DAILY INDEPENDENT

Virus concerns drive telecommuting trend, technologies

Matt Roy

August 6, 2020

Nearly every aspect of life has been transformed in the wake of the ongoing COVID-19 public health crisis — and the American workplace is no exception, as the number of employees working from home has skyrocketed this year.

Following implementation of stay-at-home orders in late March, the portion of U.S. workers telecommuting doubled as compared to before the novel coronavirus outbreak, according to a recent report from the Brookings Institutions.

“The COVID-19 pandemic is, among other things, a massive experiment in telecommuting. Up to half of American workers are currently working from home, more than double the fraction who worked from home (at least occasionally) in 2017-18,” the April 6 reports states.

An article published this week by the Associated Press suggests the telecommuting trend will likely continue, even after concerns over COVID-19 fade; this may help some workers, but could harm businesses that traditionally relied on offices and office workers to survive.

Citing University of Chicago researcher Steven Davis, the AP report concluded “… even after the virus has been brought under control, the proportion of people working from home will triple compared with pre-pandemic levels. That could result in the shuttering of many restaurants, coffee shops and other downtown businesses.”

A June 11 report from the CATO Institute drew similar conclusions.

“The rise of remote (or partially remote) work will likely be the next step in the long term trend of technology making people’s careers more satisfying and productive … The dramatic rise in telework amid the pandemic is a radical experiment, but its effects will be long lasting,” the report states.

CATO argued the trend is not only beneficial to workers, but could also provide a boon to employers, based on research published in the Quarterly Journal of Economics in March 2015.

The study followed a cohort of 16,000 call center employees at a Chinese travel agency, who were randomly assigned to work from the office or from home for nine months. Among the key findings were increases in productivity and happiness among telecommuters.

“Home working led to a 13% performance increase, of which 9% was from working more minutes per shift (fewer breaks and sick days) and 4% from more calls per minute (attributed to a quieter and more convenient working environment). Home workers also reported improved work satisfaction, and their attrition rate halved …” according to the study.

After the study, the Chinese company offered the work-from-home option to all of its employees.

Who can telework?

The U.S. Bureau of Labor Statistics in a June report revealed 31% of those employed before the novel coronavirus outbreak had switched to working from home. But even before concerns about social distancing arose, workers were more and more likely to choose remote jobs.

Based on data from the American Time Use Survey for 2017-18, the agency reported on which workers and professions believed they were most able to adapt.

That belief varied widely based on education level, with those holding a bachelor’s degree or higher (67.5%) saying they were most likely to be able to telework. Work from home was less attainable for those with only some college or an associate’s degree (36.4%); those with only a high school diploma (24.5%); and those with less than a high school diploma (10.7%).

Age appeared to be less of a factor, with workers ages 25-54 (46.7%) responding similarly to those aged 55 and over (48.1%). Workers 24 and under (23.7%) were about half as likely to work from home.

Gender appears to play a role as well, with men (40%) somewhat less likely than women (47.6%) to work from home; while marital status also appeared to be a factor, with married workers (50.2%) substantially more likely to telework than single workers (34.4%).

Considering race, non-Hispanic whites (48.7%) were most likely to be able to telework; Blacks (39.5%) were less likely; and Hispanic workers (28.9%) were least likely.

Not surprisingly, professional trades — especially sedentary, technology-based pursuits — were easiest to adapt to the home office.

The top five fields for remote workers were: management, business and financial occupations (86.6%); financial activities (77.9%); information (71.2%); professional and business services (69.9%); and public administration (65.2%).

Among occupations that could possibly work from home, the bottom five least likely were: leisure and hospitality (13%); agriculture, forestry, fishing and hunting (8.3%); installation, maintenance and repair (1%); production (.4%); and transportation and material moving (.3%).

Security concerns

The work-from-home trend has been fueled primarily by advances in communications technology. Namely, the near-universal ease of sharing information and communication via the internet to conduct business. This includes expanded access to wifi networks, portable computers and other devices, and popular and easy-to-use tele-meeting applications, like Zoom, Skype and Facetime.

To work from home, an employee must have a secure and reliable access to the internet, as well as to internal files servers and other resources at the company. They will use hardware provided by an employer or may configure their own computer or device for the job, a practice called “bring your own device,” or BYOD.

But as workers increasingly sign up to telework, hackers, identify thieves, corporate spies and other bad actors — *as ever* — seek ways to identify and exploit network vulnerabilities, posing a risk to businesses and their employees.

The National Institute of Standards and Technology at the U.S. Department of Commerce studied the issue and published a report entitled, "Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security," in July 2016.

The institute warned of a variety of risks.

"All the components of telework and remote access solutions, including client devices, remote access servers, and internal resources accessed through remote access, should be secured against expected threats, as identified through threat models. Major security concerns include the lack of physical security controls, the use of unsecured networks, the connection of infected devices to internal networks, and the availability of internal resources to external hosts," the agency stated.

But even on secure, properly functioning networks, the use of third-party and employee-owned devices presents a special challenge to IT departments, according to the agency.

"There are additional security concerns for organizations that permit the use of client devices outside the organization's control, referred to in this publication as third-party-controlled technologies. These include contractor, business partner, and vendor-controlled devices, as well as personally owned (BYOD) employee, contractor, business partner, and vendor laptops, smartphones, and tablets," the report states.

Even with agreements and controls in place, tracking and enforcing compliance can be difficult. Those who disregard the rules may expose themselves and their companies to infected files, malware and other vulnerabilities.