Building a Resilient Web Infrastructure for the Digital Business Post–COVID-19

AN IDC INFOBRIEF | JULY 2020

IDC ANALYZE THE FUTURE

Sponsored by: CLOUDFLARE

CEOs' New Agenda in the Digital Economy: Trust and Resilience

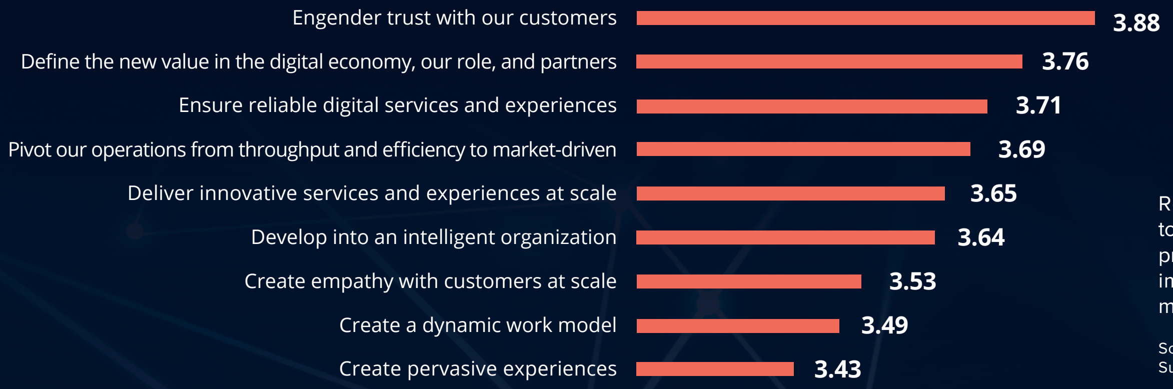
Engendering trust, defining new value, and ensuring reliable digital services rank highest in importance to a company's overall business vision, according to IDC's Asia/Pacific CEO Priorities Survey 2020.

These CEO priorities, against the backdrop of shuttered businesses to stop the spread of COVID-19, point to a stark reality: **In today's cloud era, companies that succeed in building trust with internal and external stakeholders — and strengthening their organisational resilience against business disruption — enjoy a distinct advantage**.

All-out efforts by governments across the Asia/Pacific region to stop the spread of the coronavirus have accelerated the pace of digital adoption to new heights. From online shopping and online learning to webinars and virtual events, staying digitally connected has become more important than ever. Digital connectedness is no longer an option but inextricably linked to the survival — and success — of business.

The resulting mass migration of employees, students, and other workers to the home is unprecedented and not without major implications for security and networks. For one, poor Web performance, unavailability of applications, and unsecured networks — these can *make* or *break* digital trust, and that means the difference between maintaining and losing revenue and customers.

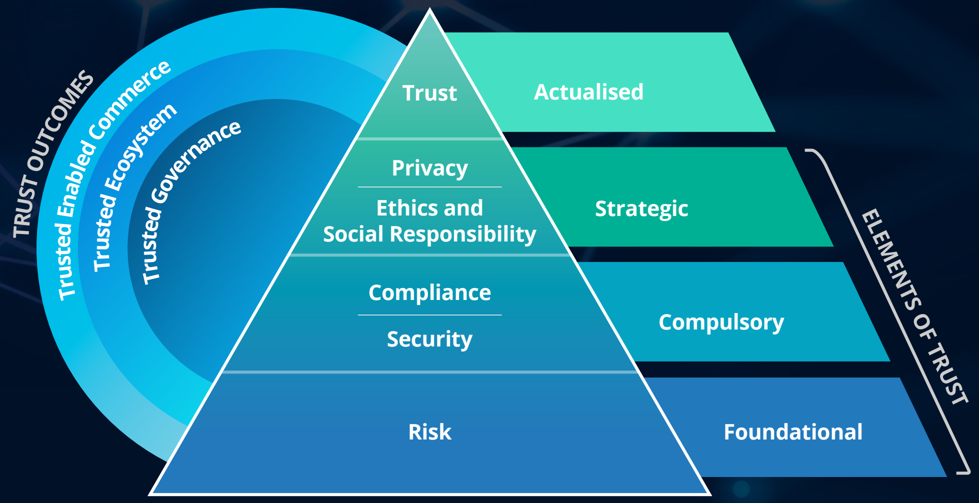
Asia/Pacific CEOs' top strategic business priorities



Respondents were asked to rank their strategic business priorities, with 1 being the least important and 5 being the most important.

Source: IDC's Asia/Pacific CEO Priorities Survey, January-February 2020 (N=80)

Trust is an uplevelling of the security conversation to include attributes such as risk, compliance, and privacy. Trust is about maximising returns and creating a differentiated impact on revenue, expenses, and shareholder value.



Source: IDC's Trust Framework

Confronting New Business Pressures: Remote Working

With businesses forced into migrating workers to remote working, extending office environments to the home throws up several issues, especially for those that have not had a work-from-home (WFH) culture.

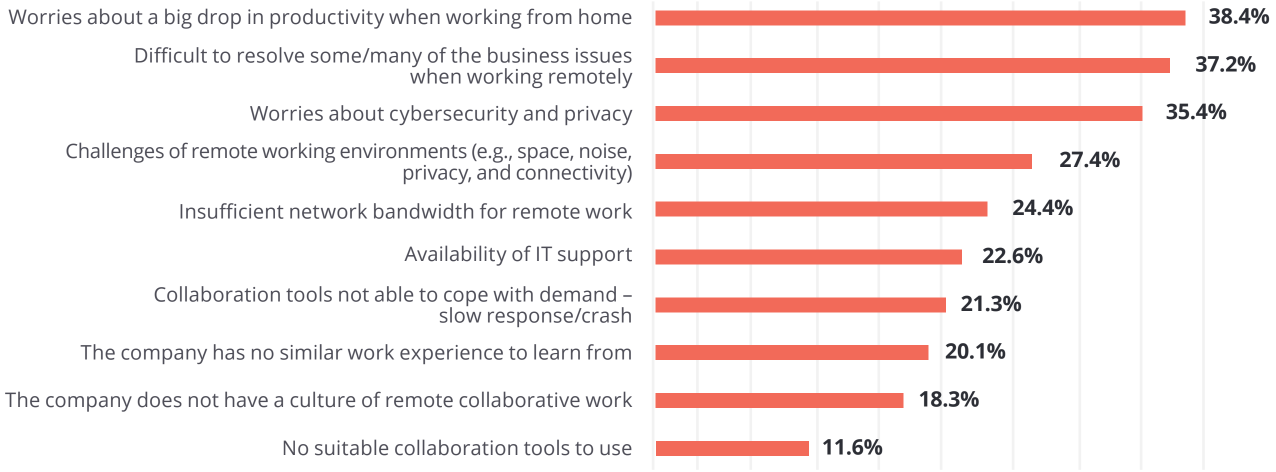
According to IDC's Asia/Pacific survey on WFH concerns and challenges, the biggest concern is the productivity of employees, alongside cybersecurity and ensuring employees have access to basic applications, such as email, file sync and sharing, and tools to collaborate.

In today's always-connected world, the immediate challenge for organisations across the board is in addressing the needs of their businesses, keeping employees engaged and staying connected with customers, vendors, and suppliers.

Employees who are working from home require remote access for a wide range of roles. While IT workers need secure, high bandwidth to access and ensure IT systems are running smoothly, other remote workers also require secure access to the same internal applications, online tools, files, and conferencing platforms as if they were in the office.

Productivity of remote workers, cybersecurity, and privacy are among the biggest concerns. Remote working presents a critical challenge as it requires access to be provided in a secure fashion.

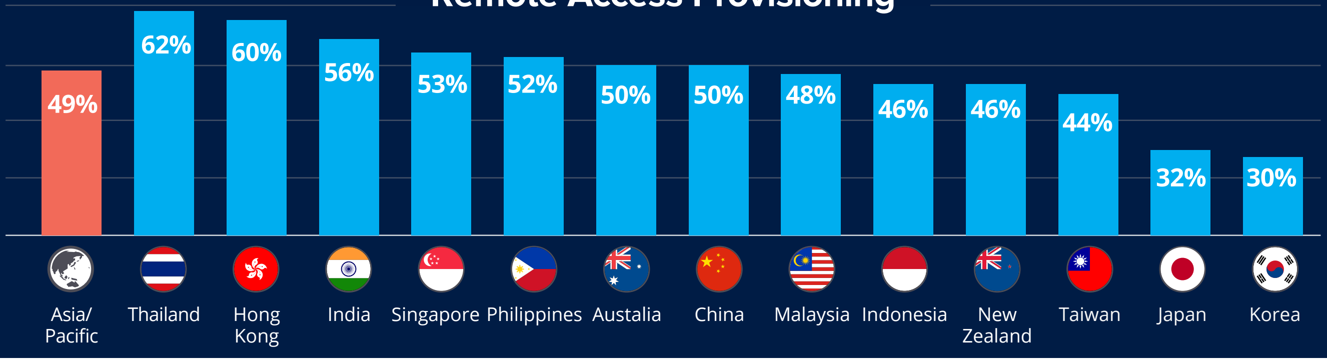
Top Remote Working Concerns



IDC's research on the impact of COVID-19 found that **60% of Asia/ Pacific employees surveyed said they needed remote access to be effective for 30% of their day. However, only 49% have remote access**.

Across the region, Taiwan, Japan, and Korea see the lowest percentage of respondents with remote access, compared with their peers in Thailand and Hong Kong. While security is generally the main concern, reservations about remote provisioning in Japan and Korea are largely due to corporate culture.

Remote Access Provisioning



Source: IDC Future of Work Employee Study 2020

Remote Access a Critical Employee Productivity Enabler

IDC's Asia/Pacific research bears out the importance of remote access technologies in keeping workers productive, a critical factor in enabling businesses to operate normally in uncertain times.

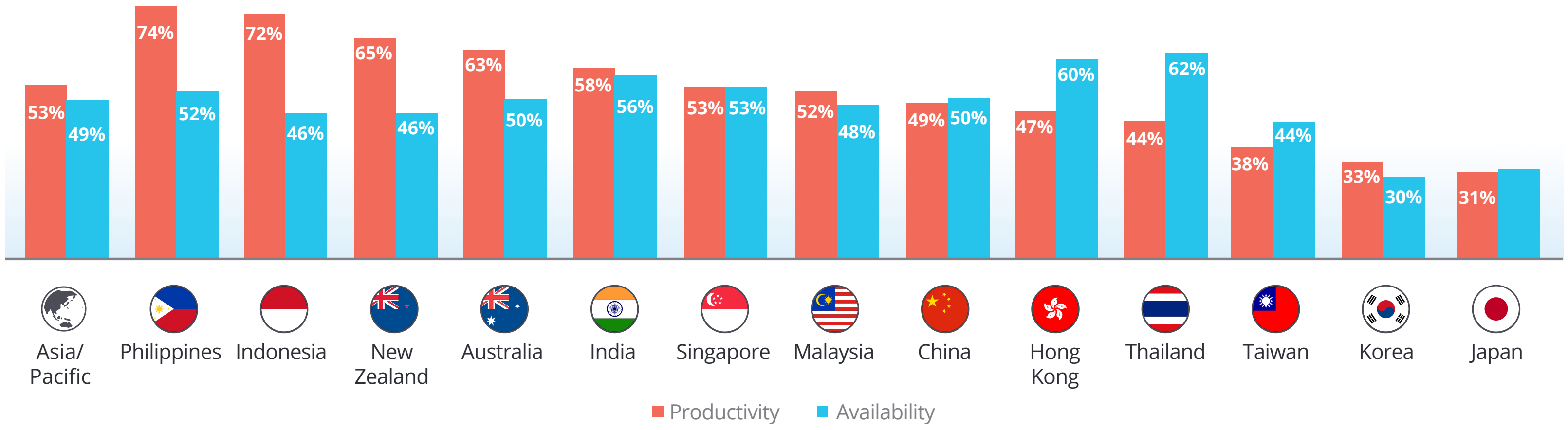
The markets in which demand for remote access is low also show higher levels of productivity driven by remote access, which could mean that increasing levels of remote access across the board could have significant productivity enhancements, assuming the infrastructure is designed for the anticipated capacity.

In Philippines and Indonesia, where traffic congestion exacerbated by geography can be considerably challenging, remote access drives productivity up significantly by allowing a "work from wherever" approach, be it on a remote island or from one's car.

In Japan and Korea, where the concept of remote work is not part of corporate culture and physical presence at the office is often considered more influential, it is clearly less understood how it can improve efficiency.

Australia and New Zealand could benefit greatly with an increase in secure remote access, as evidenced by almost two-thirds (63% and 65% respectively) of respondents indicating higher productivity due to remote access.

Productivity vs Availability of Remote Access



Source: IDC Future of Work Employee Study 2020

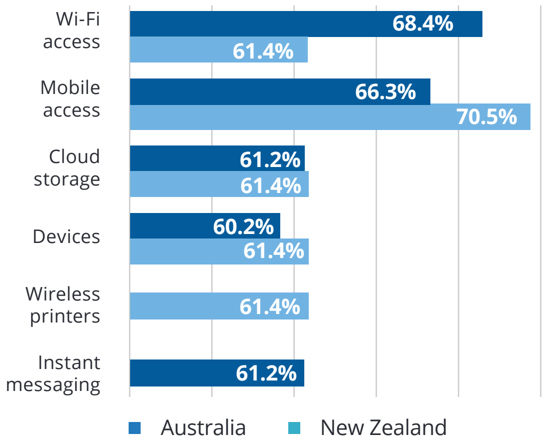
Top Employee Performance Enablers

Connectivity, Internet-connected devices, and online services all drive employee productivity.

Smartphones appear to be the device of choice for many communication activities. This is unsurprising in ASEAN which has some of the highest mobile usage across the Asia/Pacific due to the availability of affordable devices. Correspondingly, Wi-Fi and mobile access as well as access to cloud storage are high in these markets.

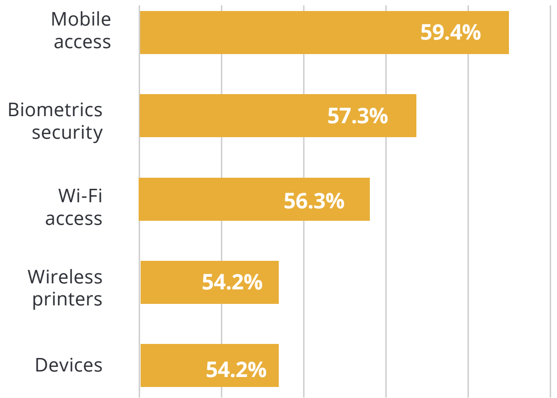
China sees Wi-Fi as a key driver, but this does not appear in the other markets. Collaboration tools do not appear as a top 5 in Hong Kong (at #9) but cloud storage does. Both Hong Kong and Taiwan see instant messaging as a key driver of productivity.

Australia and New Zealand



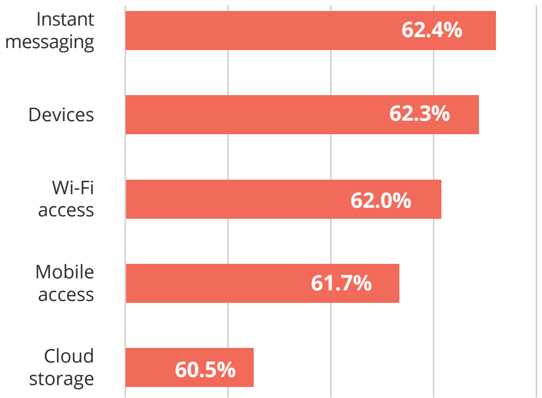
Similarities between Australia and New Zealand are around access, most likely due to geography, and cloud storage quite probably for the same reason. New Zealand has a reliance on wireless printing which could be a cause for security concern depending upon what content is being printed. Australia sees instant messaging as a key productivity enhancement.

India



Due to its vast geography and poor fixed line infrastructure compared to other markets, India is more reliant on mobile and Wi-Fi access. Devices requiring simple and easy-to-use security technology, such as thumbprint and facial recognition, are important and key to bridging the literacy and language gap in rural India.

ASEAN



Source: IDC Future of Work Employee Study 2020

Creating secure access to online tools and services will become mandatory during the pandemic and remain critical post–COVID-19.

Top Employee Communication Challenges

Further IDC research reveals several challenges that need to be addressed if businesses are seeking to boost employee productivity.

Difficulty in communicating and collaborating with external stakeholders topped the list of challenges for ASEAN respondents, whilst communication and collaboration within the walls of organisations emerged the bigger challenge for respondents in Australia and New Zealand.

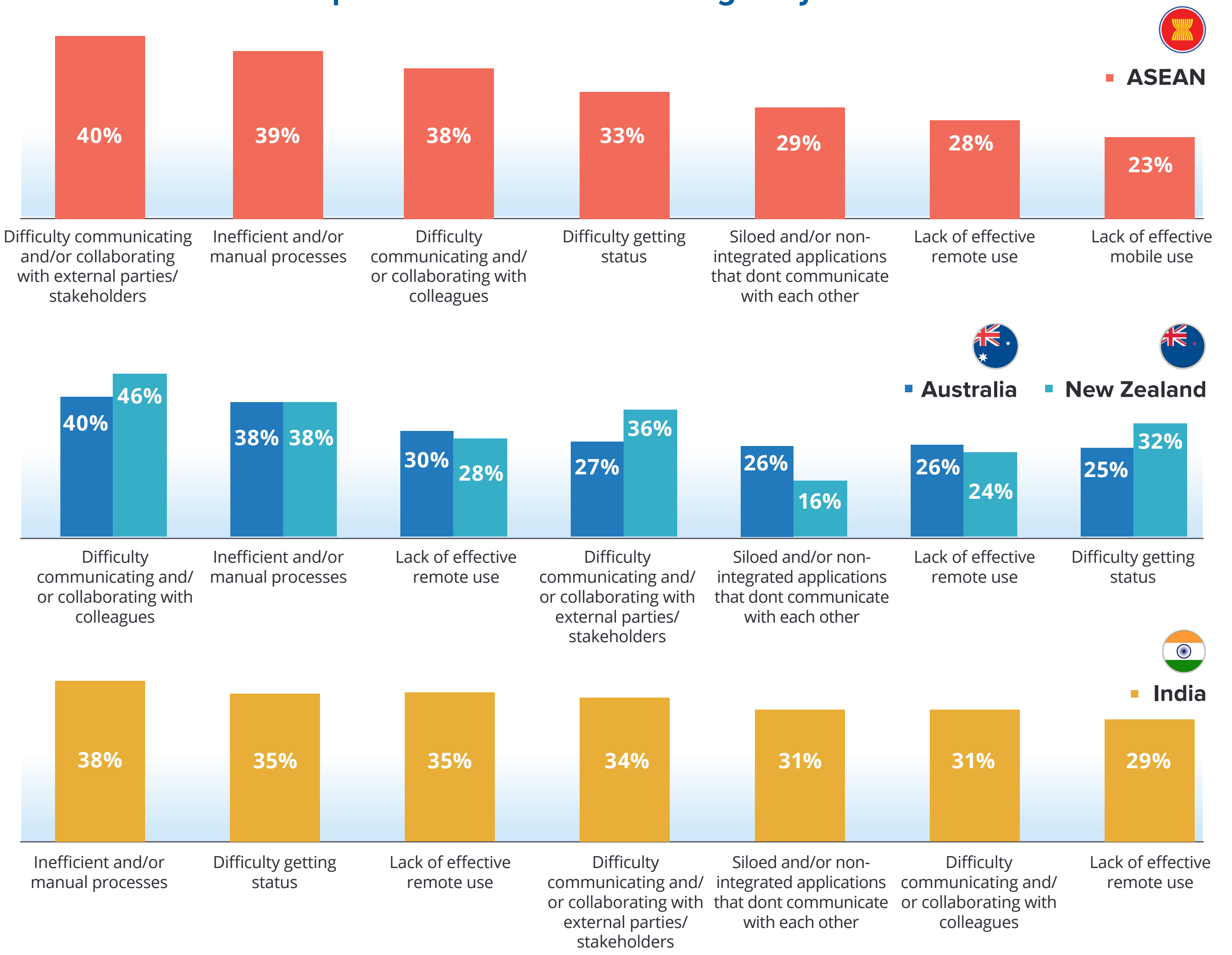
Inefficient and manual processes rank as the number 1 challenge for organisations in India (38%), but lower for their peers in Australia and New Zealand, and ASEAN.

Lack of effective remote use appeared as the number 3 communications challenge in the Australia and New Zealand as well as India.

But whether it is lack of communication and collaboration, manual processes, or lack of visibility into the state of operations, the urgent need to ensure fast, safe, and seamless access to applications, without sacrificing performance and security, is vital.

Businesses that have neither considered digitalising their existing processes nor prioritised providing secure remote access for their employees risk lagging behind their competition.

Top Communication Challenges by Market



Source: IDC Future of Work Employee Study 2020

Preparing for the New Remote Workforce With Cloud

Current events make it apparent that remote work and digital commerce are now critical to the survival of businesses.

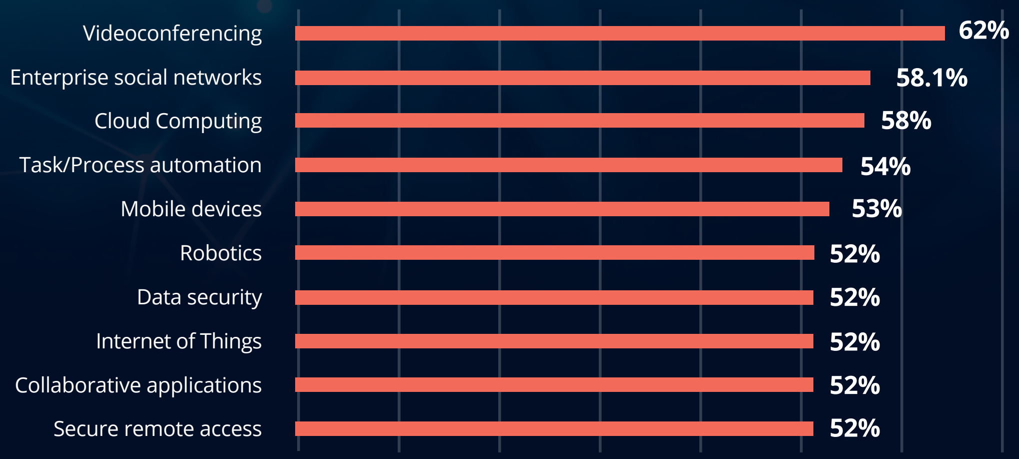
Business-to-business transacting needs to be undertaken online and in digital format whenever possible, whilst the teams of employees that support this effort need to do so from a remote location.

It is, therefore, critical that both digital and business store-fronts (in many cases a web site) and employee remote access, generally from their homes, are both made available and secure at all times.

Considering the COVID-19 challenges, businesses will not be returning to the old-style of work. The tools that ensure availability and security, along with remote access capabilities, will become a new essential component in any business of the future.

Ensuring a resilient web infrastructure is now, and will continue to be, a significantly important component of being able to conduct business.

Top Technology Investment Areas



Source: IDC COVID Wave 3 Study, May 2020

Self-discovery questions

Here is a checklist for IT Heads to consider as they prepare their organisations for the future of work.

Access

- Is remote access a major security concern?
- Are there concerns about exposing new holes in corporate firewalls?
- Is there a need for an authentication solution that can help defend against attackers using familiar single sign-on technologies?

Scalability

- Are there security, performance, and reliability concerns when it comes to multicloud deployment?
- Is consistency in enforcing the same security policies across all clouds a requirement?
- Is there demand for one solution that can scale geography and capacity?

Web application availability

- Are Web applications susceptible to outages and downtime due to spikes in traffic, high network latency or server outages?
- Is the current solution able to deliver business- and mission-critical applications with high performance and availability across the public Internet in a secure manner?
- Are there Web application performance and availability targets that require tools to monitor and report on the end-user experience?

Next Steps for a Resilient Digital Business

Business continuity is the first order of business. This means prioritising the ability to conduct business online, either on the Internet or through mobile devices, with support of remote employees — IT systems and critical lines of business.

IDC recommends the following:

Re-evaluate what business resilience means in this new environment for the business.
The focus of the business continuity plan must be on securing and ensuring the availability and reliability of systems. These include customer-facing and back-end systems, along with the need for IT to be able to support these systems remotely.

IDC predicts that by 2022, 50% of publicly traded companies will have embedded cyber-risk monitoring into their business planning and quarterly reporting. This, and the COVID-19 situation, will help garner strong support from the Board for delivering resilient web and remote access infrastructure. Funding will be less of a concern for a well thought-out plan.

Partner for cloud assurance in today's fast-changing digital environment.
Cloud computing will be a more important ingredient of the future IT architecture than it has been up until now, as it removes many of the infrastructure support issues, allowing organisations to focus on the business of doing business.

Partner right.
Look for partners that have the expertise and track record in securing cloud and web assets.

Think secure and simple.
Remote access will result in a significant increase in potential cyber risks, if not correctly addressed as early as possible, and as completely as possible at this point in time. Similarly, complex and difficult-to-use security systems will have a significantly negative impact on employee productivity, and so need to be avoided and replaced with elegant, simple to use, but secure, solutions. Look for partners that are most familiar with the securing cloud and web assets.

Assess cloud technology for a resilient web infrastructure.
Cloud providers can help address infrastructural issues and concerns, but there is still a need for secured access to the cloud for both employees and customers. This means ensuring not just access and availability but also its security. And because digital business is so critically important now, solutions that can assure the responsiveness of cloud-based applications should form part of an organisation's recovery strategy.

This IDC InfoBrief was produced by IDC Asia/Pacific Custom Solutions. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC. Any information or reference to IDC that is to be used in advertising, press releases or promotional materials requires prior written approval. For more information, visit: www.ap.idc.asia or email: AP_Permissions@idc.com