Business Continuity, Flexible Working and Adaptive Infrastructure:

Five Actions for When the Economy Reopens Following COVID-19

Contents

Executive Summary 4

Methodology 6

Shift in Strategic Priorities 6

Shift in Budgets 8

Five Actions to Consider When the Economy Reopens Following COVID-19 10

#1 Develop a Better Business Continuity Plan 12

#2 Embrace Digital Tooling for Remote Working 13

#3 Secure Collaboration 15

#4 Consider Cloud as the Only Option 16

#5 Prioritise Adaptive Networks 17

Regional Outlook and Recommendations 20

North Asia: Speed and Resilience with Remote Working 20

SEA and ANZ: Focused DX with Security and Business Continuity 20

Europe: BCP, Flexible Network and Services 21

United States: Pay-As-You-GO (PAYG), Commercial Flexibility 21

Keeping International Businesses Connected 22

Appendix 24

Executive Summary

Nearly two-thirds of respondents (IT and business leaders) believe COVID-19 has changed their organisations forever. The sentiment is even across Asia, Europe and the United States markets. Nearly 80 per cent of respondents have some employees who cannot work from home due to IT issues. COVID-19 has also changed corporate IT strategy. Some businesses have put their current plans on hold and are now addressing the more pressing needs of keeping the IT 'lights on' by provisioning for an unprecedented level of remote working and moving more workloads to the cloud.

Businesses are accelerating the final migration of data onto the cloud at a time when consumption of this data outside the firewall, from a personal device is at an all-time high. Nearly 70 per cent of respondent businesses and IT leaders believe COVID-19 has increased 'Shadow IT', which is where employees circumvent official policy.

Businesses are also re-calibrating their digital transformation (DX) strategy. While they have set out to achieve the same common objectives (e.g., generate top line revenue, cost optimisation, improving in customer and employee experience), budgets and priorities are shifting. 93 per cent of respondent businesses state that they have changed their IT priorities incrementally, either significantly or dramatically. Only 2 per cent of respondent businesses report no change to pre-COVID IT budgets and spending.

Key Findings:

- The current crisis is accelerating DX, but not in its pre-COVID state. Most businesses are increasing or re-allocating budgets. This will manifest itself in a phased approach of IT strategy. In the short term, this includes the procurement of more Unified Communications software licensing; the medium term will focus on digital tooling and Information Technology Infrastructure Library (ITIL)-aligned processes; the long-term focus will be on getting the balance right between traditional and digital channels.

- Pre-COVID, approximately one in 10 businesses did not have a Business Continuity Plan (BCP) and even the organisations that had a BCP did not have any preparations in place for unexpected global events such as pandemics. Both prepared and unprepared organisations started at the same place trying to 'keep the lights on.'

- With nearly 100 per cent of IT leaders believing that there will be an increased reliance on video conferencing to replace face-to-face meetings, there will be a once-in-a-generation shift in culture and attitude. Unified Communications and Collaboration (UC&C), including video conferencing, team collaboration tools and cloud-based contact centre solutions, are some of the most transformative technologies to the enterprise.

- Networks underpin technology. They play a very important role in connecting remote and mobile workers. They will need to be software-defined, cloud-ready and more automated and flexible. This is to support the distributed IT systems and nomadic workforce. An adaptive infrastructure will gradually overtake the legacy MPLS WAN as the primary network.

Methodology

GlobalData interviewed over 120 C-Suites and IT decision makers to better understand the impact COVID-19 is having on IT budgets, strategies and overall priorities. Respondents represented large enterprises from over 15 industry verticals. They were located in various regions such as Asia Pacific, Europe and the United States. These online and phone-based interviews took place in April 2020. The results formed the basis of the Telstra/ GlobalData study, 'COVID-19: Impact on IT Budget, Strategy and Priorities.'

Shift in Strategic Priorities

As businesses re-calibrate their DX strategy, IT priorities are shifting. Businesses recognise the need to leverage technologies to improve agility and resiliency, and they are in the midst of updating their overall ICT strategy and putting in place short-term measures to cope with the COVID-19 situation. The top priority for respondents across all regions is the need to set up policies for a remote workforce. This includes areas such as ensuring employees can connect securely, access their applications and data and have a strong user experience. In many cases, businesses have not set up any policy for remote working and/or do not have policies in place around security, regulation and compliance.

To what extent have your IT priorities changed in the past weeks as a result of COVID-19?

n=121

As businesses continue to update their overall ICT strategy to reflect the shift in priorities, the survey showed some interesting findings with regard to remote working:

Is your company updating its ICT strategy because of COVID-19?

- 90 per cent of respondent businesses from Europe have employees who cannot work due to IT issues. This can range from poor or no connectivity; or inability to access applications from a remote site. Some 10 per cent of this subset state that 50 to 75 per cent are unable to work. This was consistent with the United States, Australia/ New Zealand (ANZ) and Southeast Asia (SEA).
- Europe was also the only region reporting an excess of 75 per cent of employees unable to work during the pandemic, due to IT issues. This will have a detrimental impact on business continuity since the majority of employees are unable to connect remotely to do their jobs.
- The fact that many employees are not connecting to corporate IT can also explain why supporting remote workers is the highest priority now. 70 per cent of respondent businesses in Europe see this as the highest priority followed by SEA and ANZ at 68 per cent.

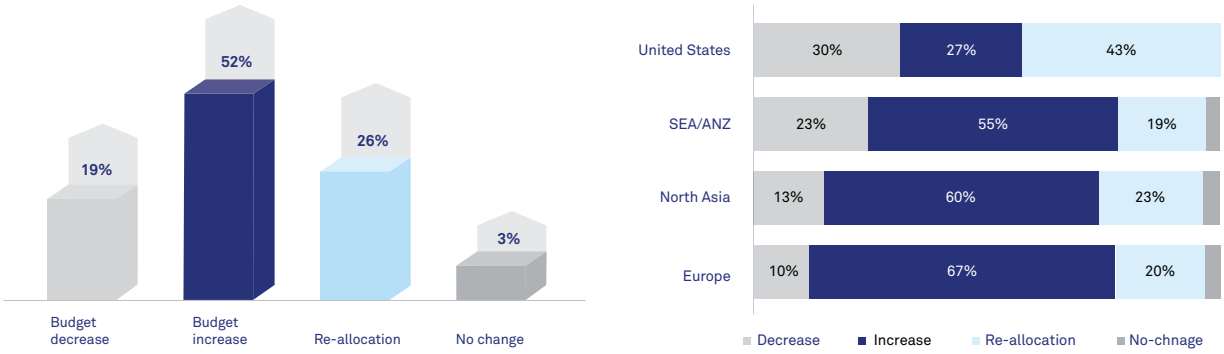
Related to the inability to connect was the need for a BCP, which was the second highest priority for two-thirds of respondents. While one in 10 businesses did not have a BCP pre-COVID, four in five did not factor in unexpected global events such as pandemics into the existing BCP. Given the inherent inadequacies pre-COVID, this will feature as another priority. It will also move from a policy that is updated periodically to one that is more dynamic. This is to promote business resiliency and continuity of operations. Creating an environment that promotes the remote and distributed workforce, as highlighted above, is one form of BCP. The survey also shows that nearly half of the businesses are planning for the possibility of long-term closures of branch offices, or reduction of the corporate headquarters office footprint. This sentiment is highest in Europe at 63 per cent and the lowest in North Asia and the United States at 40 per cent respectively.

Shift in Budgets.

The data is also showing businesses are shifting budgets. Overall, budgets increased with more than half of the respondents planning to increase spending on IT services in 2020. Over one in four businesses are re-allocating funds; one in five is cutting budgets.

Q: As a result of COVID-19, has there been any impact to the existing budget?

The data is also showing businesses are shifting budgets. Overall, budgets increased with more than half of the respondents planning to increase spending on IT services in 2020. Over one in four businesses are re-allocating funds; one in five is cutting budgets.



n=121

Among the respondents, there are also considerable differences between regions. In the United States, there is a strong sentiment to reduce budget compared with other regions. There are nearly seven businesses in Europe increasing IT budgets for every one looking to decrease. But in the United States, the number of business looking to slash budgets exceed that of companies plan to increase IT spending. Likewise, there is also a strong sentiment to re-allocate IT budgets among the United States respondents. Drilling into the percentage increase by region, there are some additional observations:

United States	SEA/ANZ	North Asia	Europe
Businesses, which are decreasing budgets, tend to be significant or substantial. 44 per cent are decreasing spending by between 6 and 15 per cent; likewise, 22 per cent plan to slash IT spending by more than 25 per cent. While some entities will increase spending, not a single respondent plans to surpass 15 per cent, which is also unique compared with other three regions.	This region leads in terms of the level of investment it plans to spend on IT services. 41 per cent plan to increase spending by over 15 per cent from the previous year. From this subset, an outlier of 6 per cent intends to increase IT spending in excess of 25 per cent from the previous year.	Overall, this region is more conservative compared with other parts of the world. Some 55 per cent of the companies that will spend more will do this within a range of 6 to 15 per cent. Likewise the 75 per cent of respondents which are reducing spend is in this same 6 to 15 per cent range.	This region is the biggest proponent of spending increases because of COVID-19 with 67 per cent moving in this direction. In 60 per cent of the cases, the increments are going to be in the 6 to 15 per cent range. However, one in five estimates the range at between 16 to 25 per cent. There are some outliers that plan to spend even more.

Five Actions for When the Economy Reopens Following COVID-19

#1 Develop a Better Business Continuity Plan

Traditionally BCP is the act of creating or updating a formal policy, which identifies potential threats to an organisation in the event of a disaster. It then defines a recovery path that promotes business resiliency to minimise downtime. Every potential threat maps to vulnerability to create a risk profile. BCP then works by creating a system of prevention and recovery. Underpinning prevention and recovery was usually a business impact analysis (BIA) which identifies areas impacted by disruption and criticality. Recovery priorities within a BCP are to be commensurate with business criticality, which then drives the Business Continuity and Disaster Recovery (BC/DR) strategy. Among the respondents, nearly 90 per cent had a BCP in place before the epidemic. The APAC region overall was the lowest reporting region at 87 per cent; the United States was the highest at 93 per cent. Europe reported BCP in the middle with 90 per cent.

'Our BCP has included scenarios such as global events and pandemics. We also had policies in place for remote working. Fortunately, we did not have any significant events. It has been BAU for us as far as the availability of IT systems is concerned.'
– Vice President, IT Risk Management Officer, UK Bank

Preparing for the Unknown, Unknowns

For the businesses that had a BCP, below are the results in terms of the level of preparation for an unexpected global event such as pandemics:

Business Continuity Planning: Preparation Levels	
No preparation	In the global results, 30 per cent of BCP focused exclusively on risks to the business. There was no preparation for unexpected global events. The number was highest in SEA/ANZ and Europe at 37 per cent; and the lowest in North Asia and the United States at 23 and 21 per cent respectively.
Some preparation	Just over half of BCPs focused mostly on risks to the business, but there was some preparation made for unexpected global events. The number was highest in North Asia at 58 per cent and the United States at 64 per cent. It was the lowest in SEA/ANZ and Europe at 41 and 44 per cent respectively.
Significant preparation	Within the subset here, 19 per cent of BCP included major preparation for global events, including pandemics. The highest reporting regions were SEA/ANZ and North Asia at 22 and 19 per cent respectively. Only 14 per cent of respondents in the United States had this level of planning.

BCP Post-COVID-19

Businesses should not only dramatically widen the scope of BCP, they should rely on more data and tools to discover the hidden relationships between data sets, identify more vulnerabilities and consider ways to generate a risk score (e.g.1 for minor, 5 for catastrophic) on a more formal and regular basis. BCP should align to businesses continuity management processes (i.e.ISO 22301). This will give a standards-based approach for regulatory compliance to reduce administrative and operational efforts and to mitigate potential breaches. This also helps to shift dependencies from individuals and departments to a more data-driven documented process. The end goal is to improve resiliency and mitigate the potential for large-scale damage. In the longer term, businesses should use outputs from the BCP to drive other decisions.

The following are some examples:

Tactical Decisions	BCP can assess the impact of remote working becoming a new norm on business resiliency. In some sectors, location independence could improve resiliency and in other sectors could be a challenge. Tactical decisions on whether or not to close more branch locations and/or reduce the overall corporate office footprint are reflected here.
Strategic Activities	An updated BCP plan should have target on data Recovery Time (RTO) and Recovery Point (RPO), for example, in case of an outage should flow through to the setting up and configuration of data centre services, including the procedures for back-up, archiving, e-discovery, and retrieval of data. This can also resurface discussions on security strategy, data classification and loss prevention.
Operational Activities	An updated BCP can also lead to redefining operational processes. This could include the creation of IT policies, driven also by HR, that support remote working, Bring Your Own Device (BYOD) strategies and acceptable use policy (AUP). Decisions here should also focus on Shadow IT and employee awareness of corporate security policy and making the average employee part of the frontline for cyber defence.

#2 Embrace Digital Tooling for Remote Working

As businesses move more workloads to the cloud, data from branch locations, including appliances, will start to disappear. This will create a scenario where premise-based firewalls protecting the perimeter, such as LAN in a branch site, will become less relevant. Digital tooling comes into play in providing a platform-centric approach to deliver the new workforce ICT capabilities that map to their role in the company, access privileges and services they need to become the most productive. Digital tooling will drive automation in areas such as provisioning and service management. It will also look to strike a balance between end user experience (e.g., access any content, from any device, in any location) and network flexibility, security, business continuity, IT governance, regulation and compliance. The following provide some considerations of what digital tooling will look like in a post-COVID-19 environment.

Security Tooling

As businesses take on more temporary workers and provision users and devices, some of the core capabilities will be in identity and access management. This is to manage the influx of new users, provide the access credentials for their roles, and enforce these rules through a single policy. Cloud Access Service Brokerage (CAS-B) will be another capability for protecting data entering or existing cloud services, which brings additional capabilities such as encryption, Security Information and Event Management (SIEM) and tools for compliance. Multi-factor authentication will also be important for advancing the concept of zero trust.

The following table considers the differences between security strategy, process and products for remote workers by regions:

Organisational Readiness: Responses by Region	
Security Strategy	**The APAC region is further ahead with an overall strategy for remote working.** 71 per cent of the global respondents state that they have an overall security strategy for remote workers. However, there are major differences between regions. The United States is the lowest reporting region at 53 per cent; SEA/ANZ is the highest with over 90 per cent; North Asia reports this figure at 77 per cent while Europe at 63 per cent.
Security Process	**European and American respondents lead in terms of having a policy to support remote workers. This is likely due to culture.** The survey shows that 56 per cent of respondent businesses have formal security policies in place for remote workers. The United States is the highest reporting region at 67 per cent and North Asia the lowest at 37 per cent. This could be due to the culture of working from an office and physical location.
Security Products	**All regions are at the same starting point for product**. The survey shows that only 56 per cent of respondent businesses are using multi-factor authentication for the remote workforce and only 40 per cent are down the path of cloud access service brokerage capabilities. In addition, eight out of 10 businesses do not have the tools to detect Shadow IT. There is little variation between regions, which suggests the potential for more growth across the board.

Cloud Governance and Shadow IT

With the broader use of cloud, it is also important with digital tooling to include cloud governance. Nearly 70 per cent of respondents believe COVID-19 has increased Shadow IT. While in most cases the motivations are benign, there are risks around security and compliance. North Asia is the highest reporting region. Some 80 per cent of respondents see a growing problem with Shadow IT, followed by SEA/ANZ at 74 per cent. Similarly, only 17 per cent of respondents believe they have a strategy and approach to address the issue with virtually no difference in responses across regions.

Businesses will also need to consider digital tooling post-COVID-19. Some of the core capabilities are in preventing 'bill shock' in cloud services by knowing exactly what is being used at any point of time. It is important that standard tooling extends to as many environments as possible as the market embraces multi-cloud. A number of these solutions send automatic alerts when IT policy is violated, which helps to detect Shadow IT. This is important for compliance (e.g. data sovereignty, General Data Protection Regulation (GDPR), or sector-specific requirements). Many of these tools will have log management capabilities, which are important for security lifecycle requirements (e.g., detection, incident response, remediation, post-event investigation and reporting). Digital tooling should also integrate with other systems such as monitoring and service catalogues.

Service Management

Digital tooling will also be important for the provisioning and management of remote users at scale. Artificial Intelligence (AI)/ Machine Learning (ML)-infused tooling will be important for driving operational efficiencies and self-service. A simple password reset per employee can cost a company US$ 30 to US$ 50 to resolve per incident with poor tooling.

IT leaders are unable to see the bottom of incident queues. Many are pending connectivity issues, which is the reason why such a large number of employees cannot work. Digital tooling offers a holistic platform to support the shift in working patterns, connectivity and security requirements.

The ability to use AI/ML to better automate repetitive operational processes is a key objective among enterprises in order to not only speed the time to service, but also time to respond to a trouble ticket. Some 52 per cent of respondents are looking at DX as a way to increase the adaptability and speed of change within an organisation. The highest reporting region is North Asia at 62 per cent. SEA/ANZ is the lowest at 45 per cent.

As a service management system incorporates intelligent process and automation, it is likely to extend into the many adjacent areas such as incident, service level, configuration, and change management. It will also tie into cloud governance, and security monitoring through APIs. Given the movement of people, and reality of managing multi-vendor environments, these platforms are important building blocks post-COVID-19.

#3 Secure Collaboration

UC&C platforms including contact centres are some of the most important capabilities for business continuity. It is not only critical for employees to connect securely, but to communicate virtually and work together across more locations.

Within the past few months, businesses have been investing significantly in UC&C. Data reported by some of the leading vendors show more licenses sold in Q1 2020 than all of 2019. Cisco reported Webex traffic quadrupled in just one month to an excess of 24 billion minutes. The data shows that businesses are not only increasing the number of software licenses with existing systems, but also investing in new technology stacks.

While there are many options in the market, the platforms that combine messaging-based communications with team and project management capabilities are more popular for the new normal. These solutions also have features for group conversations when communicating with a broader team is needed, but balance this with private messaging for more focused conversations. Many of these platforms also offer groups to be created for specific projects with task allocation and timeline features. All of these features are essential for managing projects and tasks across remote teams.

During COVID-19, businesses also experienced some challenges with customer support functions. For example, 48 per cent of respondent businesses in the survey reported an increase in traffic to the contact centre including a spike in average waiting times and abandonment rates. The same number of respondents also had to close down some of the contact centres due to mandatory quarantines, social distancing and other requirements. Less than 10 per cent of APAC and European businesses reported having no significant issues during the pandemic.

Contact Centres Post-COVID-19

Collaborative platforms appeal to younger generations as they enter the workplace. They reduce the need for employee travel, company costs and carbon emissions. Gradually this can improve work-life balance and set businesses up to win the talent acquisition war.

Nearly half of respondents are now adopting a cloud-first contact centre strategy to improve end-to-end capabilities (e.g., Auto Call Distributor (ACD), Interactive Voice Response (IVR), workflow optimisation) for speed and agility. The sentiment is the strongest in North Asia at 57 per cent followed by SEA/ANZ at 52 per cent. The United States is the lowest reporting region at 40 per cent followed by Europe at 47 per cent. These statistics reflect the relative market maturity for cloud services. In some cases, new cloud-based contact centre solutions have been spun up quickly (in days) for COVID-19 related hotlines.

Future of Video

Video is the new voice in collaboration. The data also shows a shift in culture that could be with us for many years, if not permanently. Some 98 per cent of respondents – an extraordinarily high figure with virtually no outliers – believe there will be 'an increased reliance on video conferencing to replace face-to-face meetings post-COVID-19'. If realised, this will have far-reaching implications beyond technology to improvements in greenhouse emissions, carbon neutrality and overall corporate social responsibility. This increased reliance will also be important to help drive cost savings and improve employee work-life balances.

Security

Enterprises should search for tools that are not just intuitive and easy to use, but also enterprise grade and secure. While 'free' solutions have a natural appeal, some can be lax in terms of security. In addition, there is a risk of exposure of confidential information to an external party, the theft of intellectual property, or even backdoor attacks on corporate systems. Businesses should consider vendors that have granular access and privacy controls, and the ability to audit user actions. There have been well-known hacks on some collaboration systems during COVID-19.

#4 Consider Cloud as the Only Option

The will to move to cloud is the strongest it has been in the past decade. Some 93 per cent of respondent businesses are accelerating the adoption of cloud services. Respondents in Europe and North Asia rank the highest in sentiment across the regions, with nearly all respondents (97 per cent) seeing cloud as the only option.

While there was always a view to keep some data on-site, many businesses will no longer have any physical data hosted on-premise. As businesses update their BCP, the main priorities are to improve the uptime and resiliency of data through a multi-cloud strategy. This was the case for 67 per cent of the respondents that needed business continuity with the move to support remote working.

Services Enablement and Alternative Sourcing

Enterprises should look to cloud now to accelerate their DX. As a platform, it supports many of the underlying objectives from driving top-line revenue, improving operational efficiencies, increasing agility and speed to change. It will also be a major driver for tactical deployments, as well as an alternative sourcing method if IT departments are not available or physical access to infrastructure is difficult. The following are some ways to consider the broader use of cloud post-COVID-19.

Quick Wins with an Expanded Cloud Deployment

Roles-based ICT	With so many businesses looking at building workplace ICT solutions around roles and activities, cloud is an important platform for provisioning and packaging new services with greater speed. Some solutions such as Virtual Desktop Infrastructure (VDI) can only be provisioned from the cloud.
Remote IT management	With social distancing and the potential downsizing of physical offices, alongside the continual IT difficulties in provisioning remote workers, cloud should be seen as the primary means to deliver more automation for remote workers through strong and centralised management tools.
Contact Centre	Given many breakdowns in customer support functions, nearly half of the respondents are looking for a cloud-first approach for contact centre solutions. This is the only way to support home-based solutions and deliver location-independent continuity of operations.
Security and Continuity	As businesses move from premise to cloud, there needs to be a balance between security and end-user experience. Cloud is an alternative sourcing method if the internal IT team cannot access equipment locally. Pragmatically, these solutions can be deployed more for redundancy and failover, site-to-site mirroring, back up, archival and retrieval of data.

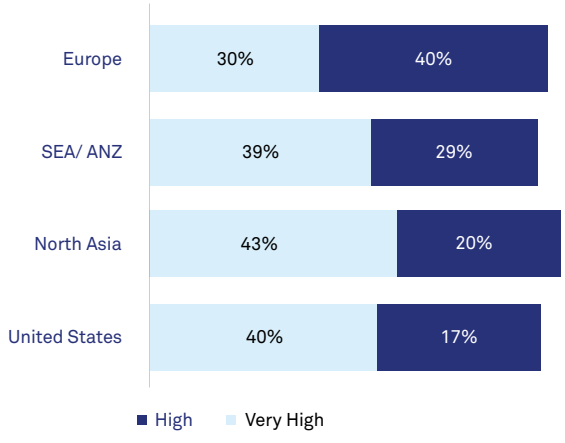
#5 Prioritise Adaptive Networks

The survey shows that one of the top immediate ICT priorities is to support the remote workforce. This sentiment is especially strong among respondents in Europe, SEA and ANZ. A distributed workforce, made even more essential now because of COVID-19, creates challenges for the enterprise network. The cloud has transformed the branch. Now, the proliferation of endpoints may have an exponential requirement on new, often temporary sites, including event pop-up locations.

Quality of service, access and control, security and management are harder to implement when most of the workforce move from a centralised office to individual locations. This means enterprises will need an adaptive infrastructure to address challenges associated with employees bringing their own devices and accessing enterprise data and applications from home.

The table below illustrates the number of respondents who see the need to roll out networking solutions for remote workers and update the overall WAN strategy as either a high or very high priority.

Updating Overall WAN Strategy



Adaptive Networking Post-COVID-19

There are many challenges in the network that are not directly visible to end-users. There are a number of common issues when connecting a large number of remote workers. Network gateways, when using a VPN, can be overloaded with authentication requests or have licensing restrictions; contention ratios in service provider networks can impact the performance in the last mile; end-to-end performance issues when connecting to the cloud; and failures in the end devices (e.g. session limitations with home router and data limitations with tethering).

Intelligent Networks

Service providers have been working on network underlay strategies which are helping to resolve many of these underlying problems. Some of the respondents use traffic engineering, often alongside the use of newer protocols, to increase throughput and lower latency to cloud services. Carriers are also improving the interconnection with third-party operators, managing these links and even increasing the number of private peering. Other areas include the ability to design a network to set policies which best support the data and applications traversing the infrastructure at any point of time. This is another way to improve overall performance and security in the core network. Post-pandemic, it is not always how well a network is designed, but how well it is peered and interconnected to deliver a business grade service for remote workers. Carriers that have implemented an underlay capability are in the best place to deliver Software-Defined Wide-Area Network SD-WAN that differentiates in performance and overall user experience.

SD-WAN

The survey data suggests that networks will become even more distributed as branch and campus sites consolidate. In addition, businesses will accelerate the migration of data and applications to the cloud in over 90 per cent of cases. Given these trends, business will also need to revamp their overall WAN strategy.

Today, not only are employees working remotely, so are their partners and suppliers. This creates a force multiplier.

Businesses should consider SD-WAN for improvements in provisioning, automation, and ease of management. Many of these capabilities are also used to provision Network Function Virtualisation (NFV) instances such as firewalls, load balancing, WAN optimisation and other technologies for remote users. SD-WAN capabilities where the application layers intuitively link to transport through APIs will lead to enhancements, such as performance, security and overall management, which are not possible with an over-the top overlay SD-WAN.

Regional Outlook and Recommendations

North Asia:
Speed and Resilience with Remote Working

North Asian respondents – Hong Kong, Korea, Taiwan and Japan – are on par with the United States in terms of having a DX strategy and slightly ahead of SEA/ANZ as a region. While respondents believe that driving top-line revenue streams is the most important objective of DX, they have a much stronger position on the need to increase speed of change. The top business priorities for North Asia focus on enabling remote working for employees, which ranks above employee health and safety by a three per cent margin. Translating business to ICT priorities, North Asia is ramping up on UC&C implementation, including video conferencing for the distributed workforce. The next task is to accelerate workloads to the cloud to support this new way of working and improve business continuity. Overtime, the region will move to role-based ICT where services are provisioned to reflect the roles and activities of employees. Unsurprisingly, the need for automation is a priority for 80 per cent of respondents, the highest among all regions. The region leads in the adoption of a cloud-first strategy for the contact centre, having experienced considerable disruptions at the peak of the pandemic. It is also leading the drive for contact centre solutions for a home-based or remote user driven by the responses in Hong Kong in particular. Underpinning the services strategy is the need to invest in the underlying network, where 63 per cent of respondents are reassessing their WAN strategy.

'Our infrastructure and systems were never designed for large remote access users. We have significant concerns with capacity and congestions and the impact on our workers. We are working closely with service providers and re-assessing our ICT requirements. The immediate future is uncertain, but if home working becomes the norm, ICT investments will follow.'
- Head of IT, Distributor of Pharmaceutical Products, Philippines

SEA and ANZ:
Focused DX with Security and Business Continuity

SEA and ANZ respondents – in Singapore, Malaysia, Philippines, Australia and New Zealand – have a strong view in ensuring the DX strategy needs to do two things: (1) increase top-line revenue and (2) improve the cost structure. While the order of priorities is similar in other regions, this region has a laser focus on these two overriding objectives. This region also has some paradoxes.

Despite the fact that the region had the most developed BCP as it has taken 'preparation for major events, including pandemics,' into consideration for BCP, it still sees the challenges of COVID-19 a calling card to execute 'dramatic,' changes to the overall IT strategy. The top business priority for SEA/ANZ is improving ICT and security resilience for business continuity purposes. This is an even higher priority than safeguarding employee health and safety by a margin of 9 per cent.

Translating the business to top ICT priorities, business and IT leaders in SEA/ANZ lead the regions in investing in UC&C tools, including video conferencing for remote working. The region is accelerating cloud adoption, and looking at role-based ICT solutions provisioned with strong automation and digital tooling. Compared with other regions, it also sees a stronger need to increase the availability of online and digital services to customers.

'COVID-19 has changed corporate thinking at the highest level. Security is most important now. We are moving to the cloud too. Having a 'Defense in Depth' strategy with multiple layers of security controls to automate and bullet proof our organisation.'
- IT Systems Engineer, Discrete Manufacturing, Singapore

Europe:
BCP, Flexible Network and Services

Universally, respondents across Europe have an active DX strategy. 47 per cent of all respondents were the CTO, CIO, Chief Security or Compliance Officer, making this the most technical audience. Some 87 per cent were also the final ICT decision makers. The other regions had more budget influencers. The biggest drivers for DX are to increase top-line revenue and personalise customer experience. While Europeans view employee health and safety as the most important business priority, enabling remote working is a close second. Translating the business to top ICT priorities, business and IT leaders in Europe are introducing new or expanding existing online UC&C tools, including video conferencing for remote working as well as rolling out standard ICT workspace solutions for remote workers. Both are tied on the top priority list. European respondents lead the other regions in their preference to accelerate cloud adoption and need to re-consider their WAN strategy.

70 per cent of European respondents are updating their BCP to reflect new realities posed by 'current and future pandemics,' putting in place the right policy frameworks for remote workers (e.g. security, compliance, customer privacy, etc.). 63 per cent are also planning for the possibility of long-term closures of branch offices, or reduction of the HQ corporate footprint. This compares with 40 per cent in North Asia and United States, and 52 per cent for SEA/ANZ. The European sentiment is to meet all of the stated IT objectives while improving overall security posture and meeting compliance commitments.

United States:
Pay-As-You-GO (PAYG), Commercial Flexibility

By some measurements, the United States is the outlier compared with all other regions. For example, it plans to reduce and/or re-allocate budgets more than what we are seeing in the other regions. Its preferences for commercial flexibility also stand out. The single biggest motivator for DX is cost savings, not top-line revenue generation, followed by the need to personalise the customer experience. More American companies had a BCP than other regions as a percentage, but the thrust was on focusing on the core business as opposed to planning for unforeseen external events. The primary business priority is employee health and safety and to minimise the impact on partners and suppliers (tied). The second priority is to double down on the efforts to support existing customers. Translating the business to top ICT priorities, the business and IT leaders in the United States are accelerating the rollout and availability of online and digital services in 73 per cent of cases. This is followed by the need for provisioning role-based ICT and setting up the policy frameworks for remote workers. In comparison with the other regions, there is less urgency to deploy UC&C or re-evaluate its WAN strategy. Likewise, only one in 10 businesses believe COVID-19 has changed IT priorities dramatically. American companies will be looking to improve their overall security posture and develop strategies to address skill shortages and staff absenteeism.

Keeping International Businesses Connected

Network infrastructure and collaboration tools play a critical role in keeping organisations connected around the world – and this is even more important in challenging times. At Telstra, our purpose is to build a brilliantly connected future so everyone can thrive. We provide a wide range of products and services to enable a flexible and scalable IT environment and allow your business to respond and adapt operations as required.

Our solutions include:

Collaboration Services	IPVPN Secure Mobile Access	Telstra Programmable Network
Integrated network and communications platforms to make virtual meetings easier for remote workforce with leading offerings such as Cisco Webex and Microsoft Teams	Provide private or secured network connection virtually on top of a public or shared network to a Telstra-based MPLS VPN	Burst bandwidth on demand in minutes and access 170+ Cloud Service Providers in over 35 global markets

Appendix

Author

Dustin Kehoe,
Services Director, GlobalData

Dustin.Kehoe@globaldata.com

Telstra

Telstra is a leading telecommunications and technology company with a proudly Australian heritage and a longstanding, growing international business. Today, we operate in over 20 countries outside of Australia, providing services to thousands of business, government, carrier and OTT customers. Telstra Enterprise is a division of Telstra that provides data and IP networks and network application services, such as managed networks, unified communications, cloud, industry solutions and integrated services. These services are underpinned by our subsea cable network, one of the largest in the Asia Pacific region, with licenses in Asia, Europe and the Americas, and access to more than 2,000 Points-of-Presence around the world.

GlobalData. | Telstra

Contact your Telstra account representative for more details.

Australia

telstra.com.au

International

telstra.com/global

Sales tg_sales@team.telstra.com

Channel Partners partners@team.telstra.com