Ensuring business continuity during COVID-19

By Jonathan Scott, Standard Chartered Bank Chief Operating Officer, South Africa & Southern Africa

COVID-19 is quickly changing how the global economy operates. As people's behaviours shift and businesses implement remote work policies, it is up to organisations to take proactive steps to maintain as much operational continuity as possible. Chief Information Officers (CIO) in particular should immediately look to expand access and capabilities in two high-priority categories of technology, including digital workplace resources and digital technologies, to serve demand. Disruptive technology is changing the way we work and the nature of our workplaces. If digital technology is fully integrated into a company's strategy, it can benefit all employees and help businesses to thrive in a time like this.

As government measures limit the amount of travel previously undertaken by organisations, companies where remote working capabilities have not yet been established have had their operations disrupted or limited. Organisations are asking their employees to work from home in order to increase social distancing, however, ensuring business runs as usual can be a difficult task for companies without business continuity plans. CIOs can take the following steps to ensure employees are equipped to stay productive and keep the business running as usual.

Stay connected

Understand the typical workflow of people who are able to do their jobs remotely and identify the systems they need to access. These range from in-house communications platforms such as email, videoconferencing or instant messaging to Microsoft Teams or Skype. Organisations are quickly adapting to non-traditional communication applications, such as Zoom, which offers the "attendee attention tracking" feature, meaning employers can gauge how engaged employees are during virtual meetings. This helps remote workers stay on track and accountable to the wider team, ensuring business as usual, despite their change in work location.

In addition to being equipped with the necessary software applications, the hardware given to employees by the organisation plays a major role in ensuring employees have full mobility to work remotely. Although the organisation is responsible for providing employees with the full range of hardware needed to work remotely, it is also up to employees to ensure they are fully equipped with a laptop, charger and headphones, as well as any additional accessories they may need.

Build capacity and adapt

Organisations must quickly adapt in times of crisis to ensure business continuity. Depending on the type of business, this can be anything from scaling technology to increasing bandwidth and network capacity to cope with an increased number of employees who are working remotely. It is up to business leaders to assess employees' ease of access to internal networks. In some cases, the company will need to renegotiate their vendors' current offerings with flexible contracts to accommodate a short-term surge in online communication.

One of the critical tools for enabling efficient remote work in the banking industry is a robust virtual private network (VPN). A VPN is an encrypted connection that helps to ensure that sensitive data is safely transmitted.

In the last few weeks alone, we have seen a global increase in VPN usage. The rate of VPN usage soared by 53 percent in the USA, 36 percent in Spain, 29 percent in Germany and 21 percent in France[1]. However, many organisations are not equipped with a VPN infrastructure able to handle a large volume of employees that are working remotely, with the need to quickly scale-up proving increasingly challenging.

Identify security needs

Review the existing security infrastructure and assess what people will need to work safely. Take into consideration the devices employees will use (company-issued or personal devices), and the networks they'll be on (public or private). For example, in order to avoid security breaches, many organisations do not use external memory drives such as USBs to share files. Instead, businesses have turned to more secure cloud services to ensure encrypted files make it difficult for hackers and third parties to access.

If cyber security wasn't at the top of a CIO's list before, it should be now. Cyber criminals are well aware of the increase in employees currently working from home and are shifting their tactics to attack home networks, in an effort to infect devices that are connected to the organisation's VPN. The UK's National Cyber Security Centre has waned that Cyber criminals are exploiting the disruption caused by COVID-19 through a range of phishing and malware attacks which are likely to proliferate. Check Point, a cyber security firm has found that since January 2020 there have been over 4,000 coronavirus-related domains registered globally with 3 per cent found to be malicious and an additional 5 per cent suspicious[2].

To counteract the threat of cyber-attacks, employees must be kept informed and updated on policies and procedures around proper data usage and protection along with guidance on how to identify phishing and malware attempt.

Test, test and test again

It is to be expected that there will unprecedented strains on technology infrastructure during this time. To circumvent this and ensure business continuity, CIO's and their teams need to be testing infrastructure and resilience of the networks (such as stress testing to monitor and manage core systems), software and hardware regularly to ensure there is no down time for the business.

Prior to employees beginning their remote working routines, IT teams should ensure all staff are equipped with the necessary tools and knowledge to manage their communications and work flow.

-End-

[1] https://www.statista.com/chart/21147/vpn-usage-during-coronavirus-outbreak/
[2] https://www.ft.com/content/cbe2b35a-66d2-11ea-a3c9-1fe6fedcca75