

CIO'S RESPONSE POST-COVID 19 ECONOMIC CRISIS - THE ACTION PLAN

Mandar Marulkar, Customer Success Director, Nutanix

In my previous blog we discussed the paralyzing impact that COVID-19 has had on the business world, including how difficult it is to stay focused on digital business strategy amid the sharp uptake in business continuity and resiliency efforts.

CIOs must ensure not only that their companies survive the pandemic, but emerge ready to lead once it has passed. To this end, I called out five strategies for CIOs to consider:

- A. Build a Work from Anywhere Platform
- B. Evaluate network, security, and privacy needs
- C. Use technology to improve business productivity
- D. Redefine people practices
- E. Improve effectiveness through insights

In this blog, I elaborate on the first three strategies in detail.

A. Build a Work from Anywhere Platform

Building a work from anywhere (WFA) platform is the first key strategy. Note that I'm calling it a platform and not just a rollout of a few tools. Following are the key objectives.

1. Enable employees to serve customers from anywhere

It's critical that CIOs shift spending to technologies that support remote work, including laptops, desktop virtualization and desktops as a service (DaaS), and (to ensure secure access) virtual private networks (VPNs) and multi-factor authentication. IT teams need to understand the importance of cloud, virtual access, remote onboarding, and collaboration technologies. The requirement as I see it is of two distinct types – specialized workstations and generic compute needs.

Specialized workstations in a remote environment was once a difficult nut to crack, particularly for designers and engineers. Nowadays, one has access to robust solutions that can provide virtualized workstations for these users. Whether on-prem or in public cloud, you can provision even GPU-based servers to create virtual machines. Nutanix has solutions that help in accessing the entire virtual machine over a browser from any of device. In case you need to authenticate with a local USB port, users can install a client and get it authenticated. Licensing servers, file servers, user drives can be hosted anywhere in hybrid mode.





The second type of users just need a generic end point. During the initial days of the COVID 19 crisis, companies ordered laptops in large quantities—not unlike consumers panic-buying toilet paper—leading to a global supply shortage. This stockpiling doesn't make economic sense and the supply issue is likely to persist in the foreseeable future. I recommend proactively stocking thin or zero clients, or redeploying old laptops as thin clients, to address the supply-chain issue. I also recommend providing employees access to virtual computers to keep the business running even if laptops are unavailable.

2. Scale cloud and XaaS

The pandemic offers CIOs an opportunity to reframe funding around cloud and everything-as-a-service (XaaS). Go to your CEO, CFO, and board of directors, who may have once hesitated at switching from fixed capacity, old generation 3-tier architecture (much of which lays dormant), and suggest a variable cost model, such as hybrid cloud based on hyperconverged architectures.

Pushing all workloads to the public cloud may seem an attractive proposition, but I recommend you tread carefully. The best thing for companies to do is to analyze their current data and compute workloads before contemplating the move to cloud to figure out the costs and potential service impacts involved. It's important to work with a solution that analyzes the behavior of machines, applications, and workloads to figure out what will work best in each cloud solution. Cloud smart, rather than cloud first, ensures you've got the right cloud for each workload.

Companies should look at cloud as an architecture rather than as a destination. For many organizations, the best approach is to build private clouds that mimic public cloud architecture, and to design flexible hybrid clouds to help port workloads seamlessly across private and public clouds.

3. Invest in Software as a Service (SaaS)

Cloud productivity tools such as Microsoft O365, Zoom, Slack, Jira, and Salesforce make it possible to work from anywhere and from any device. These sorts of flexible solutions are critical for maintaining uninterrupted business. Employees can get almost as much work done from their phones as they can from their computers.

But rolling out these tools alone will not suffice. You must nurture a culture where your teams use tools like OneDrive, Microsoft Teams, and Slack to collaborate in the cloud. These tools provide a cohesive platform that will encourage your workforce to work on and co-edit files in real-time collaboratively, without any location restrictions.

4. Boost business resiliency

While business model innovation is important, boosting business resiliency should also be part of every business transformation. CIOs should speak with senior managers to improve resiliency in a way that aligns with corporate objectives. This starts with enabling critical activities the organization requires to keep moving forward, such as bandwidth, VPN access, and cloud storage. However, resiliency also includes optimizing service delivery while reducing threats and vulnerabilities, such as cyber attacks, natural disasters, and pandemics.



Business continuity planning is crucial with the WFA model; IT needs to reduce the likelihood of failure, while also preparing to keep the business running even in worst case scenarios. Ideally, business continuity will evolve and be exercised more as a strategic, rather than simply an operational, discipline.

B. Evaluate Network, Security and Privacy needs

1. Optimize network infrastructure

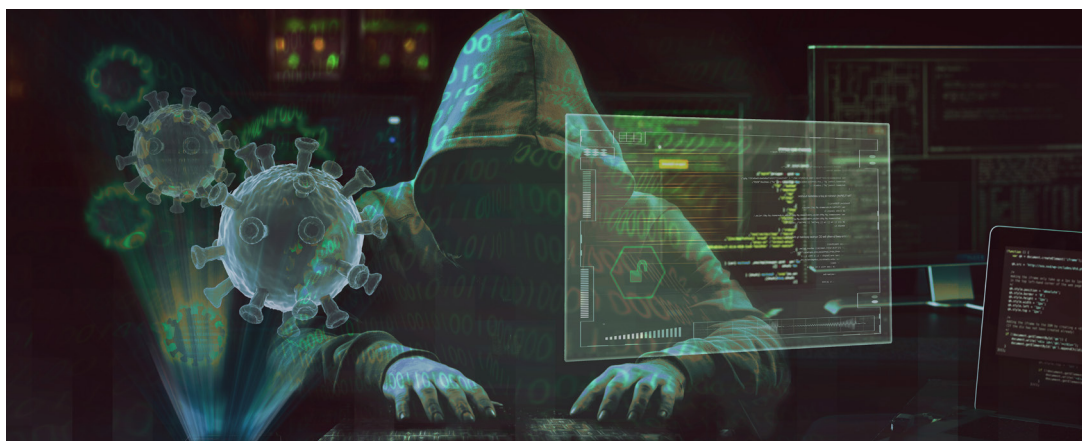
Having more remote workers means greater demand for a virtual private network (VPN). In addition to continuously monitoring VPN usage and adjusting license numbers and locations (reducing VPN idle timeout so unused licenses are available for other users), there are other steps you can take to ensure good connectivity.

For one, you could begin by investing into software-defined WAN (SDWAN) solutions versus traditional MPLS (multiprotocol label switching) or point-to-point links. SDWAN gives you the flexibility to upgrade bandwidth without getting into the complexities of buying ports and last miles.

Secondly, distribute applications across public and private cloud so that all the traffic does not flow into your corporate network. Provide clear communication on which applications require VPN, so employees only use it when necessary. Using it for all online work means traffic routes to datacenters, rather than employees' home offices, which will tank performance. Also, facilitate firmware upgrades and reboots of infrastructure equipment to provide better connection stability.

2. Reexamine your cyber security infrastructure

WFA requires separate risk assessment both from a cyber security and data privacy perspective. Unmanaged end points create additional risk of getting compromised from advance malware. Also many IT teams do not fully understand the architecture required for securing workloads in public cloud. Every company needs to start with standard security measures, including two-factor authentication, data encryption and secure transit,





and advanced security settings on physical devices and virtual desktops, to help ensure that data stays safe, even when employees are accessing systems remotely. They should have well-documented RBAC policies. They also need to architect security for cloud infrastructure using

- data leak prevention technologies
- virtual next generation firewalls (north-south)
- microsegmentation across virtual machines (east-west)
- advanced malware protection
- network and end-point anomaly detection
- sand boxing
- tools and practices for thwarting advanced phishing attacks.

3. Understand Data Privacy needs

Concerns about data governance are ongoing, and specific requirements of the GDPR and country-specific data privacy acts need to be addressed on multiple levels and by various departments within an organization. These regulations carry stiff penalties for non-compliance. Enterprises need to design their architectures to address requirements like the "right to be forgotten" and the "right to erasure." This must be achieved across all data repositories and all environments, including private, public, and hybrid clouds.

C. Use Technology to improve business productivity

1. Focus on task automation, process augmentation, and job amplification

Whether you're using robotic process automation or machine learning (ML), or the hybrid of both that comprises intelligent automation (IA), you have a great opportunity to start scaling up investments in ML and other advanced automation technologies to augment a capacity constrained workforce.

With the advent of cognitive technologies and sophisticated products, as many as 50 percent of our traditional jobs are at risk as software bots take over automated tasks. But remember that using powerful BOTs is not simply about reducing the number of employees in companies. It's about competitive efficiency and effectiveness. Only if we automate faster than our competitors and automate a broader number of tasks, will we have a competitive edge. Falling behind is bad enough when shifts in the market are linear; it becomes significantly more problematic when the shifts are exponential. Don't forget that automation can mean freeing up employees for different work that brings greater value to customers.

2. Boost customer engagement with self-service

Companies should ramp up their digital strategies by investing in customer engagement, self-service, digital workplace and knowledge management tools. For those who haven't built self-service capabilities, there's no better time to start. Self-service channels and platforms will help employees, customers, and partners get what they need with little to



no intervention from IT and the business. Transparency about service and process changes are critical to maintaining customer satisfaction. Collectively, these tactics will improve business resilience and create a path to future profitable growth.

3. Balancing between surveillance and trust - measuring productivity

Organizations need to understand work-related activities so they can have a clearer picture of employee productivity; objectively measured productivity levels help keep the company running even without workers being physically present. Developing this framework during standard operations helps establish productivity benchmarks that are critical to implementing successful work-from-anywhere programs.

These benchmarks should include actual time spent completing work (including each team's core responsibilities), attending meetings, etc. Once benchmarks are established, goals can be set as necessary to minimize distractions, eliminate unproductive habits, and increase actual productivity levels wherever needed. These benchmarks and goals hold constant no matter where any employee works from. They become the objective standards against which any employee's efforts can be judged, instead of relying on "the time put in at the office." Managers should have a built-in platform for determining the success of any project or team, as well as mentoring and managing employee efforts and output.

Organizations should have insights into the impact WFA has on productivity, efficiency, and employee engagement. They need a data-driven approach that illuminates work patterns and behavior within the organization. This allows them to automate the reporting of work patterns, time, and activity, and helps create baselines of expected work output as well as team goals. Tools need to be deployed to automatically gather and analyze the data to measure team engagement and productivity. CXOs can get a cross functional view of the efforts, while managers can see true capacity utilization, and employees can get insights into their own work routines.





Conclusion

The WFA platform, robust evaluation of network, privacy, and security needs, and proper use of technology to boost productivity, will be the top three strategies for setting the organization on a new trajectory. These approaches, along with a culture of trust and collaboration, will help the organization prosper during these volatile times.

Stay tuned for the next and final edition of this blog series, where we will focus on people practices and hiring.



AUTHOR 'S BIO:

Mandar is a Customer Success Director at Nutanix, a leading Enterprise cloud technology provider. Before joining Nutanix, Mandar was Chief Digital officer at KPIT Technologies. In that role, he was responsible for creating digital offerings for customers, driving digital transformation for KPIT, building Think Digital culture, setting up Digital infrastructure and alliance ecosystem. Mandar has over 25 years of experience and played roles of Chief Information Officer, Chief Information Security officer and Head, Infrastructure Management Services business in the past.
