Managing The Workforce Revolution

New technologies and increasing mobility are revolutionising the workplace, with huge implications for businesses. Not since the industrial revolution of the late 18th and early 19th century have we faced such far-reaching change and, just as then, there is tremendous opportunity mixed with unprecedented risk. Companies that embrace new technologies and adopt new working practices will succeed in the battle for talent and skills, but only with careful management of the risks that these changes bring.

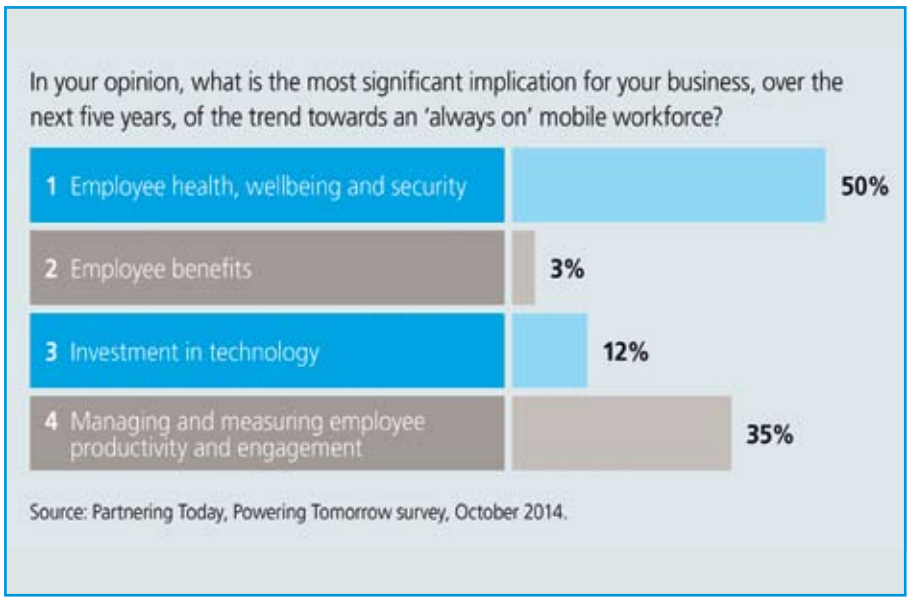
Our view is that the risks associated with mobility, keeping up with technology, cyber security and employee satisfaction are interconnected. As such, a holistic approach that manages workforce risks and business risks together, is the key to making the workforce revolution a success.

Work Practices On The Move

New technologies are fundamentally changing the way we all work, throwing up new risks and challenges for businesses and employees. The changes are coming so fast that employers, employees and lawmakers, haven't yet entirely figured out the best way to go forward. The multiple dimensions technology, business practices, attitudes and laws are interconnected and so are the risks, not just within the realm of mobility, but beyond.

The biggest change has come from mobile devices, such as smart phones and tablets, which allow individuals to connect, including to work, anywhere, anytime. The Millennials, those now aged 18-29, have grown up with this technology. It is integral to their daily lives. It is 'always on' and in many ways it molds their ambitions and expectations of life and work. Older employees have also seen great change, as mobile devices connect them to the workplace at night, at weekends and while sitting by the pool on holiday.

At a recent Zurich event that focused on managing risk in the changing world, the audience was asked, "What is the most significant implication for your business, over the next five years, of the trend towards an 'always on' mobile workforce?" Here are their responses, the line between business and pleasure is blurring and this brings advantages to employers, but the quid pro quo for employees must surely be more flexible working, including working from home. This, of course, brings its own risks – successful businesses need cohesion and this may be increasingly difficult to achieve if homeworkers never see each other.



Many global organisations have long faced the challenge of inculcating values in employees spread over many locations; now they have to worry about the same task for workers who may be in the same city yet aren't often physically present at the office. The remedy for mobile workers is the same as for those in foreign offices – regularly scheduled face-to-face gatherings, where people can get to know each other as more than a voice on a phone or a name on an email.

Companies also face the question of responsibility and benefits when employees are injured outside the workplace, whether while travelling or while working from home. Although it's unlikely a company would deny a claim by an individual working from home who falls down the stairs and breaks a leg, the risk of abuse is certainly there.

Technology As Role-Changer

Mobility is also upending corporate roles and chains of command. In a typical hierarchical office, a worker with a problem would tell their manager, who may pass it further up or refer it to the relevant person in another location. Now, the person who has the information is talking directly to the person most in need of the information, increasing effectiveness and efficiency.

This shows that while the risks are interconnected, so are the benefits. Technology shortens lines of communication and gives workers flexibility in time, location and kind of device, resulting in happy workers.

'Bring Your Own' Gathers Pace

Technological change is now so rapid that companies are finding it too hard and too costly to provide their employees with the tools they expect. The Millennials, again, place huge importance on the technology that they have available in the workplace – so much so that it has a bearing on their choice of employer. This is leading to rapid growth in companies adopting a 'bring your own device' (BYOD) policy. This is faster, more cost-effective and satisfies the demands of employees, but it raises major security risks for the business network, not to mention potential legal wrangles over the data, both business and personal, that sits on the employee's device.

BYOD is a double-edged sword. If you opt for BYOD to respond to the risk of fast-changing technology, you expose yourself to the related risk of not having complete control over employee-owned devices which are connected to your network.

Three-quarters of mobile applications will fail security tests through next year, according to a report by Gartner. The report adds that the applications are developed with a focus on usefulness, but that related security testing is often casual. It shows how difficult it is for companies

to ascertain their BYOD risk, amid the multitude of applications.

Data At Risk

A survey last year by TEKsystems of 2,000 IT professionals, found that 38% thought more than half their companies' sensitive data is at risk and 20% thought all corporate data could be compromised because of BYOD.

BYOD puts corporate computers in the middle of a web of interconnected risks: intruders seeking entry to the corporation, hackers and thieves seeking the employee's personal information, employee error or carelessness, inappropriate employee behaviour and more.

What if an employee's device is compromised by a virus that shuts down the corporate IT system, or an application for personal use gives a third party access to corporate networks? What if an employee's device is lost or stolen?

Most IT departments wipe clean a compromised BYOD, but that deletes the employee's personal data, and employers need to get the employee to sign a waiver to allow the deletion, according to Route 1, a digital security and identity-management solutions company.

At the same time, once an employee leaves a company, the employer may no longer have a way to get back data stored on the BYOD.

What an organisation can do in the name of cyber security, and what is a violation of privacy, pose two more interconnected risks. BYOD is still so new, there's not yet legal precedent in major jurisdictions, leaving it in a grey area. As of February, there were no BYOD-specific cases at the European level, nor at the country level in France, Germany, Italy, Spain or the Netherlands. However, other privacy cases have illustrated that limits do exist on companies' monitoring of their workers' private email accounts. For example, a German company was fined more than 1 million Euros for screening employee data to combat corruption and for monitoring communication sent by external e-mail accounts by employees.

While companies may do their best to maintain security, the vast possibilities for attack make it hard to keep up, especially when so many flaws may seem benign. However, an attitude of 'if it isn't broken, don't fix it' doesn't work with BYOD. A study by Dell of customers with BYOD policies found half have suffered a security breach.

To protect themselves, companies are increasingly looking to cyber insurance. In a survey of US companies late last year by Zurich and Advisen, almost 55% said they planned to buy cyber insurance in the next year, almost double the rate of the year earlier. New lines of insurance coverage are being created to keep up with the evolving risks. Cyber insurance options can include extortion, privacy liability, breach mitigation costs, consumer redress, electronic vandalism, errors and omissions liability and more.

Companies need to consider how they treat other risks in order to adjust their BYOD policies and risk management to their overall risk profile.

Downsides Of Always-On Work

The risks from the overlap of personal and business on BYOD go beyond technology to interconnect with other areas, such as talent management.

Some recent studies have found that productivity is higher for employees who work from home. One Chinese travel agency reported a 13% increase in productivity during a nine-month experiment with home-based working. The gains inspired the company to let all employees choose whether to work from home – more than half switched and productivity rose by 22%. Productivity aside, though, will people know where to the draw line between work and home life?

In a survey of 1,000 UK workers by file-sharing company Egnyte and TLF Research, 40% of respondents said they would feel obliged to work during personal time if their employer introduced a BYOD policy.

The knock-on effects of this change could be damage to family life and increasing stress levels, in turn leading to long-term illness and rising costs for health and protection insurances.

Consequently, some companies are already taking steps to address this issue. For instance, Daimler AG lets workers set an out-of-office message telling the sender which colleague is handling their responsibilities and then deletes the email.

Companies are still working out the answers to the questions that increased mobility poses, and the task is getting harder as new devices with new capabilities go on the market, opening up more new territory in the brave new world of connectivity.

Succeeding In The Workforce Revolution

Rapid technological change and increasing mobility present new opportunities, but they also present new, interconnected risks, such as keeping up with technology, cyber security, employee satisfaction, and corporate culture. While BYOD gives workers flexibility and lets employers get the latest technology without paying, it also takes away freedom and opens more doors than ever for breaking into corporate networks.

To be successful, companies therefore need to consider policies around mobility and BYOD in a holistic way that reflects how interconnected the implications are.

Source: Adapting To A Changing Workforce And Work Practices On The Move
For further information visit www.knowledge.zurich.com

The Takeaways

- The risks of mobile employees are interconnected: keeping up with technology, cyber security, employee satisfaction, corporate culture
- Companies need to consider policies around mobility and BYOD in a holistic way that reflects how interconnected the implications are
- BYOD gives workers flexibility but takes away freedom, lets employers get the latest technology without paying, but opens more doors than ever for breaking into corporate networks.

Stewart Allanson
Zurich Corporate Life & Pensions is a leading provider of international pension plans.
For more information, please email: stewart.allanson@zurich.com or telephone on +44 (0) 1242 664443.