Hide and Seek - Cybersecurity and the Cloud

Merritt Gigamon
Research results

August 2017

VansonBourne

Demographics

500 IT decision makers, with responsibilities such as CloudSecOps (386 respondents), SecOps (367 respondents), and data privacy (358 respondents) were interviewed in May 2017, split in the following ways...

…respondent country

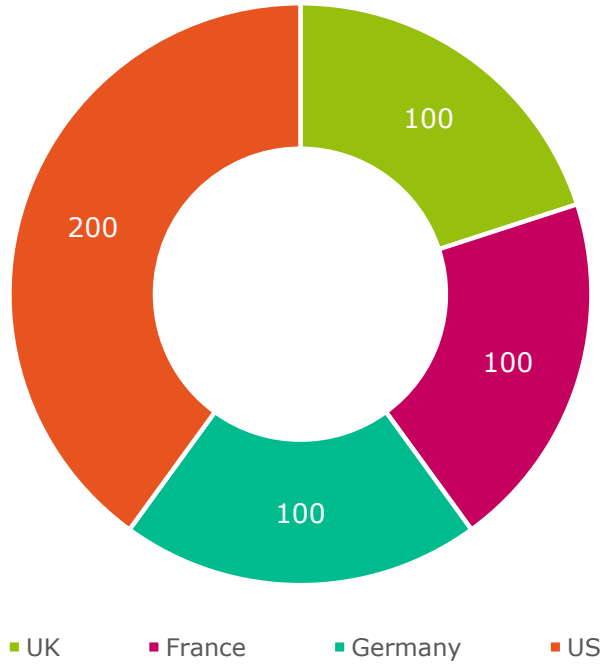


Figure D1: *Analysis of respondent country, asked to all respondents (500)*

…organization size

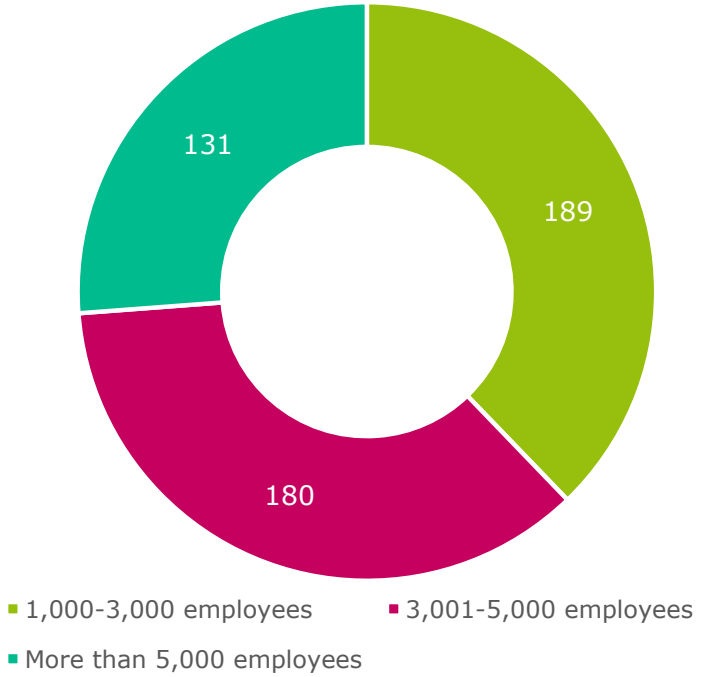


Figure D2: "How many employees does your organization have in your country?", *asked to all respondents (500)*

…organization sector

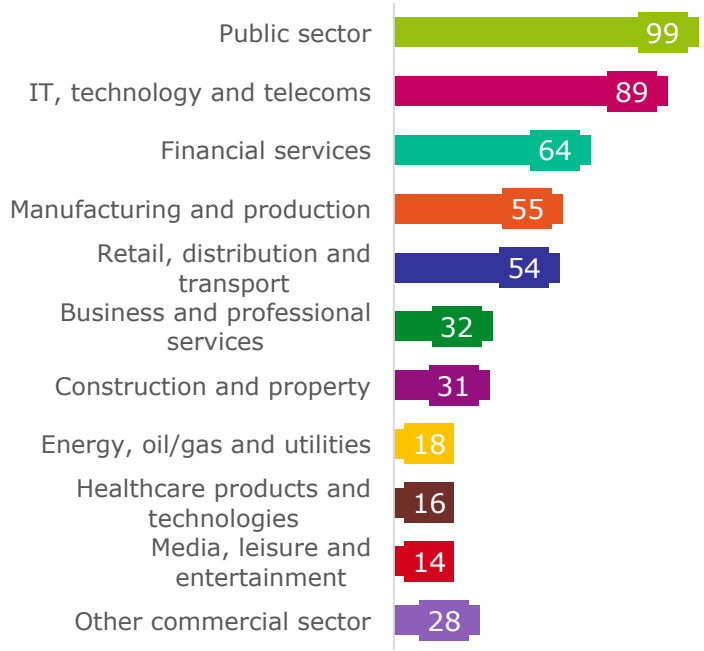


Figure D3: "Within which sector is your organization?", *asked to all respondents (500)*

VansonBourne

Four areas of interest:

1: Cloud migration
2: Visibility
3: Security
4: GDPR

VansonBourne

1: Cloud migration

Current and expected cloud use

It is anticipated by 73% of respondents that, in three years' time, the majority of their organization's application workloads will be in either the public or private cloud…

…compared to only 14% who think the majority will still be on premise

This highlights a clear predicted shift towards the cloud in the coming years as currently, over half (54%) of respondents report that the majority of their organization's application workloads are located in on premise data centers, with only 37% reporting that they are located in a public or private cloud environment

Historically, IT decision makers have been somewhat suspicious of the benefits that the cloud can bring to their organization, but this figure shows that there is a growing acceptance that this is the direction organizations are heading in

What is being migrated to the cloud?

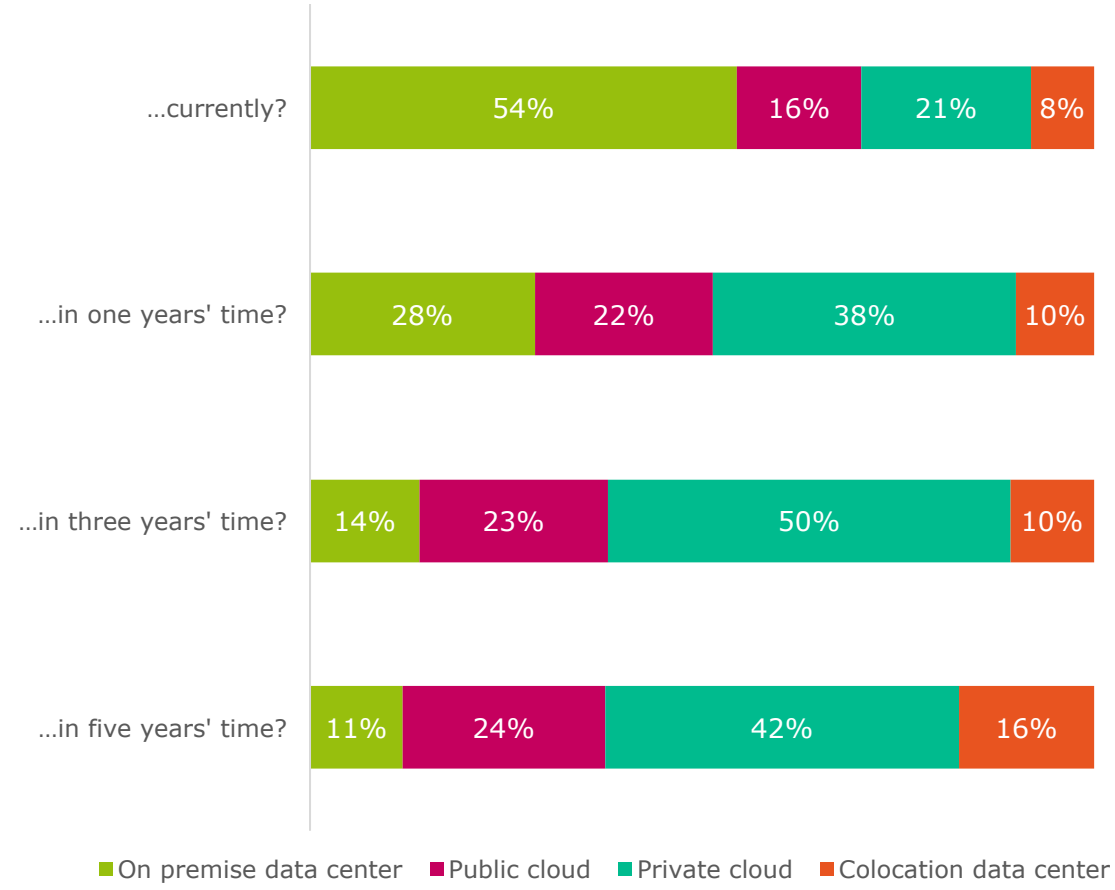


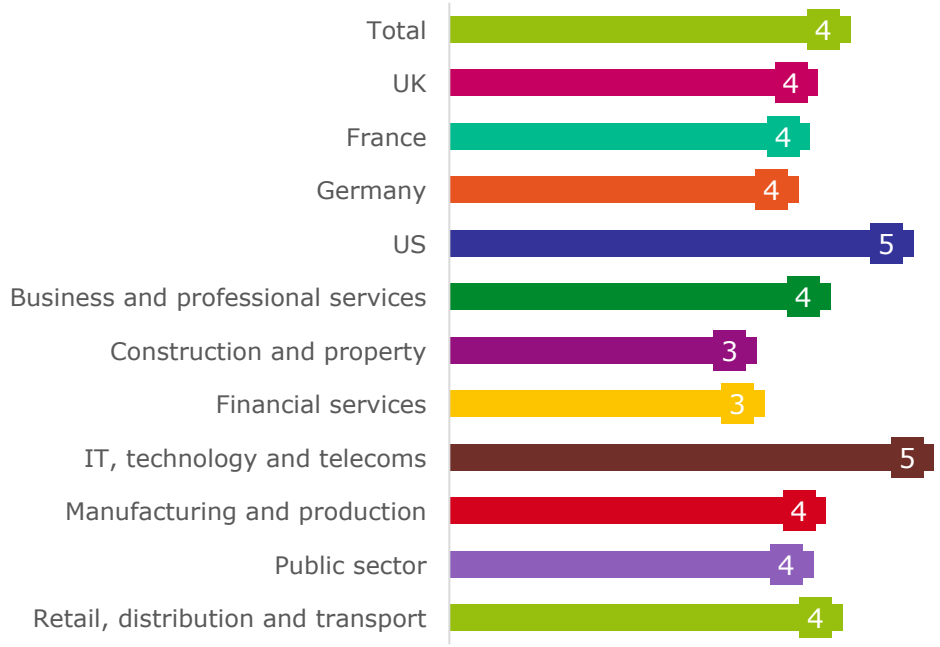
Figure 1: "Where are the majority of your organization's application workloads located/going to be located…", *asked to all respondents (500)*

VansonBourne

Number of cloud providers and asset migration

The shift towards cloud is prevalent, with almost seven in ten (69%) respondents' organizations already migrating day to day work information (fig. 3)

Some organizations are even migrating high risk information such as proprietary corporate information (56%) or personally identifiable information (47%) (fig. 3)



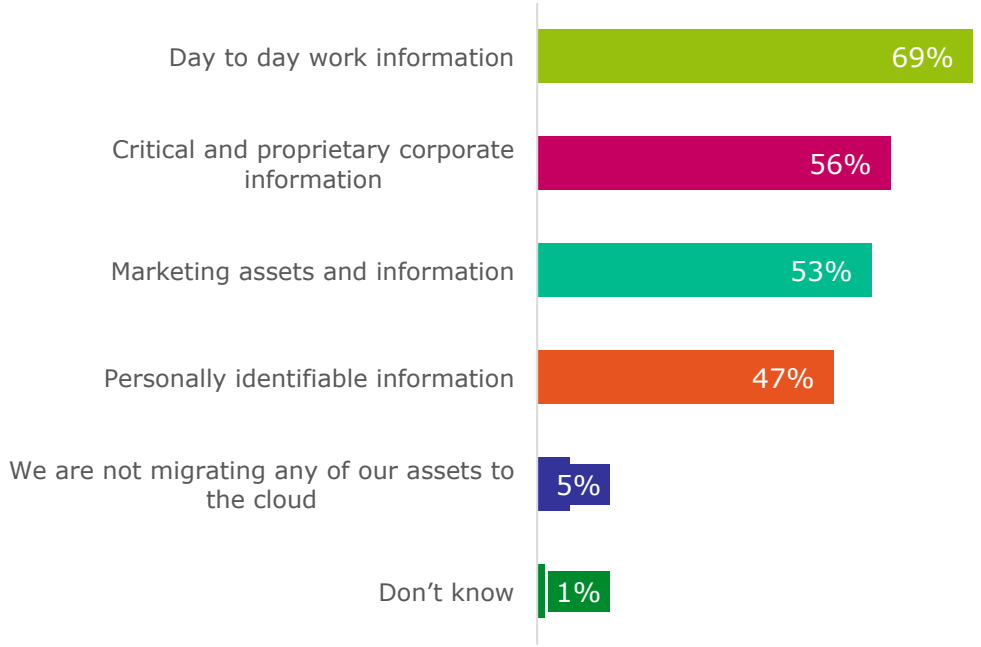


Figure 2: *Analysis showing the average number of cloud providers that respondents' organizations are using, split by country and sectors with a base greater than 30, asked to all respondents (500)*

Figure 3: "What types of assets are you migrating to the cloud?", *asked to all respondents (500)*

VansonBourne

Security in the cloud

Only just over a third (35%) of respondents' organizations are planning to approach network security in the cloud in exactly the same manner as they do with their on premise security operations

While respondents' organizations are not desperate to change their approach, 65% feel that an element of change is necessary, suggesting that they have learnt from their on premise mistakes

This is particularly clear in the UK, where only 24% want to approach network security in the cloud in exactly the same manner as they do with their on premise security operations

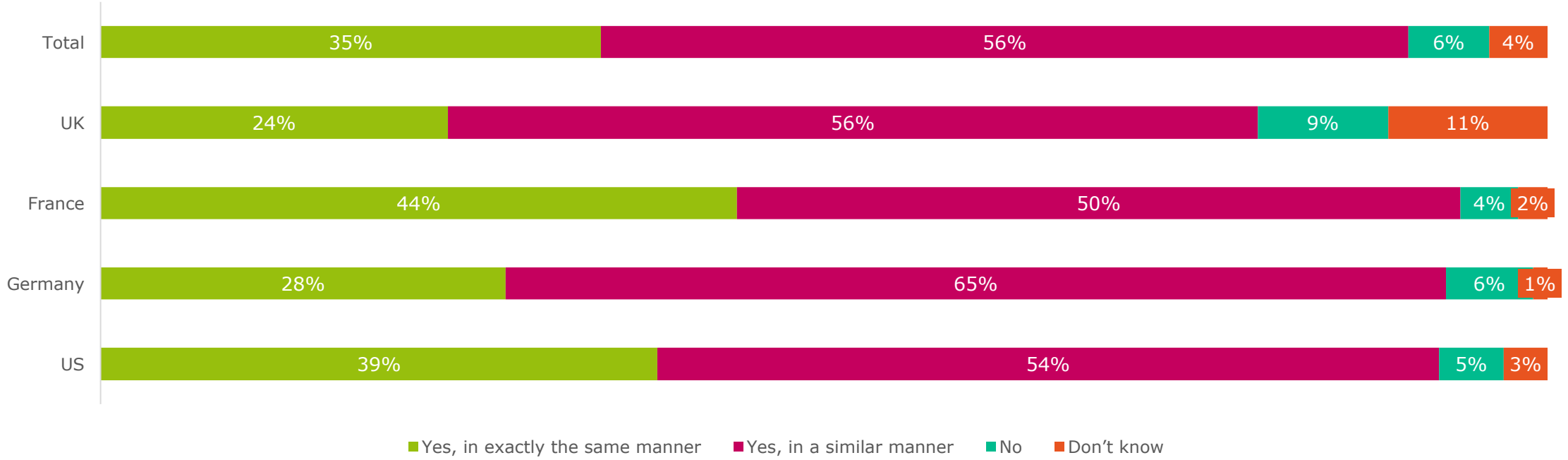


Figure 4: "Is your organization planning to approach network security in the cloud in the same manner as it does with its on premise security operations?", *split by country, asked to all respondents (500)*

VansonBourne

2: Visibility

VansonBourne

Missing information

Around half of respondents who do not have complete visibility over all of the data traversing their organization's network report that they are missing information regarding the identification of threats (50%)…

…as well as the ability to understand what is being encrypted (48%), or insecure applications or traffic (47%)

The most common type of missing information varies between the different organization sizes, clearly showing that no matter how small or large they are, a lot of organizations are struggling with missing data

This could cause severe security difficulties especially for those who cannot access the relevant data regarding threats, or insecure applications

Where is this data hiding?

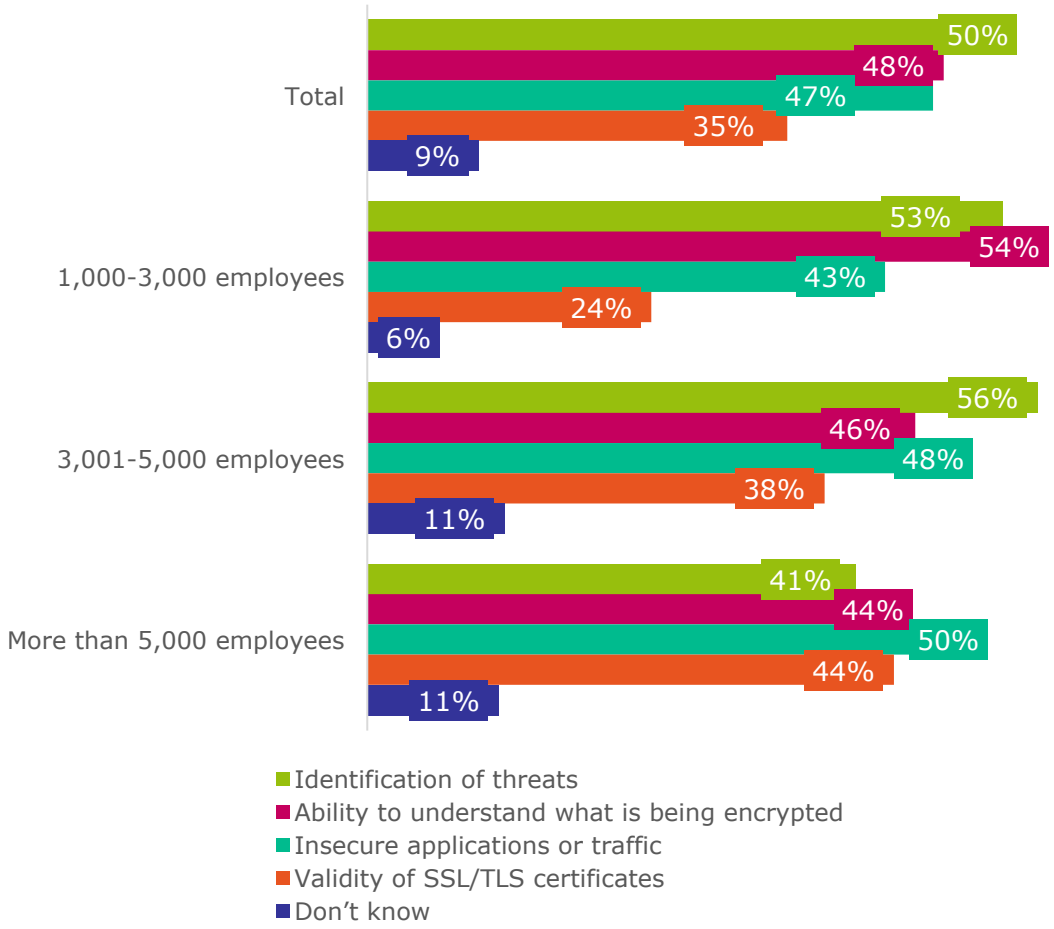


Figure 5: "What information are you missing about the data traversing critical parts of your organization's infrastructure?", *split by organization size, asked to respondents who do not have complete visibility into all of the data traversing their organization's network (215)*

VansonBourne

Hidden data

Surveyed decision makers cite a multitude of problems regarding hidden data, including that data is most siloed when it is held between SecOps and NetOps (78%), or that they spend a long time searching for data that they do not have visibility over (57%)

Almost half agree that their hybrid cloud environment prevents them from seeing where data is really stored (49%), or that their organization cannot access a lot of its data because it is encrypted (46%)

These issues are being universally experienced by organizations from all sectors and countries, and they could really bring about some serious security concerns – especially relating to the hybrid cloud environment if the predicted shift towards cloud occurs (fig. 1)

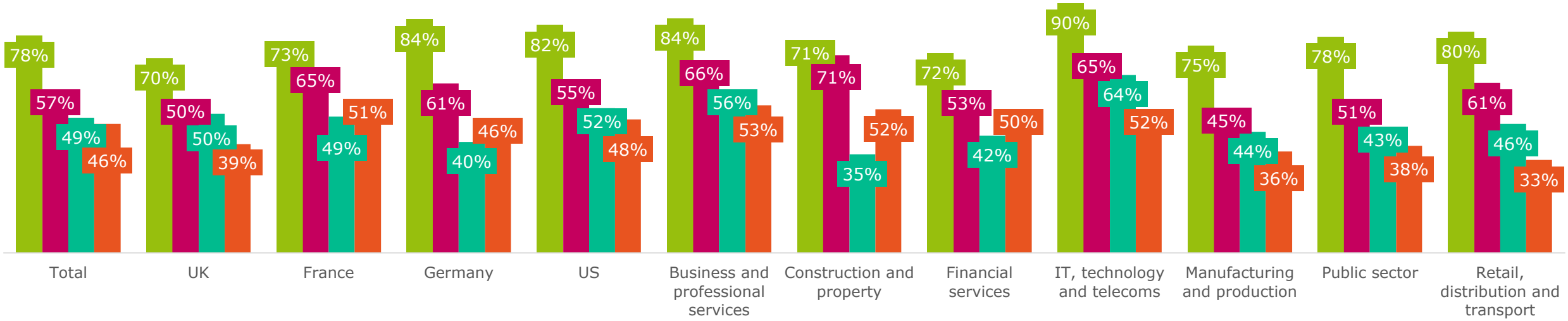


Figure 6: *Analysis showing the percentage of respondents who agree with the above statements regarding data in their organization, split by country, and sectors with a base greater than 30, asked to all respondents (500)*

VansonBourne

Infrastructure scaling

An overwhelming 72% of respondents' organizations have not scaled their network infrastructure to meet the needs of handling increased data volume - this figure increases in organizations from the financial services (80%) and public sectors (78%) and is also slightly lower (79%) in organizations from France

It is clear that organizations are aware that they are going to have to scale their network infrastructure at some point in the not too distant future, with 61% of respondents reporting that this is planned within the next year

This shows an obvious awareness that something needs to be done regarding increased data volume in order for the organization not to become swamped in data

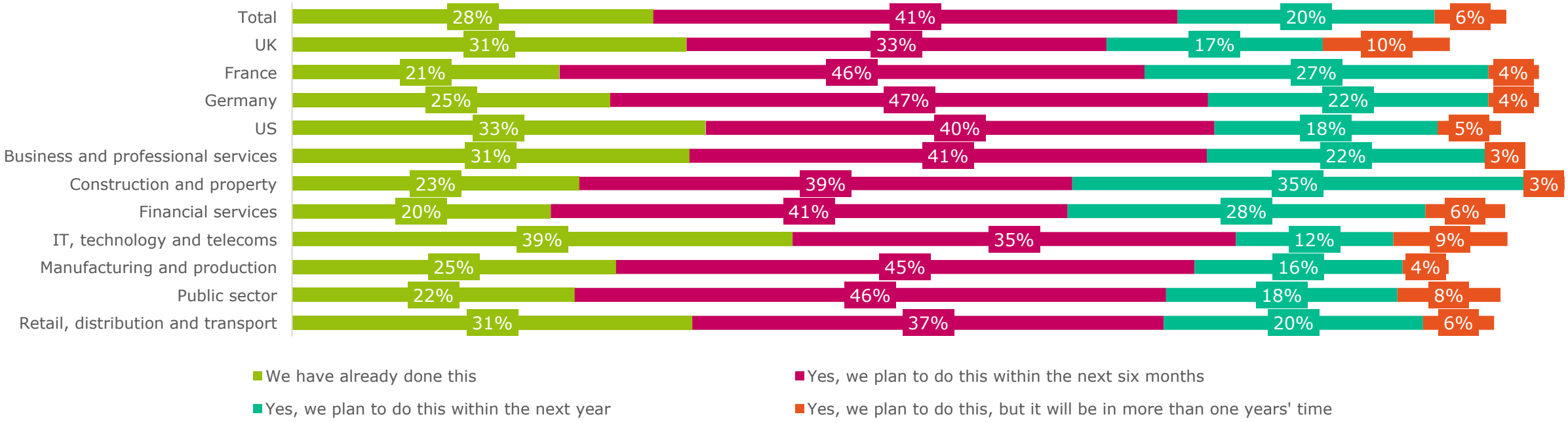


Figure 7: *Analysis showing the percentage of respondents whose organization has already scaled their network infrastructure to meet the needs of handling increased data volume, or knows the timescale for their plan to do so, split by country and sectors with a base greater than 30, asked to all respondents (500)*

VansonBourne

SecOps concerns

The most commonly reported concern by respondents regarding their organization's security operations is increased complexity with security tools (56%)

However, it is clear that there are various concerns across all countries – in the US the most common concern is increased traffic volume (61%), but respondents from organizations in France are more likely to highlight the increased use of encryption (57%) as concerning

It seems clear that there is a desire for simplicity and efficiency with regard to security operations, as too many complex tools that do not integrate well together can cause security gaps in the network, leaving organizations vulnerable

How much of a problem is visibility?

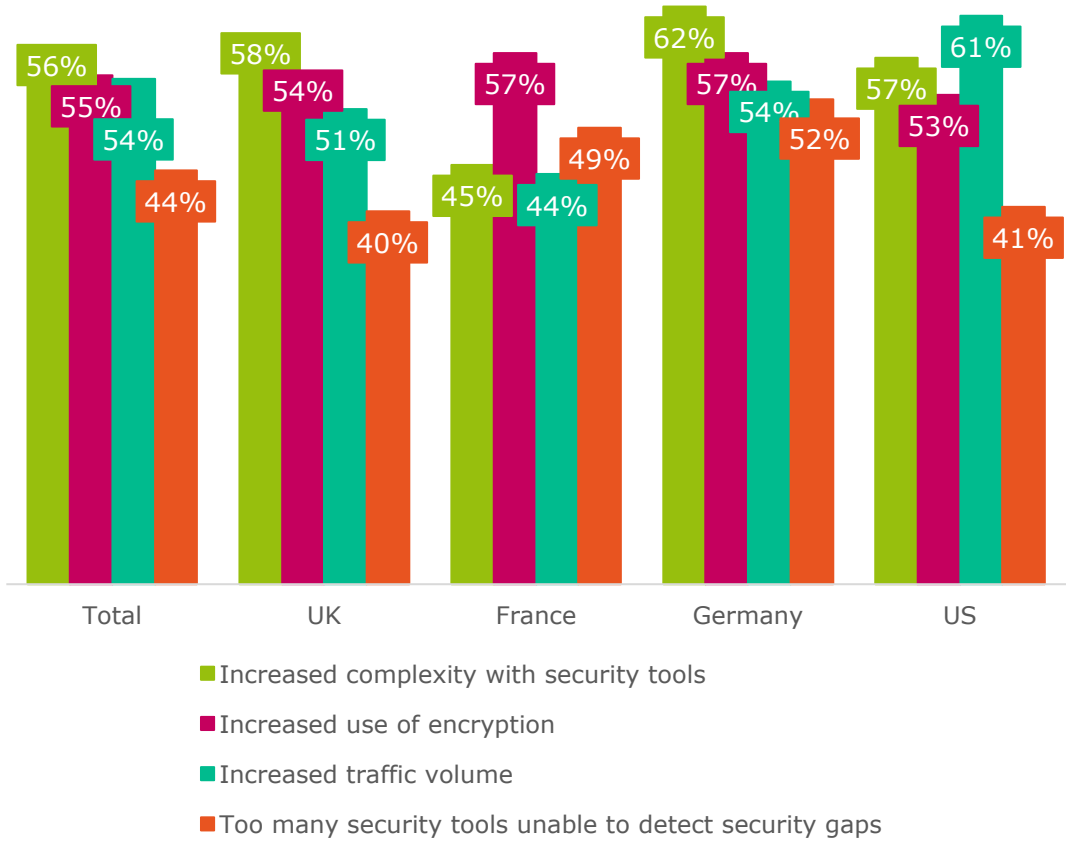


Figure 8: *Analysis showing respondents' organizations' top four most common concerns regarding security operations, split by country, asked to all respondents (500)*

VansonBourne

Network visibility

Just over two thirds (67%) of respondents agree that network blind spots are a major obstacle to data protection in their organization (fig. 9), while only just over a third (34%) rate their organization as "excellent" with regard to visibility into all network traffic in their data center (fig. 10)

Network blind spots being an obstacle is a clear challenge that is experienced universally across organizations from all countries, sizes and sectors. Respondents from organizations in Germany (23%) and the public sector (23%) are a little more reserved when rating their organization on visibility into data center traffic

Poor network visibility does not only provide data protection issues, but also compliance issues with the EU GDPR only just around the corner

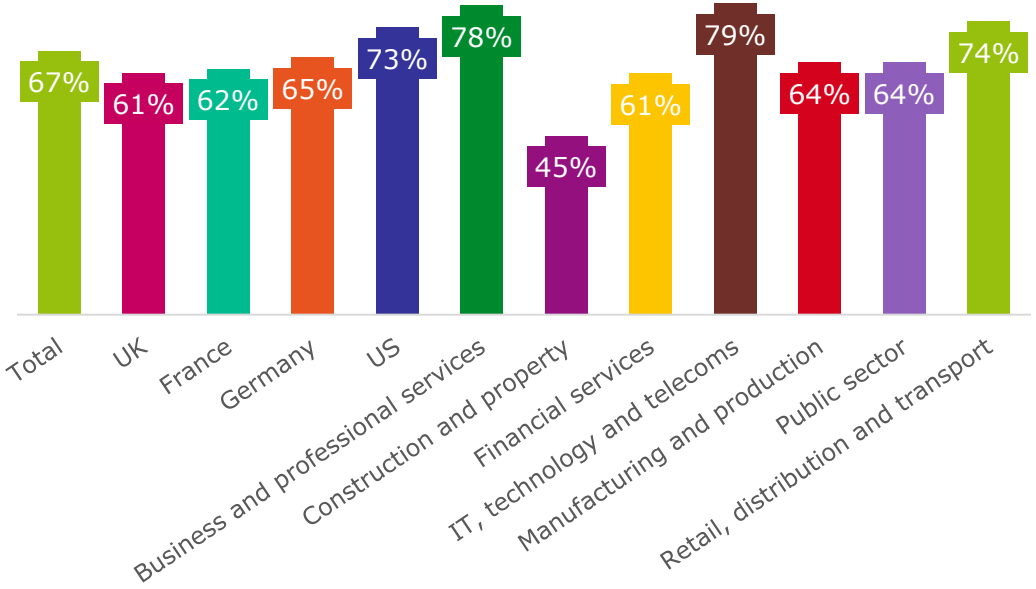


Figure 9: *Analysis showing the percentage of respondents who agree with the following statement: "Network blind spots are a major obstacle to data protection in my organization", split by country and sectors with a base greater than 30, asked to all respondents (500)*

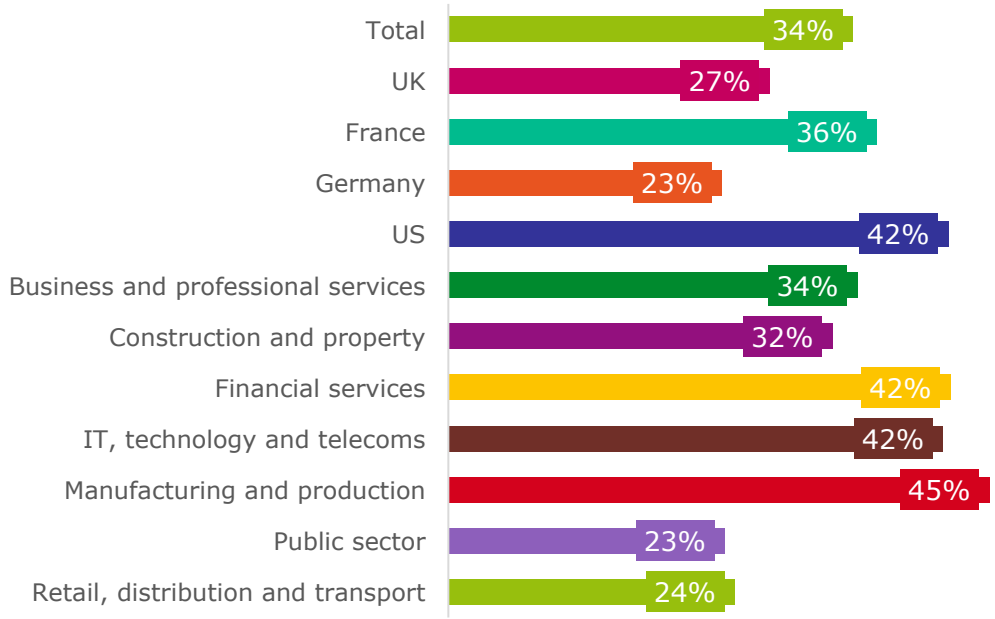


Figure 10: *Analysis showing the percentage of respondents who would rate their organization as "excellent" with regard to visibility into all of the network traffic in their data center, split by country and sectors with a base greater than 30, asked to all respondents (500)*

VansonBourne

Desired capabilities for SOC

Control of network traffic and data (62%) is the most commonly reported capability that respondents would want from their organization's Security Operations Center (SOC)

Other desirable capabilities include immediate detection and response capabilities to malicious threats and attacks (50%) and awareness of network traffic and data (50%)

This shows that respondents feel that it is important to wrestle back control regarding their organization's security operations, but are still aware that speed of response is crucial when it comes to malicious threats and attacks in order to prevent a serious incident

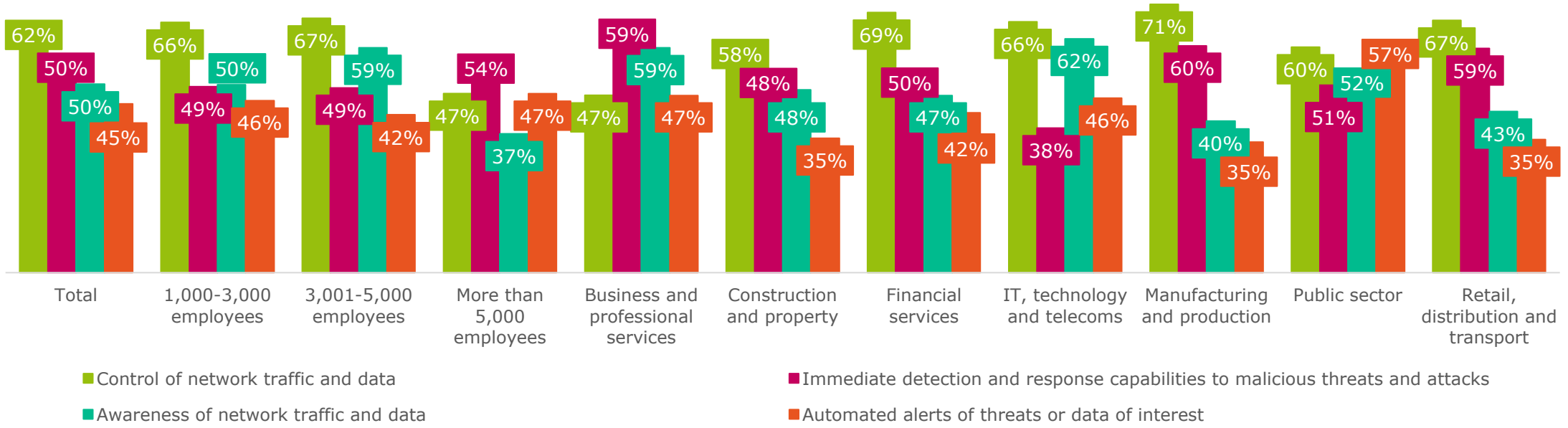


Figure 11: *Analysis showing respondents' top four most common capabilities that they would want in their organization's Security Operations Center (SOC), split by organization size and sectors with a base greater than 30, asked to all respondents (500)*

VansonBourne

3: Security

VansonBourne

Ownership and confusion with cloud security

In general, it would appear that the SecurityOps (69%) team is accountable for cloud security in respondents' organizations

However, in around half of organizations, CloudOps (54%) and NetworkOps (47%) are also involved (fig. 12)

When looked at in conjunction with the fact that over a third (36%) of respondents believe that there is confusion within their organization over which team owns the cloud security problem, potential problems begin to arise (fig. 13)

With no team taking the lead and possible poor collaboration between teams, an element of confusion has arisen and this in turn could open the door for cloud security issues

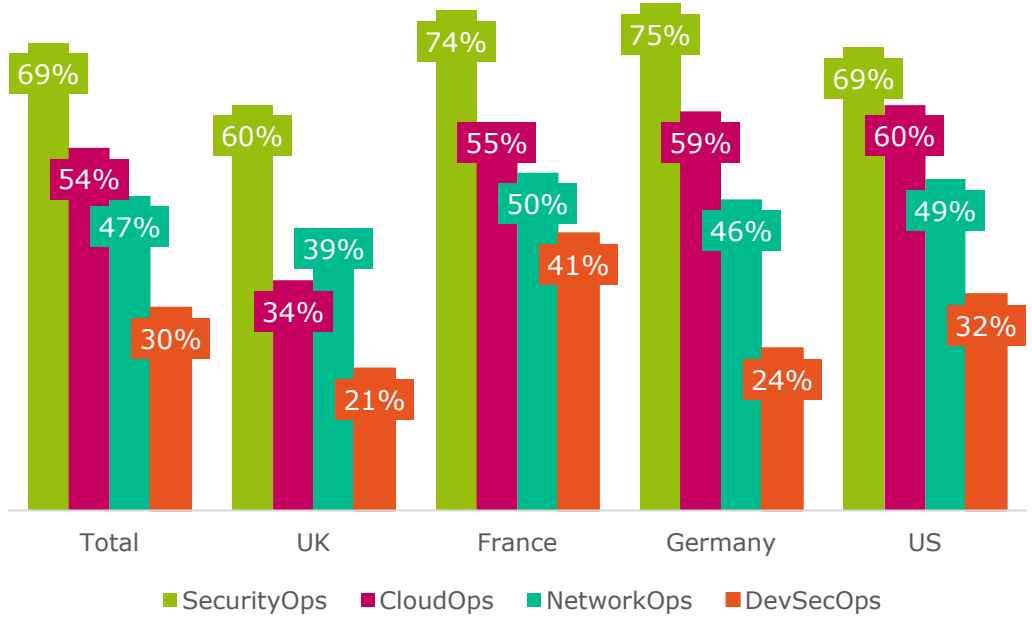


Figure 12: *Analysis showing which teams are accountable for cloud security in respondents' organizations, excluding 'no team is accountable' and 'don't know', split by country, asked to all respondents (500)*

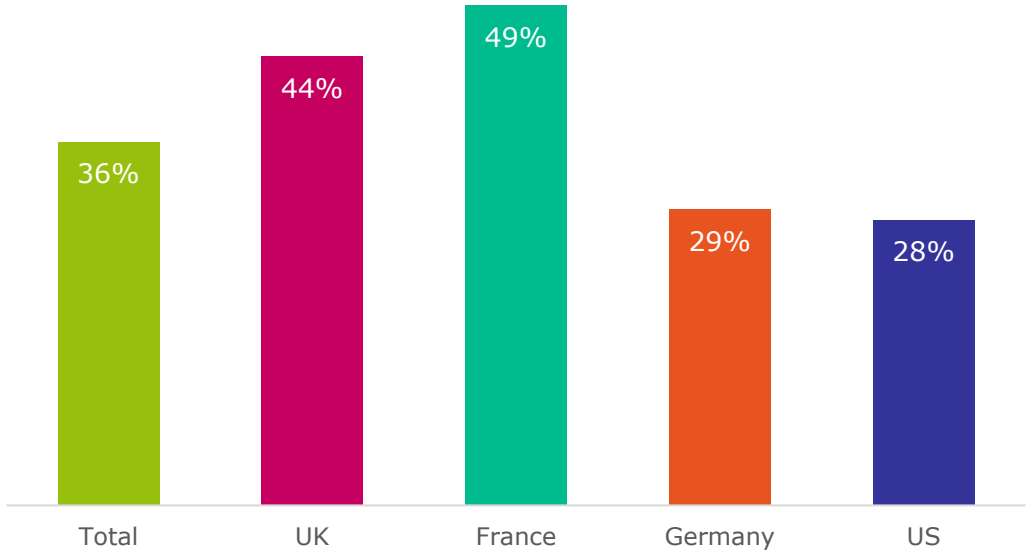


Figure 13: *Analysis showing the percentage of respondents who believe that there is confusion within their organization over which team owns the cloud security problem, split by country, asked to all respondents (500)*

VansonBourne

Cloud framework/strategy

53% of respondents' organizations have not yet implemented a cloud security framework/strategy, and this proportion surges to 64% in organizations from the UK and 63% in France

This is perhaps no surprise considering the higher levels of confusion in organizations from these countries regarding which team owns the cloud security problem (fig. 13). However, implementing such a framework/strategy is clearly on the minds of these organizations, with 49% of respondents reporting that their organization is planning to do this at some point in the future

It may be necessary for one team to take the lead with implementation (fig. 12) to reduce the possibility for confusion or gaps in the strategy

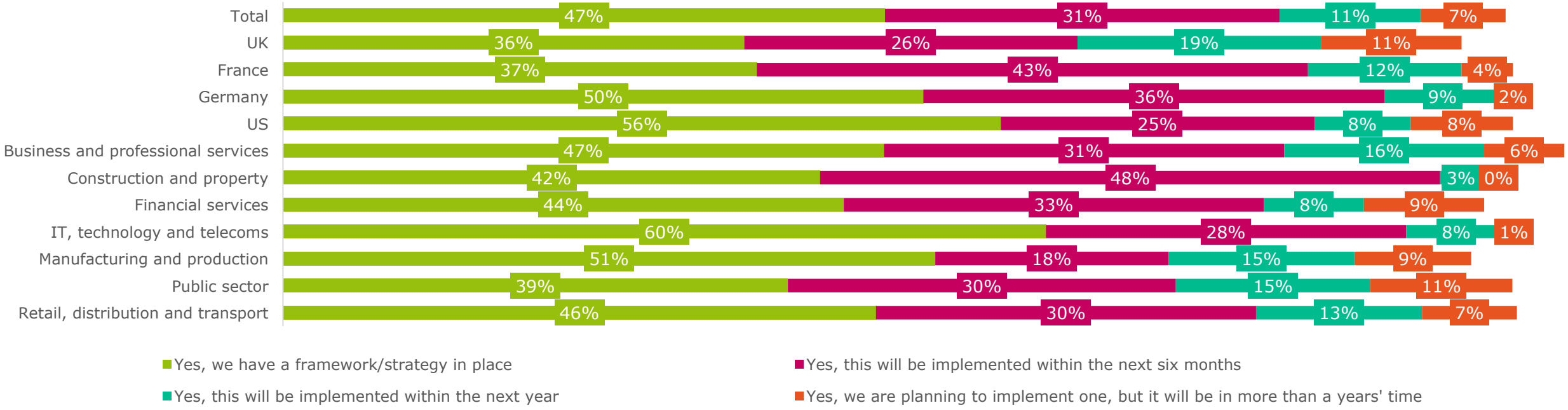


Figure 14: *Analysis showing the percentage of respondents' organizations who have already implemented a cloud security framework/strategy, or are planning to in the future, split by country and sectors with a base greater than 30, asked to all respondents (500)*

VansonBourne

Security vs. innovation

Cloud security is still a clear concern for respondents' organizations, with 85% reporting that it is at least a slight concern…

…and is holding them back from using the latest technologies such as IoT

Respondents from organizations in Germany appear to see cloud security more as a slight concern (60%) than a major concern (28%), but it still shows that this is an issue that needs to be addressed before they will be confident in adopting new technologies

If organizations do not come to terms with cloud security issues then it does not only leave them open to a possible attack, but it seems as though it could stop them innovating which could also leave them lagging behind their competitors

How much is being spent on cybersecurity?

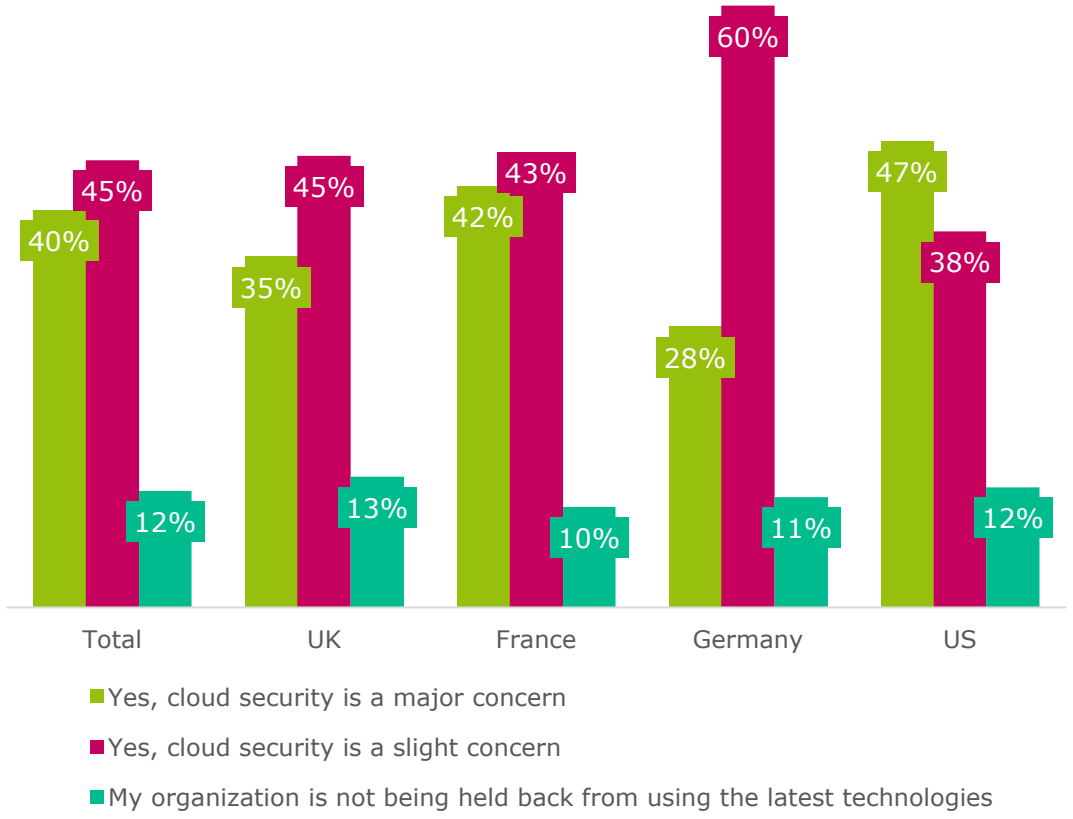


Figure 15: *Analysis of the extent to which cloud security concerns are holding back respondents' organizations from using the latest technologies, split by country, asked to all respondents (500)*

VansonBourne

Cybersecurity spend

On average, surveyed decision makers report that their organization's cybersecurity spending has increased by 30% in the last three years and they also forecast that this spending will increase by 36% in the next three years (fig. 16)

Despite this increase in spending, seven in ten (70%) respondents would agree that greater expenditure on security does not necessarily mean stronger security (fig. 17)

This highlights the fact that there is likely other underlying problems with security processes and/or strategy in these organizations that cannot necessarily be solved by further investment alone

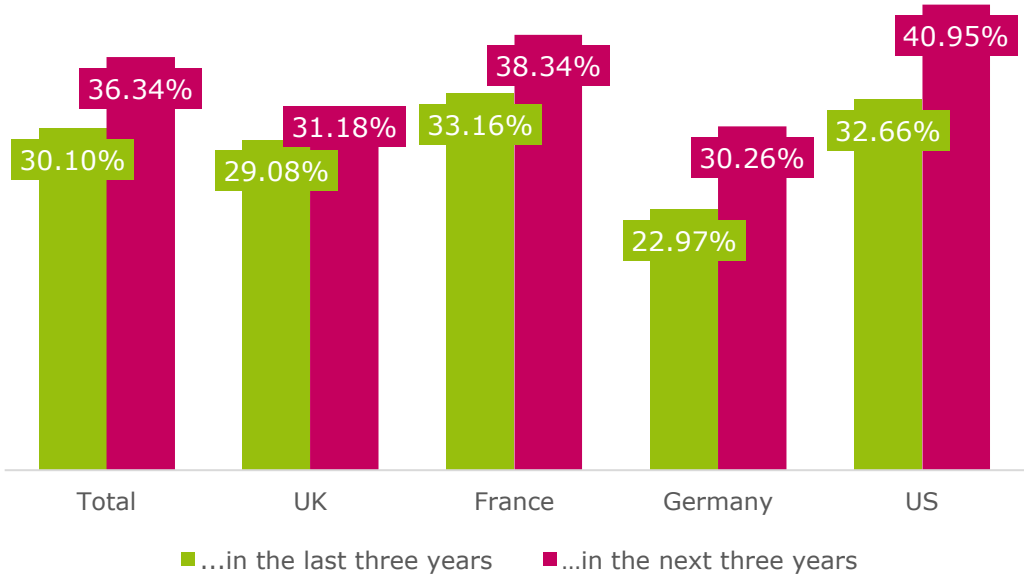


Figure 16: *Analysis showing the average percentage change in respondents' organizations' cybersecurity spending in the last three years, and predicted percentage change in the next three years, split by country, asked to all respondents (500)*

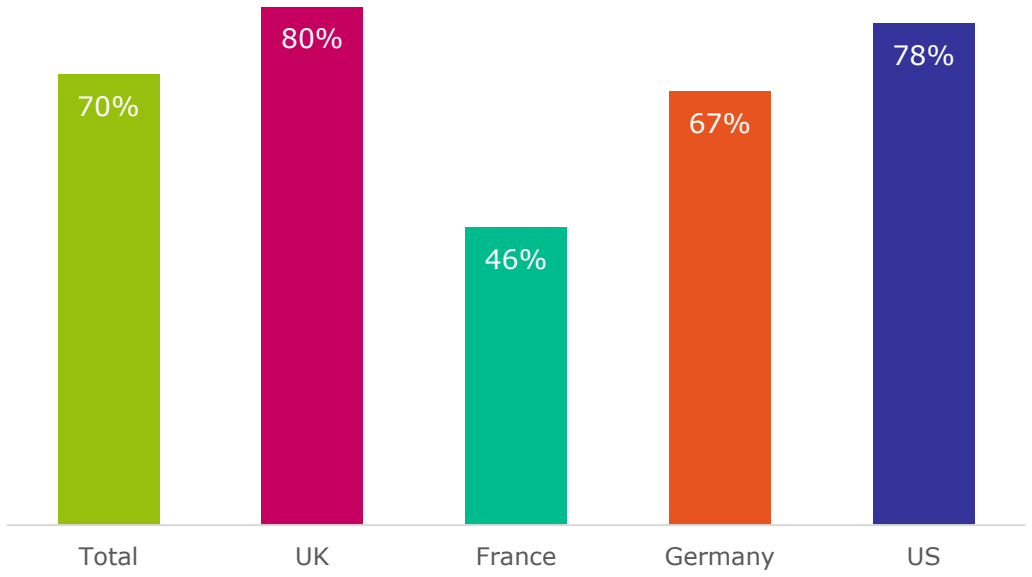


Figure 17: *Analysis showing the percentage of respondents who agree with the following statement: "Greater expenditure on security doesn't necessarily mean stronger security", split by country, asked to all respondents (500)*

VansonBourne

Infrastructure/processes for a breach

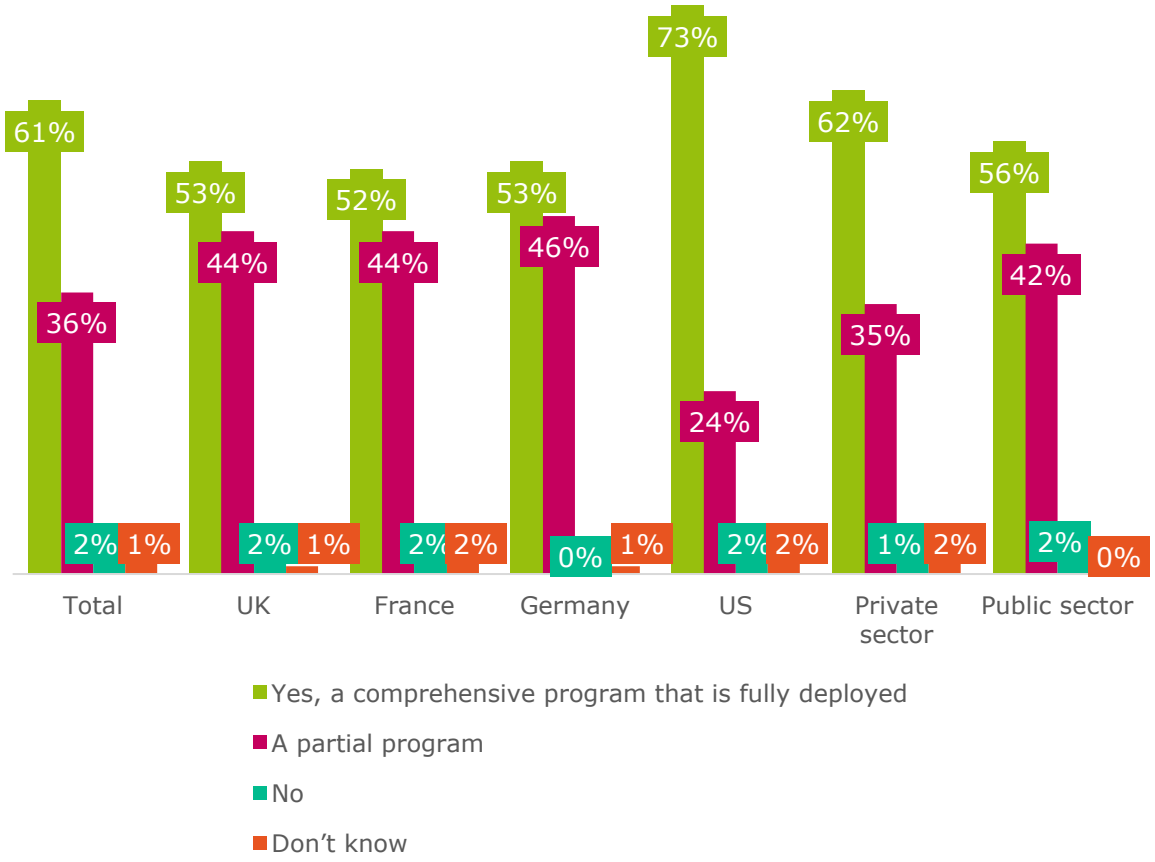


Figure 18: "Does your organization have infrastructure and/or processes in place to identify, notify and remedy a breach?*", split by country and sector, asked to all respondents (500)*

Around four in ten (39%) respondents' organizations do not have a comprehensive, fully deployed program…

…and/or processes in place for identifying, notifying and remedying a breach

It shows that they are leaving themselves unnecessarily vulnerable as they do not have rigorous processes in place to protect their organization efficiently

The story is slightly more positive in organizations from the US, where 73% have a comprehensive program fully deployed, but there is still room for improvement across all countries

What are the roadblocks to identifying and reporting a breach?

VansonBourne

Roadblocks to identifying and reporting a breach

Collaboration amongst teams (48%) is the most commonly reported roadblock to identifying and reporting a breach

However, there are many roadblocks being experienced by large proportions of organizations including knowing which data is important to protect (44%) and knowing where data is located (39%). These roadblocks appear to be universal, which shows that there is work to be done in all areas and as previously seen, it is not just a case of increasing expenditure because this is not the best solution

Organizations need to regain control of their data and also improve collaboration between teams before they can start to move forwards

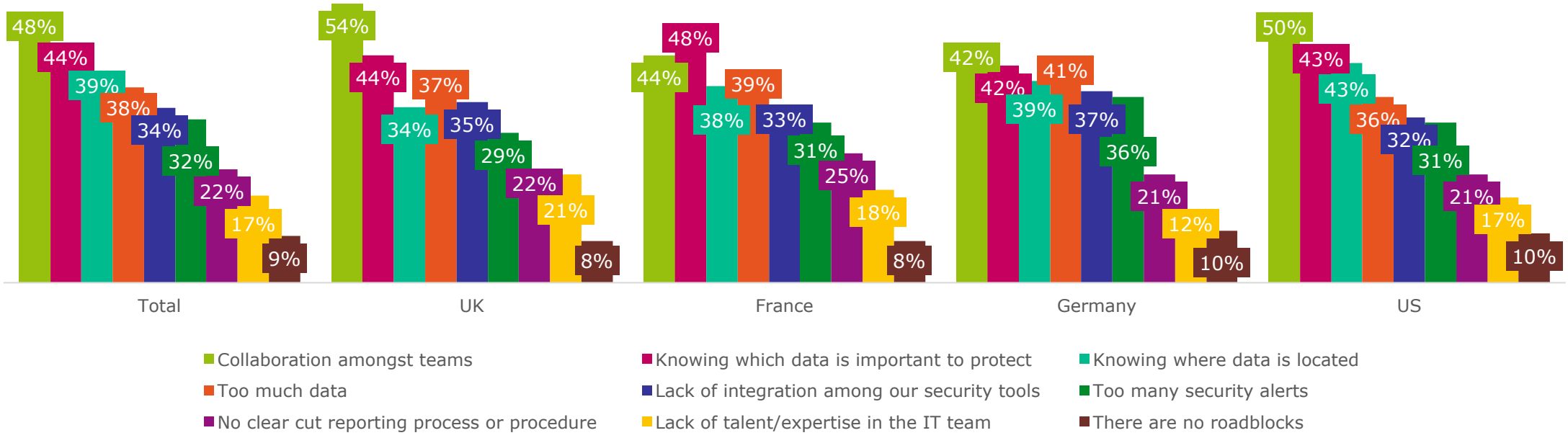


Figure 19: "In your organization, what are the most important roadblocks to identifying and reporting a breach? Combination of responses ranked first, second and third", *split by country, asked to all respondents (500)*

VansonBourne

Keeping up with increasing numbers of attacks

Only just over a quarter (27%) of respondents believe that their organization's security infrastructure has totally kept up with the increase in threats and attacks. This is hardly surprising considering that 39% of organizations do not have comprehensive, fully deployed infrastructure and/or processes to identify, notify and remedy a breach (fig. 18)

As seen with regard to the amount of time it takes to identify and report on a breach, organizations from the business and professional services sector (19%) are lagging when it comes to totally keeping up with threats and attacks

The threat landscape is continuously changing, and organizations need to adjust how to approach their security to ensure they are one step ahead

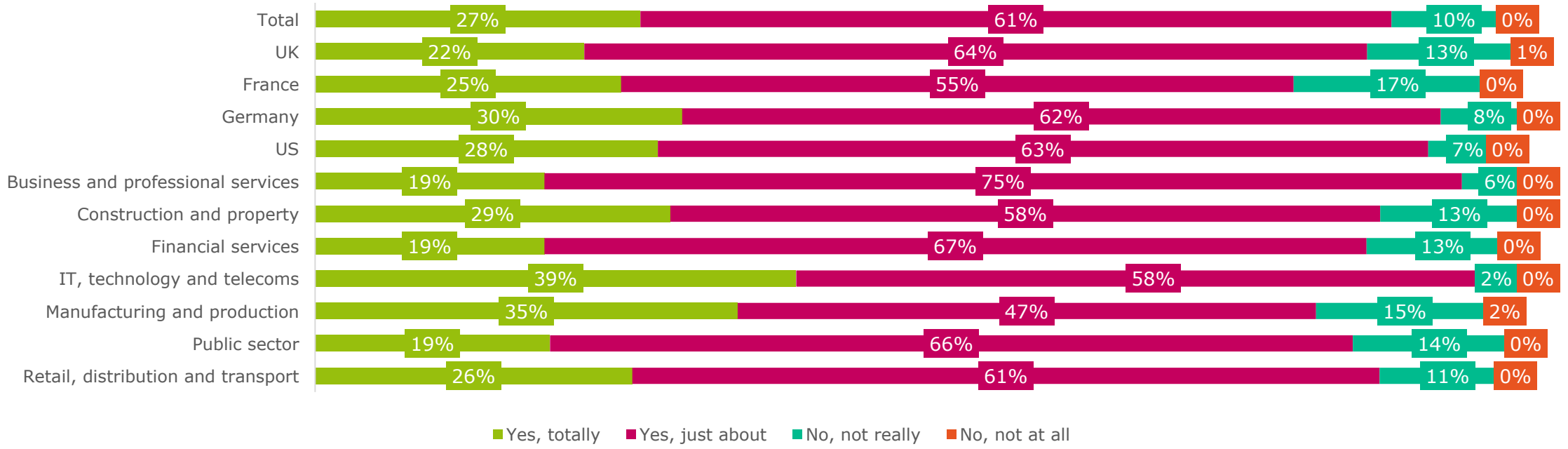


Figure 20: *Analysis showing whether respondents believe that their organization's security infrastructure has kept up with the increase in threats and attacks, excluding "Don't know" answers, split by country and sectors with a base greater than 30, asked to all respondents (500)*

VansonBourne

4: GDPR

VansonBourne

EU GDPR awareness

With only a few more months to go until GDPR becomes mandatory, 59% of respondents believe that their organization has not started to develop programs, policies and notification processes or are even still unsure of what the GDPR entails

The EU GDPR comes into effect in less than one years' time meaning that time is running out for organizations to implement the necessary policies and notification processes or they risk being heavily fined for non-compliance

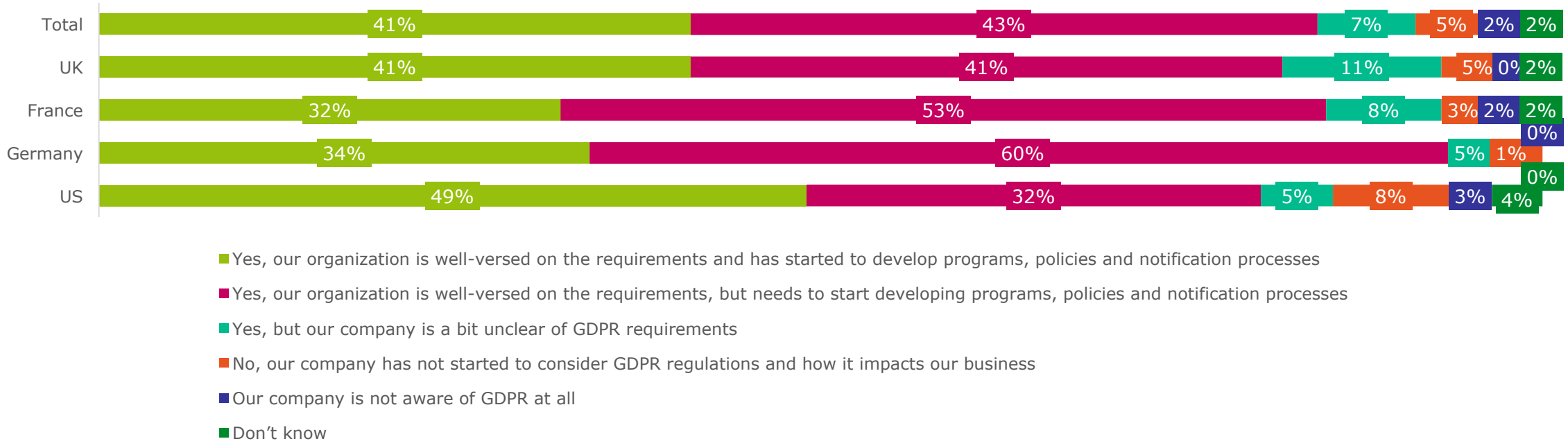


Figure 21: "Is your organization aware of the breach notification requirements of the European Union's GDPR?"*, split by country, asked to all respondents (500)*

VansonBourne

EU GDPR strategy and spend

Similarly, 57% of respondents report that their organization does not have a robust strategy outlined for the GDPR (fig. 22), with only 24% of respondents' organizations' IT budgets being allocated to GDPR compliance, on average (fig. 23)

The proportion of organizations who have a robust strategy outlined drops to 32% in the public sector (fig. 22)

This lack of readiness must be a serious cause for concern for these organizations because, if they are not compliant by the May 2018 deadline, then the fines imposed could have crippling side effects

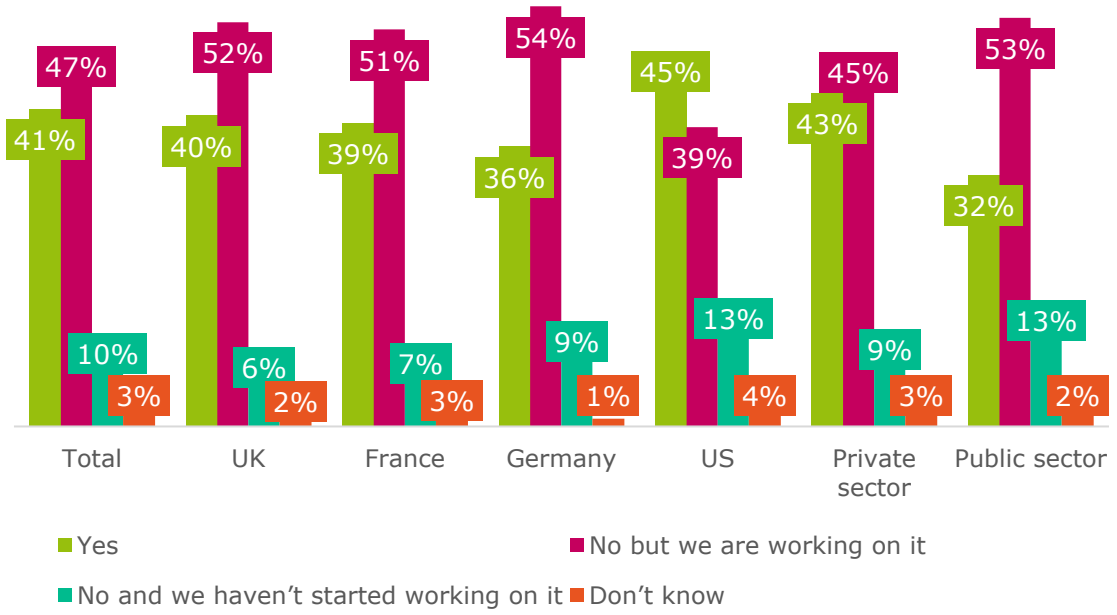


Figure 22: "Do you have a robust GDPR strategy outlined for your organization?", *split by country and sector, asked to all respondents (500)*

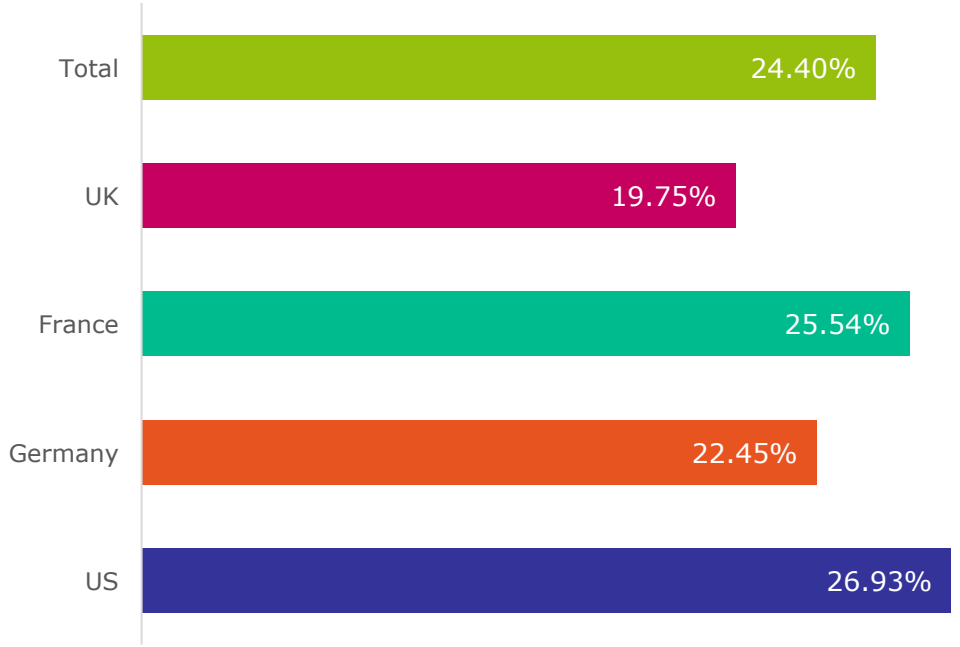


Figure 23: *Analysis showing the average percentage of respondents' organizations' IT budgets that have been dedicated to GDPR compliance, split by country, asked to all respondents (500)*

VansonBourne

NetOps/SecOps readiness for GDPR

Two thirds (66%) of surveyed IT decision makers agree that a lack of visibility over data makes GDPR compliance difficult (fig. 24), and this could be contributing to why only 59% of respondents believe that their organization's network/security operations will be fully ready to execute GDPR policies and programs by the May 2018 deadline (fig. 25)

Respondents from organizations in France are the least confident (44%) that they will be fully ready (fig. 25)

Network visibility has already been cited as a problem by respondents (fig. 9) and it not only has implications for data protection, but GDPR compliance also – organizations could be at risk of a security incident and/or large financial penalties if they are not compliant

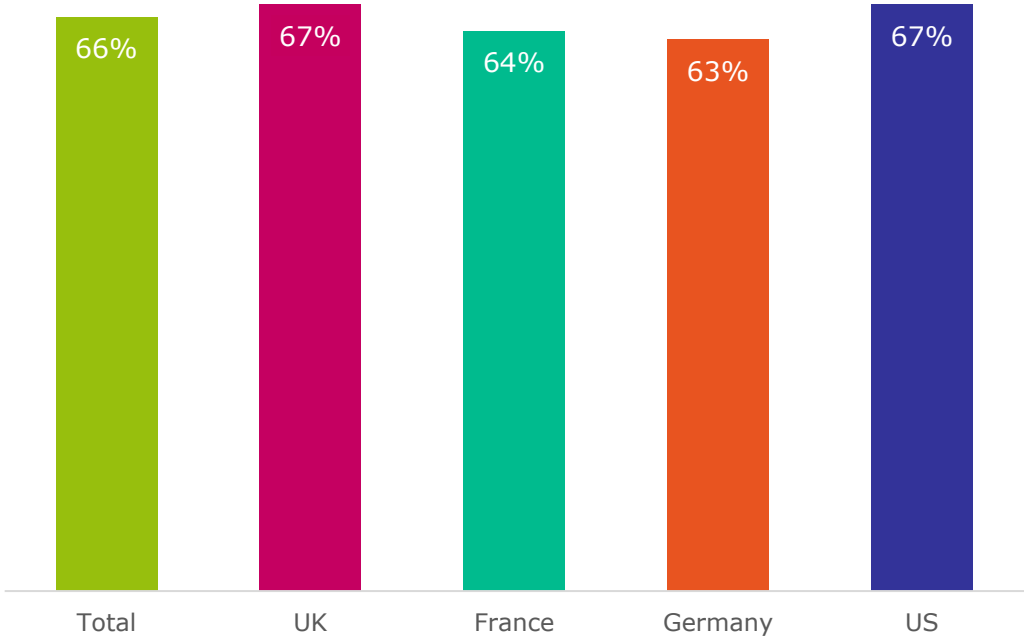


Figure 24: *Analysis of respondents who agree with the following statement: 'A lack of visibility over data makes GDPR compliance difficult', split by country, asked to all respondents (500)*

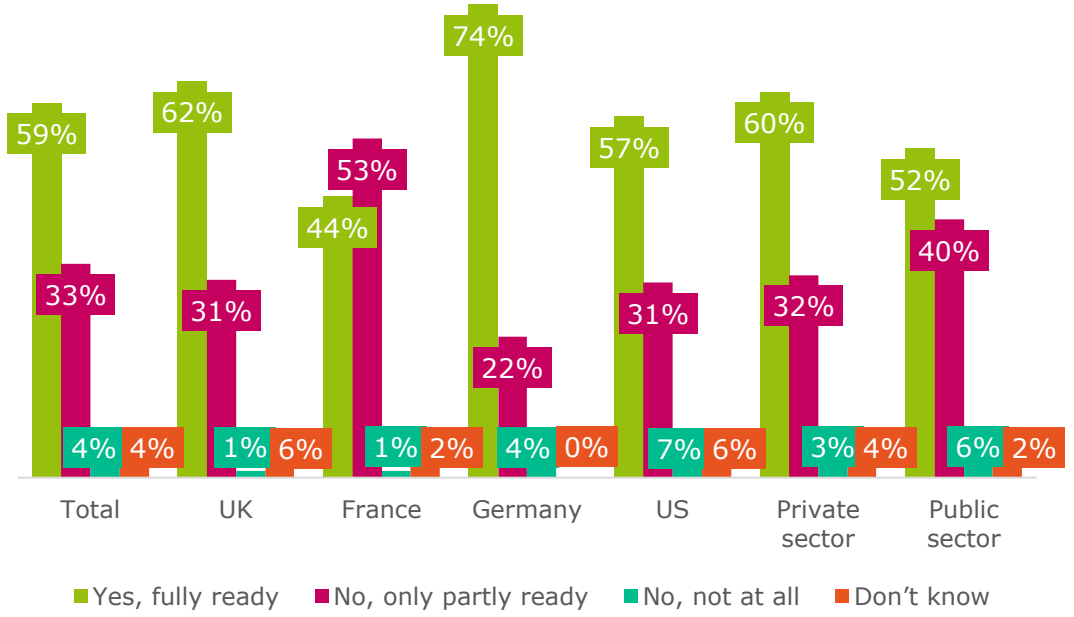


Figure 25: "Will your organization's network/security operations be ready to execute GDPR policies and programs by the May 2018 deadline?", *split by country and sector, asked to all respondents (500)*

VansonBourne

In summary…

- There appears to be a clear movement towards the cloud, with only 37% of respondents reporting that the majority of their organization's application workloads are currently located in a public or private cloud environment, but 73% believing this will be the case in three years' time
- Respondents report that their organization is migrating the "crown jewels" to the cloud – corporate information (56%) and personally identifiable information (47%)
- 43% of respondents' organizations do not have complete visibility into all of the data traversing their network
- 78% of respondents agree that data is most siloed between SecOps and NetOps, and 49% agree that their hybrid cloud environment prevents them from seeing where their data really is
- Over two thirds (67%) of those surveyed report that network blind spots are a major obstacle to data protection in their organization
- 40% of respondents cite cloud security as a major concern holding their organization back from using the latest technologies
- Cybersecurity spending is predicted to increase by 36% in the next three years, on average, but this does not necessarily mean stronger security according to 70% of respondents
- Only 59% of surveyed IT decision makers believe that their organization's network/security operations will be fully ready to execute GDPR policies and programs by the May 2018 deadline

VansonBourne

Hide and seek - Cybersecurity vs. the cloud

Merritt Gigamon
Research results

July 2017

VansonBourne