Coronavirus & Working from Home: Part 4

Key Technology Platforms
From Employee Collaboration Tools to Cloud-Based Systems

by Frankie Commans Jr.

Here at Alliances Management, our entire U.S. and international workforce has been working remotely since 2006. For some perspective, that was before the launch of the iPhone and the boom of easy, continuous connectivity. Suffice to say we are career remote workers and have had the opportunity to work through its various challenges and pitfalls.

For more than a decade our company has worked remotely. Our clients live in the U.S., Europe, and Asia. "Remote work" is a way of life for us and our clients. However, we're aware that most employees still go into an office.

Writing a set of technology recommendations for all employers and all employees in all industries is impossible; the aim of this article isn't to suggest a one-size-fits-all set of applications, but rather, call attention to the types of functions that will be necessary for employees to be successful while transitioning to work-from-home mandates in the face of the COVID-19 outbreak.

> **This is Part 4 of our series**
> ***Coronavirus & Working from Home.***
>
> It includes insights from Alliances Management staff, who have worked remotely since the company's inception in 2006.
>
> The entire eight-part series can be viewed on our website.

Employee Resources

Employers should be prepared for the moment when an employee says, "I can't do my job unless I have X." Employers should consider empowering employees to make purchases or sign up for services they deem necessary to fulfill their job functions.
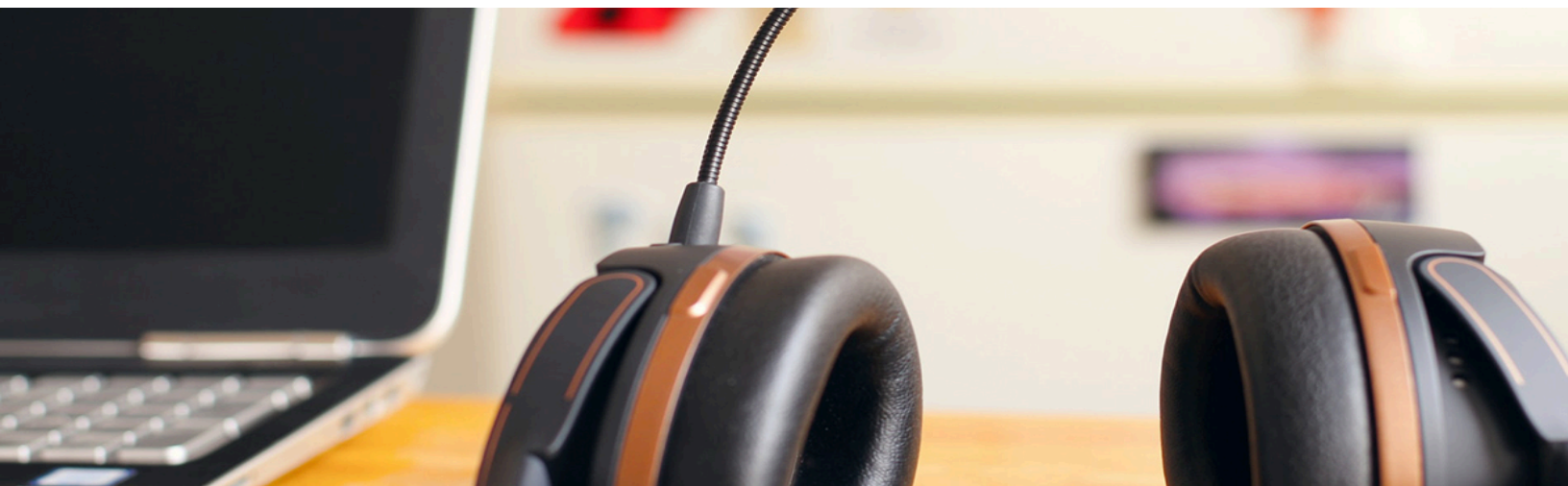
There are a host of technology-related equipment and services that knowledge workers are accustomed to but may be taken for granted at a traditional office but, depending on an employee's job function, may need to be implemented at home, for example:

- Computer
- Headset
- High-speed Internet
- Telephone line
- Printer
- Shredder
- Shipping services
- Ergonomic chair & desk
- Locking filing cabinets (if confidential storage is required)

Employee Communications

With no watercooler, break room, or common area, employees will need different types of applications and resources when working from home. Many large employers already have these tools in place—an Intranet or employee portal with all information, common collaboration systems, and more. For these employers, the only need is to ensure that employees have the necessary credentials, training, and access rights to use these technologies at home.

For employers without existing companywide technology platforms, ensuring efficient employee communication will be essential. Employees need to have access to the same platforms, know where and how to find each other, and understand company expectations for how to leverage these systems to complete company work. Functions that should be considered are as follows:

- **Email** – Many employees are accustomed to accessing their email from their work computer, whether through Outlook or another desktop application. Employers need to ensure that employees have credentials to access email remotely via Web-based platforms, such as Office 365 Online.
- **Common Chat Function** – Whether they use Skype, Slack, Microsoft Teams, or a proprietary company application, all staff should create accounts on the same messaging platform so that they can send quick messages, either individually or in project-specific groups. These applications can help transmit information quickly without having to bring everyone into a meeting.
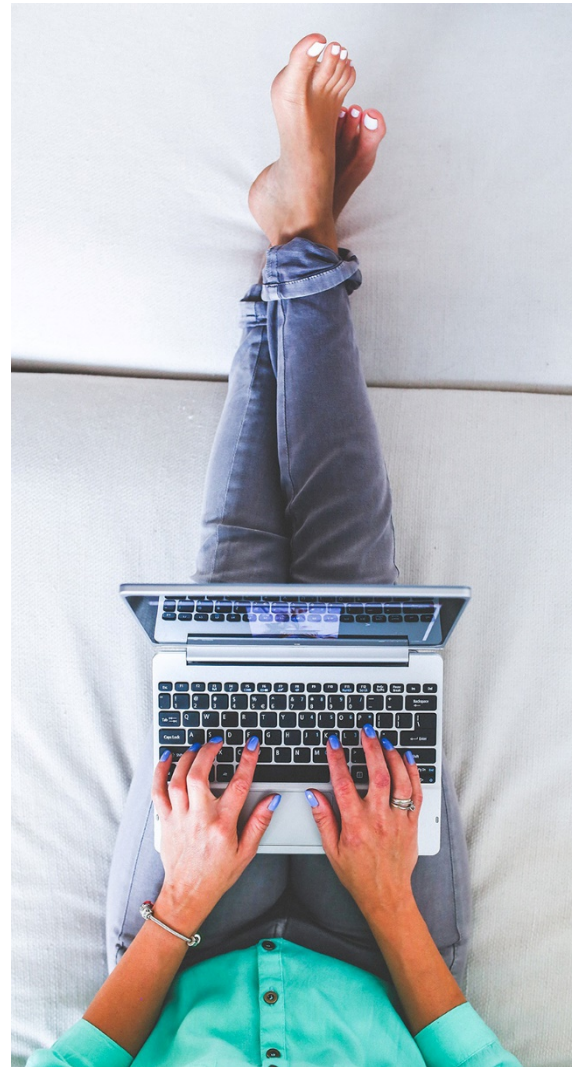
- **Meeting Platform** – The chat applications referenced above also allow meeting functionality, with voice and chat and sometimes video. Some of these applications are best for smaller, impromptu discussions; other platforms—such as GoToWebinar, WebEx, Microsoft Teams, or Zoom—are more effective for larger meetings or broadcasts. As other articles in this series have discussed, employers should establish expectations for arrival, meeting length, agendas, and more.
- **Mobile** – Each of the applications referenced above exists for both desktop and mobile applications. If employees will not be desk-bound, they should ensure that these applications are synced on both their home computers and mobile devices.

File Storage

As with employee communications, many large employers have cloud-based file storage implemented for staff. If this is the case, employees need access instructions and training but should otherwise be able to work normally.

For companies without such an easy solution, consider the following:

- **Leveraging the Company's Existing System** – Unbeknownst to employees (and perhaps even senior management!), many companies have already implemented technologies that can be used remotely. Many employees may be accustomed to using Office 365 or G-Suite, but these tools are configured for their work computers. For these companies, the good news is that work-from-home opportunities already exist; the challenge is for the IT department to provide staff with explicit instructions on how to access these resources remotely, where to find each familiar application, and whom to contact for assistance.
- **Shared File Storage** – For companies without existing storage systems, employers should immediately select a single file storage service (Dropbox, Google Drive, OneDrive, iDrive, etc.). The company's IT manager can establish a corporate account and distribute credentials or employees can create their own accounts and link up with team members.

Security

Proper "security" protocols vary wildly by industry. At the office, a lot of thought has gone into both physical and digital security. Employers should consider how remote workers need to alter their workflow to follow proper protocol. Consider the following:

- **Physical Security** – Does your industry require compliance with certain physical security standards? These can range from requiring locks on office doors to mandating that computers be physically attached to desks. Other common requirements include locked file cabinets or procedures for shredding documents.
- **Digital Security** – Larger companies may require use of a VPN and employees can work mostly as usual. However, cloud-based information requires different levels of security. Office 365 or similar enterprise packages offer some support, but employers should consider whether the company needs to modify its processes for security reasons. If your company stores or distributes confidential information, this information should be encrypted before being transmitted and should be stored on encrypted drives.
- **Operating Systems** – IT departments should ensure that remote employees' devices are running the most up-to-date versions of software.
- **Device Security** – Companies should establish policies requiring, at a minimum, strong passwords to unlock work devices. Newer mobile devices or computers offer biometric and/or second-factor authentication, which add further layers of security.

As noted at the outset, different companies will have different needs, but hopefully these ideas will help.

About Alliances Management

Alliances Management is a consulting, association management, and strategic staffing firm that delivers top-quality project management, operations, and administrative services. Visit us at www.am.consulting or on LinkedIn.