. This connects to both the growing adoption of IaaS, PaaS, and SaaS, as well as to the fact that almost 70% of European organisations already have on-premise encryption deployed to some extent within their environments.

Quantum Computing Data Security Concerns Are on the Horizon

Data security will only get harder with the advent of quantum computing. The impact of quantum computing is on the horizon as 69% of European organisations see it affecting their cryptographic operations in the next five years (see Figure 9). Cryptography requirements highlight a critical security issue brought on by the power of quantum computing. Ninety-three percent of respondents are concerned quantum computing will create exposures for sensitive data, with 30% very/extremely concerned.

> "Ninety-three percent of respondents are concerned quantum computing will create exposures for sensitive data."

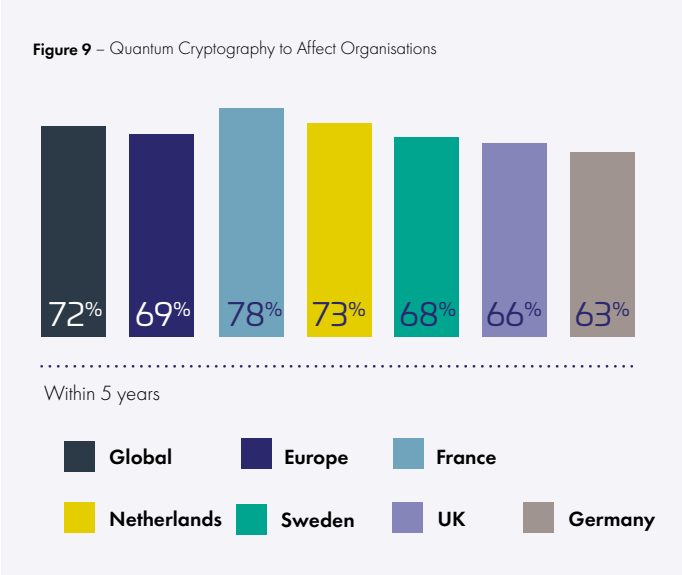


Figure 9 – Quantum Cryptography to Affect Organisations

Source: 2020 Thales Data Threat Report Survey, IDC, November 2019

Top plans to offset quantum computing threats are switching away from symmetric cryptography (cited by 31% of European respondents) and key management that supports quantum safe random number generator (cited by 30%). But many European organisations are uncertain how to respond and are open to try anything even though threats may surface within the next five years.

Organisations' Sense of Data Security at Odds with Reality

Despite the pervasive and expanding threats to data security, enterprises feel less vulnerable in 2019 than they did in 2018. Sixty-eight percent of organisations felt vulnerable in 2019, down from 86% in 2018, even as security risks grow (see Figure 10). This sense of better protection may be due to the substantial leap of security investment in preceding years and the level of security program maturity reached under continuous regulatory pressure. At the same time, the dial has shifted from traditional security indicators and routines towards business-driven objectives and compliance, which may result in a false perspective. France perceived itself to be least vulnerable of the European countries surveyed with 44% saying they are "not at all vulnerable.

> "Sixty-eight percent of organisations felt vulnerable in 2019, down from 86% in 2018, even as security risks grow."

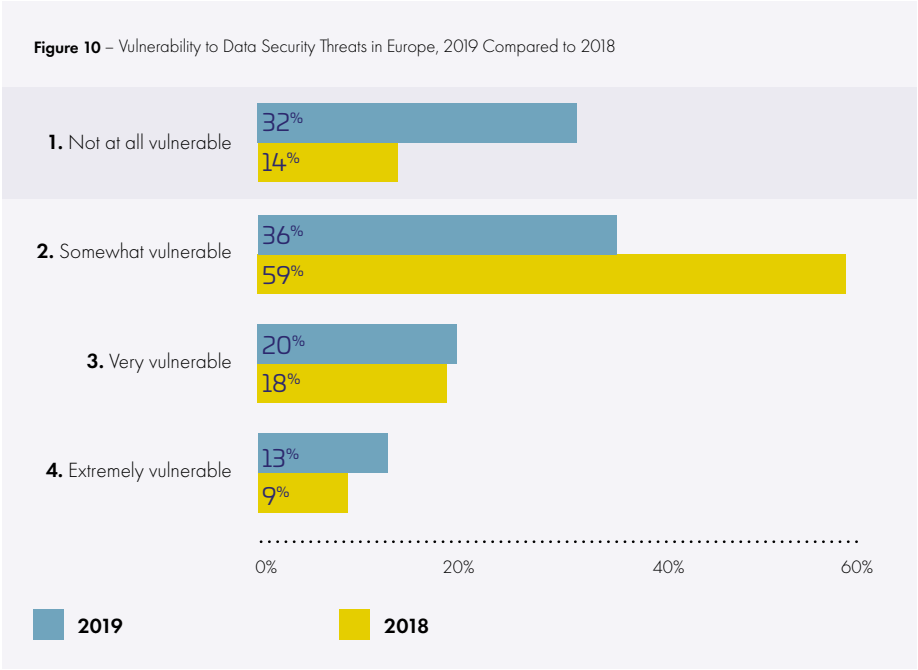


Figure 10 – Vulnerability to Data Security Threats in Europe, 2019 Compared to 2018

Source: 2020 Thales Data Threat Report Survey, IDC, November 2019

These low levels of perceived vulnerability point to a disconnect between perception versus reality. This confidence is not supported by data security practices or investments. European organisations haven't significantly changed their security estates by using tools that would actually make them less vulnerable. As previously mentioned, encryption and tokenisation rates of sensitive data in the cloud are low. Furthermore, only 52% of European respondents implement database encryption (lower than the global sample at 59%) and 51% implement file encryption (lower than the global sample at 61%) (see Figure 11).

Figure 11 – Implementation of Encryption and Data Security Tools in European Organisations

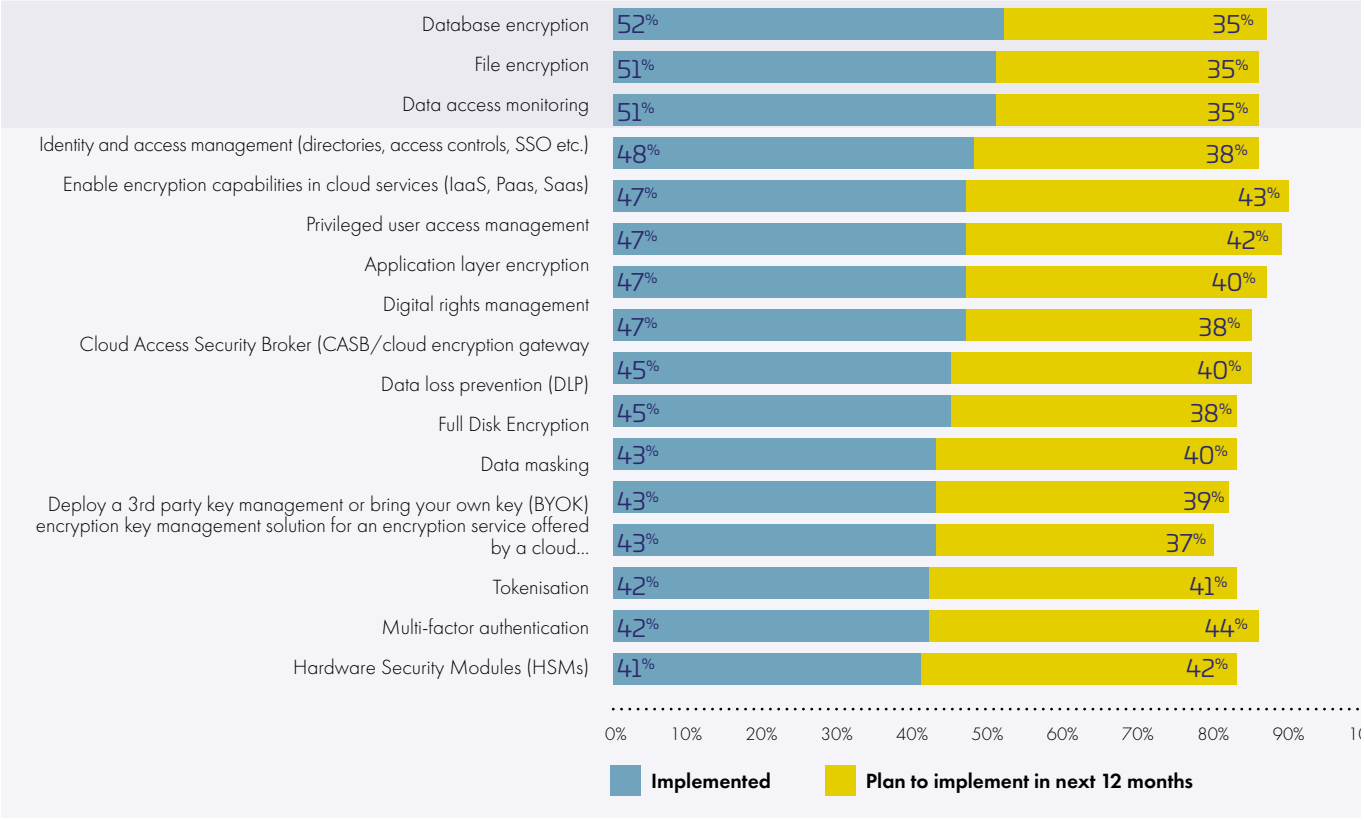


Figure 11 – Implementation of Encryption and Data Security Tools in European Organisations

Source: 2020 Thales Data Threat Report Survey, IDC, November 2019

> "Only 52% of European respondents implement database encryption and 51% implement file encryption."

Security Spend is Higher but With Less Focus on Data Security vs. Network Security

European organisations plan to spend more money on data security in the upcoming year, though at growth rates slightly lower than last year. Thirty-eight percent of respondents said they would be spending somewhat or much more on data security in 12 months' time. But data security budget growth is declining slightly, and one in five European organisations plan to decrease data security spending in 2020 (see Figure 12).

> "Thirty-eight percent of respondents said they would be spending somewhat or much more on data security in 12 months' time."

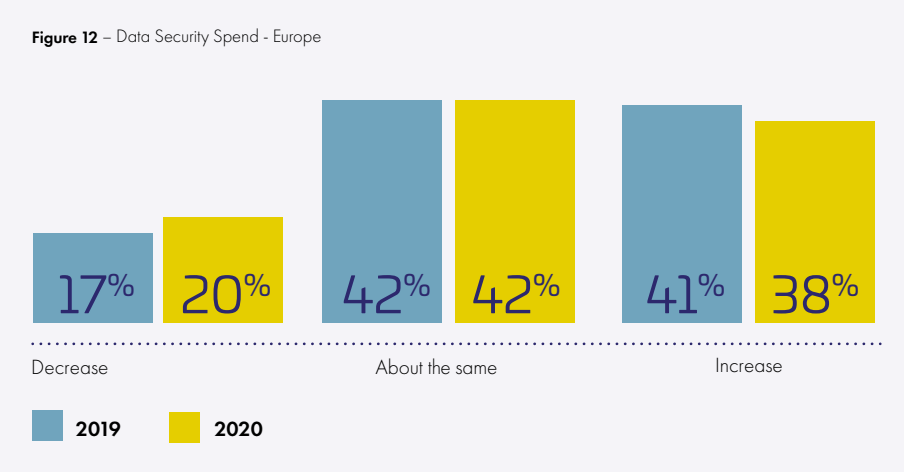


Figure 12 – Data Security Spend - Europe

Source: 2020 Thales Data Threat Report Survey, IDC, November 2019

Additionally, at 38%, European respondents saw lower growth in 2020 data security budgets than the global total (49%) (see Figure 13). Only the U.K. was near the global average with 49% of respondents planning to grow data security spend. And organisations in France and Sweden see budgets declining the most with 29% expecting budget decreases in both countries.

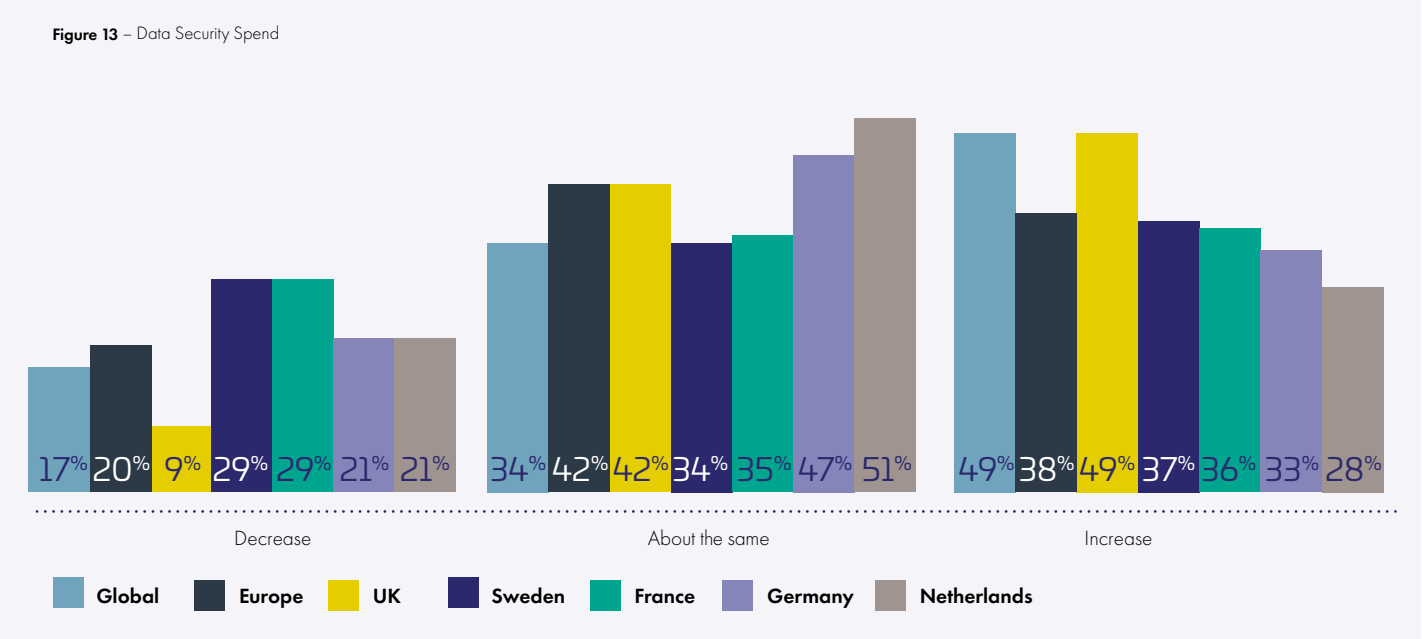
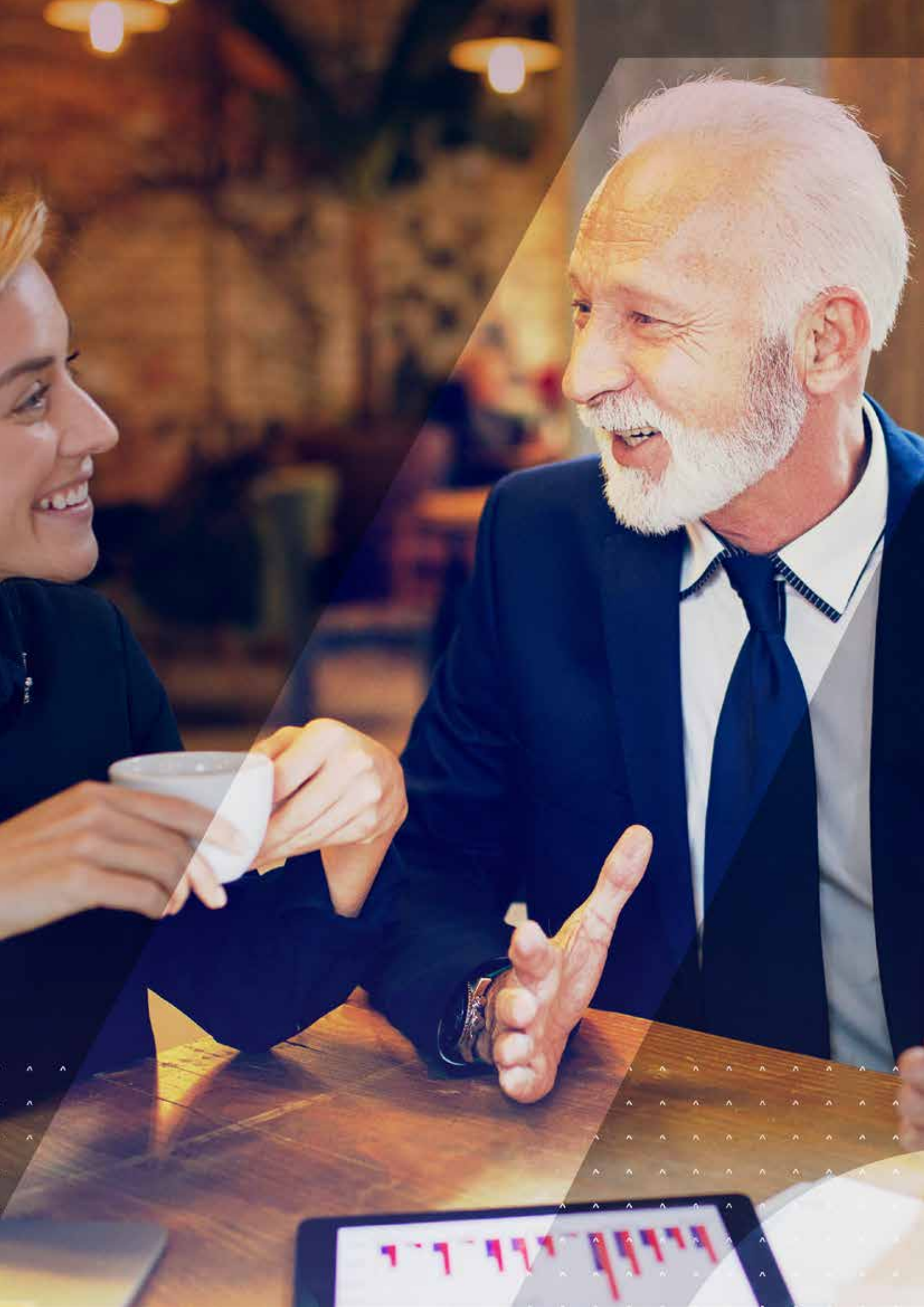
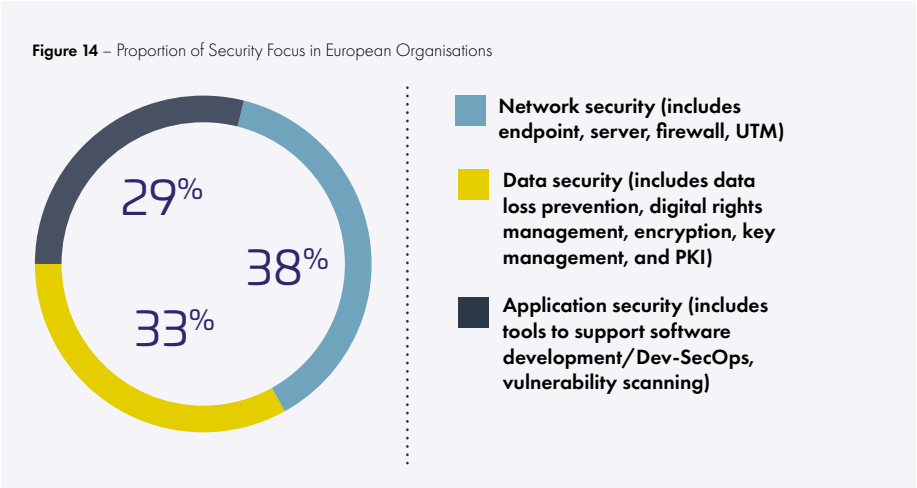


Figure 13 – Data Security Spend

Source: 2020 Thales Data Threat Report Survey, IDC, November 2019



European organisations are still predominately focused on network security (38%), followed by data security (33%), and application security (29%) (see Figure 14). And while 33% of security focus is on data security, data security spending falls below that rate of attention and only 14% of security budgets is spent on data security.



> "Sixty percent of European companies are worried about cybercriminals who steal data for profit."

Figure 14 – Proportion of Security Focus in European Organisations

Source: 2020 Thales Data Threat Report Survey, IDC, November 2019

Further demonstrating a disconnect between security budgets and the focus of security departments, respondents believe that malicious actors like cybercriminals and terrorists present the greatest risk to their data. Sixty percent of European companies are worried about cybercriminals who steal data for profit, followed by 50% concerned about industrial espionage from competitors and 49% worried about cyberterrorists who damage companies by making them look bad publicly.

Interestingly, European respondents are less concerned about day-to-day issues, which may actually be a greater threat. These are issues they have more control over, including non-privileged user access, partners with internal access, and privileged user access (see Figures 15 and 16). Companies must be careful of overprovisioning quantity and breadth of accounts as the risk from internal data threats is often more about carelessness than malicious behaviour.

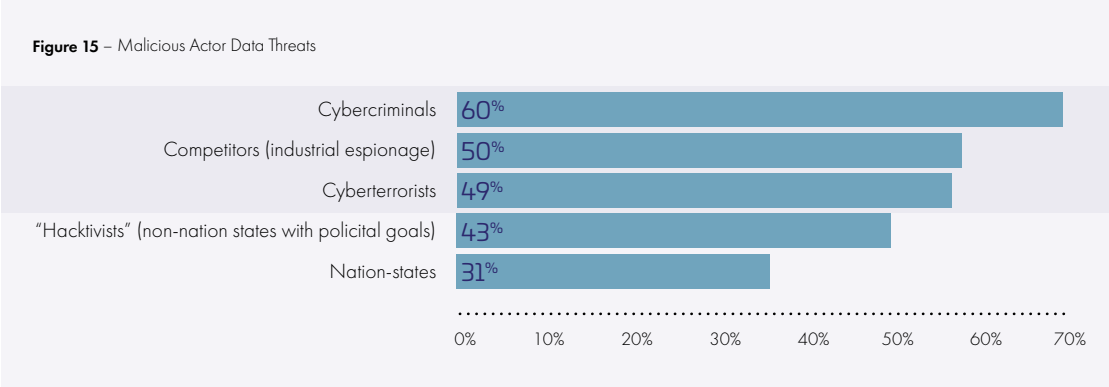


Figure 15 – Malicious Actor Data Threats

Source: 2020 Thales Data Threat Report Survey, IDC, November 2019

Figure 16 – Internal Data Threats

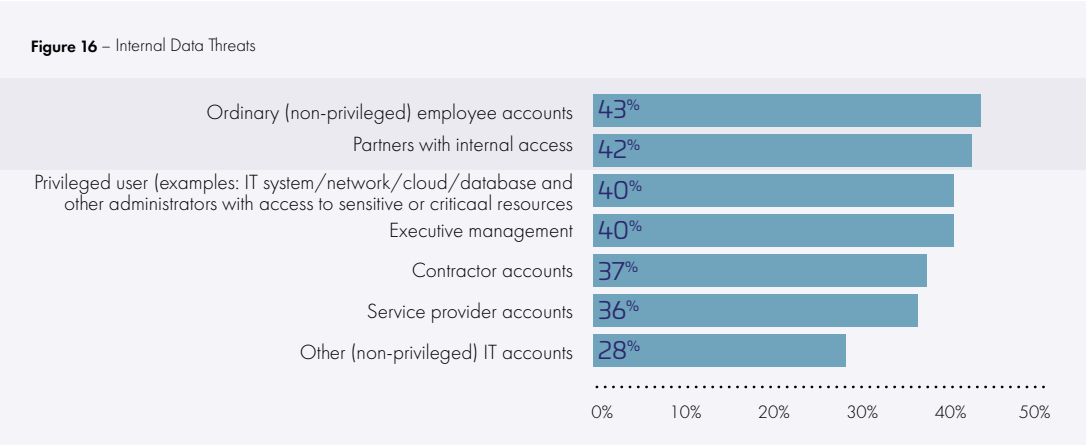


Figure 16 – Internal Data Threats

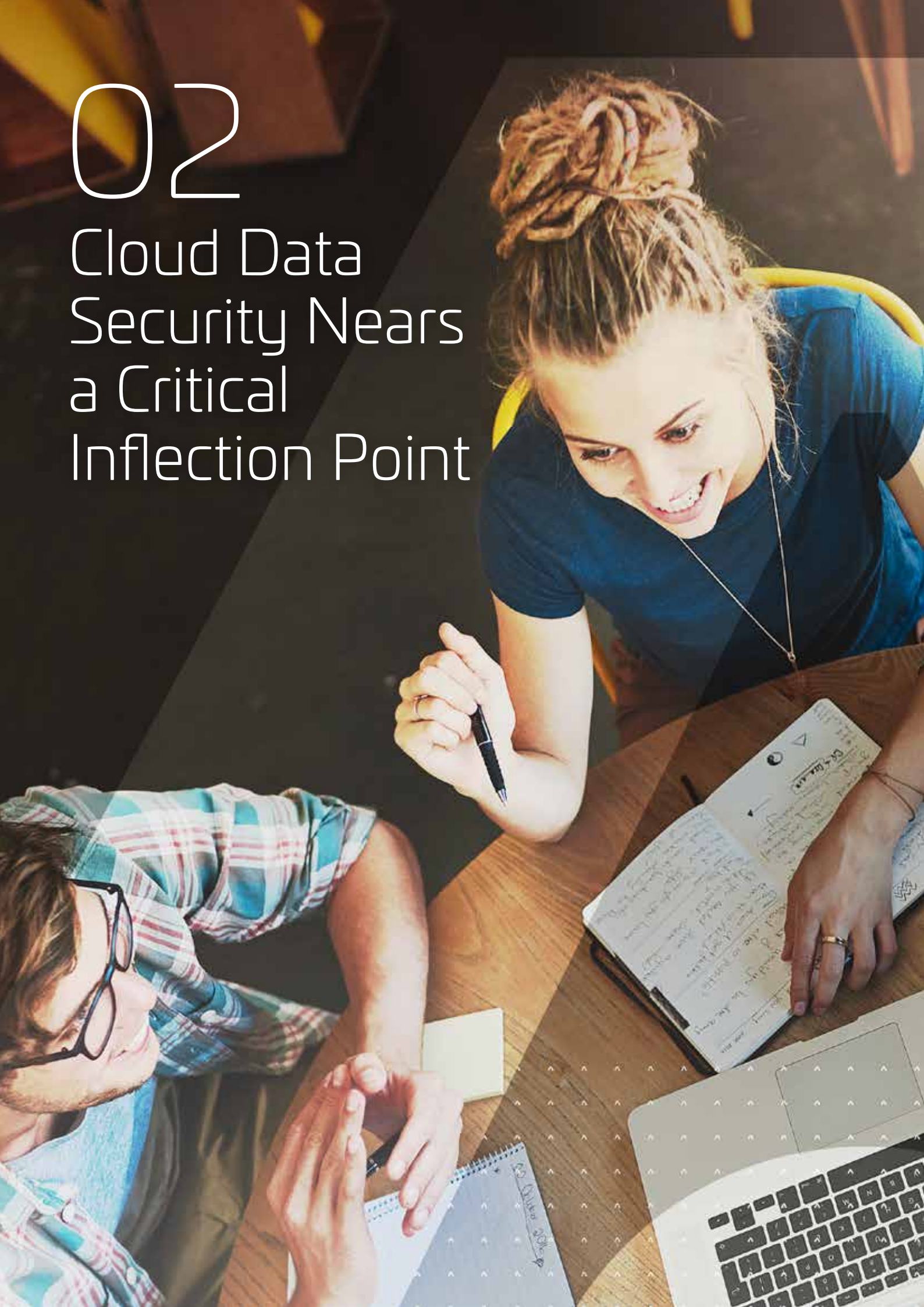
Source: 2020 Thales Data Threat Report Survey, IDC, November 2019

Nearly half of European company and organisational data is now stored in the cloud, with a significant portion of that data being sensitive. As a result, IT security departments must now, more than ever, embrace and own their portion of the cloud shared responsibility model and implement data security best practices, as the cloud provider most often does not guarantee security at the data level.

"Nearly half of European company and organisational data is now stored in the cloud, with a significant portion of that data being sensitive."

02

Cloud Data Security Nears a Critical Inflection Point



Companies are concerned about many data security issues regarding the cloud. Yet, European organisations are more concerned about issues owned by their cloud providers, like shared infrastructure, data privacy policies, and regulatory compliance (see Figure 17). Although valid concerns, the real possibility of these concerns resulting into security issues are quite low. These same organisations are less concerned about issues over which they have direct control, and which represent greater potential vulnerabilities, like encryption key management.

Figure 17 – Cloud Security Concerns

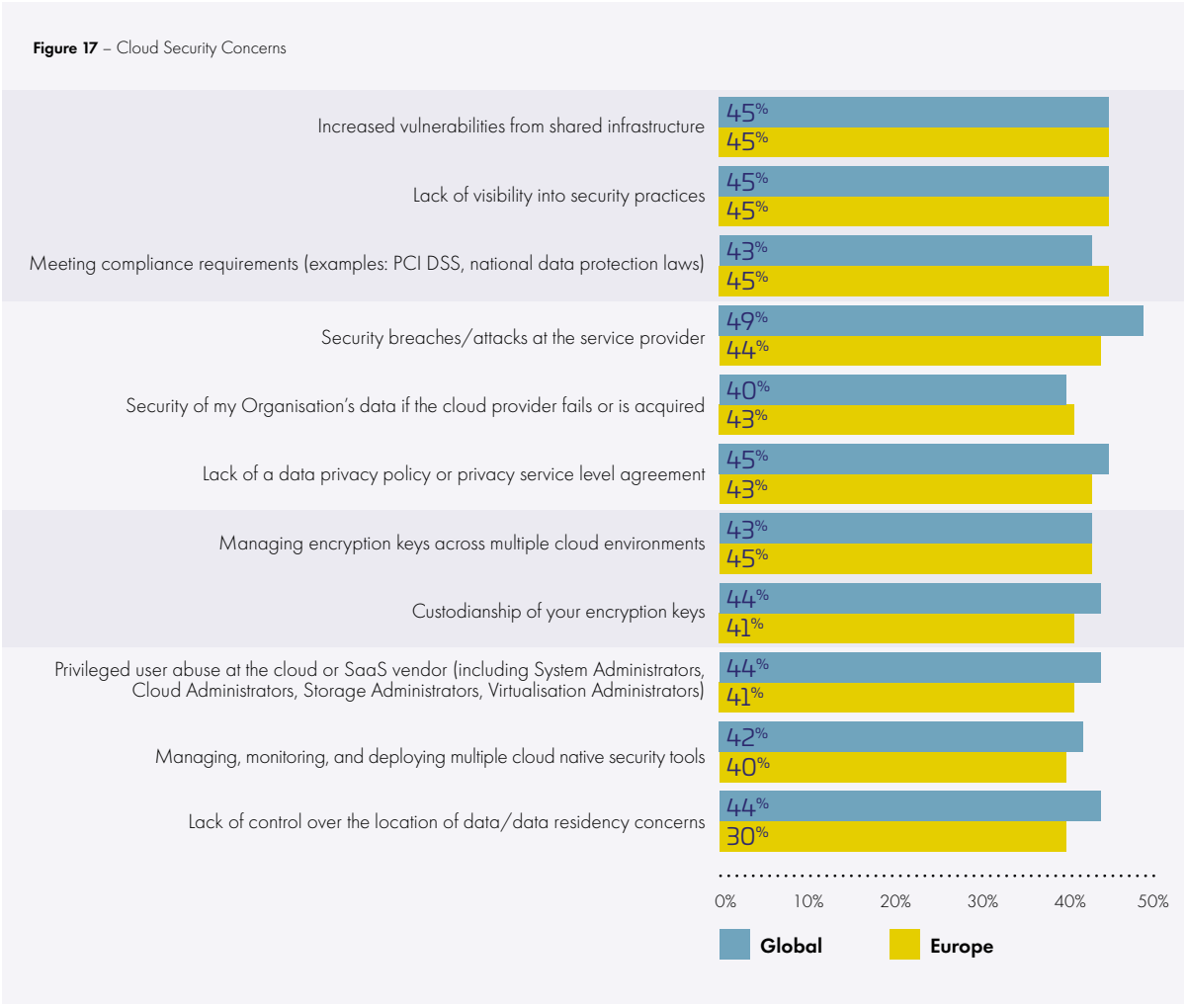


Figure 17 – Cloud Security Concerns

Source: 2020 Thales Data Threat Report Survey, IDC, November 2019

This mismatch between threats respondents perceive and those for which they should actually be concerned implies that respondents have not fully considered data security in a cloud-first world. Each type of cloud environment requires a shift in security responsibility for identities, data, applications, operating systems, server virtualisation, network, infrastructure, and hardware. European organisations should place their cloud security focus and concern on the portion of the shared responsibility model where the organisation can influence the security of its data (see Figure 18).

Figure 18 – Shared Responsibility Model

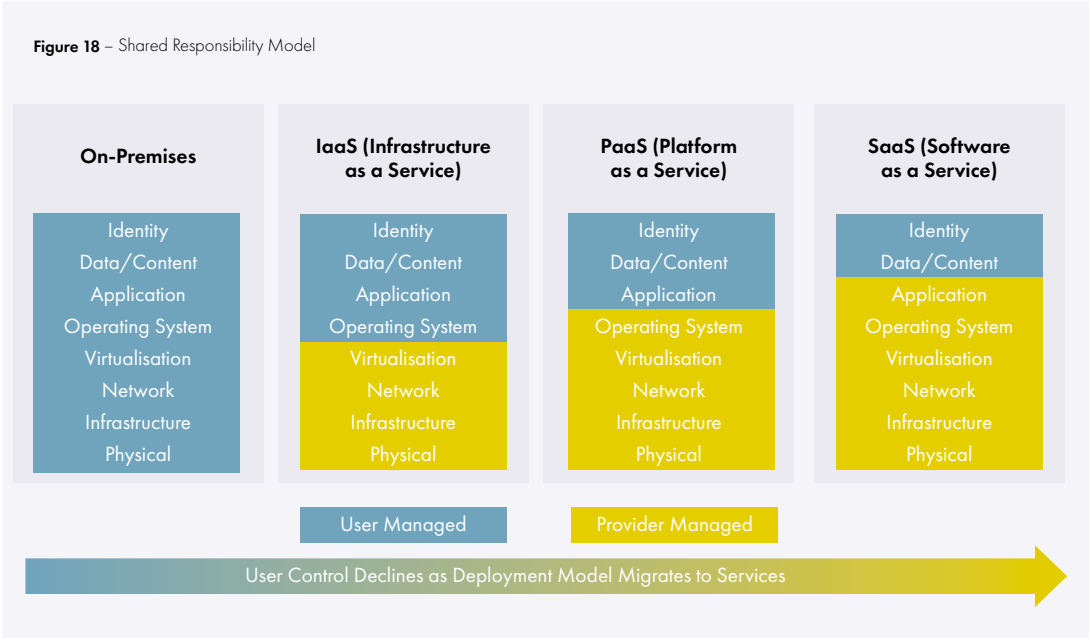


Figure 18 – Shared Infrastructure Model

Source: IDC, November 2019

> “Ninety-three percent of European respondents have at least some level of concern over data security of SaaS applications.”

Cloud security concerns also grow as organisations deploy more data into SaaS, IaaS, and PaaS environments.

According to our study, 93% of European respondents have at least some level of concern over data security of SaaS applications. SaaS security concerns span a broad range of risks, with written compliance commitments, proper data control configurations, local key management, and encryption of data within the service provider's organisation leading the list (see Figure 19).

Figure 19 – SaaS Security Concerns

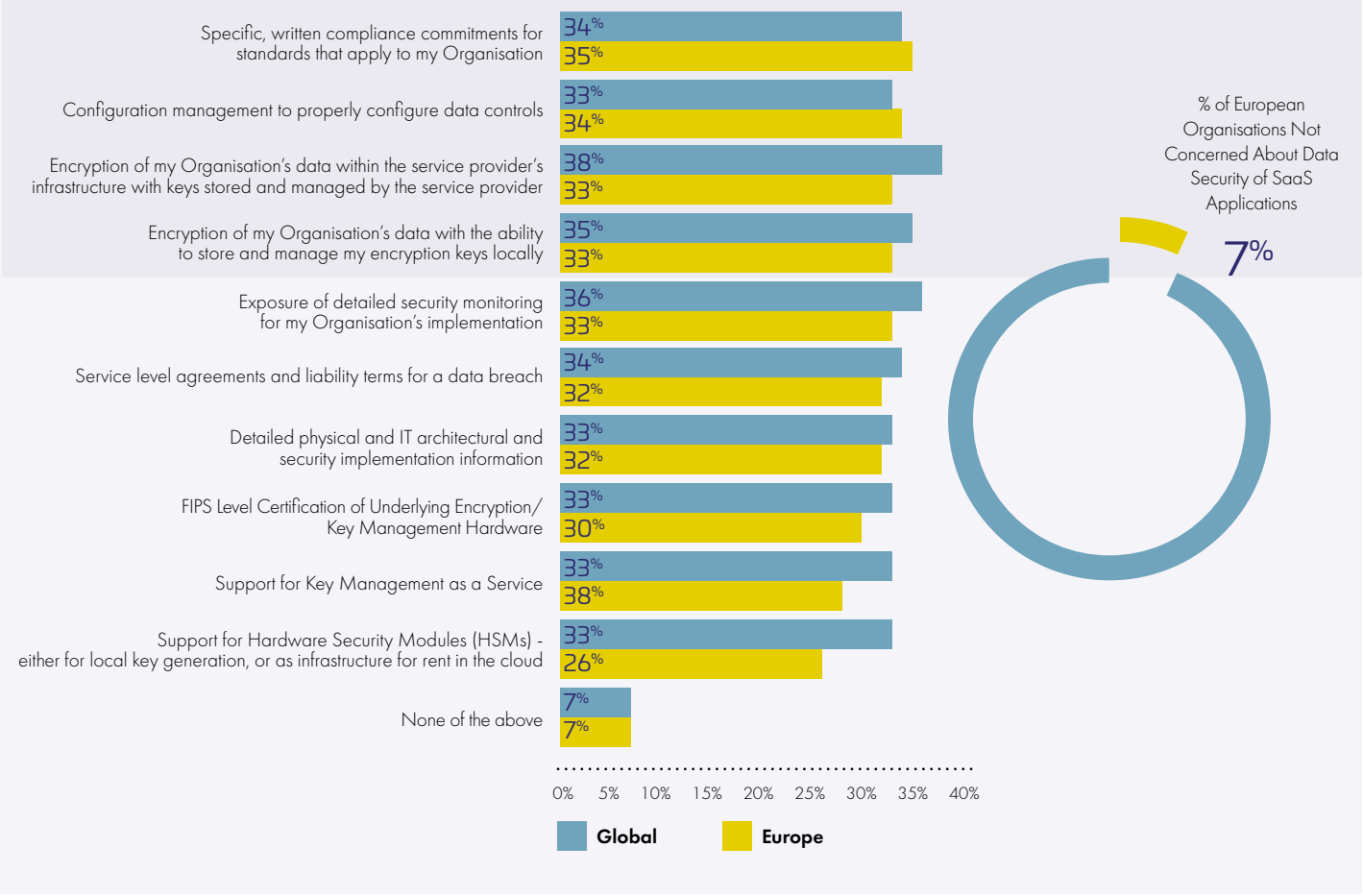


Figure 19 – SaaS Security Concerns

Source: 2020 Thales Data Threat Report Survey, IDC, November 2019

Eighty-nine percent of European respondents have at least some concerns over data security of IaaS environments. IaaS security concerns also cover a broad range of issues with key management within a service provider's infrastructure, key management as a service, and local key integration as top concerns (see Figure 20).

Figure 20 – IaaS Security Concerns

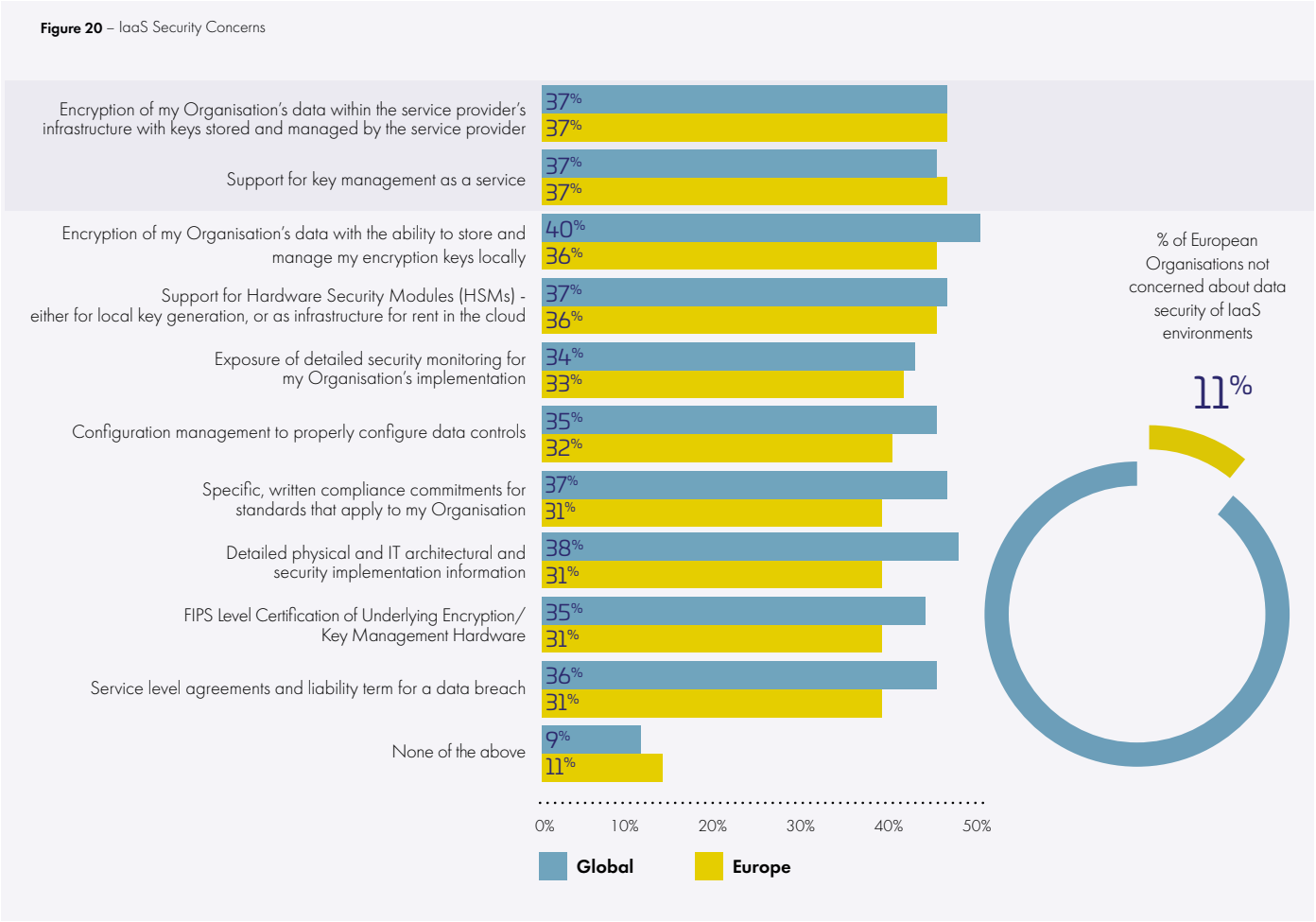


Figure 20 – IaaS Security Concerns

Source: 2020 Thales Data Threat Report Survey, IDC, November 2019

Eighty-nine percent of European respondents also have at least some concern over data security of PaaS environments with data encryption, service level agreements, and local key storage leading the way (see Figure 21). This concern will grow as organisations move their focus from IaaS to PaaS deployments to support their application development initiatives in DX.

Figure 21 – PaaS Security Concerns

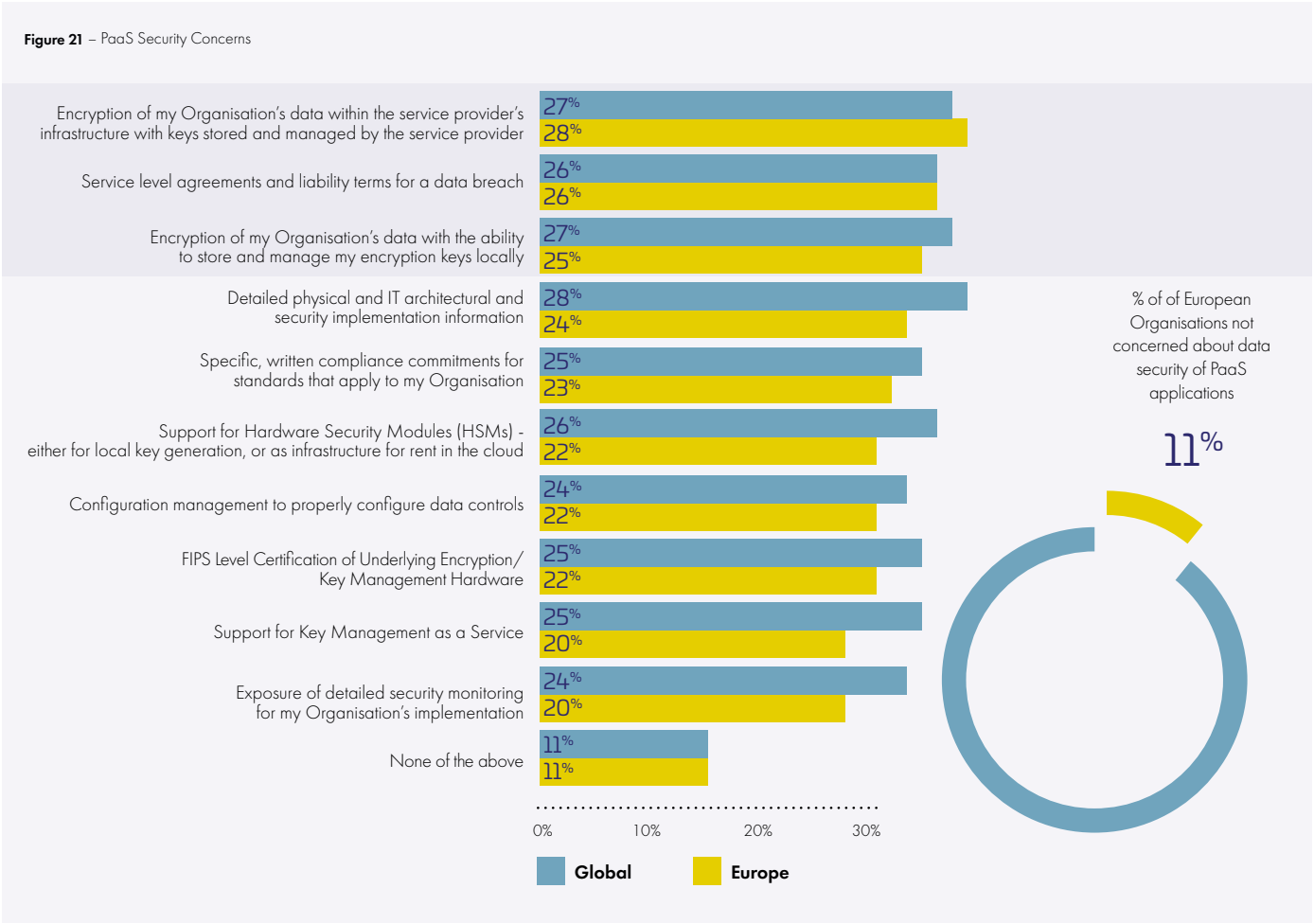


Figure 21 – PaaS Security Concerns

Source: 2020 Thales Data Threat Report Survey, IDC, November 2019

03

Security Concerns and Methods of Alleviation by Data Environment

Just as digital transformation creates opportunities for new technologies, it also introduces new security concerns. Transformational technologies like IoT and mobile payments allow enterprises to engage customers where they are but extend security concerns away from on-premise to cloud environments. Big data, containers, and DevOps technologies support the cloud and edge computing. With expanding use of these technologies, discovery of sensitive data and key management take on an even more critical role in data security. Yet data discovery and key management are not perceived as top concerns by European companies, creating potential gaps in data security practices.

Eighty-six percent of European companies in this study feel at least moderately secure as they push more data to these new technology deployments, with 61% feeling very or extremely secure (see Figure 22).

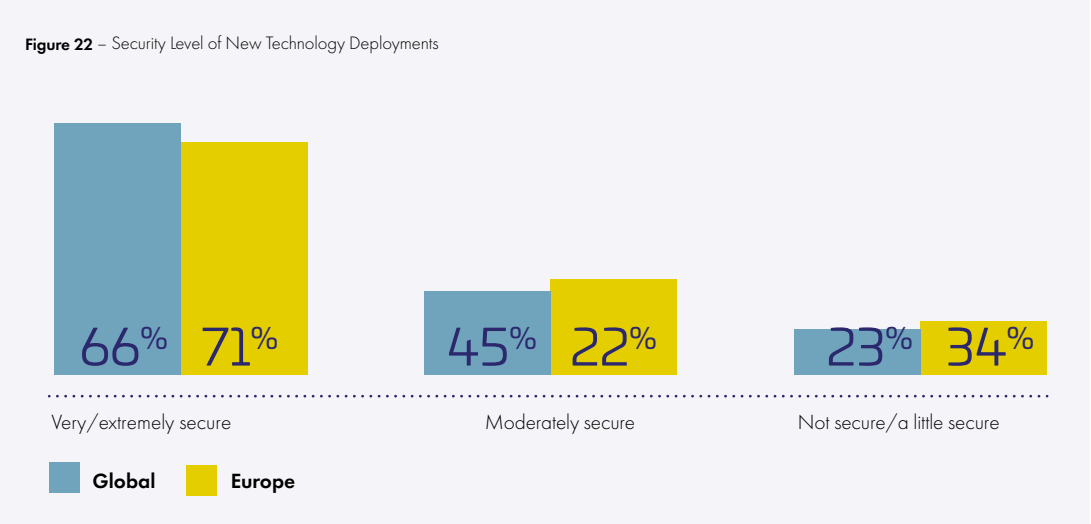


Figure 22 – Security Level of New Technology Deployments
Source: 2020 Thales Data Threat Report Survey, IDC, November 2019

> "Eighty-six percent of European companies in this study feel at least moderately secure as they push more data to new technology deployments."

Big Data Security Concerns

Ninety-nine percent of European respondents are concerned about data security in their big data environments. The leading big data security concerns are non-sensitive data becoming sensitive, access controls, and data quality. Interestingly, data discovery concerns as a priority are low (Figure 23). Leading methods to alleviate big data security concerns include stronger authentication, data discovery, and compliance certifications.

Figure 23 – Big Data Security Concerns

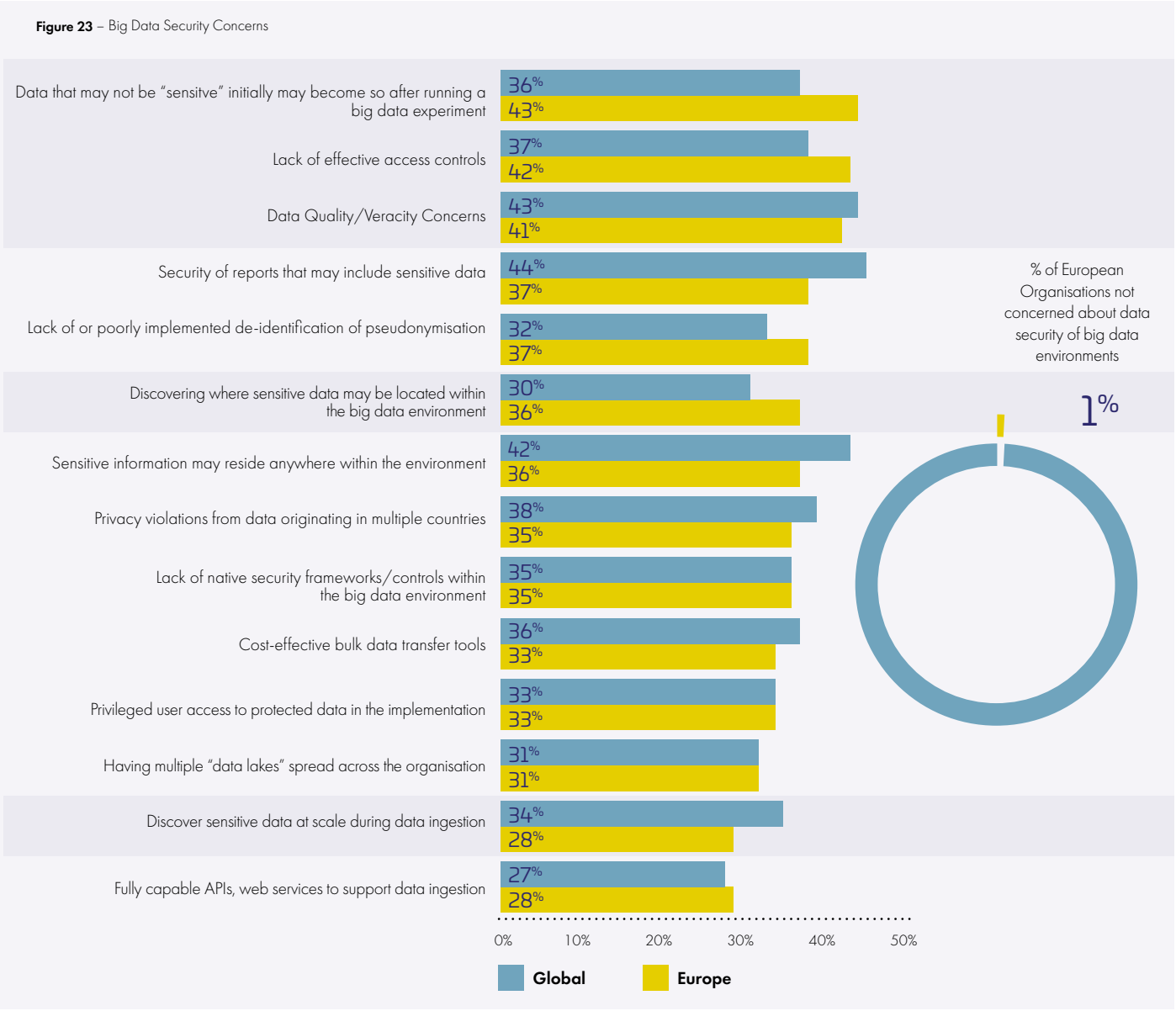


Figure 23– Big Data Security Concerns

Source: 2020 Thales Data Threat Report Survey, IDC, November 2019

> "Ninety-nine percent of European respondents are concerned about data security in their big data environments."

Internet of Things Security Concerns

Top IoT security concerns from the 99% percent of European respondents who have an IoT data security concern include lack of skilled personnel, device attacks, and encryption/tokenisation (see Figure 24). Digital identity authentication, anti-malware, and perimeter/gateway protection are top responses to address IoT security concerns. As IoT devices are deployed, key management is increasingly important to effectively implement identity security and data encryption on these IoT devices.

Figure 24 – Internet of Things Security Concerns

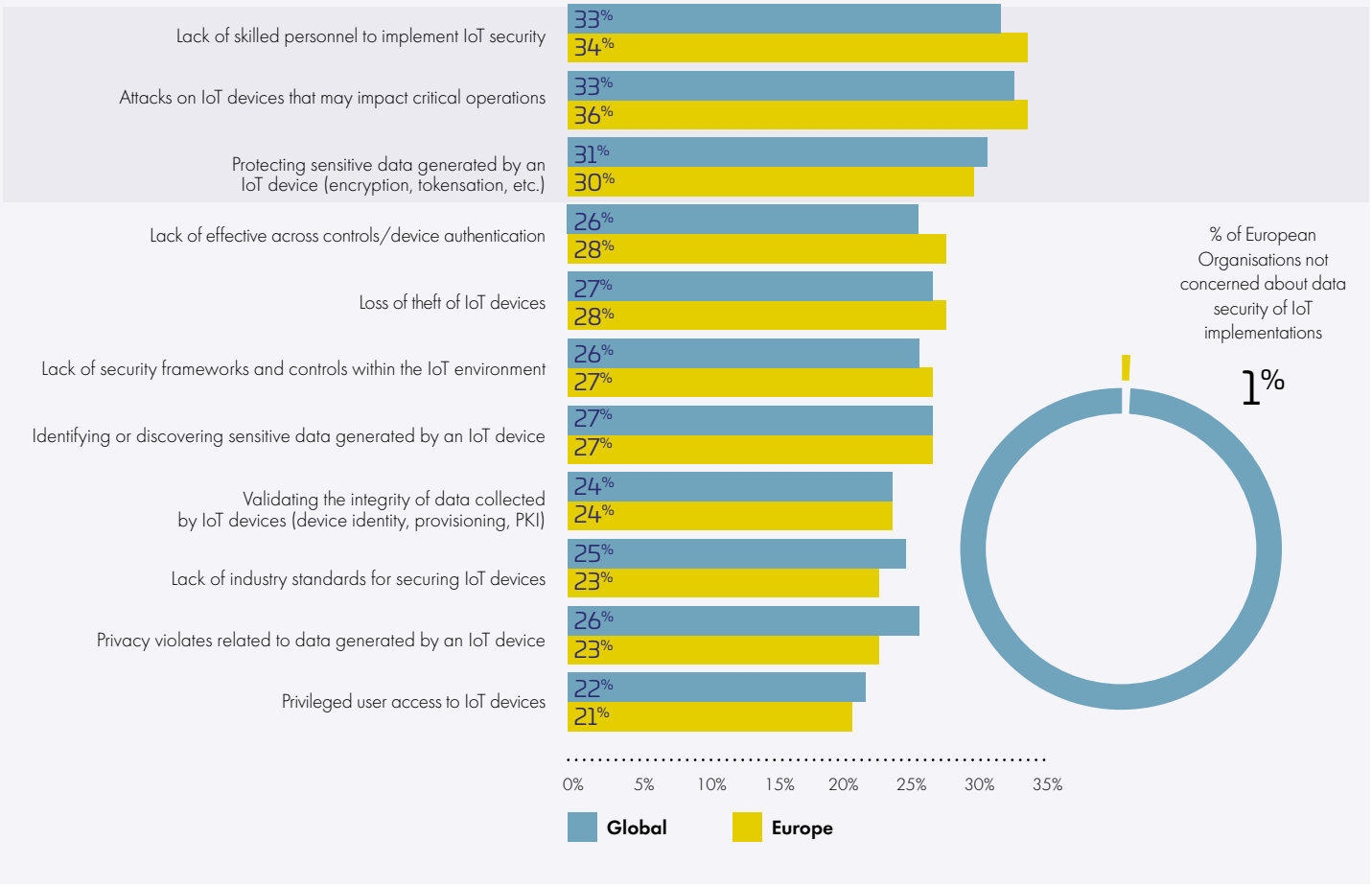


Figure 24 – Internet of Things Security Concerns

Source: 2020 Thales Data Threat Report Survey, IDC, November 2019

Mobile Payments Security Concerns

Ninety-eight percent of European respondents have at least some data security concerns with mobile payments. Fraudsters using mobile payment apps for new account fraud and exposure of personally identifiable information (PII) are top concerns (see Figure 25). Many wide-ranging solutions are considered to address mobile payment security. Chief among them are password controls, secure state validation, and data encryption.

Figure 25 – Mobile Payments Security Concerns

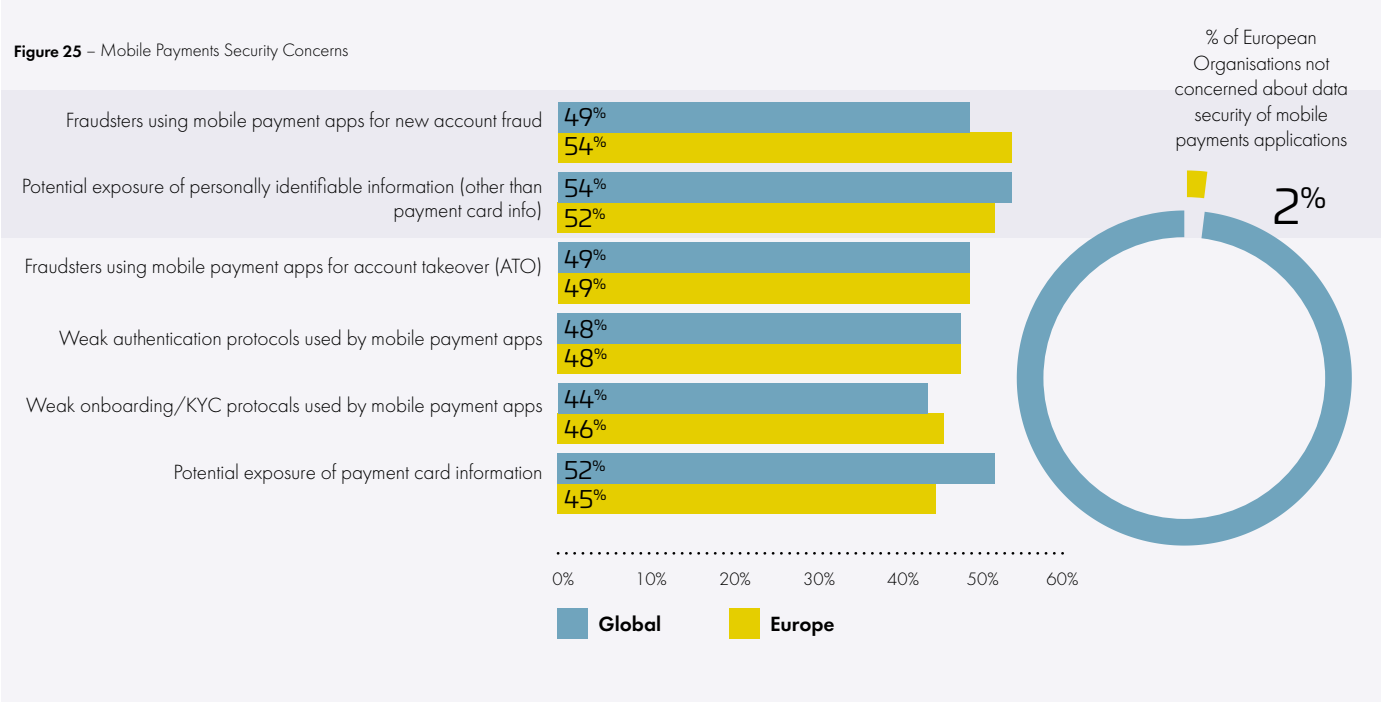


Figure 25 – Mobile Payments Security Concerns

Source: 2020 Thales Data Threat Report Survey, IDC, November 2019

> "Ninety-eight percent of European respondents have at least some data security concerns with mobile payments."

Container Security Concerns

Reflecting the relative lack of maturity of container-related security technologies, European organisations are concerned about many different issues as they continue to better understand containers and container security, although 97% express some data security concerns with containers. Vulnerability of container images, privacy violations, and lack of compliance certifications lead the list (see Figure 26). Anti-malware, monitoring, and encryption are important solutions for organisations to employ as container understanding develops.

Figure 26 – Containers/Docker Security Concerns

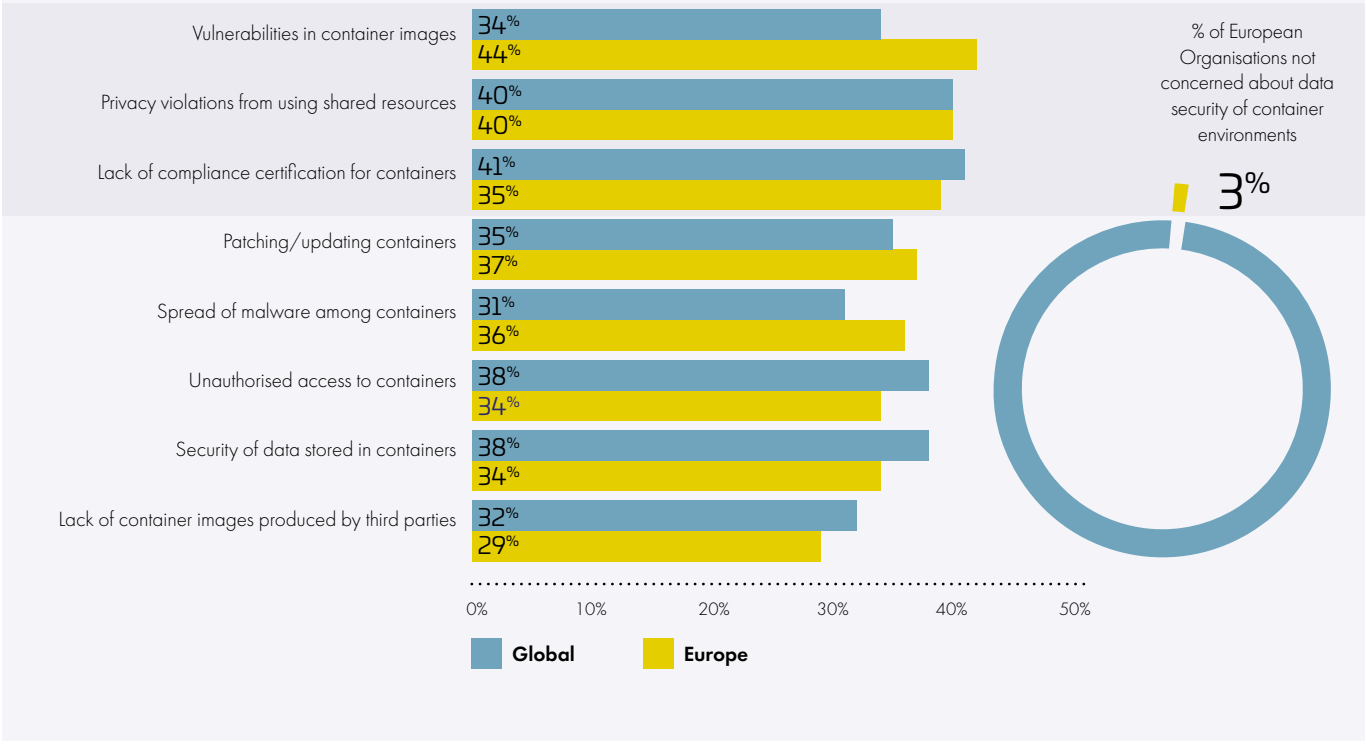


Figure 26 – Containers/Docker Security Concerns

Source: 2020 Thales Data Threat Report Survey, IDC, November 2019

> "Ninety-seven percent of European organisations express some data security concerns with containers."

DevOps Security Concerns

When it comes to DevOps environments, 98% of European respondents are concerned about data security of their DevOps environment. Organisations are most concerned about privileged access controls, unsecured cloud infrastructure, and DDoS attacks on their DevOps environments (see Figure 27). Many different approaches are being considered to alleviate DevOps security concerns, led by automated vulnerability assessment, continuous security monitoring, and comprehensive activity logging.

Figure 27 – DevOps Security Concerns

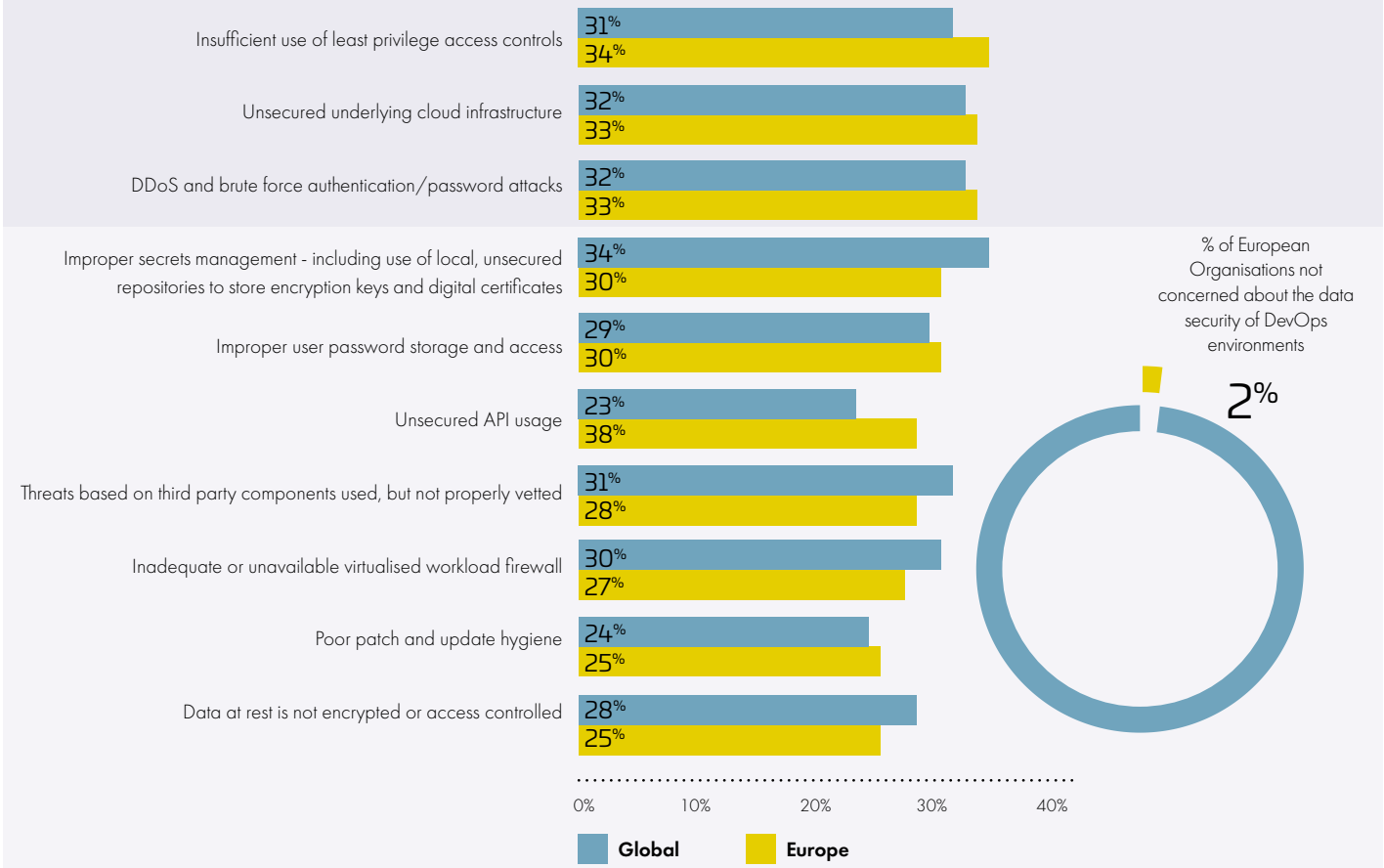


Figure 27 – DevOps Security Concerns

Source: 2020 Thales Data Threat Report Survey, IDC, November 2019

> "Ninety-eight percent of European respondents are concerned about data security of their DevOps environment."

04
IDC Recommendations

European organisations face expanding and more complex data security challenges as part of implementing their cloud and digital transformation strategies. The following are IDC's guidance and key takeaways to help these organisations elevate their data security posture and evolve their security policies:

- **Invest in modern, hybrid and multicloud-based data security tools that make the shared responsibility model work. More sensitive data is stored in the cloud than ever.** Organisations should focus on solutions that can simplify the data security landscape and reduce complexity across multiple clouds and legacy environments, as well as modern, cloud-based digital transformation technologies. For example, companies should consider data security solutions that enable protection of data moving between clouds and out of the cloud to on-premise environments and should leverage centralised security solutions that orchestrate data security across multiple cloud platforms vendors. In a shared responsibility model, organisations should not overly rely on service providers for data security measures. Organisations must consider all the data security elements directly in their control, like identity and data security.

- **Consider a secure least privileged model that secures both data and the users accessing the data.** Organisations still focus on network security as they aim to control access at the perimeter. Data security should go beyond that traditional edge, whether it's in the cloud, virtual environments, data centres, or other DX technologies like blockchain. Least privilege access approaches, though extremely important to support data security, are not complete solutions. Least privileged access protections provide network and application access protection to data, but they do not protect the data itself. Challenging data environments require a more persistent data security approach grounded in cryptography should access protections fail. Think defence in depth.

- **Increase focus on data discovery solutions and centralisation of key management to strengthen data security.** Data security concerns should evolve as the edge expands with greater adoption of the cloud, big data environments, IoT devices, mobile payments, containers, and DevOps environments. Greater emphasis on sensitive data discovery in these environments, as well as for existing environments, strengthens an organisation's data security stance by enabling the organisation to know where sensitive data is and how to access it. Additionally, as organisations increase their use of encryption to protect sensitive data, they should centralise key management to help simplify key management operations in otherwise complex environments.

- **Augment discovery with robust classification for risk-based execution.** Using tools for automated data classification and clusterisation gives a boost to both security frameworks and governance, risk and compliance programs. Not only does this allow organisations to apply policies appropriate to the risk and value, it also helps to simplify the security architecture and procedures while minimising resource burden and potential friction from blanket deployments of ultimate encryption mechanisms. Strategic implementations will reduce costs and consequently increase ROI for business-focused discussions.

- **Prepare for quantum computing's impact on cryptography.** Data security doesn't get any easier as the power of quantum computing may expose sensitive data sooner rather than later. Organisations must begin planning their infrastructure and key management adjustments to counter fundamental changes to cryptography brought on by quantum computing.

- **Focus on the right threat vectors.** Yes, bad actors are evolving their methods daily. Security professionals need to continually evolve their methods to match. But organisations should focus on the threat vectors within their direct control. Organisations must be careful of overprovisioning quantity and breadth of accounts both internally and externally with service providers and contractors.

- **Data security solutions, especially rights management and encryption, are critical to remain vigilant against the post-COVID-19 data risk reality.** This point is especially relevant today more than ever as the work from home migration has increasingly forced corporate data to be accessed remotely, sometimes on BYO devices. Even if an organisation loses visibility as to where data resides, data security technologies such as encryption protects corporate data in a location agnostic manner.

- **Are we certain that our employees will return to the premises?** Organisations need new data security methods to protect the post COVID-19 IT landscape as data migrates away from the enterprise premises and to the cloud and back to the premises. There is no certainty that all employees will choose to come back of the office as the migration to work from home may be permanent for many. Post-COVID-19 data protection starts with user access management controls and encryption and moves to smart encryption with built-in data rights management controls as the post-COVID-19 perimeter moves to the data itself and the users accessing it.

THALES

350 Longwater Avenue, Reading,
Berkshire RG2 6GF

0118 943 4500

>cpl.thalesgroup.com <

cpl.thalesgroup.com/Euro-DTR
#2020DataThreat