Five practical steps to optimise the new, dynamic world of work

IDG okta

Introduction

We're all aware of the need to think differently about how and where work takes place in the light of the lingering effects of the pandemic. Outside of outliers such as Goldman Sachs and JP Morgan, there appears to be little appetite for going back to work in the traditional form of commuting, fixed desks and regular office hours. According to a Eurofound poll, about 40 per cent of Europeans worked remotely during the health crisis in 2020. But only 13 per cent of UK working parents said they want to go back to pre-pandemic working, according to Bright Horizons, a nursery provider.

Indicators suggest that most employers are sympathetic to that emotion with a Gartner survey pointing to 90 per cent of HR chiefs being likely to grant work-from-home rights in a post-vaccination world. That makes strategic sense at a time when talent recruitment and retention is so important. It's therefore almost a certainty that the new working environment for information workers will be hybrid, with employers affording greater openness as to where we work and/or when we work. That may take the form of anything from absolute freedom to work from wherever and with highly flexible working hours or an approach that offers just a minor relaxation of the old rules.

Many of us will have experienced new working processes being suddenly thrust upon us when 'stay at home' orders were given and companies raced to fill the void via IT and lashed-together new processes. Most of us somehow coped with working from home but we can't go on with an improvised, free-form solution. This is a complex problem that requires a systemic approach where all parties know what is permissible and what isn't, where employee choice and wellbeing are factored in and where the right tools and secure environments are provided. Companies will doubtless experiment and learn but the question becomes: how do we optimise working and apply the lessons of 2020-2021 for the long-term future? Here are five practical steps.

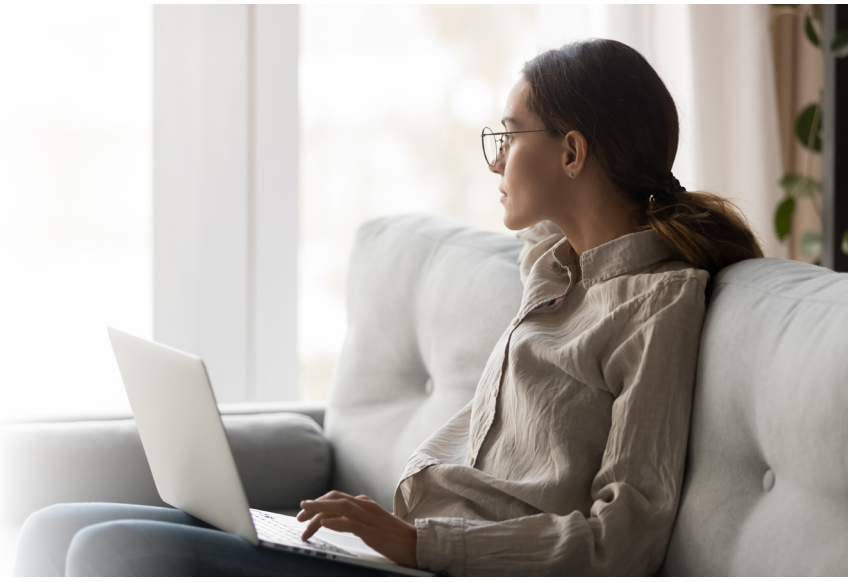
Start with identity and give employees the tools they need to succeed

Identity and access management (IAM) is central to the future of any organisation that has some staff working remotely at least some of the time. Covid-19 opened up a Pandora's Box of security scares as attackers attempted to intercept communications and hack into systems via vulnerable endpoints, lacking the usual protections and consumer-grade routers or used phishing and social engineering to persuade users to give away passwords and login details.

Safe access to core systems, applications and data will be the table stakes for the new-look, modern workforce... and they really already should be in a world that has the mobile tools and connectivity to make people productive from anywhere. Providing security has become even more important with the lifting of strict forms of lockdown. Today, it's fair to say that 'working from home' really means working from anywhere: coffee shops, clubs, libraries, gyms and myriad other locations.

A password defence might have sufficed for some in an office where perimeter security is difficult to breach but stolen or compromised passwords today can lead to highly significant infractions when the user is mobile. But accessing services must also be easy for the user. That means companies need a combination of better password management or password-less approaches, single sign-on, biometrics, push messaging notifications, secure sharing, encrypted credential sharing and strong, multi-factor authentication to defend themselves.

And it's already happening. PwC suggests that 70 per cent of leaders plan to increase spending on IT infrastructure to create more secure virtual connectivity. So, if you haven't already looked at refreshing your approach to identity management for new-look working, start now.



Redesign and rethink the traditional office space

Offices have changed greatly in the past 20 years and are continuing to change as we re-evaluate what an office is and what it can be. In a new world where some of us use offices only some of the time, it makes no sense to pay for the full-blown capacity of an old-style space designed for the possibility of every staff member being there at the same time.

The emerging consensus is that cubicles and fixed desks are going but that's not just because offices will be under-capacity. Perhaps influenced by the office designs of Silicon Valley, for a long time now we've slowly become accustomed to offices as fun places that create sparks and excitement. We can't all afford the running tracks, gyms, yoga studios, candy walls, pools, games, slides, greenhouses and eateries of the technology giants but we can co-opt their ethos for making people optimally enabled, collaborative and creative.

That means open spaces where teams can brainstorm, quiet rooms for videoconferencing and screen-sharing sessions and plenty of 'bump spaces' where people can meet spontaneously and learn by osmosis. We need water coolers and coffee junctions and space for classes so that people naturally get to meet and understand each other better and foster a spirit of knowledge sharing. According to PwC, 83 percent of employers and 71 per cent of employees said remote work had been a success but 87 per cent of employees see value in offices for building relationships and collaboration.

After the worst of the pandemic emergency is behind us, offices will have changed their purpose. We already know that work is becoming a thing we do, rather than a place we go. But offices will still be important destinations that act as the glue that maintains loyalty, camaraderie and a sense of shared purpose. They will become meeting points, conference spaces and central points for deal making but also, they will become providers of facilities because we won't necessarily have the printers, copiers, scanners, stationery, white boards, and large-screen conferencing systems that offices can afford.

Even in the world of Zoom, Microsoft Teams and the rest, visceral, face-to-face interaction will still be key. That applies to onboarding and helping young people and newcomers understand roles and culture. But it also applies to ensuring that people generally feel part of a collective effort and that they share goals. Many of us were highly productive during the pandemic but some of us suffered under the strain of pressure to look after families and friends and there is clear evidence that we missed the teamwork and empathy of colleagues. Offices will be key to ensuring that we do our best to stop employees feeling a sense of angst or disengagement.

Cultivate a trust-driven culture

As the Harvard Business Review has said:

'As difficult as it is to build and maintain trust within organisations, it's critical. An established body of research demonstrates the links between trust and corporate performance. If people trust each other and their leaders, they'll be able to work through disagreements. They'll take smarter risks. They'll work harder, stay with the company longer, contribute better ideas, and dig deeper than anyone has a right to ask. If they don't trust the organization and its leaders, though, they'll disengage from their work and focus instead on rumours, politics, and updating their résumés ... A high percentage of consulting engagements that seem to be about strategic direction or productivity turn out to be about trust, or the lack thereof."

Trust is critical to successful management but it comes various forms. There is strategic trust where employees trust leaders to make the right calls and personal trust that employees have in managers to act fairly. And then there is organisational trust where employees feel the company sticks to what it promises. Any failure in trust will lead to demotivation, eroded loyalty, high staff churn rates, recruitment challenges and perhaps even brand damage.

In the new workplace, trust will be even more important than usual. Company leaders need to trust their people to behave responsibly when not physically present. Of course, there will need to need to be some degree of oversight into productivity and project status, but any attempts to micro-manage or detect when users are at their computers or requirements for micro-detailed timesheets will likely lead to a fear of 'Big Brother' behaviour, disillusionment and a creeping culture of discontent.

Don't treat home working as a bonus or perk you're giving to employees. People have responsibilities to families; they may want to use hours in the day to exercise or pursue wellbeing routines and that may mean they don't work the usual working hours. But is the timing of when people work important to you? And if it is, consider ways to allow this freedom without impacting productivity or collaboration. This should be as simple as negotiating times when people needn't be available and when they must be.

Companies will benefit from having staff that can manage their lives with more freedoms than in the past but working from home isn't an employee incentive. Note also that many members of staff will have practical reasons for preferring not to work from home on the other hand so we shouldn't impose new ways of working on people who don't want them.

Establish a zero-trust security approach rooted in identity

Even before coronavirus, the emerging mantra was to “never trust, always verify”. The phrase is linked to the Zero Trust security model that dispenses with the old security model where internal networks are viewed as trustworthy and external networks as untrusted. Soaring use of mobile and cloud working were already seeing fast-growing Zero Trust adoption but the pandemic has hastened its progress and is also showing how limited the old “castles and moats” model is in the modern age.

In today’s security landscape, we no longer care so much about the network because that network could be a café, club or other Wi-Fi router that is out of the reach for corporate IT security. Instead we focus on controlling access to individuals.

Here, IAM is the foundation for Zero Trust, ensuring that only trusted individuals gain access to appropriate resources in an appropriate context. By consolidating user identity and allowing administrators to make informed decisions on granular access to services, we can protect data and services even if attackers have gained access to passwords. This can be extended via an ‘identity cloud” where the IAM service links to other security services and applications for broader protection. The result is that companies gain real-time, adaptive control over security.

Listen... and then don't stop talking

Success in building the new working patterns will ultimately be based on excellent communications, so talk with peers. Get advice from your fellow leaders to understand best practices in secure access, productivity, office design and staff wellbeing. But don't forget to listen too: by auditing your workforce you can challenge false assumptions and hidden biases, and gain living insights into people's perceptions of actions taken.

Talk to staff too and poll them to gain quantitative insights: what you might expect and what is reality may be poles apart. For example, surveys suggest younger people might be keener on offices than grizzled veterans because they provide opportunities to learn by osmosis, to socialise and to work in a supportive environment. Workplace veterans on the other hand, often welcome new working freedoms to spend a little more flexible time with families and friends after decades of an office-centric, 9-5 routine.

Share your plan. Implement changes with advanced notice and don't stop communicating. This communication in effect will probably translate into a mixture of face-to-face conversations, emails and use of business communication platforms as well as public and private forums where people can speak freely without fear of being penalised or ostracised.

Install regular stage gates too. It's better to course-correct early than too late so set formal parameters for analysis and potential reassessment. Everyone knows that change is tough and uncomfortable so spell out goals and why actions are being taken for your best chance of a positive response.

Finally...

The new world of dynamic working is exciting. It promises new levels of individual freedom but the price of freedom is eternal vigilance and companies must always be aware of the multiplying, morphing risks as attackers continually see new ways to breach defences.

Organisations need to look at both the 'soft' issues of people management and the hard issues of protecting services and data via identity management in order to prepare for a future where the concept of work is more liquid than ever before.

About IDG Communications, Inc.

IDG Communications' vision is to make the world a better place by enabling the right use of technology, because we believe that the right use of technology can be a powerful force for good.

IDG is a trusted and dependable editorial voice, creating quality content to generate knowledge, engagement and deep relationships with our community of the most influential technology and security decision-makers. Our premium media brands including CIO®, Computerworld®, CSO®, InfoWorld®, Macworld®, Network World®, PCWorld® and Tech Hive® engage a quality audience with essential guidance on the evolving technology landscape.

Our trusted brands, global 1st party data intelligence and Triblio platform identify and activate purchasing intent, powering our clients' success. We simplify complex campaigns that fulfill marketers' global ambitions seamlessly with consistency that delivers quality results.

About Okta

Okta is the leading independent provider of identity for the enterprise. The Okta Identity Cloud enables organizations to securely connect the right people to the right technologies at the right time. With over 7,000 pre-built integrations to applications and infrastructure providers, Okta customers can easily and securely use the best technologies for their business. More than 10,000 organizations, including JetBlue, Nordstrom, Slack, T-Mobile, Takeda, Teach for America and Twilio, trust Okta to help protect the identities of their workforces and customers.

For more information, visit www.okta.com/uk/