Cripps

Making hybrid working work: Amplifying opportunity and reducing risk for businesses – technology

Technology is both the best enabler of, and the biggest threat to successful remote and hybrid working. While Zoom, MS Teams and other collaboration tools allowed businesses to continue to operate throughout the pandemic, screen fatigue has since set in, employees found they missed the physical presence of their colleagues and cyber security attacks increased.

How can businesses continue to utilise technology to support remote working, while avoiding the potential pitfalls?

Tech as an enabler of hybrid working

Technology has been the saviour of many businesses since March 2020 and the pace of change has been rapid. At the start of the pandemic Microsoft had around 32 million daily active users of Teams. That figure jumped to 75 million in a matter of weeks when businesses closed their doors and since then the number of monthly active users has continued to climb and now surpasses 270 million.

Zoom, which was lesser known than Teams at the start of the pandemic, was propelled into the limelight in 2020. By offering free use for the general public, Zoom became a household name with many people using it to catch up with friends and family during lockdown. Today, the number of annual meeting minutes on Zoom is over 3.3 trillion.

The impact of technology on wellbeing

Whilst technology helped families keep in touch and saved many businesses from failure during uncertain times, it has brought its own challenges, not least of which is the impact on employee wellbeing.

A poll by The Royal Society for Public Health (RSPH) found that people who switched to working from home as a result of COVID-19 had experienced health and wellbeing impacts. The most common was feeling less connected to colleagues (67%), taking less exercise (46%), developing musculoskeletal problems (39%) and disturbed sleep (37%). More recently, a global study by Tinypulse, an employee engagement software company, found that 72% of employees who undertook hybrid working experienced exhaustion.

Current technology is attempting to reduce these negative impacts. Google's G suite of tools provide video conferencing and chat apps that help employees feel more connected.

The Asana workplace tool has functionality to help employees stay focused and productive and the Slack communication application enables employees to raise issues that aren't addressed in team or one-to-one meetings, or to ask quick questions in the way they usually would in person.

Continuous performance management solutions like 15Five can also be helpful when it comes to facilitating effective feedback and regular check-ins between employees and managers. These elements help to maintain an engaged and motivated team.

Working from home or living at work?

Whilst technology is available to enable employees to work from home as if they were in the office, home working has blurred the boundaries between home and work. Unlike an office, homes don't have closing times and it's hard to see when you're the last one left at work. Being chained to one's home desk (or kitchen table) can have health consequences. A joint study by the Universities of Derby and Plymouth found that 70% of participants who had begun working remotely during the pandemic now have a more sedentary lifestyle compared to their pre-pandemic days.

Plainly, it is becoming more important for organisations to develop a culture that encourages employees to separate their work and home life when working from home. This includes encouraging employees to take breaks from work communications outside of core working hours.

Seemingly, having a workforce working longer hours and contactable 24/7 might sound like an employer's dream. However, many businesses are aware that failure to establish and maintain boundaries can lead to mistakes, burnt out and demotivated staff. This is an area where technology is once again providing a solution.

Screen management tools have been available on Android and iOS devices for some time. Apps such as Facebook and Instagram allow users to set time limits to prevent hours of scrolling. These tools are being introduced to the workplace with employers encouraging, incentivising and sometimes even forcing employees to limit the time they spend online.

These moves appear likely to be welcomed by employees. A report published by international health benefits provider, Aetna International, entitled 'The digital health dilemma: Is technology keeping workers healthy or making them ill?' found that 70% of employees said they would exercise more if they spent less time at their PC and 76% felt that reduced or restricted out of hours technology use would help them manage their physical health better, if it was provided by their employer. Whilst this type of workday monitoring by employers may be seen as a positive thing, what happens when employers' use of technology is seen as more akin to spying on their staff?

The impact of tech on productivity

Since March 2020, the extent to which employers are monitoring their employees online has grown. Whilst employees have long been aware of their work emails being monitored, digital surveillance has become considerably more sophisticated.

Software is now available which enables employers to track workers' keystrokes and mouse movements and webcam monitoring software can even measure things like eye movements, facial expressions and body language. The World Health Organization (WHO) has recently warned against overly intrusive workplace surveillance, calling on employers to promote the 'right to disconnect'.

Even less invasive solutions still enable managers to view statistics to see who logged in and for what duration. In some companies, staff who do not open work applications early in the morning could be viewed as being late for work.

The data which is collected from employee monitoring can provide employers the ability to draw conclusions about how best to maximise employee wellbeing and productivity. However, there is also the possibility that employees will consider such monitoring to be intrusive, leading to anxiety, decreased morale and resignations.

In addition to the impact on staff wellbeing, companies that are considering introducing employee monitoring technology need to be mindful of their legal obligations. The UK's Data Protection Act 2018 sets out six principles which need to be followed if employers wish
to monitor their employees:

1. Monitoring must be lawful, fair, and transparent.
2. The purpose of the monitoring must be specified, explicit, and legitimate.
3. If employee monitoring involves collecting or using personal information, the data collected must be adequate, relevant, and not excessive.
4. The personal data must be accurate and kept up to date.
5. If personal data is collected, it shouldn't be kept for any longer than is necessary.
6. Information gathered through monitoring should be kept secure.

Businesses also need to understand that employees have a right to a certain degree of privacy, even when they are at work and even more so when that work is conducted in their own homes. Striking a balance between their own interests and their employees' expectations of privacy will be essential and any monitoring processes should be fair and reasonable.

Tech procurement considerations

If investment in technology is required in order to facilitate or enhance hybrid working, businesses should follow a procurement process to mitigate risks and safeguard successful adoption. This process should always begin with clearly identifying your business needs and constraints, before selecting potential vendors and products. For instance, will an "off-the-shelf" solution be sufficient, or is a bespoke product required? It is vital to carry out due diligence on the short-listed vendors, including company checks, financial checks and product reviews. Speak to other customers of the vendor to gain a clear understanding of their experiences, before proceeding with any purchase.

Cyber security risks should always be considered with any new technology purchase. This may involve checking if the vendor holds certifications, is performing penetration testing and is carrying out physical site visits. If you are licencing a software, check that the licence terms cover all the users who might reasonably be expected to require access to the software, both now and in the future.

It is important to ensure any licence restrictions are acceptable to you. Be sure to check that the vendor's maintenance obligations are clearly defined and consider how future interoperability issues will be handled. When it comes to the contract, clearly understand in which circumstances it can be terminated and how notice to terminate should be served. Make sure you explicitly know what termination means. Will termination end all your access to the software, or just terminate the support and maintenance obligations, leaving you with an ongoing (perpetual) right to use the software unsupported?

For more detailed information to ensure your procurement process is pain-free, read our top tips for tech procurement.

The rise of cyber attacks

In addition to data protection implications of employee monitoring, remote and hybrid working also comes with a myriad of security risks. Employees are often relying on their own home networks, sometimes their own devices, in order to carry out their work. Without the security protections that office systems provide and with an increased reliance on technology, businesses are now far more vulnerable to cyber-attacks.

In a survey of almost 1000 UK businesses carried out by the British Chambers of Commerce in partnership with IT firm Cisco, more than half of firms believed their exposure to cyber threats has increased due to working from home arrangements, with one in 10 firms having fallen prey to a cyber-attack in the last year.

As Aine Rogers, Head of Small Business at Cisco UK and Ireland, aptly puts it: "The lines between professional and personal are more blurred than ever. Organisations are no longer just protecting an 'office' but a workforce at the kitchen table." However, the pandemic has stretched IT resources and led to competing priorities between investing in IT service continuity and fortifying cyber security. Recent high-profile cyber-attacks, including the Solar Winds and Microsoft exchange data breaches, demonstrate how disruptive and damaging (to both businesses and consumers) such incidents can be. Companies need to take robust measures to ensure all staff can do their bit to mitigate risks.

Increasing employee awareness about the most common cyber risks – such malware, phishing, social engineering, ransomware, malicious websites and hardware loss or theft – can help sharpen defences against hackers.

A report by the security firm KnowBe4 revealed that phishing email attacks increased by 600% in the first quarter of 2020, with many of those attacks cashing in on the uncertainty surrounding the pandemic. Social engineering attacks (whereby psychological manipulation is used to trick users rather than sophisticated hacking techniques) have also increased. Teaching staff how to spot scammers has never been more important.

Recommendations

For both businesses and employees, a hybrid working model which embraces technology, has the potential to increase productivity, encourage greater collaboration and have a positive impact on wellbeing.

Our top tips for embracing technology to support hybrid working:

- **Prioritise investment in collaboration and communication tools.** Consider security and reliability, but also ease of use to ensure increased productivity and widespread user adoption.
- **Provide ongoing technology training opportunities for employees to ensure adoption.** These should be a mix of in-person and online training, quick user tutorials and knowledge shares.
- **Invest more in security software and cyber security training.** Employees must be educated on storing devices securely, creating strong passwords and what suspicious cyber activity might look like.

- **Have clear, written policies on working away from the office.** These should include security awareness and transparency on monitoring employee activity.

Kathryn Rogers

Partner