REMOTE-WORKER EMPOWERMENT: ENSURING THE RELIABILITY OF REMOTE CONNECTIONS

THE EFFECTIVENESS OF REMOTE EMPLOYEES IS ONLY AS DEPENDABLE AS YOUR NETWORK. HERE'S HOW TO MAKE SURE YOUR REMOTE CONNECTIONS – AND YOUR WORKFORCE – STAY UP AND RUNNING.

Has your organization joined the ranks of those with a mostly remote workforce? There's good news and bad news.

The good news is that the work-from-home model has delivered unexpected benefits. From an HR perspective, employees now have greater flexibility to balance their professional and personal lives. "That can make them more productive and increase their job satisfaction, improving engagement and performance," says Chris Park, director of Workplace Experience Services and Technology for Computacenter.

From a business perspective, a remote workforce allows you to reconfigure your buildings to shrink footprint and save costs. You can reduce expenses for heating, cooling, electricity, and real estate. You can also reconfigure spaces for team collaboration and customer engagement.

The bad news is that remote work involves a single point of failure: your network connection. Actually, it's multiple points of failure, because everything from an employee's home router and WiFi signal to your organization's VPN tunnel can cause a break in the chain. And when employees can't connect, your business grinds to a halt.

That's why smart organizations are making investments – in technologies and in strategies – to shore up the reliability of their remote connections and optimize the uptime of their remote workers.

RISE OF REMOTE, THREAT OF DISRUPTION

The Covid-19 crisis has dramatically accelerated the adoption of telecommuting – and the technologies that enable it. The videoconferencing market has exploded. Deployments of collaboration tools have soared. Investments in desktop as a service, which separates the desktop environment and applications from the user's device, have skyrocketed. (See the Figure.)

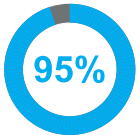
FIGURE: GROWTH IN REMOTE-CONNECTIVITY TECHNOLOGY

as much as **600%**

Growth in collaboration tools such as Microsoft Teams, Cisco Webex, and Zoom in the first months of the Covid-19 crisis[1]

2X

Projected growth of the global videoconferencing market, from $6B in 2019 to $12B in 2027[2]



Growth in desktop-as-a-service (DaaS) investments in 2020, to $1.2B[3]

But remote work presents a host of new challenges. For starters, most employees' home-network equipment is consumer-grade, not business-grade. They often have problems with WiFi, which is how most of them connect to the internet. They're subject to unexpected outages – for example, when a neighbor digs a hole and severs a fiber-optic cable.

In addition, "many home connections are asymmetrical, which means they have a lot of bandwidth coming in, to handle video streaming, but not a lot of bandwidth going out," explains Dan Brunton, systems engineer for Intel, a Computacenter partner. "We've all experienced times when co-workers say they can't access a conference call. That's typically because of bandwidth issues."

IT support is another challenge. Because workers now have to interact with your Service Desk remotely, they can find it harder to resolve issues. That will affect perceptions of the IT function, Park predicts.

"When people talk to the IT department, it's often because they have a problem, and those interactions can be strained," he says. "Working remotely only exacerbates those challenges." In response, you'll need to invest in support services, tools, and skills that make remote issue resolution easier.

Remote work also raises the bar on cybersecurity. "Endpoints tend to be the weakest link in the security chain, because they're not behind the locked doors of the datacenter," Park notes. Security teams have always struck a balance between protecting against cyberattacks and giving users easy access to the capabilities and data they need. But "when your entire workforce is working remotely, you might want to err on the side of safeguarding your network," Park says.

REMOTE STRATEGIES YOU CAN CONNECT ON

Several strategies can boost the reliability of your remote connections. Start with access to applications and data. While you might need to keep mission-critical resources behind your firewall, you can migrate appropriate applications, such as collaboration tools, to the cloud. That will enable employees to avoid VPN bandwidth restrictions. It will also allow them to use a mobile device to access resources if they have an issue with their laptop.

"The move to cloud-based applications has been a trend, and the pandemic just accelerates it," Brunton says. "The cloud lets you scale up quickly and smoothly in response to market changes – like when you suddenly need to convert an entire workforce to remote access."

Next, educate employees on how to set up a reliable home network. "Remote work shifts some of the responsibility for network reliability from IT to users," Brunton believes. Employees might need to consider:

- Subscribing to a higher-speed internet service
- Upgrading the standard router that comes with their internet service
- Switching to WiFi 6, which can better handle multiple simultaneous devices

Your organization should consider whether it can help optimize home networks. For example, you might offer workers a stipend for everything from headsets to mobile devices. “In the future, organizations might provide hardware such as routers, as well as configuration support, for home networks,” Brunton predicts.

Finally, prioritize your connectivity investments based on user personas. Some roles might be able to handle a lot of their work offline. Company executives might have a greater need for always-on access. “You could provide executives with a cellular hotspot to ensure a connection even when their internet is out,” Brunton says.

Your employees will probably continue to work from home for the foreseeable future. Investing in the reliability of your remote connections will help make sure your far-flung workers can optimally contribute to the success of your business.

GET IN TOUCH

While you might need to keep mission-critical resources behind your firewall, you can migrate appropriate applications to the cloud. To learn more, visit us at www.computacenter.com/us.

1 “Use of Cloud Collaboration Tools Surges, and So Do Attacks,” CSO , May 2020.
2 “Video Conferencing Market Forecast to 2027: COVID-19 Impact and Global Analysis by Type, Deployment,” Research and Markets, April 2020
3 “Forecast: Public Cloud Services, Worldwide, 2018-2024, 2Q20 Update,” Gartner , July 2020

Computacenter

Computacenter(US)
2 Bryant St, Suite 150, San Francisco, CA 94105

www.computacenter.com/us
1 800-228-8324