Sending them home was the easy part: IT departments are bracing for the challenge of keeping employees safe when they can work anywhere, anytime

A hybrid workforce in which some workers are remote and some are hybrid will push many companies to broaden their cloud computing and security. Kosamtu / Getty

- **Remote work was the easy part — IT departments are preparing for the challenge of office returns.**
- **Rather than returning to the office in a mass migration, employees hybrid work routines will vary.**
- **Security investments now will pay dividends in keeping workers safe from cyberattacks, experts say.**
- **See more stories on Insider's business page.**

It turns out, sending workers home to work may have been the easy part.

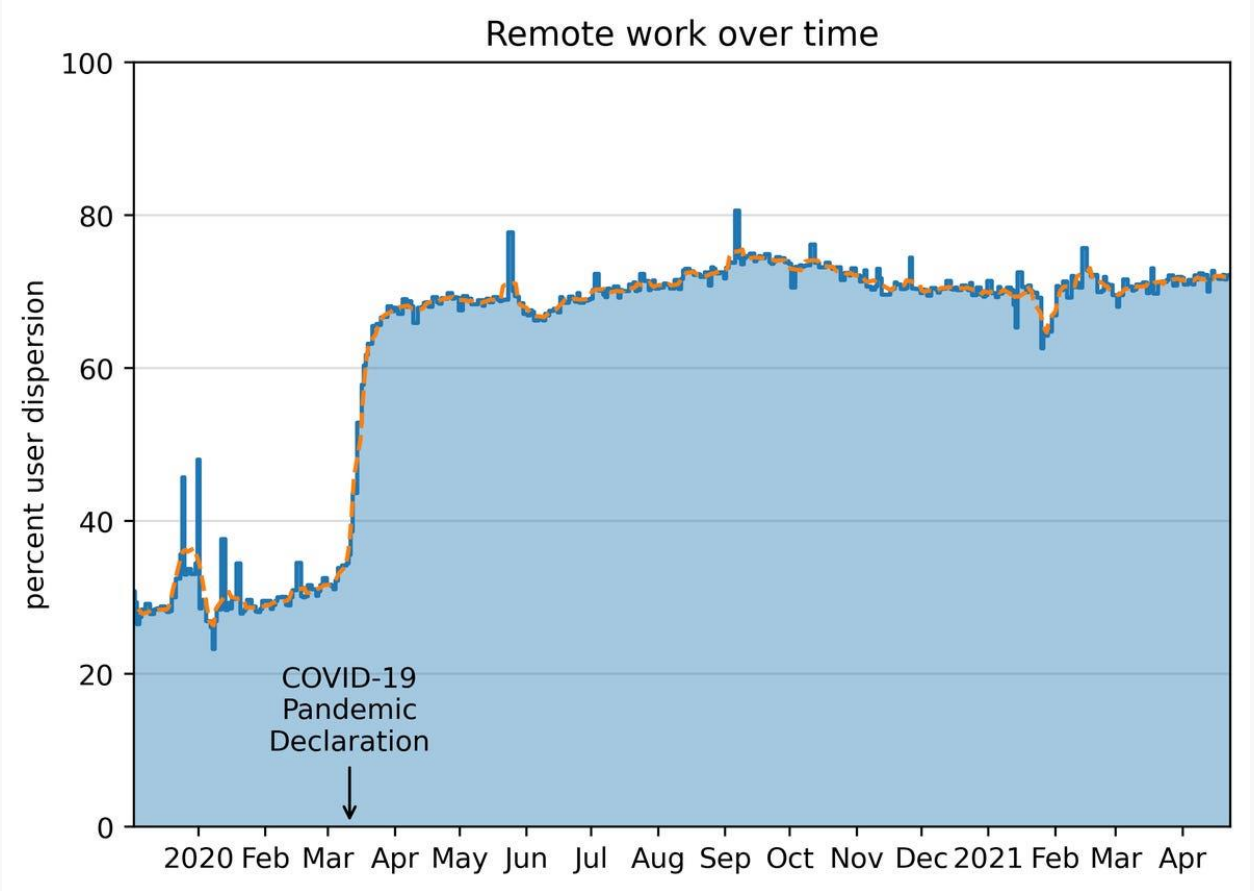
"Coming back scares the heck out of me," Tim Nall says. As the chief information officer of Brown-Forman, the 151-year-old alcohol and beverage brand that makes Jack Daniels, Nall must keep an eye on the productivity and security of 5,000 workers.

"We're going to have people in the office, people in their homes, people in different offices," Nall says. "It's definitely going to be a challenge."

More than 140 million Americans have received at least one vaccine dose – roughly half of US adults – and some companies are eager to return to offices as the threat of COVID-19 wanes. Google is pushing for a return to offices, capping employees' work-from-home to 14 days per year, while JP Morgan Chase CEO Jamie Dimon predicts that no more than 10% of his employees will work from home permanently.

But early data suggests that most offices won't be filled to full capacity anytime soon. In 2020 we went from working in the office to all working remotely. In 2021, we'll be both, and every employee will have their own path, Sanjay Beri, the CEO of the $3 billion cloud security startup Netskope, told Insider. "Every company has become more geographically dispersed. People are everywhere."

A recent PwC survey of US executives found that only 20% of employers want workers back in the office five days a week, even as companies like Atlassian give their employees unprecedented flexibility to work wherever they want on a permanent basis. In a separate survey of offices based in New York City, the average employer said they expect 56% of workers to return to offices on a regular basis while the rest work remotely.



This Netskope graphic shows the steep increase in remote work, which has not receded. Netskope

Even as workers trickle back into offices, employers are signalling that they'll grant workers flexibility to come and go from offices as they please to keep capacity low in the wake of the pandemic. But all of that flexibility, and all of that uncertainty, introduces new kinds of challenge for IT departments everywhere.

Because while the move to remote work certainly wasn't a walk in the park, it was manageable: You knew, more or less, where every employee was located and how they were connecting to the network. With employees more freely splitting their time between the home, the office, and perhaps even the open road as a digital nomad, the situation gets much more complex. That complexity creates opportunities for the bad guys to exploit, the experts warn.

John Davis of Palo Alto Networks, a vice president in the area of public sector enterprises like government agencies, told Insider that "What we see most is hybrid – it's part on-prem, part remote. And when it's cloud-based, it's multi-cloud. So security is an enormous problem."

The hybrid workforce is inevitable, but will make protecting employees a challenge

The hybrid workforce is inevitable, says George Kurtz, the CEO of the $47 billion cloud security company CrowdStrike, which has seen its stock price triple over the past 12 months as it picks up new business protecting remote workers' laptops.

"People really want to get back out, and socialize at work, connect with each other. The social impact is important here," Kurtz told Insider. The CEO has calls with 25-30 companies a month, he said, and he is hearing that the drawbacks of working from home are mounting. "I think there's a negative to working from home, and that is it's meeting to meeting to meeting. There's no natural breaks in there. Dogs are barking, kids are screaming."

Still, Davis of Palo Alto Networks warns that a hybrid, multi-cloud workforce "opens up the attack surface, and once you're attacked, you're playing catch-up."

IT departments keep an eye on companies' computer programs, data, and employees. In the old days, that was all in one place: on the company's network in the office. Now the computer programs are on different servers – some on the companies' own on-premises servers, and some in the public cloud, stored on remote servers run by Amazon, Microsoft, Google, and others.

The data may be in all those different servers, but also being processed in cloud software run by the likes of Salesforce, Snowflake, Databricks, and others. And employees may access the programs and data from their laptops and mobile devices using third-party apps on the companies' WiFi networks, their own home WiFi networks, and other WiFi networks when they commute or work elsewhere.

Things often break where they connect, and every one of those connections – an employee connecting to an app, an app connecting to WiFi, WiFi connecting to data – is a place where criminals use increasingly sophisticated tools to break into a companies' system and steal data – like the account numbers of bank accounts, or credit card numbers. Or the criminals may lock up the whole operation by encrypting everything with a secret code – and demanding a ransom be paid before it is released, playing into the ransomware crisis sweeping the globe.

In other words, in a hybrid workforce, every employee represents multiple targets for criminals – and IT teams won't know who is where, and when.

Crowdstrike CEO George Kurtz CrowdStrike

Nobody could have seen this coming, but savvy IT departments are already addressing the problem

This dynamic creates an urgency for every IT department. CrowdStrike's Kurtz says "companies are getting in motion. Some are already there. Some haven't started."

The ability to get in motion and adapt to a hybrid workforce depends on how much companies embraced digital transformation – cloud computing, AI, automation, and cloud-based cybersecurity under the so-called "zero trust" model, which can better sift out those who should be accessing the data from those who, well, shouldn't.

"Some companies made the switch. You know, they invested in more systems and upgrades. Then there are others who didn't. There are going to be haves and have-nots," Kurtz said.

Agility and resilience will determine winners and losers, says Larry Link, CEO of Cequence Security, a 55-person startup in Silicon Valley. Link, a former Palo Alto Networks executive, helps to protect big companies' public-facing websites from getting hacked. He has big customers eager to work with a startup with new cloud-based, security approaches. "They know they need much more flexibility and much more agility as they are trying to figure out the changes. You don't know exactly how the workforce is going to evolve over these next two years."

It would be simple to say every company should have invested heavily in cloud-based security when COVID-19 hit. But a year ago, the world didn't know that the remote workforce just getting settled in at home was going to be more productive in many cases than it was in the office, not less — or that employee burnout would be such an issue.

And companies didn't know that cloud computing was going to fare much better than on-premises networks. For while two of the largest cyberattacks in history rattled the world during quarantine – the SolarWinds supply chain hack and Microsoft Exchange Server attacks – they were primarily centered in the servers of empty offices, not in their cloud computer assets.

And yet, some did foresee the challenge of hybrid work. In May of 2020, Bret Arsenault, Microsoft's chief information security officer, warned that bringing people back into offices would be a gradual process. Now, Arsenault thinks of that process as "the next great disruption that is hybrid work," requiring cloud-based security tools that work "wherever your employees choose to work and connect from."

The past 12 months "fundamentally shifted the way many people think about security," which is now a matter of "protecting workers wherever they're doing their jobs," Okta CEO Todd McKinnon told Insider.

Long-term investments in the cloud are paying off now

Investments in cloud-based "zero trust" cybersecurity are paying off for companies now, but protecting a hybrid workforce requires more than just buying equipment. It requires retraining employees who have just been through a year like no other. Beri, the Netskope CEO, says that the human aspect of digital transformation is important for companies to grasp.

"Your people have to be transformed," Beri told Insider. "They now have to learn – not the way they used to work, and maybe not the way they want to work – at first. And there are some who look at it the wrong way. They fear a power shift, a loss of power

because they are losing territory. But the people and companies who have already gone down this course, adopting new tools, are more ready."

Tim Nall is the chief information officer of Brown-Forman, a 151-year-old beverage and liquor company. Tim Nall

And the prepared firms aren't necessarily smaller, younger companies. "Jack is over 150 years old, and Brown-Forman is 151 years old, so a lot of people think that we're just this old, established company," says Nall, the CIO at the beverage and liquor company. That hasn't stopped the company from aggressively modernizing its IT strategy, he says: "We've been in the cloud since 2010."

Nall believes that prepares his company well for the many difficult changes that are coming. Over the past year his company has cranked out more work than ever, rebounded well from a ransomware attack, and begun the process of coming back to the office. Nall says his company is better prepared "because of the investments that we made pre-pandemic" in cloud-based security products like Okta's multi-factor authentication products.

His people have grown more comfortable with change like adopting new cloud-based security tools, Nall says. That familiarity and open-mindedness is crucial for managing

the change, he believes. After a year in lockdown, workers are venturing into a new hybrid workplace that will be filled with challenges.

"We used to worry a lot more about how our employees were going to accept changes," Nall says. "I don't worry about that anymore."