Infoblox
NEXT LEVEL NETWORKING

GLOBAL SURVEY

Zogby Analytics

COVID-19 Challenges for the Borderless Enterprise

A 2020 Global Survey of IT Decision-Makers

TABLE OF CONTENTS

Executive Summary

Prior to the COVID-19 crisis, 21% of organizations globally had over half of their workforce working remotely. China, Germany and Australia had the fewest such workers, while the US had the most.

The COVID-19 crisis has forced companies to become “borderless,” pushing these numbers up in both the short- and, it appears, long-term. The “borderless enterprise” is one that is characterized by high levels of remote work, high adoption of cloud-based services and applications, and a large number of dispersed IoT, mobile and other devices.

In every country surveyed, businesses had to go borderless to survive the crisis. Globally, 70.1% of companies had over half of their workforce working remotely due to the pandemic. Furthermore, the crisis affected expectations going forward with 40% of surveyed organizations globally now expecting more than half of their workforce to be working remotely—nearly double the pre-pandemic percentage. Clearly, the borderless enterprise is here to stay.

Accelerating the Adoption of the Borderless Enterprise

The sudden jump in the need to work from home did not catch businesses around the world flat-footed. An overwhelming majority of surveyed businesses report being at least somewhat prepared when it came to having the right technology or cybersecurity in place for their employees to work remotely. The US and Australian businesses were best prepared for the transition to a borderless enterprise, while the UK, Japan and China reported lower, but still high, levels of preparedness.

Distributing approved devices, building network infrastructure and securing users’ network/Internet activity were the biggest tech-related challenges organizations faced in transitioning to work from home. However, the relative challenges they posed differed among surveyed countries. In the US and the UK, securing network activity was the biggest challenge, followed by the distribution of approved devices. In China and Germany, building network infrastructure, followed by distributing approved devices were perceived as the biggest challenges.

Prior to the pandemic and associated shutdown, VPN access, secure DNS, secure web gateway, and cloud security solutions like cloud access security broker were the most commonly provided network cybersecurity services. While Germany and Japan followed the global pattern of provision, other countries had more distinct profiles. In China, secure DNS and secure web gateway were available at a much higher proportion than globally. In contrast, the US lagged the global numbers in three out of four categories, but especially in secure web gateway. The pandemic didn’t move these numbers much.

These new services are overwhelmingly perceived as effective in securing employees and protecting networks, both globally and among individual countries surveyed. Almost all surveyed decision-makers rate them as at least somewhat effective, including 50% who rate them as very effective. Surveyed decision-makers in Australia and the US were the most enthusiastic, while those in China were more reserved.

But the Pandemic Still Drove Change

The addition of secure DNS and endpoint security, followed by the addition of AI to detect anomalous behavior, multi-factor authentication, DDI for network and device visibility and security as a service offering were the most common actions taken to secure networks and employees while teleworking during the shutdown. Adding secure DNS was particularly common in China and Australia.

Only a small proportion of organizations have not shifted IT resources as a result of the COVID-19 pandemic. However, diametrically opposed approaches were almost equally common. Globally, 46% of surveyed organizations shifted IT resources towards cybersecurity to protect their network, while 38% shifted resources away from cybersecurity to help set up remote workers. Organizations in China, Australia, the UK and the US were all significantly more likely to shift IT resources towards cybersecurity to protect their networks while those in Japan and Germany were more likely to shift IT resources away from cybersecurity to help set up remote workers. As a result of the COVID-19 pandemic, the healthcare industry is moving resources away from cybersecurity while the finance/banking industry is moving them towards it.

Also as a result of the crisis, over half of organizations globally, as well as in each individual country surveyed, have changed at least some policies about the use of personal applications—such as Skype, WhatsApp, Zoom and Houseparty—on work devices. In each country, the number of organizations that now allow these apps is higher than the number of organizations that prohibited them in response to the pandemic. In fact, the percentage of organizations globally that allow these applications rose by 50%, from 42.0% before the crisis to 63.1% after.

Challenges and Opportunities for the Future

Approximately half of surveyed businesses globally, as well as in individual countries, have changed their cybersecurity plans for the time when the employees return to the offices. In addition, roughly a third of businesses have not yet changed their plans, but intend to do so.

People preferring working from home and more people bringing their own devices to the office are top challenges surveyed decision-makers expect to face when they return to the office after the crisis. The concern that people will prefer working from home is particularly high in the US and Japan–in contrast, it is relatively low in China. Conversely, the concern that more employees will be bringing their own devices to the office is most prevalent in China and relatively less so in the US.

Half of surveyed businesses globally are seeing more attempted cyberattacks, while a quarter are seeing fewer. The biggest increase in attempted cyberattacks was reported from China and Australia, while the UK and Japan are seeing the smallest increases in the number of attempted attacks. Malware exploits targeting the edge and phishing and other social engineering attacks were the most common types of attacks noticed by our global respondents.

Cloud-managed DDI, multi-factor authentication and DNS security, followed by VPN usage are the most common additional investments surveyed organizations globally plan to make in remote-working technologies or infrastructure. Only 6% of surveyed organizations do not intend to make any additional investments, most often because their organization was already prepared for remote work or because other investments were deemed to have higher priority.

There exists a significant variability in investment strategies among the countries surveyed. Cloud-managed DDI is the most invested-in technology in China, Australia, the UK and the US. In contrast, 80% of surveyed organizations in Japan plan to invest in VPN usage, a technology that businesses in other surveyed countries put relatively less emphasis on. Companies with large revenues plan to invest more in all listed remote-working technologies.

Fewer than 10% of surveyed business decision-makers–both globally and in all individual countries–do not consider investments in their digital and cloud-managed services a priority. Everyone else is either re-evaluating their digital transformation and cloud strategy or has already made significant investment in their digital and cloud-managed services. The UK organizations lead the way with almost half already having made the investments. In China, Germany, Japan, the US and Australia, over half of surveyed organizations report re-evaluating their digital transformation and cloud strategy.

Organizations in healthcare and software and IT industries are more likely to be currently re-evaluating their cloud strategy while those in the finance/banking industry are more likely to have already made the investments.

Lack of team expertise is the biggest obstacle organizations, both globally and in China and Japan, face in moving more operations to the cloud. However, cost is also a significant consideration, especially in Germany, Australia, the UK and the US. While uncertainty regarding security compliance in the cloud is relatively less important, it is still a significant obstacle both globally and in all countries individually, especially Japan, Australia, and the UK.

Better threat detection and/or mitigation for remote work tools, better visibility into devices connecting to the corporate network, visibility into all cloud apps employees are using and better visibility into devices that are compromised would all help enable more remote work for employees, both globally and in all countries surveyed. Better threat detection is considered particularly helpful in China, Australia and Germany, while better visibility into devices that are compromised is relatively more valued in Japan than in other countries.

Methodology and Sample Characteristics

Zogby Analytics was commissioned by Infoblox, Inc. to conduct an online survey of 1,077 IT business decision-makers in nine countries: Australia, China, Germany, Japan, the Netherlands, Singapore, Spain, the UK and the US.

Using internal and trusted interactive partner resources, thousands of business decision-makers were randomly invited to participate in this interactive survey. Each invitation was password coded and secure so that one respondent could only access the survey one time.

Based on a confidence interval of 95%, the margin of error for 1,077 is +/- 3.0 percentage points. This means that all other things being equal, if the identical survey were repeated, its confidence intervals would contain the true value of parameters 95 times out of 100. Margins for nine countries are shown in the following table.

Sample	No. of completes	Field Dates	MOE
Australia	77	7/23/2020 – 7/27/2020	+/- 11.2 Percentage Pts
China	203	7/23/2020 – 7/27/2020	+/- 6.9 Percentage Pts
Germany	150	7/23/2020 – 7/28/2020	+/- 8.0 Percentage Pts
Japan	102	7/23/2020 – 7/27/2020	+/- 9.7 Percentage Pts
Netherlands	27	7/23/2020 – 7/28/2020	+/- 18.9 Percentage Pts
Singapore	30	7/23/2020 – 7/27/2020	+/- 17.9 Percentage Pts
Spain	32	7/23/2020 – 7/27/2020	+/- 17.3 Percentage Pts
UK	202	7/23/2020 – 7/27/2020	+/- 6.9 Percentage Pts
US	254	7/23/2020 – 7/27/2020	+/- 6.2 Percentage Pts

Subsets of the data have a larger margin of error than the whole data set. As a rule we do not rely on the validity of very small subsets of the data especially sets smaller than 50-75 respondents. For this reason, country-level data from the Netherlands, Singapore and Spain are not included in the charts or discussed in the text.

Additional factors can create error, such as question wording and question order.

About Zogby Analytics:

Zogby Analytics is respected nationally and internationally for its opinion research capabilities. Since 1984, Zogby has empowered clients with powerful information and knowledge critical for making informed strategic decisions.

The firm conducts multi-phased opinion research engagements for banking and financial services institutions, insurance companies, hospitals and medical centers, retailers and developers, religious institutions, cultural organizations, colleges and universities, IT companies and Federal agencies. Zogby's dedication and commitment to excellence and accuracy are reflected in its state-of-the-art opinion research capabilities and objective analysis and consultation.

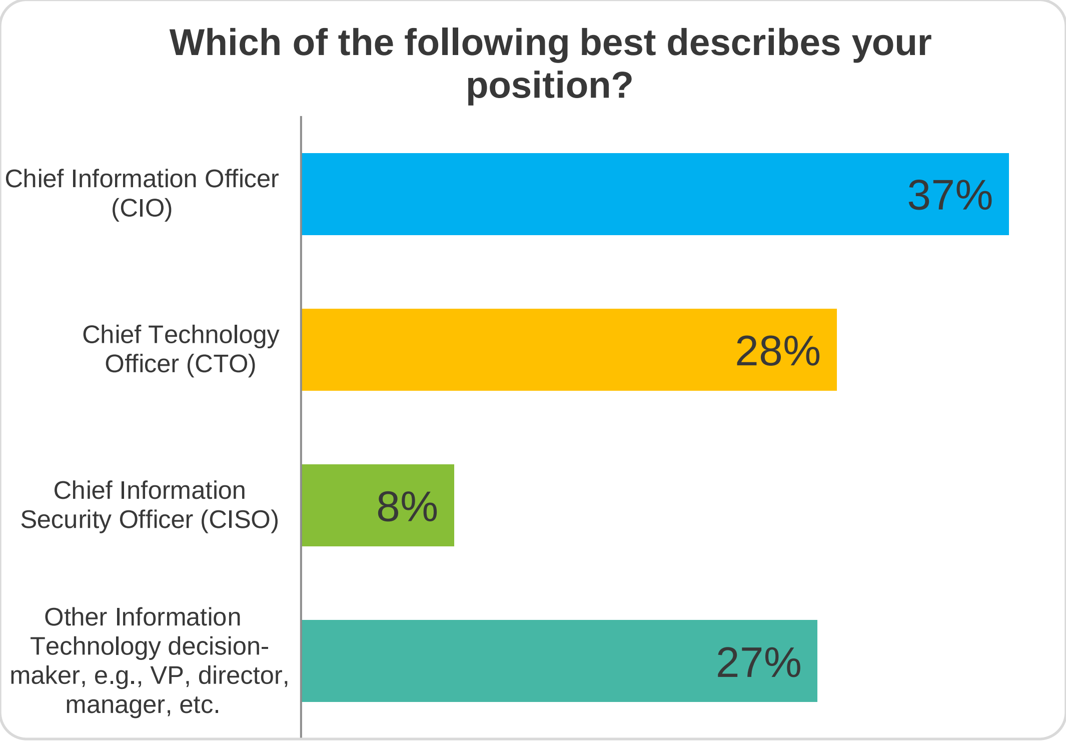
Location of Respondents

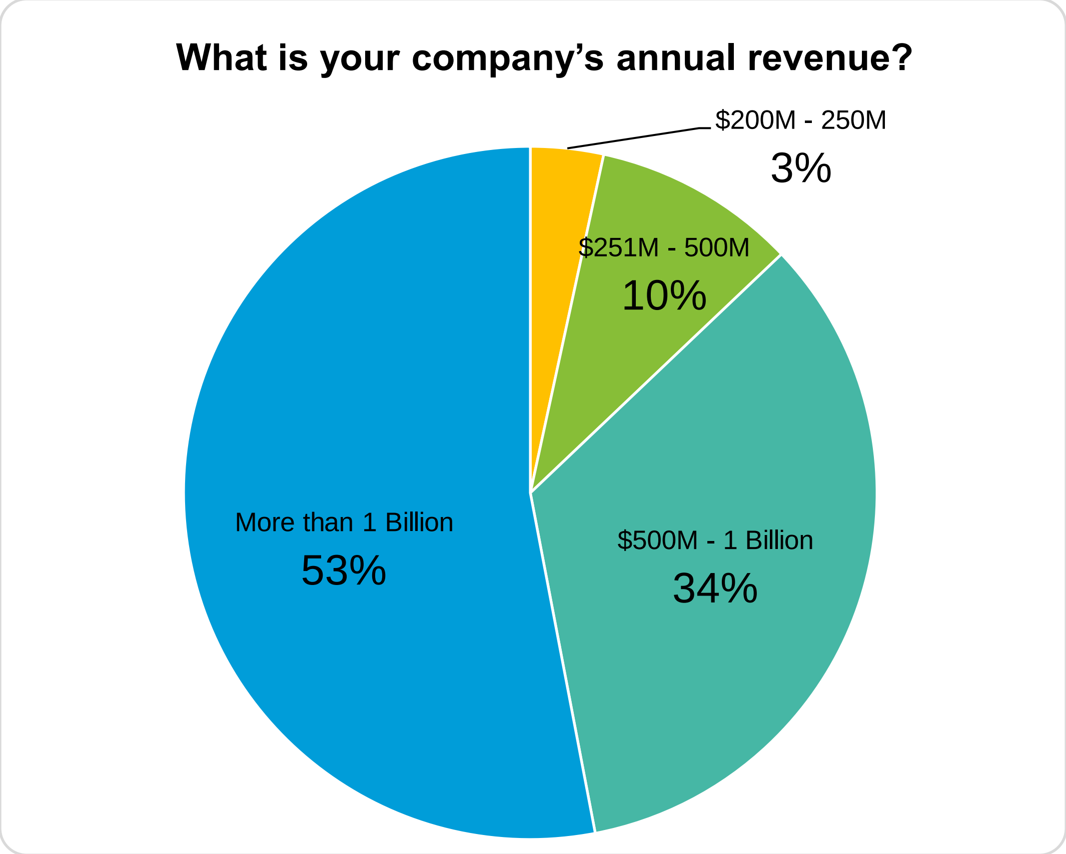
Country	Frequency	Valid Percent*
Australia	77	7
China	203	19
Germany	150	14
Japan	102	10
Netherlands	27	3
Singapore	30	3
Spain	32	3
UK	202	19
US	254	24

*Percentages may not equal 100% due to rounding.

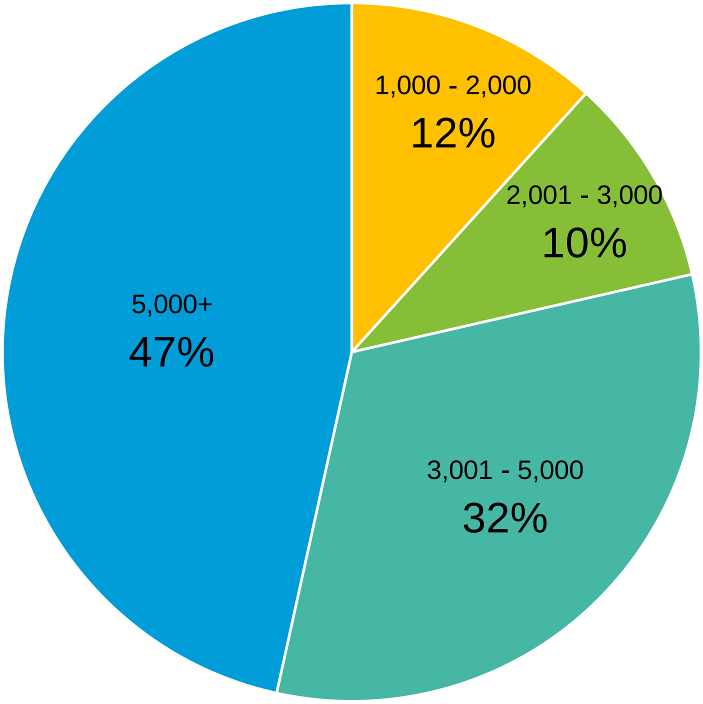
What industry is your company in?

Industry	Frequency
Hardware	25
Software	114
Telecommunications	68
Security	14
Value Added Reseller	2
Food and Beverages	11
Electronics	15
Technology	75
IT Services	253
Biotech / Pharmaceuticals	22
Infrastructure / Construction	35
Automobile / Transportation	27
Finance / Banking	96
Healthcare	131
Media / Entertainment	2
Retail	80
Energy	19
Real Estate	8
Utilities	12
Education	13
Agriculture	2
Government	18
Legal Services / Lawyer	2
Insurance	14
Business / Consulting Services	12
Manufacturing	7


Which of the following best describes your position?
Chief Information Officer (CIO)
37%
Chief Technology Officer (CTO)
28%
Chief Information Security Officer (CISO)
8%
Other Information Technology decision-maker, e.g., VP, director, manager, etc.
27%


What is your company's annual revenue?
$200M - 250M
3%
$251M - 500M
10%
$500M - 1 Billion
34%
More than 1 Billion
53%

Which of the following best describes the number of employees in your company?



Survey Highlights

The Pandemic Accelerated the Shift to a Borderless Enterprise

Key trends in business technology and employee preferences were driving businesses to adopt the basic characteristics of the “borderless enterprise,” even prior to the COVID-19 crisis. Indeed, remote work in particular was globally present in notable but far from overwhelming numbers. The numbers were lowest in China, Germany and Australia and highest in the US. Thus, before the pandemic, a vast majority (79%) of surveyed organizations had fewer than half of employees working remotely, while only 1 in 10 organizations in China (90% of surveyed organizations had fewer than 50% of employee working remotely), Germany (88%) and Australia (87%) had more than half of employees working remotely. The US had the most remote workers with more than a third (37%) of surveyed organizations reporting that more than half of their employees worked remotely.

The COVID-19 crisis has had a tremendous impact on the adoption of remote work and the transition to a borderless enterprise. During the crisis, in all surveyed countries, more than half of organizations had over 50% of their workforce working remotely. Germany (53% of organizations had more than 50% of employees working remotely), China (63%) and Australia (68%) again had fewest such workers, while the US (80% of organizations had more than 50% of employees working remotely) had the most. The impact was especially strong among businesses with relatively fewer employees–globally, 79% of all surveyed businesses with 1,000-3,000 employees had more than half of their workforce working from home during the COVID-19 crisis (compared to 64% for businesses with more than 5,000 employees). The healthcare industry was the least affected by the crisis (50% of surveyed organizations have more than half of their workforce working from home) and finance/banking industry was the most (88%).

The crisis, in turn, affected expectations going forward. Clearly, the borderless enterprise is here to stay. Globally, 40% of surveyed organizations expect more than half of their workforce to be working remotely–a number nearly double the initial 21%, though lower than the 70% observed during the peak of the crisis. Germany (17% of surveyed businesses expect more than half of their employees to continue to work remotely following the crisis) and China (16%) expect the smallest changes from the initial levels. In contrast, the US (58% – 21 percentage points higher than already high level of remote work before crisis), Japan (54% – 28% percentage points higher than before the crisis) and the UK (46% – 27% percentage points higher than before the crisis) expect the largest shifts in the transition to a borderless enterprise. Fifty-seven percent of businesses in the software industry expect to have more than half of employees working remotely after the crisis (this was the highest level among all industries with good representation in the survey sample; it was 36% before the crisis and 78% during it).

Preparedness Was a Critical Factor in the Transition

An overwhelming majority (85% “very prepared” and “somewhat prepared” combined) of surveyed businesses report being at least somewhat prepared when it came to having the right technology or cybersecurity in place for their employees’ work from home. US (54% “very prepared”) and Australian (52%) businesses were best prepared, while the UK (32% “very prepared”), Japan (38%) and China (38%) reported lower, but still high, levels of perceived preparedness.

Distributing approved devices (35% globally reported this as their biggest tech-related challenge), building network infrastructure (35%) and securing users’ network/Internet activity (29%) were the biggest tech-related challenges organizations faced in transitioning to work from home. However, the relative challenges they posed differed among surveyed countries. In the US and the UK, securing network activity was the biggest challenge (38% in the US, 39% in the UK), followed by distribution of approved devices (35% in the US, 31% in the UK). On the other hand, in China and Germany, building network infrastructure (44% in China, 43% in Germany), followed by distribution of approved devices (40% in China, 32% in Germany) were perceived as the biggest challenges. Distributing approved devices was seen as the biggest challenge in software (48%) and IT services (40%) industries, while building network infrastructure (40%) and securing network activity (37%) were the biggest challenges in the finance/banking industry (40%).

Prior to the pandemic, VPN access (72%), secure DNS (67%), secure web gateway (59%) and cloud security solutions like cloud access security broker (55%) were the most commonly provided network cybersecurity services. While Germany and Japan followed the global pattern of provision, other countries had more distinct profiles. In China, secure DNS (86%) and secure web gateway (80%) were available at much higher proportion than globally. In contrast, the US lagged the global numbers in three out of four categories, but especially in secure web gateway (46% of US businesses provided this technology compared to 59% globally and 80% in China).

The pandemic didn’t move these numbers much. Global numbers remained essentially unchanged. The most notable changes were an increase in availability of cloud security solutions in Japan (from 42% to 59%) and a decrease in VPN access in Australia (from 82% to 74%).

These new services are overwhelmingly perceived as effective in securing employees and protecting networks, both globally and among individual countries surveyed. Thus, 93% (“very effective” and “somewhat effective” combined) of surveyed decision-makers rate them as at least somewhat effective, including 50% who rate them as very effective. Surveyed decision-makers in Australia (68% rated the services as “very effective”) and the US (64%) were the most enthusiastic, while those in China (34% rated them as “very effective” though 62% rated them as “somewhat effective”) were a bit more reserved.

Addition of secure DNS (60% did so globally) and endpoint security (54%), followed by addition of AI to detect anomalous behavior (50%), multi-factor authentication (48%), DDI for network and device visibility (47%) and security as a service offering (46%) were the most common actions taken to secure networks and employees as a result of the pandemic. Adding secure DNS was particularly common in China (78%) and Australia (71%). In Japan, 20% of businesses have not taken any additional action, by far the highest among all the countries surveyed. The US and the UK organizations were also, overall, less likely than those in other countries to undertake specific additional actions.

Enterprises Revisited Their Plans and Policies

Only a small proportion of organizations (16% globally–highest in Japan at 24%) have not shifted IT resources as a result of the COVID-19 pandemic. However, diametrically opposed approaches were almost equally common. Globally, 46% of surveyed organizations shifted IT resources towards cybersecurity to protect their network, while 38% shifted resources away from cybersecurity to help set up remote workers. Organizations in China (56% towards security, 39% away from it), Australia (53% vs. 35%), the UK (48% vs. 32%) and the US (48% vs. 35%) were all significantly more likely to shift IT resources towards cybersecurity to protect their networks. In contrast, surveyed organizations in Japan (56% shifted resources away from IT security, 26% towards it) and Germany (45% away, 34% towards) were more likely to shift IT resources away from cybersecurity to help set up remote workers. As a result of the COVID-19 pandemic, the healthcare industry is moving resources away from cybersecurity (60% away, 35% towards), while the finance/banking industry is moving them towards it (54% towards, 26% away).

Also as a result of the crisis, over half of organizations globally (69%), as well as in each individual country surveyed, have changed at least some policies about the use of personal apps, such as Skype, WhatsApp, Zoom and Houseparty, on work devices. In each country, the number of organizations that now allow these apps is higher than the number of organizations that prohibited them in response to the pandemic. In fact, the percentage of organizations globally that allow these applications rose by 50%, from 42% before the crisis to 63% after. However, the relative strength of these contradictory policies was different among surveyed countries. In Australia, in particular, there was a much stronger trend towards allowing the apps (57% vs. 14%) while things were much closer in China (46% vs. 31%) and the UK (39% vs. 23%). In the healthcare industry, 68% of organizations now allow apps that were previously prohibited. Similarly, high numbers (60%) are reported in the software industry. The finance/banking industry is more cautious as 36% of businesses allow apps that were previously prohibited and 31% prohibit apps that were previously allowed.

Approximately half of surveyed businesses globally as well as in individual countries have changed their cybersecurity plans for the time when the employees return to the offices. In addition, roughly a third of businesses have not yet changed their plans, but intend to do so. The number of organizations with no intention to change cybersecurity plans ranges from 3% in China to 17% in Japan. Companies with large revenues are more likely to have changed their cybersecurity plans–51% of companies with more than $1 billion in revenue have done so compared to 36% of companies with $250M-500M in revenue. Seventy-seven percent of organizations in the healthcare industry have already changed their cybersecurity plans for when their employees return to the office after the crisis, a number much higher than those observed in other industries.

People preferring working from home (63% anticipate this challenge globally), and more people bringing their own devices to the office (58%) are the top challenges surveyed decision-makers expect to face when they return to the office after the crisis. The concern that people will prefer working from home is particularly high in the US (73%) and Japan (73%); in contrast, it is relatively low in China (47%). Conversely, the concern that more employees will be bringing their own devices to the office is most prevalent in China (73%) and relatively less so in the US (50%).

Addressing the Growing Challenge of Cybersecurity in the COVID-19 Era

Half (47%) of surveyed businesses globally are seeing more attempted cyberattacks, while a quarter (25%) are seeing fewer. The biggest increase in attempted cyberattacks is reported from China (61% are seeing more such attempts) and Australia (55%), while the UK (37%) and Japan (39%) are seeing the smallest increases in the number of attempted attacks. Larger companies, both in terms of revenue and number of employees, are more likely to be the target of cyberattacks as a result of the COVID-19 crisis–52% of companies with more than $1 billion in revenue and 49% of companies with more than 5,000 employees are seeing more cyberattacks, compared to 37% of companies with $250M-500M in revenue and 40% of companies with 1,000-2,000 employees. Seventy percent of healthcare businesses and 65% of software businesses are seeing more attempted cyberattacks.

Malware exploits targeting the edge (74%) and phishing and other social engineering attacks (73%) were the most common types of attacks noticed by our global respondents. The same is true in each country surveyed though malware exploits tended to be relatively more common in Australia (89%) and China (83%) and relatively less common in the UK (62%), Japan (66%) and the US (67%).

Cloud-managed DDI (67%), multi-factor authentication (60%) and DNS security (59%), followed by VPN usage (54%) are the most common additional investments surveyed organizations globally plan to make in remote-working technologies or infrastructure. Only 6% of surveyed organizations do not intend to make any additional investments, most often because their organization was already prepared for remote work (44%) or because other investments were deemed to have higher priority (37%).

There exists a significant variability in investment strategies among the countries surveyed. Cloud-managed DDI is the most invested in technology in China (83%), Australia (77%), the UK (62%) and US (62%). In contrast, 80% of surveyed organizations in Japan plan to invest in VPN usage, a technology that businesses in other surveyed countries put relatively less emphasis on. Companies with large revenues plan to invest more in all listed remote-working technologies. The contrast is most pronounced with multi-factor authentication–66% of companies with more than $1 billion in revenue plan to invest in this technology, compared to 44% of companies with $250M-500M in revenue.

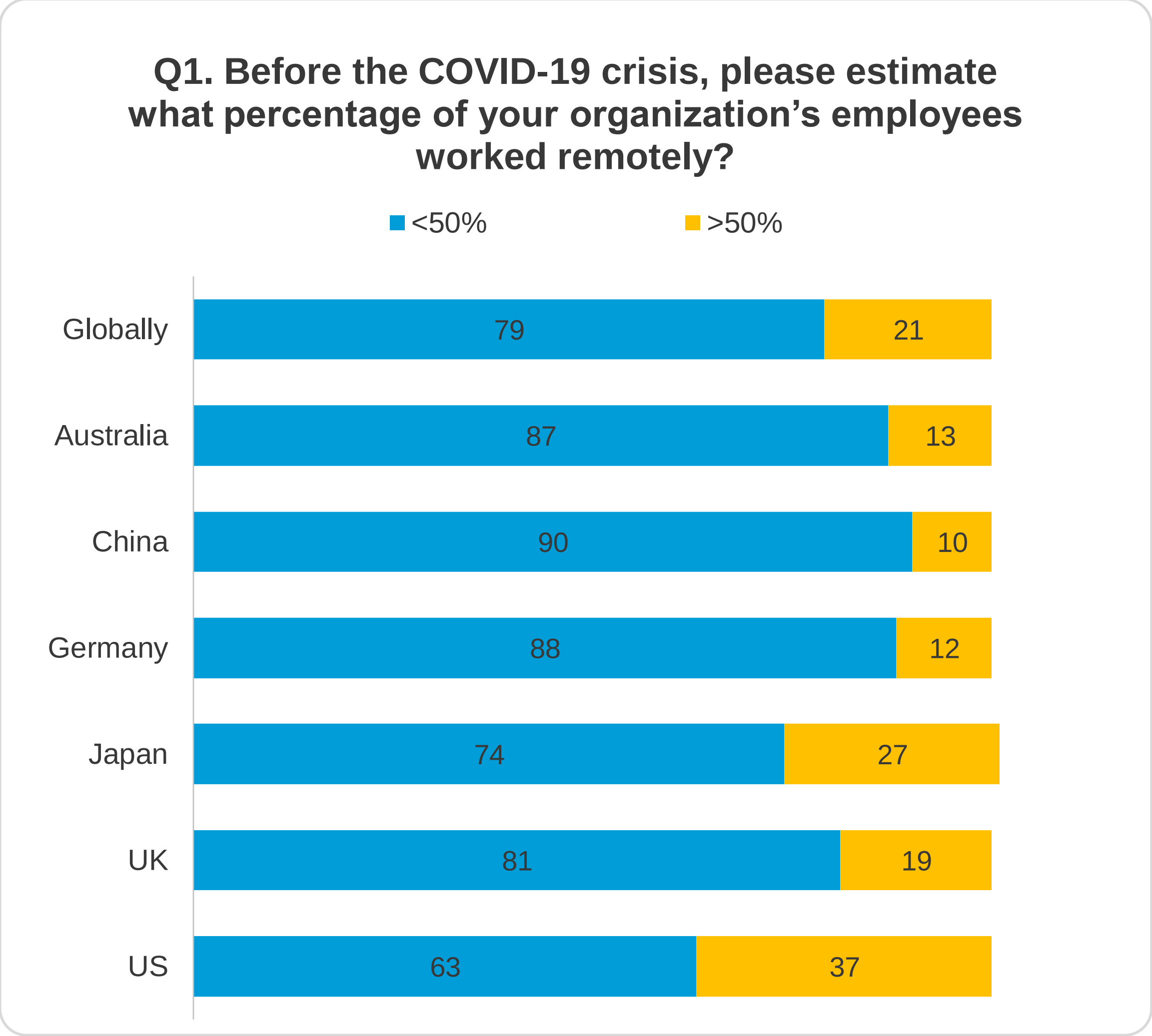
Preparing for the Post-COVID Future

Fewer than 10% of surveyed business decision-makers–both globally and in all individual countries–do not consider investments in their digital and cloud-managed services a priority. Everyone else is either re-evaluating their digital transformation and cloud strategy or has already made significant investment in their digital and cloud-managed services. The UK organizations lead the way with almost half (47%) already having made the investments, followed by Australia (44%). In China (60%), Germany (55%), Japan (54%), the US (54%) and Australia (53%), over half of surveyed organizations report re-evaluating their digital transformation and cloud strategy. In the healthcare industry, 73% of businesses are currently re-evaluating their cloud strategy while 25% have already invested significantly in cloud-managed services. A similar, albeit not so lopsided, ratio is reported in software and IT services industries. In the finance/banking industry, the ratio is reversed–54% of businesses have already invested significantly in cloud-managed services while 40% are currently re-evaluating their cloud strategy.

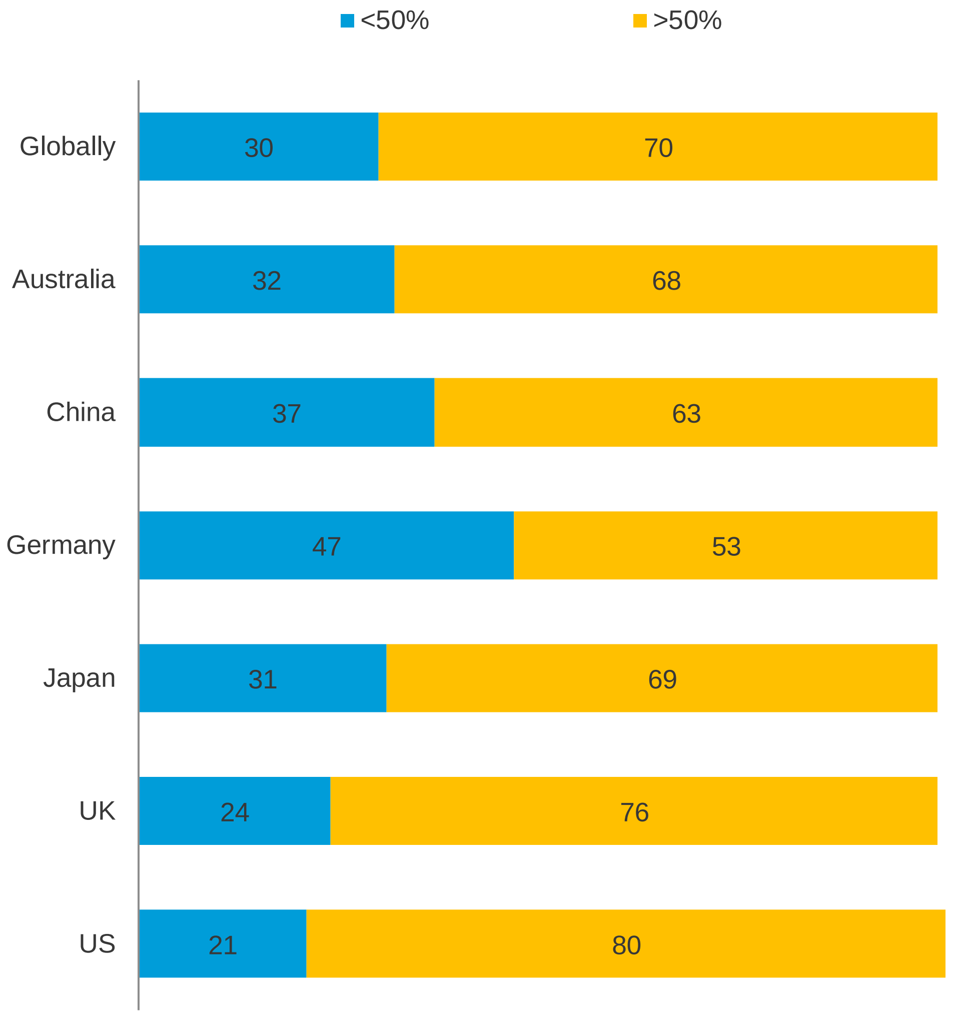
The lack of team expertise is the biggest obstacle organizations, both globally (33%) and in China (54%) and Japan (36%), face in moving more operations to the cloud. However, cost is also a significant consideration, especially in Germany (36%), Australia (35%), the UK (34%) and the US (32%). While uncertainty regarding security compliance in the cloud is relatively less important, it is still a significant obstacle both globally (25%) and in all countries surveyed, especially Japan (31%), Australia (29%), and the UK (27%).

Better threat detection and/or mitigation for remote work tools (68% of surveyed respondents globally say this would help enable more remote work for their employees), better visibility into devices connecting to the corporate network (65%), visibility into all cloud apps employees are using (61%) and better visibility into devices that are compromised (46%) would all help enable more remote work for employees, both globally and in all countries surveyed. Better threat detection is considered particularly helpful in China (80%), Australia (79%) and Germany (77%), while better visibility into devices that are compromised is relatively more valued in Japan (62%) than in other countries.

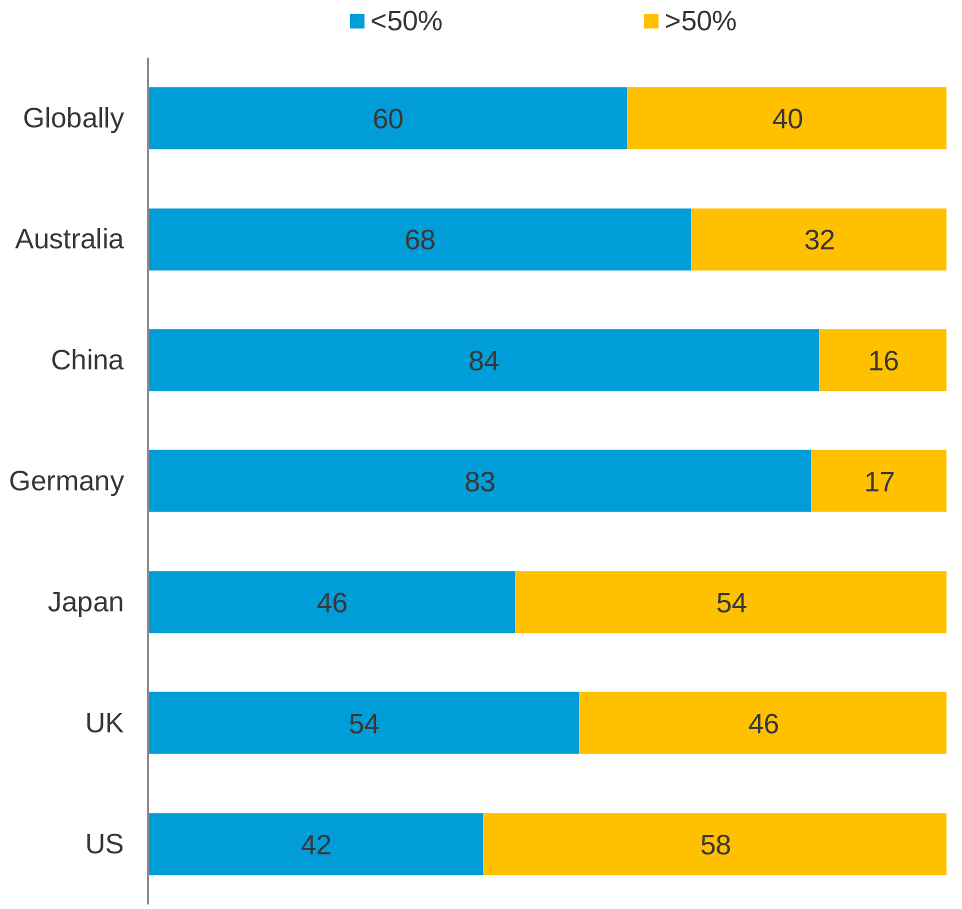
Graphs and Tables

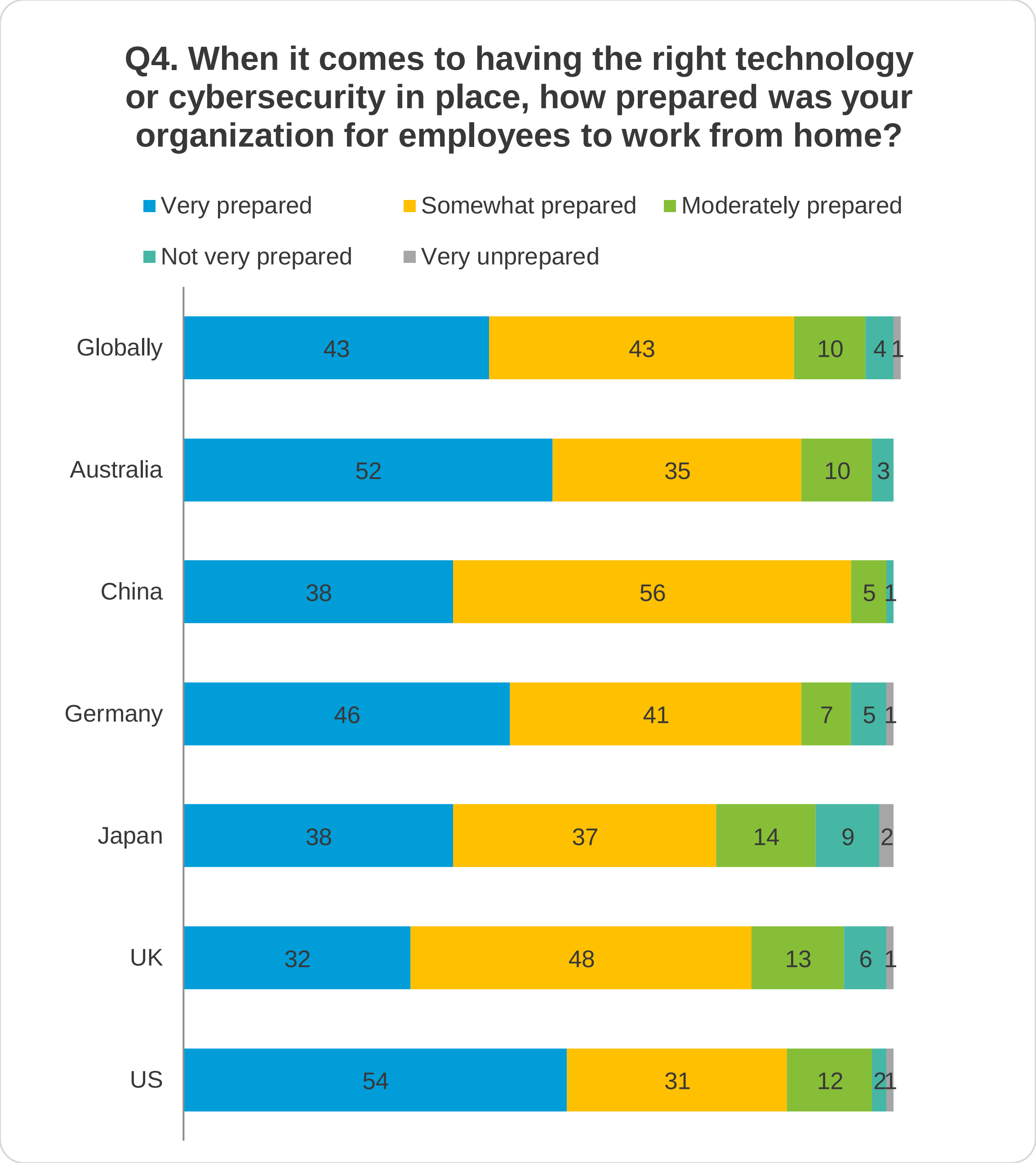


Q2. Please estimate what percentage of your organization’s employees are working from home during the COVID-19 crisis?



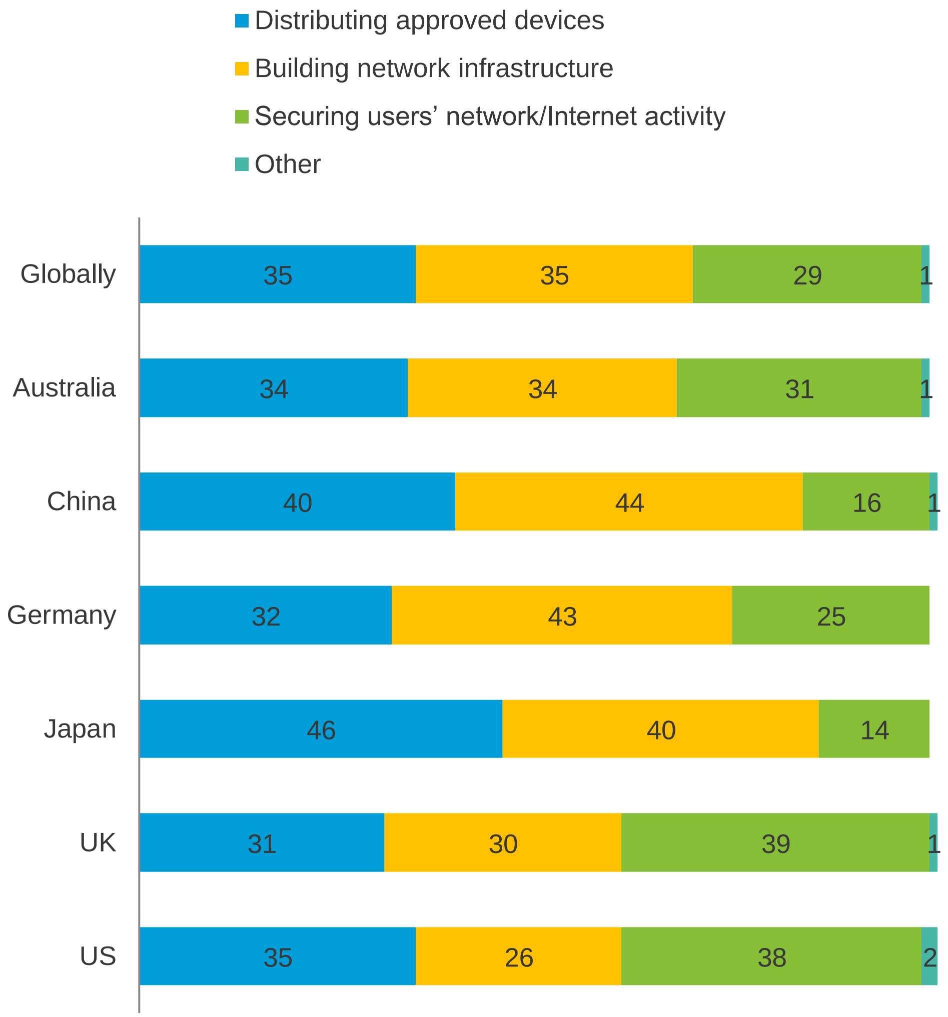
Q3. Please estimate what percentage of your organization’s employees you think will continue to work remotely following the COVID-19 crisis?



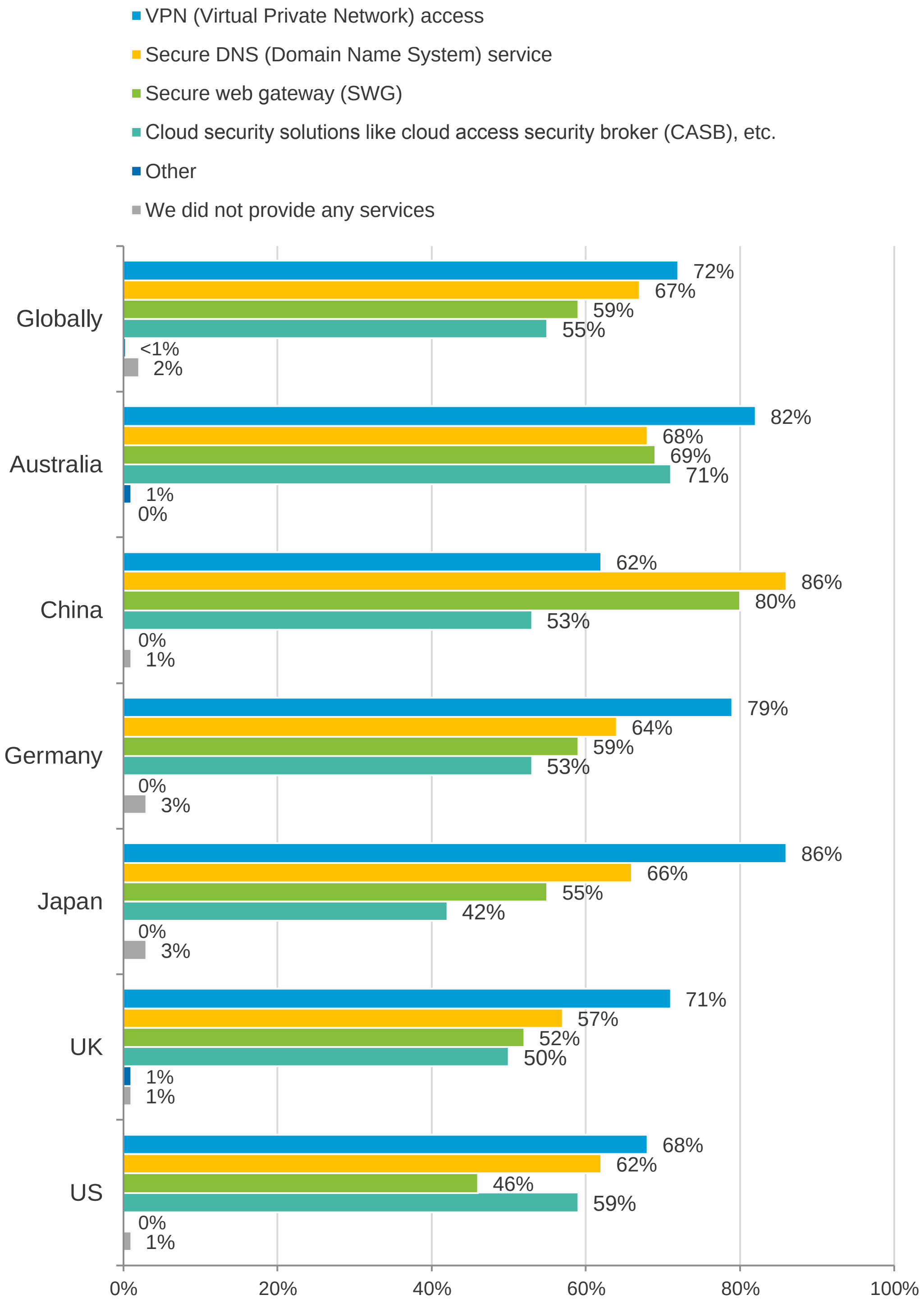


Q4. When it comes to having the right technology or cybersecurity in place, how prepared was your organization for employees to work from home?

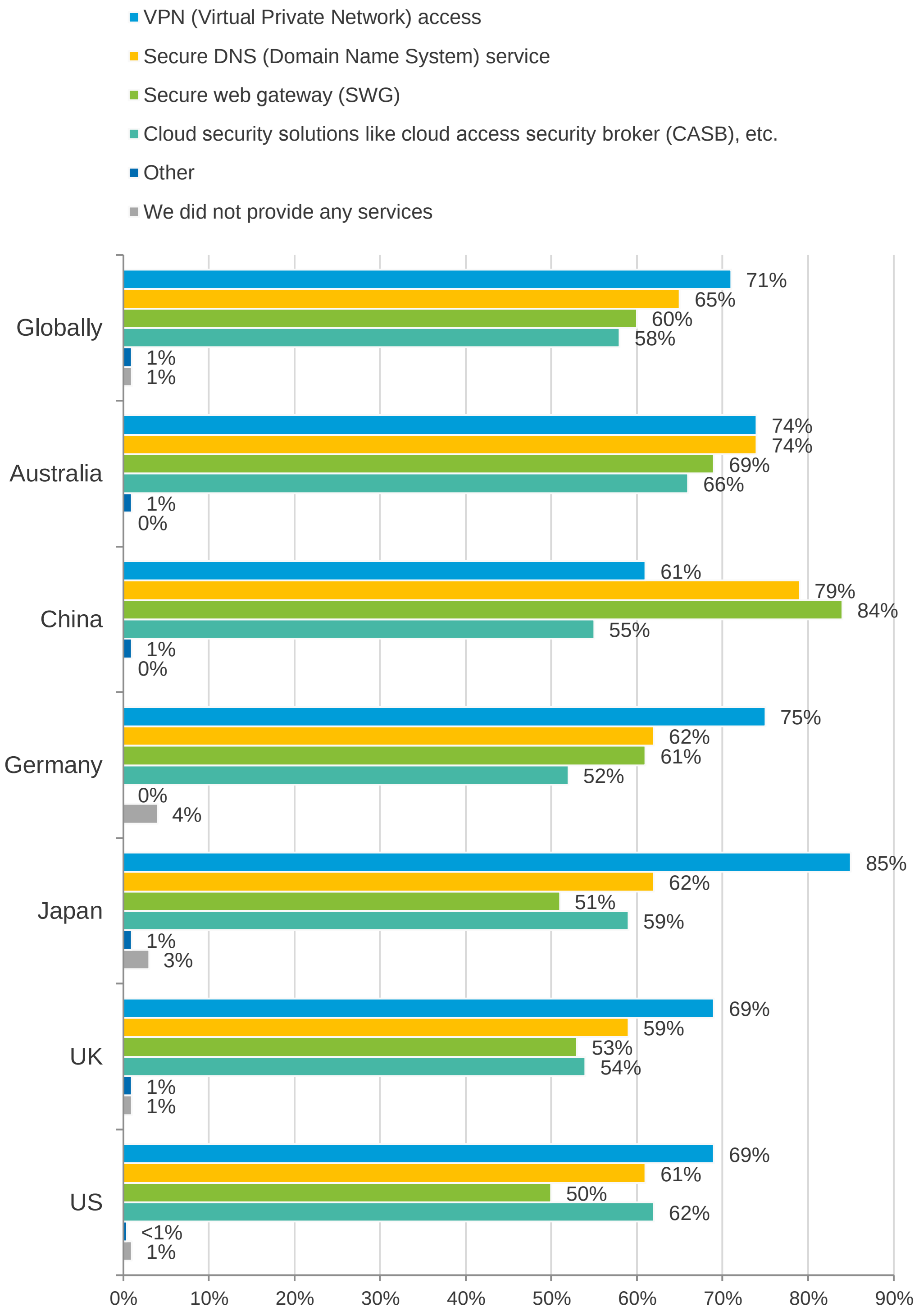
Q5. What was the biggest tech-related challenge your organization faced in transitioning to work from home?



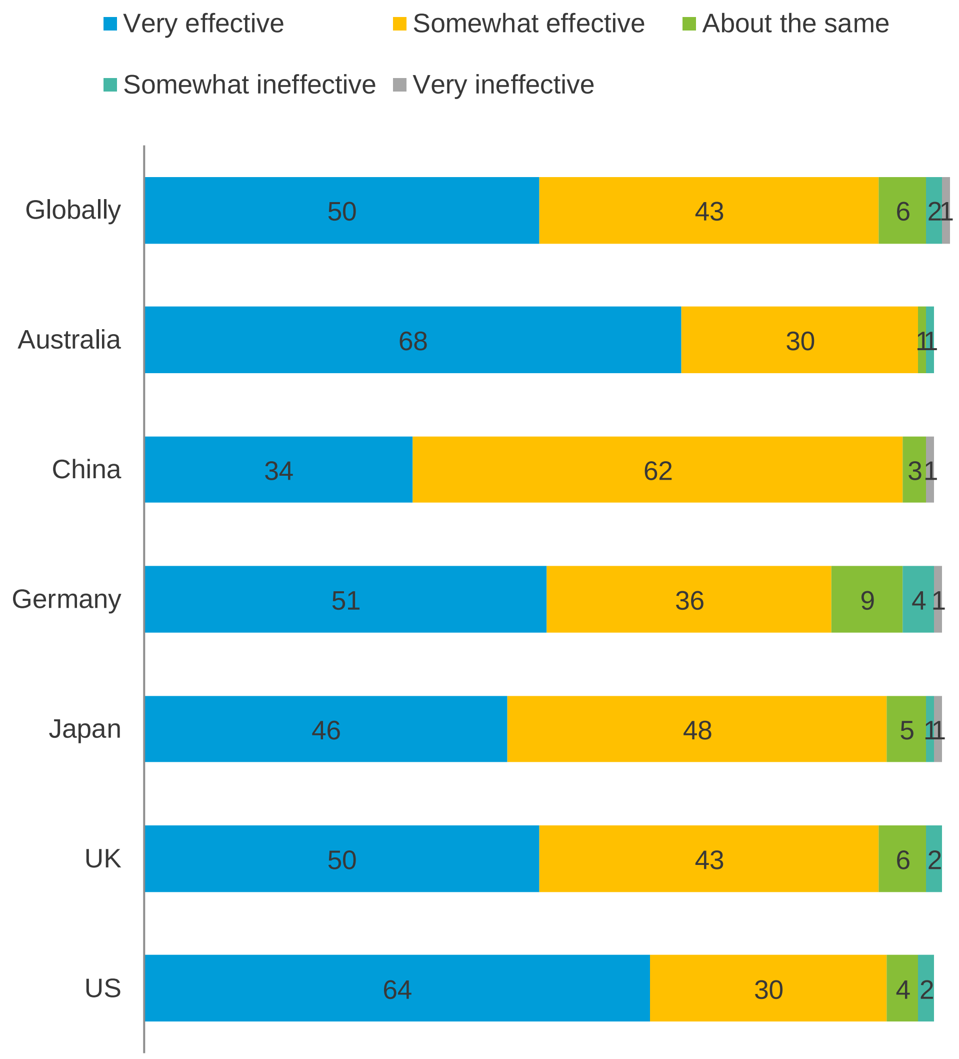
Q6. Prior to this pandemic, what network cybersecurity services did your organization provide to enable employees to securely work from home? (Select all that apply)



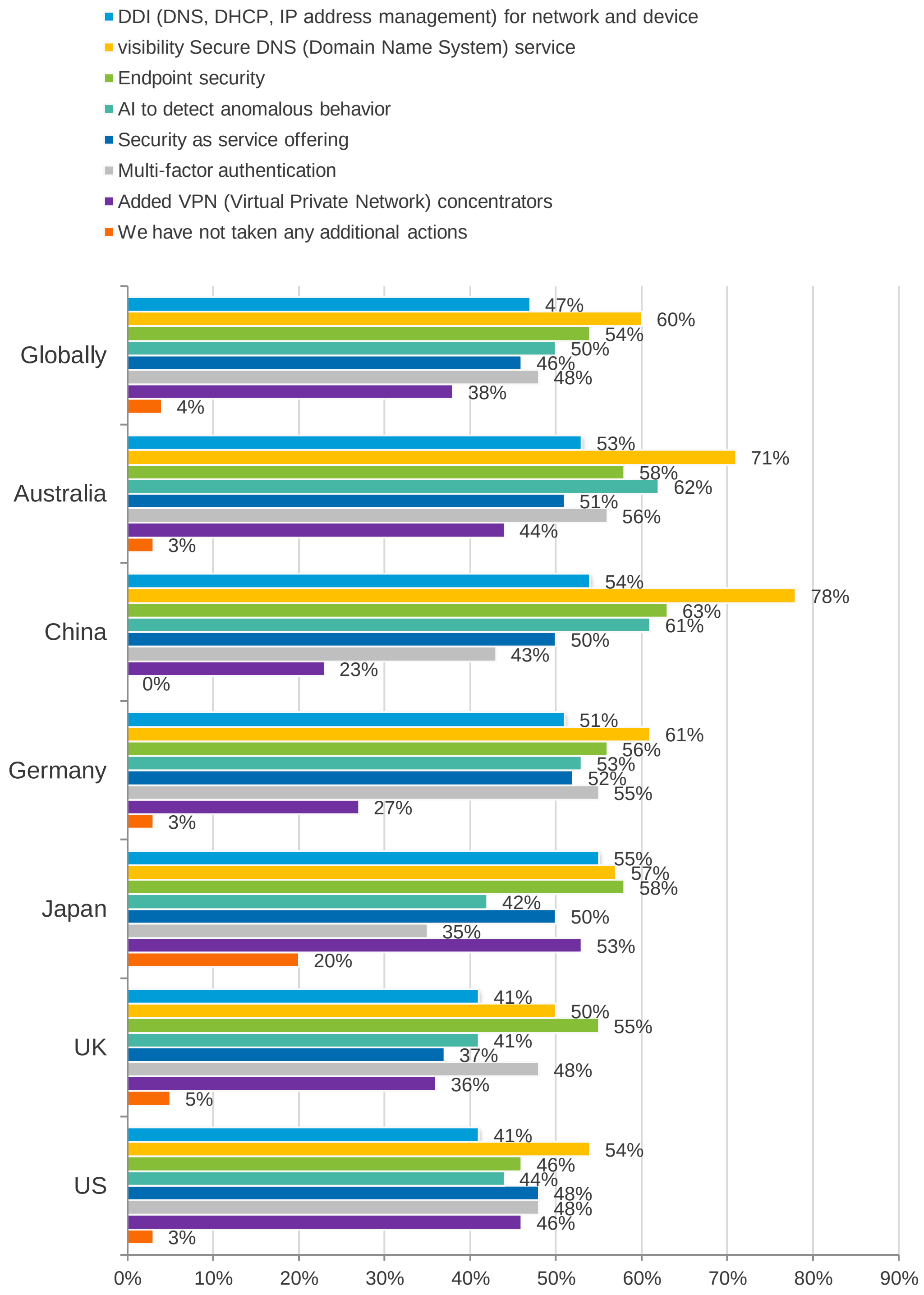
Q7. Which cybersecurity services has your organization provided to employees to enable them to work from home securely, as a result of the COVID-19 pandemic? (Select all that apply)



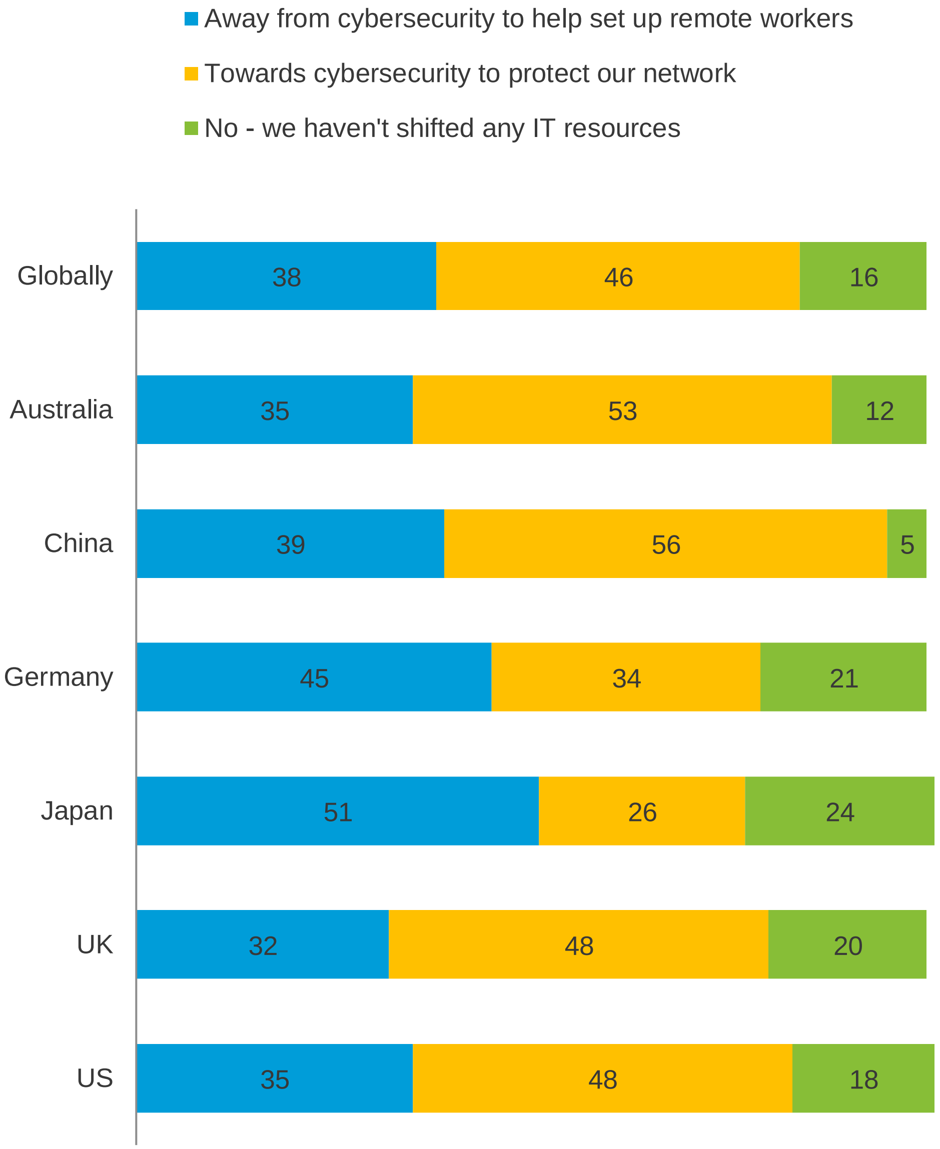
Q8. How succesful have these new services been at helping to secure your employees or protect your network?



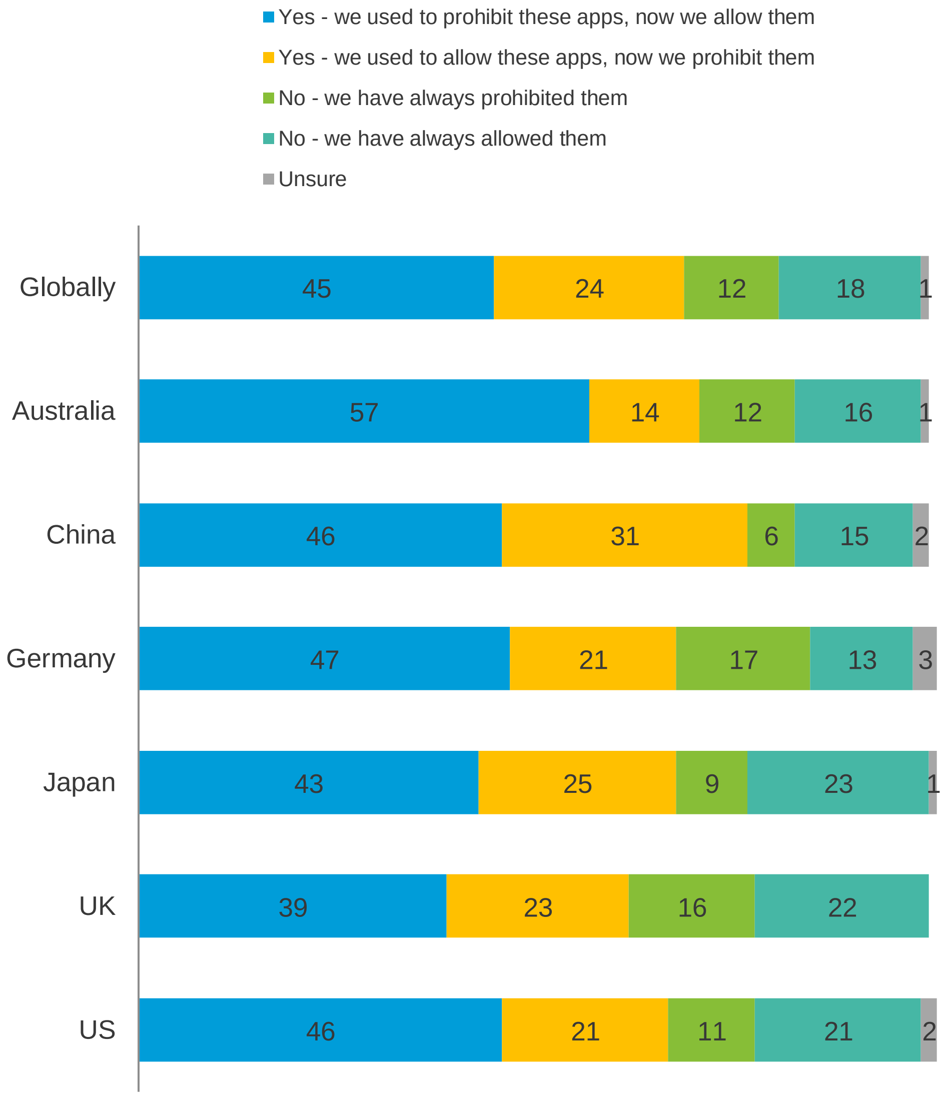
Q9. What additional actions has your organization taken to secure your networks and employees as a result of the COVID-19 pandemic? (Select all that apply)



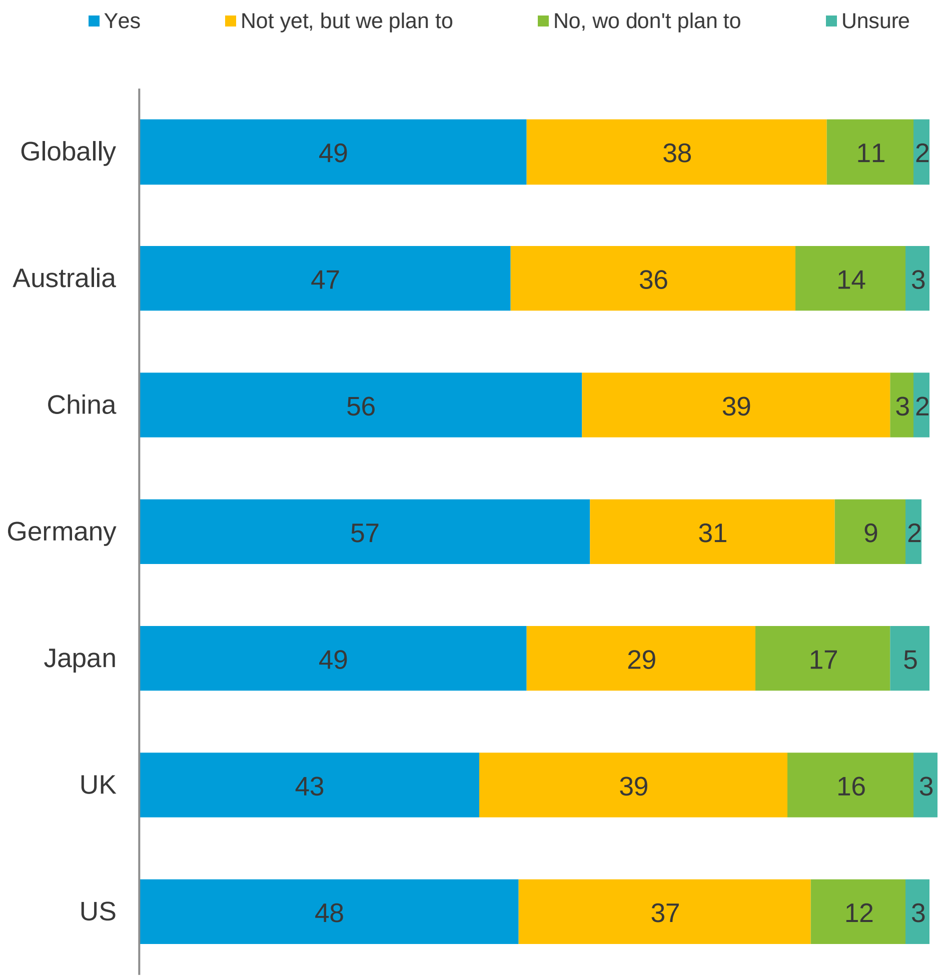
Q10. Has your organization shifted IT resources as a result of the COVID-19 pandemic?



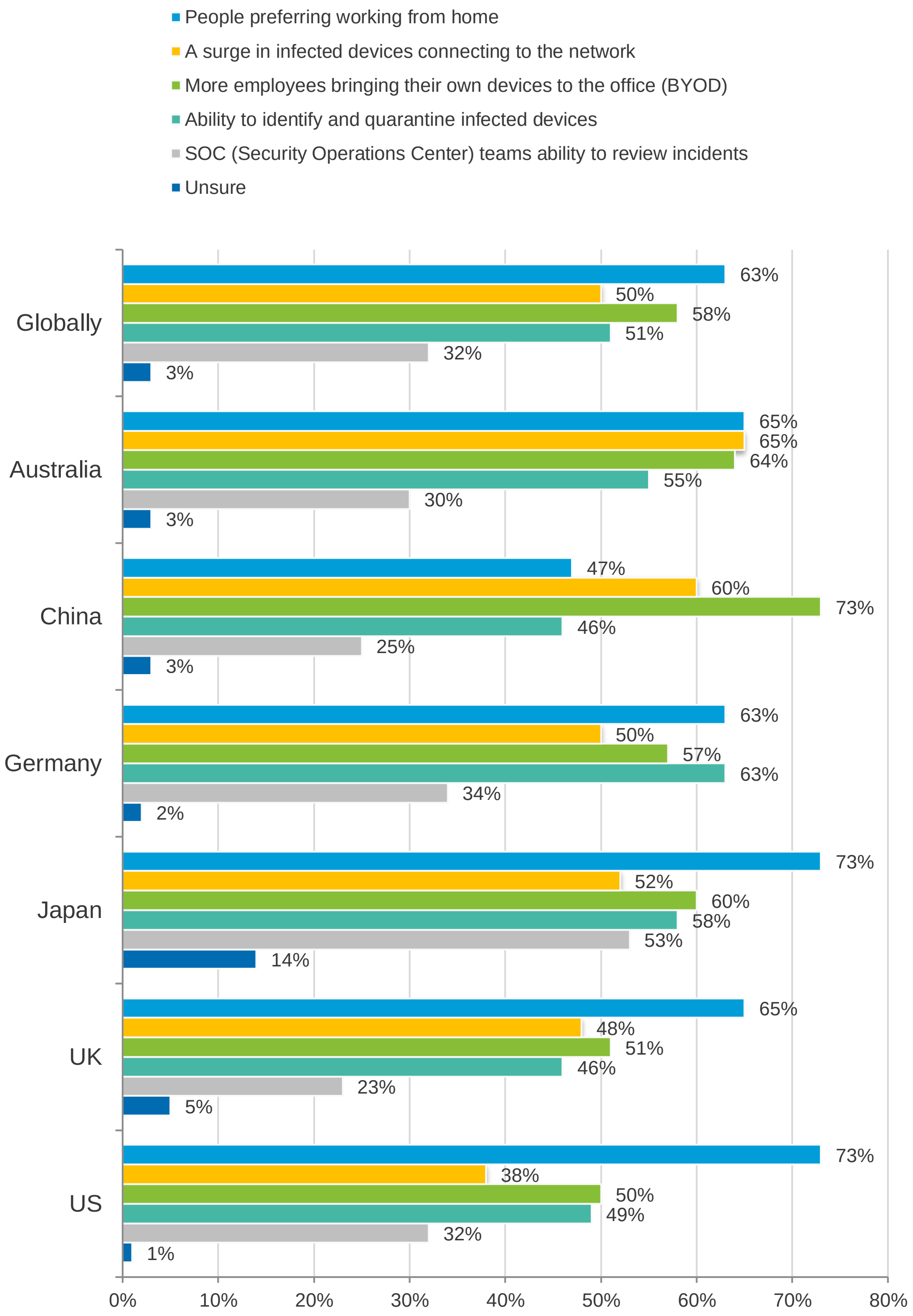
Q11. Has your organization changed any policies about the use of personal apps (e.g., Skype, WhatsApp, Zoom, Houseparty, etc.) on work devices as a result of the crisis?



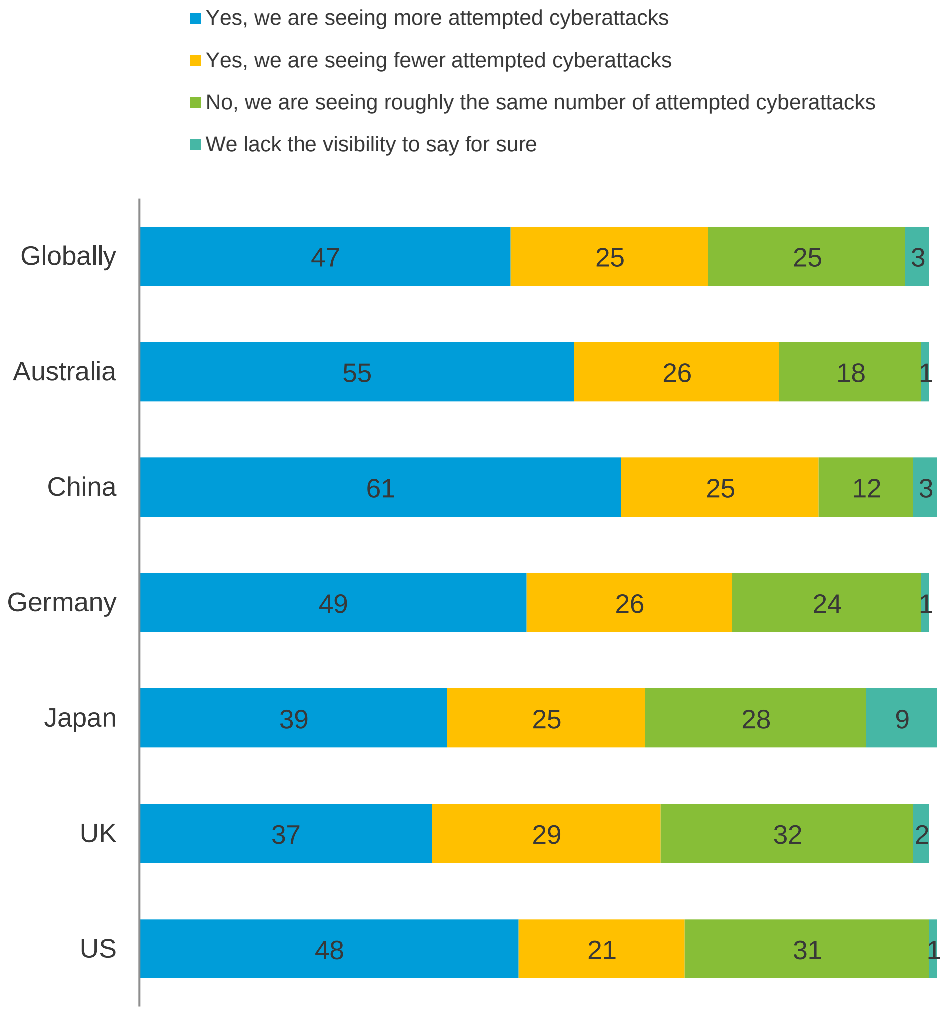
Q12. Has your organization changed its cybersecurity plan for when your employees return to the office after the crisis?

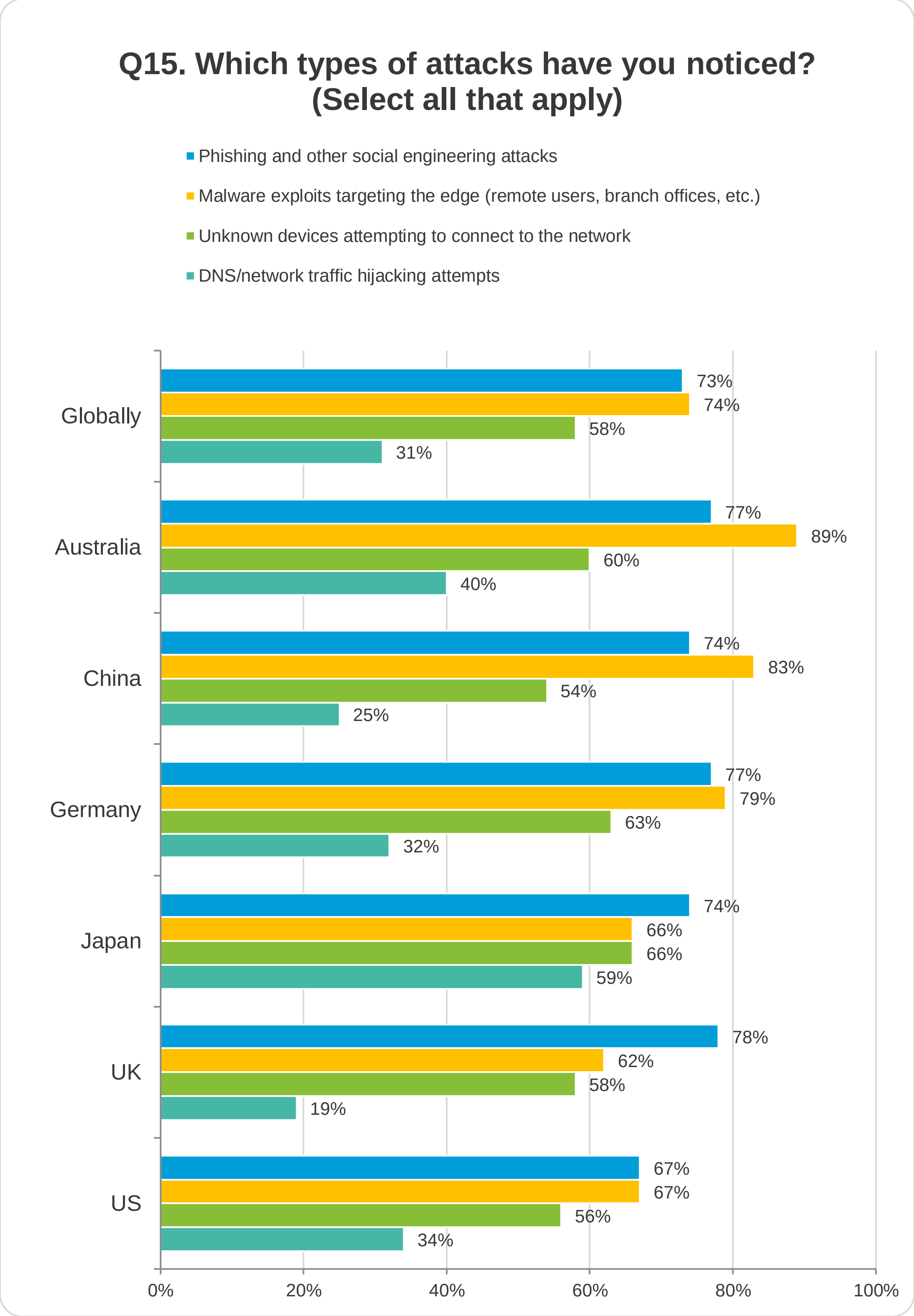


Q13. What cybersecurity challenges does your organization expect to face when returning to the office after the crisis? (Select all that apply)

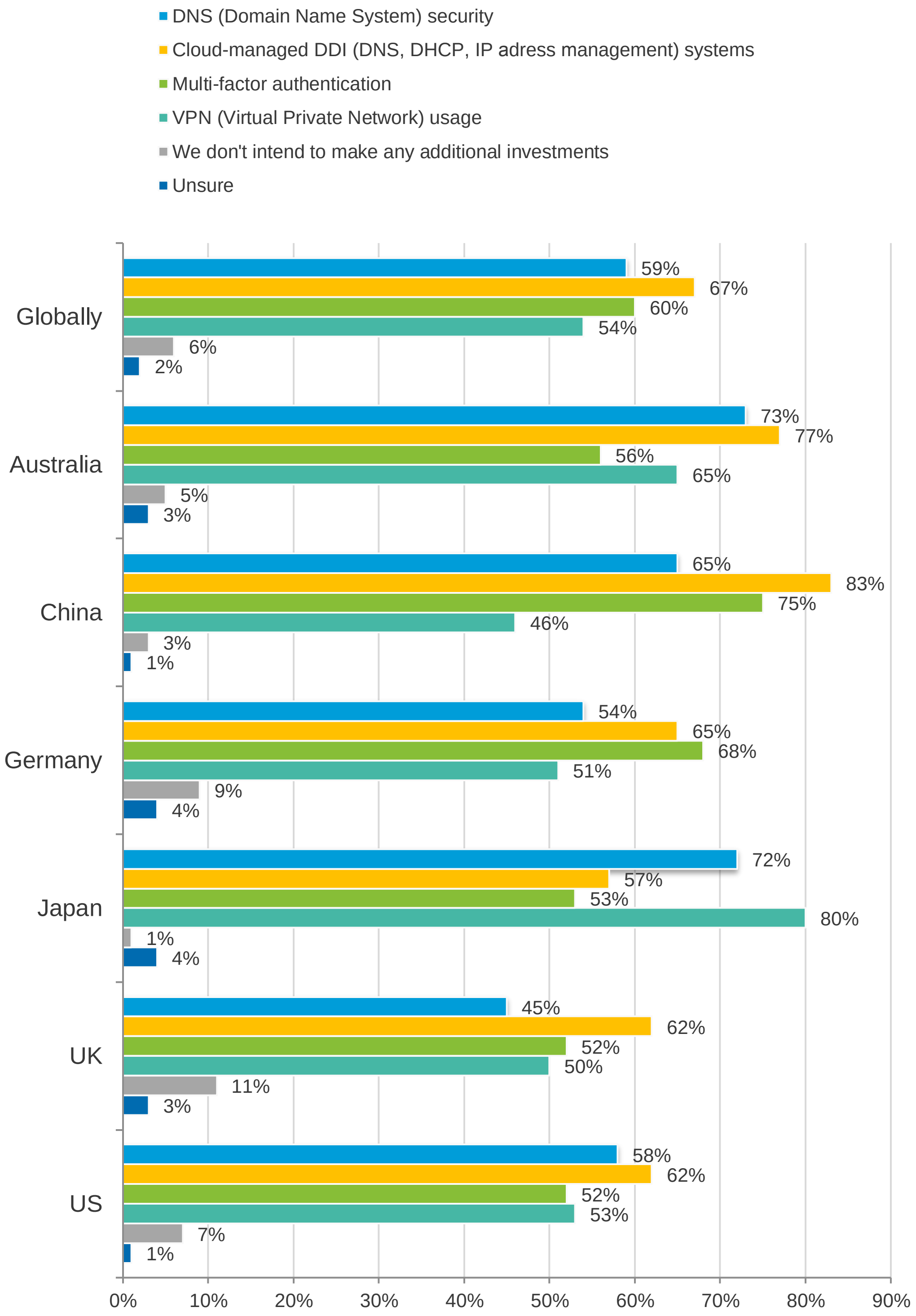


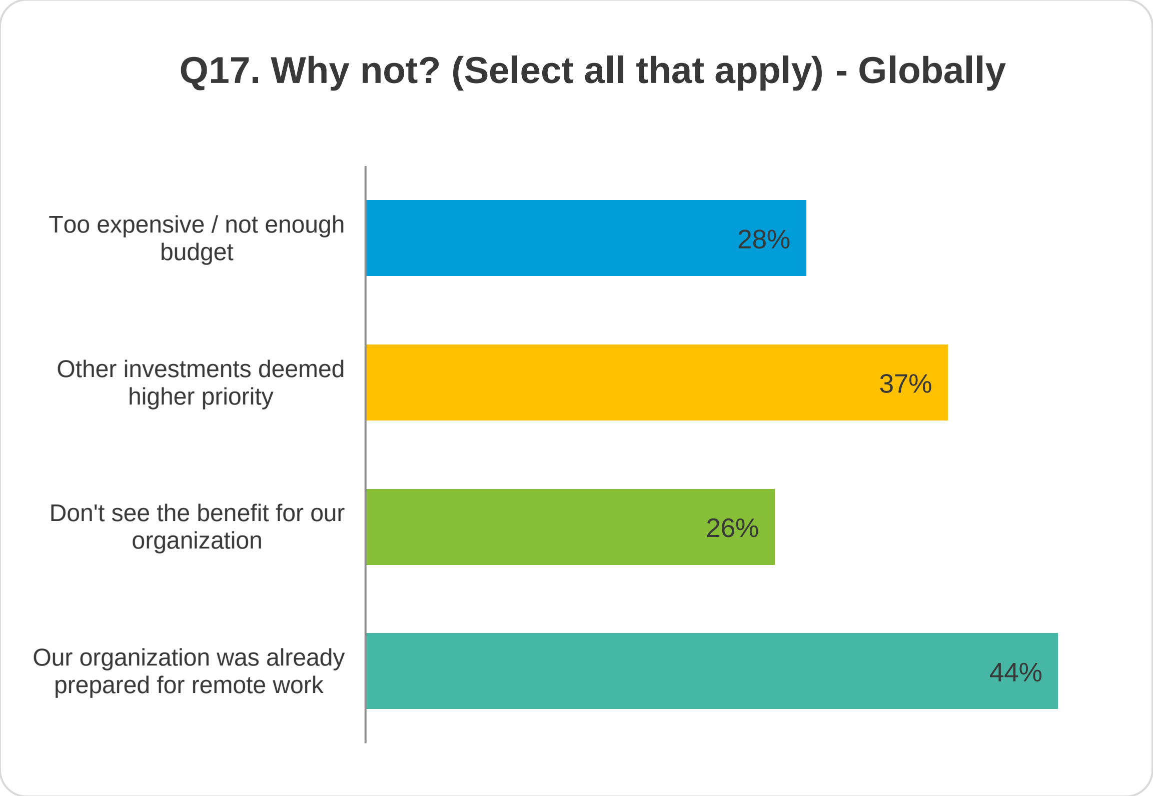
Q14. Has your organization seen a change in number of attempted cyberattacks as a result of the COVID-19 crisis?




Q15. Which types of attacks have you noticed? (Select all that apply)
Phishing and other social engineering attacks
Malware exploits targeting the edge (remote users, branch offices, etc.)
Unknown devices attempting to connect to the network
DNS/network traffic hijacking attempts
Globally
73%
74%
58%
31%
Australia
77%
89%
60%
40%
China
74%
83%
54%
25%
Germany
77%
79%
63%
32%
Japan
74%
66%
66%
59%
UK
78%
62%
58%
19%
US
67%
67%
56%
34%
0%
20%
40%
60%
80%
100%

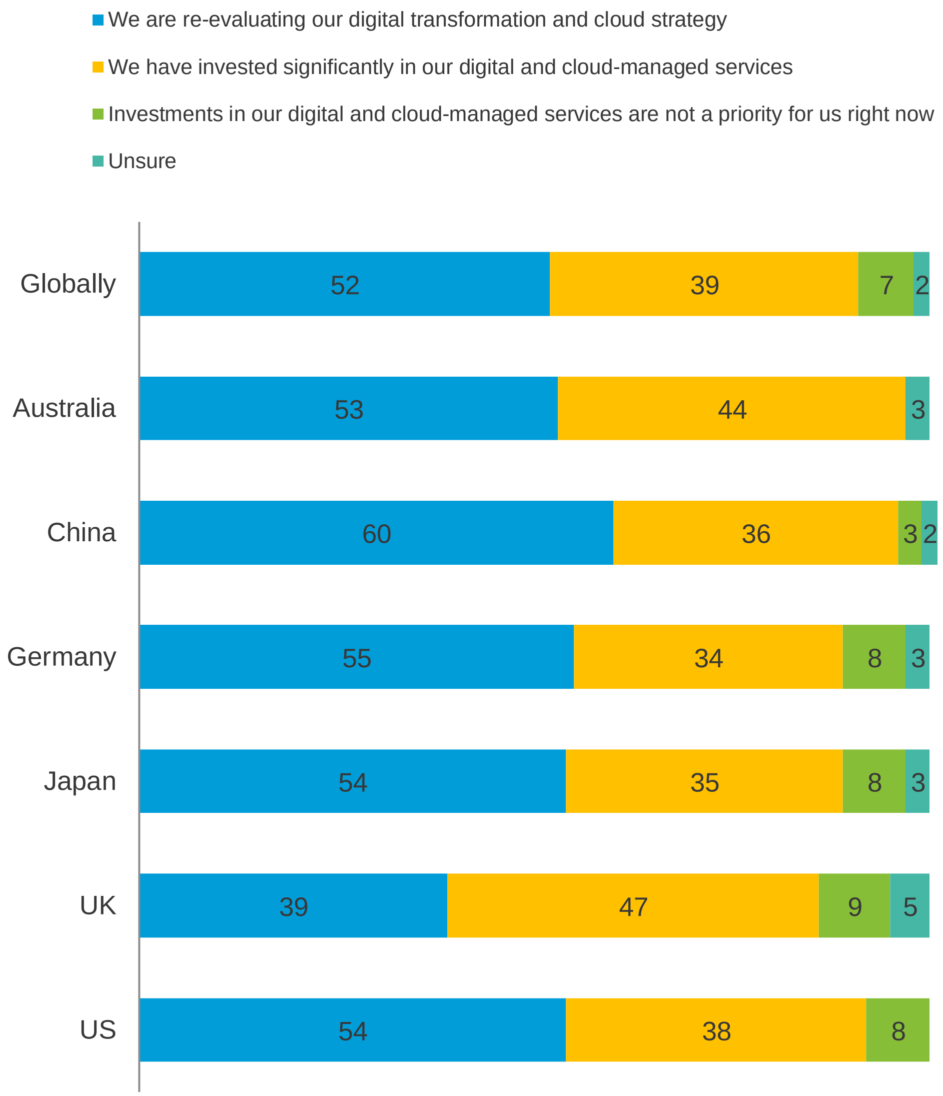
Q16. What additional investments is your organization planning to make in remote-working technologies or infrastructure? (Select all that apply)



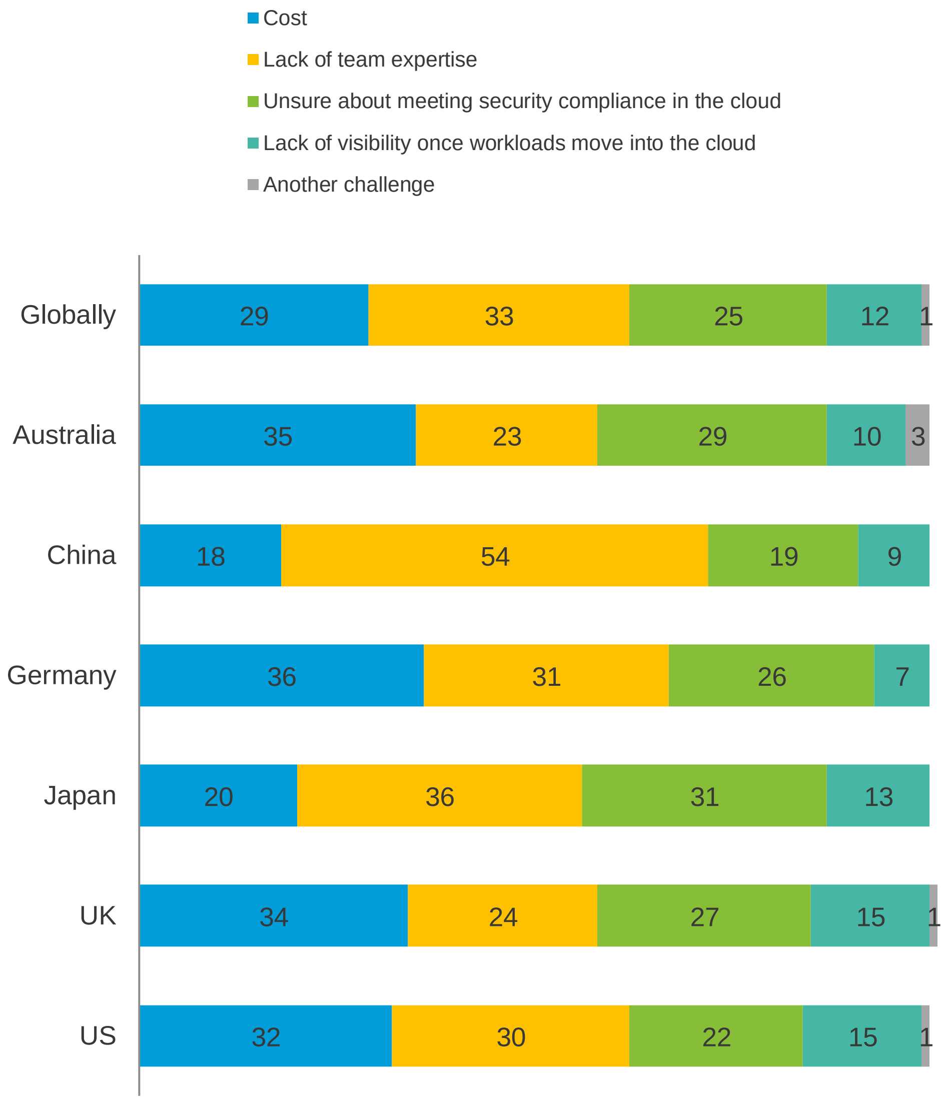


Note: sample size = 90

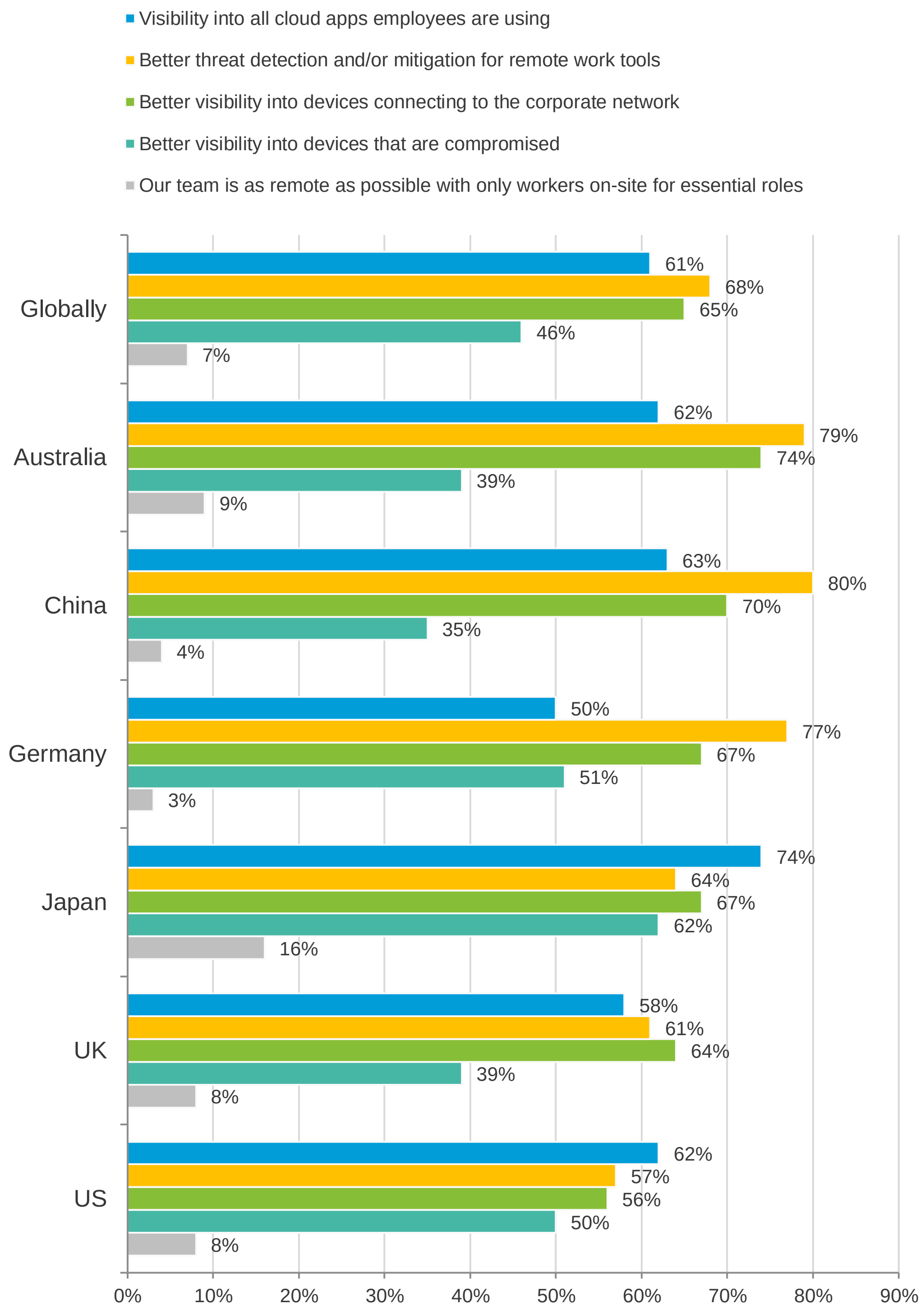
Q18. Has COVID-19 changed your investments (or planned investments) in cloud-managed services?



Q19. As part of your COVID-19 remote work response, what is the biggest obstacle you face in moving more operations to the cloud?



Q20. Which of the following would help enable more remote work for your employees? (Select all that apply)



Infoblox NEXT LEVEL NETWORKING

Infoblox is leading the way to next-level DDI with its Secure Cloud-Managed Network Services. Infoblox brings next-level security, reliability and automation to on-premises, cloud and hybrid networks, setting customers on a path to a single pane of glass for network management. Infoblox is a recognized leader with 50 percent market share comprised of 8,000 customers, including 350 of the Fortune 500.

Corporate Headquarters | 3111 Coronado Dr. | Santa Clara, CA | 95054
+1.408.986.4000 | 1.866.463.6256 (toll-free, U.S. and Canada) | info@infoblox.com | www.infoblox.com