+ Know Your Network

The Technology You Need for the Work-Anywhere Future

BROUGHT TO YOU BY COMCAST **BUSINESS**

Nimble companies with a hybrid model to support office and remote workers are positioned to succeed in the post-Covid economy.

Even as some workers in some parts of the country have begun returning to the office, experts and executives anticipate that many businesses will permanently employ remote workers at much higher levels than they did pre-Covid. Many organizations will settle into a hybrid model, where some employees are in the office and some are remote.

The distributed workforce has created a sudden and dramatic shift in the way that companies do business. Whether serving customers, connecting with staff or communicating with vendors, businesses are approaching operations today with a remote-first mindset. That may require a reshaped network topology that can help facilitate higher levels of agility and accommodate the increased need for bandwidth required by a greater focus on digitization and data strategy.

We talked to **Jay Reed**, a partner with CIO consultancy CIO Suite and former CIO of Aimbridge Hospitality, and **Christian Nascimento**, Vice President of Product Management at Comcast Business, about how IT decision makers are finding new ways to support employee work and improve customer communications.

More than half of HR leaders say that poor technology or infrastructure for remote working is the biggest barrier to an effective transition to a distributed workforce. What's been the experience of IT executives over the past few months as they transitioned to supporting a hybrid employee base that includes both in-person workers and those logging in from a distance?

Jay Reed: Those who already had a good, remote solution that was scalable, along with good documentation and policies around remote work, had it much easier than others. The most prevailing need from all business departments was the need to better communicate.

Everybody had email, but products like instant messaging or chat, and video conferencing, those obviously increased across the board. That changed the type of traffic, so there's less email but more bandwidth demand. Also, hackers might act like they are one of the employees working from home on chat or video conferencing platforms and try to get into your environment. CIOs have to support these new tools, but also make sure that they keep these tools cyber secure.

Christian Nascimento: The pandemic accelerated the openness of organizations to work-from-home or remote work. People who never would have expected to work outside of an office realized that they could be as productive or even more productive while working from home, as long as they have the proper connectivity and applications available to them.

Many businesses already had some remote working capabilities or procedures in place, and the rest quickly scrambled to implement employee communication applications. But as remote work becomes a long-term reality, IT executives are well aware of the need to fortify work-from-home setups with business-grade Internet connections that provide the reliability and security needed to conduct business.

It really comes down to, how do you ensure that your remote employee has the same connectivity available to them that someone at the office does? And many people were not designing their home network, or making home internet speed decisions based on what they would need to work full-time on a permanent or semi-permanent basis – even without taking into consideration increased activity in the home outside of work, like e-learning, increased gaming and streaming.

How IT Supports the Distributed Workforce

Most common technology measures taken to accommodate remote workers

Read the report on "Crisis-Tested IT Teams Accelerate Digital Agility Plans"

Read the report on "Crisis-Tested IT Teams Accelerate Digital Agility Plans"

How has the shift to remote work impacted network and connectivity requirements?

JR: There are a lot of bandwidth concerns, when people are working from home. When your family is there, you've got kids who need to stream to access online classes or to play videogames. So you're competing with the kids, plus there are all the other devices in the house, like smart speakers, that could be on the network. CIOs should want workers to use a VPN or a guest network in their home and prioritize their traffic over the kids' gaming traffic.

CN: Companies are realizing that the corporate network now is not just the connection on the premises, but it's the connectivity on multiple premises where the workforce may live and now work. In this cloud-based application world, you have the ability to access many or all of the tools that you need on any number of devices.

The foundational need is internet connectivity speed, to allow the breadth of activities – uploading files, downloading presentations, collaborating on documents and participating in video conferences – that a remote worker participates in. Beyond that, LTE backup for connectivity is a smart move, as hours of backup battery power and an automatic wireless connection can help a remote worker remain connected, even when weather doesn't cooperate. Finally, a remote access solution, like a VPN (virtual private network), can ensure that a telecommuter has access to files, systems and applications on the corporate network in a secure way.

We've had some customers ask for their senior leadership to get commercial modems for wired internet connections in their homes. That way executives have a dedicated connection for their work activities and can stay connected regardless of what their family or children are doing on the network.

Training employees in best practices around cybersecurity was among the first tasks that IT implemented at many companies when they put remote work in place. Why is cybersecurity so important when supporting a distributed workforce, and what other measures are companies putting in place?

JR: It used to be that virus protection was enough, but now we're moving more toward endpoint protection, where you're not only looking out for viruses, but you're able to monitor your device using artificial intelligence.

With endpoint protection, you're monitoring for the use of PC operating system commands that are indicative of a bad actor on the machine or network. If something is detected, it will signal auto shutdown capabilities to block those commands from executing and alert the group monitoring the situation, so they can restrict and investigate. That level of security should be the norm now.

CN: Security becomes even more critical when you have a distributed workforce because you don't have the same certainty around what security measures are in place when the workforce is connecting from locations outside of the business premises.

Using a VPN enables a remote worker to connect directly to the corporate network, which will allow the remote worker to leverage the functionality and security of that network. So there is real value there, especially if the remote worker needs to access certain applications.

Software-defined networking can assist even further by giving IT managers the ability to control applications, users, and traffic on this now distributed corporate network — all from a single pane of glass.

Some experts predict that more than a quarter of the workforce will permanently work from home at least a few days a week, post-coronavirus. If a distributed workforce becomes the "new normal," what will IT decision-makers need to think about going forward?

CN: All facets of business are changing. For example, CIOs and IT leaders need to think about what it looks like to onboard an employee. It used to be they just needed a laptop and a phone, but do they need a camera now? What type of internet connection do they need?

It may become the case where IT managers are purchasing a range of connectivity solutions for employees at a greater scale to make sure that they're connecting in a way that's not only safe and secure, but also has the appropriate bandwidth for the new work environment.

Technology leaders are starting to rethink planning and purchasing decisions. They need to think through all of the ways that business could change and make sure that the technology that they're deploying gives them the flexibility to manage through these changes.

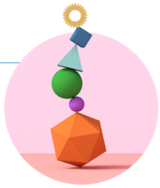
Know Your Network

Know Your Network explores how tech decision makers can use network technology to enhance their business

Business Agility

The CIO's New Mandate: Deliver Digital Agility Now

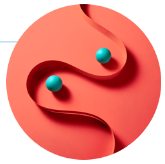
Read Now →



Customer Experience

Network Solutions Create Digital Agility for Businesses

Read Now →



Customer Experience

Expert Advice on How to Enhance CX With Software-Defined Networks

Read Now →

Brought to you by

Brought to you by

COMCAST BUSINESS