BRING YOUR OWN DEVICE
How mobile technology is revolutionising the workplace

supported by
SONY VAIO
**FACTS & FIGURES**

**Bring-your-own-device: the story in numbers**

- 42% of people use their own laptop for work purposes
- 51% of the UK population own a smartphone
- 66% of people take their work laptop home each day
- 58% of people in the UK use a mobile device for work
- 31% of senior managers use personal smartphones in the workplace
- 23% of UK businesses have introduced a BYOD policy

- **37min** the average time saved by BYOD per employee each week

- **40%** Percentage of employees who think they will be more productive using their own device

**The global view: percentage of companies stating job satisfaction as a key benefit of BYOD**

- 21% in China
- 16% in the UK
- 15% in the US
- 14% in India
- 10% in Japan

16% of companies worldwide perceived job satisfaction as a benefit of BYOD

**Top 5 reasons why employees like BYOD**

1. **37%** like to work with any device, anywhere
2. **35%** like to combine work and personal use
3. **31%** like because it avoids usage restrictions
4. **30%** want a consumer experience at work
5. **27%** want to access non-work apps while at work
Flexible working is here to stay

How are you reading this supplement? Chances are you will be accessing it online, via either a tablet or smartphone, some 128 million and 1.4 billion of which are currently in use worldwide, respectively – figures that are set to rise dramatically as we head into 2014.

Our love of technology is not only changing the way we access information, it is also having an impact on our working lives. As this supplement, supported by Sony VAIO, shows, the increasing use of portable devices is enabling more mobile working practices. The ability to work from anywhere, any time, offers many benefits for both employer and employee, including the opening up of opportunities for people who need flexibility in their working hours, such as parents and carers.

However, as more personal devices are brought into the workplace, a number of challenges arise, such as how to manage security risks and ensure data remains protected. This supplement addresses these issues and more.

This supplement, and other policy reports, can be downloaded from the NS website at newstatesman.com/supplements
THE SPONSOR’S VIEW

Welcome to the world of BYOD
by Ruth Storey

In a few short years we have undergone a mobile revolution, and there are more exciting developments to come.

By the end of this year, there will be 1.4 billion smartphones in use on the planet – one for every fifth person alive. Here in the UK, over half the adult population owns one. Worldwide, an estimated 128 million tablets were shipped globally last year, a year-on-year rise of almost 80 per cent, with tablets now found in nearly a quarter of UK households. Laptop computers, once considered a luxury, are now the UK’s most popular electronic device – 80 per cent of us have one at home.

It was less than a decade ago that people started taking about “the internet going mobile”. Ofcom’s inaugural Communications Market Report, way back in 2004, revealed that operators would soon be offering “internet content specifically tailored for reception on a mobile phone”.

The mobile revolution has impacted both on the way we live and the way we work. Today, most of us can’t imagine living without the internet in our pockets. The smartphone has become synonymous with agility, data and connectivity. Progress has been exhilarating: the tablet; the rise of technology; GPS location tracking; remote lock-down; biometrics; encryption; and the latest on data security – all of which underpin Sony’s business-focused devices. This is important. Our 2013 VAIO Digital Business report revealed the extent of some of these challenges. For example, one in four UK businesses have had a laptop stolen, equating to around a million missing computers. Successful implementation of BYOD and other agile working habits requires a balance between managing corporate and personal information. Fortunately, we’re faced with a range of solutions that can enable any business – small or multinational – to jump the hurdles and maximise the positives of a happy, flexible workforce.

In many ways, it seems we are all living the technology dream smarter, faster and more responsively. Our Ultrabooks, for example, are slim and easily portable, with the advantage of durability and long battery life. Our designs have advanced with the demands of consumers who see their devices as indispensable – a fluid part of life that caters seamlessly to personal and professional needs. Meanwhile, cutting-edge, user-focused security features are on the rise: anti-theft technology; GPS location tracking; remote lock-down; biometrics; encryption; and the latest on data security – all of which underpin Sony’s business-focused devices. This is

THE SPONSOR’S VIEW

Welcome to the world of BYOD
by Ruth Storey

In a few short years we have undergone a mobile revolution, and there are more exciting developments to come.

By the end of this year, there will be 1.4 billion smartphones in use on the planet – one for every fifth person alive. Here in the UK, over half the adult population owns one. Worldwide, an estimated 128 million tablets were shipped globally last year, a year-on-year rise of almost 80 per cent, with tablets now found in nearly a quarter of UK households. Laptop computers, once considered a luxury, are now the UK’s most popular electronic device – 80 per cent of us have one at home.

It was less than a decade ago that people started taking about “the internet going mobile”. Ofcom’s inaugural Communications Market Report, way back in 2004, revealed that operators would soon be offering “internet content specifically tailored for reception on a mobile phone”.

The mobile revolution has impacted both on the way we live and the way we work. Today, most of us can’t imagine living without the internet in our pockets. The smartphone has become synonymous with agility, data and connectivity. Progress has been exhilarating: the tablet; the rise of technology; GPS location tracking; remote lock-down; biometrics; encryption; and the latest on data security – all of which underpin Sony’s business-focused devices. This is important. Our 2013 VAIO Digital Business report revealed the extent of some of these challenges. For example, one in four UK businesses have had a laptop stolen, equating to around a million missing computers. Successful implementation of BYOD and other agile working habits requires a balance between managing corporate and personal information. Fortunately, we’re faced with a range of solutions that can enable any business – small or multinational – to jump the hurdles and maximise the positives of a happy, flexible workforce.

In many ways, it seems we are all living the technology dream smarter, faster and more responsively. Our Ultrabooks, for example, are slim and easily portable, with the advantage of durability and long battery life. Our designs have advanced with the demands of consumers who see their devices as indispensable – a fluid part of life that caters seamlessly to personal and professional needs. Meanwhile, cutting-edge, user-focused security features are on the rise: anti-theft technology; GPS location tracking; remote lock-down; biometrics; encryption; and the latest on data security – all of which underpin Sony’s business-focused devices. This is
Flexible working is itself flexible: there are several types of working arrangements that come under this heading. Under government legislation, parents and carers have a right to request it, and to deny it an employer must show how it could have a negative effect on its operations. Framing alternative arrangements in this way can make it seem adversarial.

Flexible working is a way for businesses to respond to the needs of their employees, for individuals to engage and participate more at work, and for the economy as a whole to be more productive and diverse.

There are two main formats of flexible working: the type which enables different types of people to participate in work, and the type which enables different types of work. Both are increasingly important for economic growth and competitiveness.

At the heart of the concept of flexible working is trust. Trust is vital between the employee and the employer. All the various arrangements depend on it, whether the flexibility is based on flexitime or staggered hours, teleworking or job sharing. The employer must trust the employee to be diligent away from the gaze of management, and the employee must trust the employer to maintain their rights and opportunities while following what is still a less-common approach to work. Trust, however, cannot be given, only earned. And it cannot work in only one direction.

All parties win when there is trust between the employer and employee, and between the manager and the worker. When a business is able to trust an employee, they are likely to grant them more discretion and control over their work. (Flexible working is, of course, an aspect of control over work in itself.) Employees with this discretion feel more engaged in their roles. Meanwhile, engagement is linked to all the qualities an employer could hope for in their staff: greater productivity, better health and wellbeing, reduced turnover, improved innovation...

For many people, flexible working can be a way to stay at work when life circumstances change, whether this is to do with responsibilities to children or relatives at home or to do with their own retirement or ill-health. For others, it can be a way back to work. We all benefit, as an economy and a society, when a broader range of prospects are open to those who otherwise may not be able to work full time or otherwise.

Flexibility also enables different kinds of work to take place. At the moment, remote working is often seen as the preserve of a certain kind of job; as a recent Wired article put it, for office drones typing “go-page memos on paper-clip appropriations”. But, as the UK Commission for Employment and Skills (UKCES) is finding in its ongoing research into the mega-trends driving the future of jobs and skills, flexible and remote working are likely to disrupt many more varied occupations. A vivid example is RAF officers living in Lincolnshire, commuting to an office to fly drone missions over Afghanistan. Another, more prosaic, trend is for work to take place on a subject or project basis rather than a geographic one. Research suggests 57 per cent of workers had seen an increase in collaboration from different locations. The emerging findings suggest these trends will continue.

This can lead to real agility, particularly in small businesses. Being able to draw on talent across the region, nation or planet can lead to spectacular growth. But shifting to a more flexible culture is not without its challenges. As UKCES research on the digital economy makes clear, trends such as bring-your-own-device (BYOD) can enable great flexibility, but they are an example of employees changing their work environment. This is a turnaround from a world where, particularly in the largest firms, companies are more used to moulding their employees.

The shifting demands on both sides require a change in the approach to skills and learning at work. Managers used to command-and-control must themselves learn to cope with flexibility. Workers need to be comfortable with taking more responsibility for prioritisation and being more proactive. But both of these changes are undoubtedly positive. At work, as in life, a little flexibility can help us all.

Iqbal Wahhab is founder of Roast Restaurant and a commissioner at the UKCES
The business environment has changed dramatically since the 1980s. Advanced technologies, rapid globalisation, changing demographics and new societal values have completely redefined the corporate landscape, creating opportunities and challenges that require different approaches to our ways of working. Working practices, however, have largely failed to adapt sufficiently to meet these opportunities.

The challenges of today’s corporate landscape require businesses to establish the optimal workforce to support their objectives by harnessing demographic and societal changes and by maximising the use of new technologies to the benefit of both employers and employees. Business competitiveness is dependent on adapting agile working practices; failure to do so will limit growth and inhibit the UK’s ability to compete globally.

Last year, at the request of the Deputy Prime Minister, I launched the Agile Future Forum (AFF) with leaders from 22 of our most successful companies. While these members differed in terms of sector, size and location, they all shared a common view that a more agile approach to work is a necessity for the whole of UK plc.

Greater agility boosts financial returns

by Sir Win Bischoff

The competitiveness of UK plc depends on greater workforce agility

The business environment has changed dramatically since the 1980s. Advanced technologies, rapid globalisation, changing demographics and new societal values have completely redefined the corporate landscape, creating opportunities and challenges that require different approaches to our ways of working. Working practices, however, have largely failed to adapt sufficiently to meet these opportunities.

The challenges of today’s corporate landscape require businesses to establish the optimal workforce to support their objectives by harnessing demographic and societal changes and by maximising the use of new technologies to the benefit of both employers and employees. Business competitiveness is dependent on adapting agile working practices; failure to do so will limit growth and inhibit the UK’s ability to compete globally.

Last year, at the request of the Deputy Prime Minister, I launched the Agile Future Forum (AFF) with leaders from 22 of our most successful companies. While these members differed in terms of sector, size and location, they all shared a common view that a more agile approach to work is a necessity for the whole of UK plc.

Flexible working hours have become fairly standard and are usually positioned as an employee benefit. Many companies have introduced them as a means of attracting and retaining employees who are seeking to improve their work/life balance. However, agile working practices extend beyond the introduction of flexible hours and have been proven to directly benefit overall business performance – not just employees.

The AFF, supported by McKinsey, carried out research defining the business value of workforce agility in supporting the competitiveness of UK plc. This showed that significant value is already being realised by those businesses applying agile working practices – value equivalent to 3 to 13 per cent of workforce costs. The research also demonstrated that most current practices could be extended to capture additional business benefit valued at 3 to 7 per cent of workforce costs and a sales uplift of 11 per cent.

Implementing agile working practices effectively cannot remain solely in the domain of HR departments. Chief executive leadership is vital – creating the right culture from the top down. However, in the CBI’s 2011 survey of businesses, 32 per cent of leaders surveyed believed extending agile working practices would have a negative impact on productivity.

BYOD AND THE ECONOMY

Flexible working hours have become fairly standard and are usually positioned as an employee benefit. Many companies have introduced them as a means of attracting and retaining employees who are seeking to improve their work/life balance. However, agile working practices extend beyond the introduction of flexible hours and have been proven to directly benefit overall business performance – not just employees.

The AFF, supported by McKinsey, carried out research defining the business value of workforce agility in supporting the competitiveness of UK plc. This showed that significant value is already being realised by those businesses applying agile working practices – value equivalent to 3 to 13 per cent of workforce costs. The research also demonstrated that most current practices could be extended to capture additional business benefit valued at 3 to 7 per cent of workforce costs and a sales uplift of 11 per cent.

Implementing agile working practices effectively cannot remain solely in the domain of HR departments. Chief executive leadership is vital – creating the right culture from the top down. However, in the CBI’s 2011 survey of businesses, 32 per cent of leaders surveyed believed extending agile working practices would have a negative impact on productivity. With little available research into how businesses
BYOD can bring additional value to UK companies

They themselves can benefit from agile working, it is not surprising that workforce agility is still perceived to be a cost and threat to business, rather than a necessity to ensure growth and maintain competitiveness.

This is precisely why the AFF was established. In addition to the research to date, we are sharing our newly developed business value assessment with organisations across the UK through a seminar programme. Our report and website set out detailed case studies of how founding members have benefited from agile working. Importantly, we also provide guidelines as to how other businesses can replicate these benefits.

Workforce agility offers benefits for all, but it is not a one-size-fits-all. All members of the AFF – which includes large firms and SMEs – are committed to sharing what they have learnt as individual companies in order to enable other companies and organisations to assess the potential business value of agile working practices.

For example, when the legal firm Evergreen’s had to move towards implementing agile working practices, failure to do so will limit growth and inhibit the UK’s ability to compete globally. The faster we move towards implementing agile working practices such as BYOD, the more competitive UK plc will be.

Sir Win Bischoff is chair of the Agile Future Forum and chair of Lloyds Banking Group.

We have found that BYOD is an important tool to help support greater agility within the business, Colleagues in the pilot have increased their productivity as BYOD provides a more flexible and efficient way of working. The costs of the scheme are off by these enhanced efficiencies and levels of productivity. For Lloyds Banking Group, for example, BYOD is proving to be a win-win for both the business and its employees.

“I think the smartphone and tablet are as personal as a fountain pen or a wallet – both things that they replace. They’re moulded to the way you arrange your life and BYOD means that I can work when I want, where I want. That means I benefit and so does the business,” says Rupert McNeil, director of group HR at Lloyds Banking Group.

Cisco, a founding member of the AFF, has had a BYOD scheme since 2009 and includes its ‘Any Device’ programme, which provides corporate resource access to Cisco employees securely, from any location, any device, anywhere. Internal reviews have demonstrated that, on average, the mobile device user gained at least 15 minutes of productive time per day. This 15 minutes a day, is estimated to have a value of US$300m a year,” says Ian Fodder, chief technology officer at Cisco UK&I.

BYOD is an excellent example of how advanced technologies can be harnessed to increase the agility of workforces of any size and structure – increasing productivity, delivering tangible benefits to the overall business and individual employees.

The examples mentioned within this article have been successful in driving agility because they have been business-led, extending beyond the traditional HR remit of employee benefits. The schemes have also arisen from a thorough understanding of the needs of the business and its workforce.

Business competitiveness is dependent on adapting agile working practices, failure to do so will limit growth and inhibit the UK’s ability to compete globally. The faster we move towards implementing agile working practices such as BYOD, the more competitive UK plc will be.
People are used to interacting digitally in their personal and social lives, be it looking at their friends’ holiday photos on Facebook, or engaging with others via Twitter on their tablet while watching their favourite TV programme, all from the comfort of their sofa.

With the advent of smartphones, people have been able to pack the same punch as a PC from their pocket. As such over the past few years, people have got to a stage where the devices they use in their personal life (such as smartphones and tablets), often outstrip and outperform what they would commonly use in their office environment.

What’s more, people quickly become used to their own devices, as buying them was a conscious, personal decision. In the office environment, you are constrained to use the devices provided by the company’s IT department. Your personal device becomes comfortable and second nature, keenly exemplified by the tribal like competition between Apple and Android users. This is the real genesis of BYOD; people want to bring their own device to work because it is better, they’re used to it, and they are more competent using it.

Productivity and morale are clearly linked and have huge implications for any business; after all a happy worker is a productive worker. Organisations shouldn’t fear the rise of BYOD, thinking it’ll be difficult or costly to implement. Rather, they should acknowledge and embrace it, as otherwise they’ll soon have demotivated and disenfranchised employees, who won’t be as productive in the working environment. BYOD makes people more productive for two main reasons. First, they are using a device they are comfortable using and are therefore more likely to make more use of it in the working environment. Second, although BYOD is characterised by people bringing devices into work, companies also benefit from employees working outside the office. The mobility of devices allows employees to use them at home, when travelling or on a customer site, since their device is so easy to use and to connect to the internet. All this is good news for the employer because in a BYOD culture people can and usually do give more hours of productive time to the business.

Productivity is not the only benefit. BYOD creates an environment in which better collaboration and communication is possible. The use of audio or video conferencing, and the ability to pass documents back and forth, allows greater mobility to the workforce and better productivity. This has clear benefits for small businesses, which can often provide greater mobility to their workforce.

The benefits that come from BYOD can be huge; companies no longer need to provide every employee with all devices. The maintenance of devices can also become more of a self-supporting community affair, detached from corporate control. Although BYOD is often typified by smartphones and tablets, there are many people who use their own laptop in the working environment. Internally, we’ve seen wikis set up by Cisco employees on how to troubleshoot their Macs for example, helping the load off the IT department and what’s expected of them.

Cautious employers may incorrectly equate BYOD with social media, and feel that allowing staff to bring their smartphone to work may encourage them to use it more during working hours. But, BYOD does not mean abandoning traditional methods of communication; employees still have access to email, and can still use social media from home. The benefits far outweigh the risks.

Managing the office in your pocket

by Donald McLaughlin

Bring-your-own-device is here to stay. So how do we make it work?

The benefits companies receive far outweigh the risks

Using personal devices also encourages better collaboration and communication between workers. This is hugely important for businesses which may use audio or video conferencing on the go from a tablet or smartphone. This has clear benefits for global organisations, which can now provide greater mobility to their workforce. But it’s not only global players who benefit, since small businesses will get greater impact from their resources. It also means home workers can access meetings from their device, improving productivity and eradicating the need for expensive conference phones. Improved collaboration has always meant companies can be much more productive, as it helps bring people together and speeds up decision making. BYOD technology merely facilitates this collaboration, allowing employees to join meetings from any device, wherever they are.

Recognising the trend of BYOD is only the first stage; adapting to the change is another. Companies should be organised and set up to embrace it, from an IT perspective, as well as being culturally and technologically flexible enough to allow workers to bring their devices to work. As is to be expected, cost factors are always front of mind. But this goes beyond ensuring that the network is able to support personal devices; BYOD can actually be a huge IT procurement cost saver since the organisation will no longer have to provide every employee with all devices.

What’s more, the maintenance of devices can also become more of a self-supporting community affair, detached from corporate control. Although BYOD is often typified by smartphones and tablets, there are many people who use their own laptop in the working environment. Internally, we’ve seen wikis set up by Cisco employees on how to troubleshoot their Macs for example, helping take the load off the IT department and what’s expected of them.

Cautious employers may incorrectly equate BYOD with social media, and feel that allowing staff to bring their smartphone to work may encourage them to use it more during working hours. But, BYOD does not mean abandoning traditional methods of communication; employees still have access to email, and can still use social media from home. The benefits far outweigh the risks.
spend all day on Facebook, for example. Yet at the heart of the cultural shift, there needs to be the realisation that the benefits companies receive from increased productivity far outweigh the risks, and that BYOD encourages empowerment that underpins the employer/employee relationship.

Companies hesitant to adopt BYOD run the risk of not only demotivating their workforce but also losing talent to competitors willing to embrace it. It is a huge consideration for the next wave of employees, especially Generation Y, who in many cases consider flexibility and device choice more important than a higher salary.

Once BYOD is accepted in theory, the key is to ensure its success in practice. The first focus point from an internal perspective will be the technological framework, making sure it’s fit for purpose and able to facilitate the change. Security risks will be the major concern for an IT department, since if a user is able to access the corporate network on their phone, what are the implications for security? Could external viruses be introduced and could sensitive company data and intellectual property be taken by errant employees? Second, the calibration and policies of the network may not allow non-corporate devices to be connected and would need to be reconsidered. However, it must be stressed that both of these concerns can be easily mitigated by having the right network infrastructure in place. A company may wish to impose a geographical restriction, for example, which would only allow employees to access sensitive company information while in the office. Essentially, all that is required is a common-sense approach to policies which address these security concerns, while allowing employees to access company programmes and systems.

It’s important to recognise that the cultural and technological considerations are of equal importance; that to successfully implement BYOD, an organisation should have executive-level buy-in and high-level sponsorship that recognises the way people want to work and is able to facilitate that to drive improved morale and motivation. The rules of engagement for BYOD are the same, whether you’re a tech company or a retailer; the only difference is the internal adoption culture. Similarly, the IT requirements for smartphones or tablets are the same; it’s merely a question of the user’s device preference.

In terms of trends, there is every indication that people will have more devices in the future. There is always a hype cycle around new technology, exemplified by the new wave of wearable technology such as Google Glass and the smart watch. It’s hard to imagine that five years ago we could have predicted the huge uptake of tablet computing. Consumers have an insatiable appetite for the latest and greatest gadget, and this will continue to feed BYOD culture.

In much the same way that flexible home working challenged the corporate status quo that employees were only working if they were in the office, BYOD shifts the goalposts for collaboration and productivity. It has many positive benefits for organisations, from employee morale and retention to attracting new talent into the business. BYOD is here, and more importantly it’s here to stay.

Donald McLaughlin is director of UK Collaboration Sales at Cisco
C
olin Rees knows more than most
about other people’s eating habits,
their takeaway habits at least. As IT
director for Domino’s he can tell, for ex-
ample, that the most popular time to
order a pizza across the week is between
7pm and 9pm on a Friday, Saturday and
Tuesday night (Tuesday is special offer
night). That’s the pattern that can be guar-
anteed across the UK. In Germany, where
Domino’s has recently opened stores and
where Sunday lunchtimes prove popular
for pizza, the pattern is different but no
less consistent.

The past decade has witnessed, if not a
revolution, then certainly a clear evolution
in the way we all handle and access infor-
mation on the move.

Whether it’s through a portable laptop,
smartphone or tablet, the majority of us
now own a mobile device and, according
to a study commissioned by our office,
almost half of us (47 per cent) are currently
using it for work purposes.

As this supplement has explored, al-
lowing employees to use personal devices for
work can bring numerous advantages. The
organisation concerned does not have to
pay for a device that a person already owns
and the employee will already be familiar
with the device and therefore should have
fewer problems using it to carry out many
of the most common daily tasks, such as
accessing emails and editing documents.

So it’s easy to see why the trend of allow-
ing employees to use personal devices for
work is continuing to grow.

While this is all very well and good, the
practice raises clear concerns around
whether the personal information being
processed on these devices is being looked
after properly. The Data Protection Act is
clear: the responsibility to make sure that
personal information is being handled
correctly lies with the data controller –
normally the organisation collecting and
using the information – not their individ-
ual employees. If the information is lost or
compromised, it is the employer that is ul-
timately responsible and therefore in line
for potential enforcement action from my
office, the Information Commissioner’s
Office (ICO), as the regulator of the Act.

If you consider that we can, in the most
serious cases, issue monetary penalties of
up to £500,000 and that a serious data
breach can have an even bigger impact on
an organisation’s hard-earned reputation,
it is clear that responsibility to make sure
that personal information is handled
properly lies with the data controller –
overall the organisation collecting and
using the information – not their individ-
ual employees. If the information is lost or
compromised, it is the employer that is ul-
timately responsible and therefore in line
for potential enforcement action from my
office, the Information Commissioner’s
Office (ICO), as the regulator of the Act.

You can see from some of our recent
monetary penalties where things can go
wrong. In June 2013, a penalty of £150,000
was issued against Glasgow City Council
for the loss of two unencrypted laptops,
one of which contained the personal in-
formation of 20,143 people. In August
2013, a penalty of £88,000 was issued
against Aberdeen City Council after inad-
equate homeworking arrangements led to
39 pages of personal data being uploaded
on to the internet by a council employee.

Ensuring the safe and secure deletion of
data is also important if the individual is
no longer an employee, or they subse-
quently want to sell or trade in their
device. Let us not forget that our office
has already served monetary penalties
totalling £525,000 against two organisa-
tions who failed to ensure that hard drives

DATA LAWS

Protecting
your assets

by Simon Rice

Handling information in the correct way when using portable
devices is critical. Failure to comply to strict data protection
laws could land organisations in hot water

Colin Rees knows more than most
about other people’s eating habits,
their takeaway habits at least. As IT
director for Domino’s he can tell, for ex-
ample, that the most popular time to
order a pizza across the week is between
7pm and 9pm on a Friday, Saturday and
Tuesday night (Tuesday is special offer
night). That’s the pattern that can be guar-
anteed across the UK. In Germany, where
Domino’s has recently opened stores and
where Sunday lunchtimes prove popular
for pizza, the pattern is different but no
less consistent.

The past decade has witnessed, if not a
revolution, then certainly a clear evolution
in the way we all handle and access infor-
mation on the move.

Whether it’s through a portable laptop,
smartphone or tablet, the majority of us
now own a mobile device and, according
to a study commissioned by our office,
almost half of us (47 per cent) are currently
using it for work purposes.

As this supplement has explored, al-
lowing employees to use personal devices for
work can bring numerous advantages. The
organisation concerned does not have to
pay for a device that a person already owns
and the employee will already be familiar
with the device and therefore should have
fewer problems using it to carry out many
of the most common daily tasks, such as
accessing emails and editing documents.

So it’s easy to see why the trend of allow-
ing employees to use personal devices for
work is continuing to grow.

While this is all very well and good, the
practice raises clear concerns around
whether the personal information being
processed on these devices is being looked
after properly. The Data Protection Act is
clear: the responsibility to make sure that
personal information is being handled
correctly lies with the data controller –
normally the organisation collecting and
using the information – not their individ-
ual employees. If the information is lost or
compromised, it is the employer that is ul-
timately responsible and therefore in line
for potential enforcement action from my
office, the Information Commissioner’s
Office (ICO), as the regulator of the Act.

You can see from some of our recent
monetary penalties where things can go
wrong. In June 2013, a penalty of £150,000
was issued against Glasgow City Council
for the loss of two unencrypted laptops,
one of which contained the personal in-
formation of 20,143 people. In August
2013, a penalty of £88,000 was issued
against Aberdeen City Council after inad-
equate homeworking arrangements led to
39 pages of personal data being uploaded
on to the internet by a council employee.

Ensuring the safe and secure deletion of
data is also important if the individual is
no longer an employee, or they subse-
quently want to sell or trade in their
device. Let us not forget that our office
has already served monetary penalties
totalling £525,000 against two organisa-
tions who failed to ensure that hard drives
containing sensitive personal data were securely destroyed after use.

For some time, the ICO has been aware of this growing trend and the implications that the insecure use of such devices has for an organisation’s compliance with the Data Protection Act. This is why, in March of this year, we published new guidance called Bring Your Own Device (BYOD).

The guidance aims to help organisations develop their own policies by highlighting the issues they must consider. First and foremost, organisations must be clear with staff about the types of personal data that can, and more importantly can’t, be stored on personal devices.

An obvious risk from the outset is that the device, and therefore the information stored on it, will be lost or stolen. There is also a worry that the device may be misused. Employers will therefore need to consider how they will mitigate this risk.

A very simple way to achieve this is to reduce the volume or type of personal data available. For example, does a medical professional need to carry around copies of all their patients’ medical records, or would it suffice to only store the personal telephone numbers of patients in case they need to contact them at short notice?

If remote access is required to the records of a specific patient, these could be transferred onto the device on the day required and removed afterwards. Remember, it is important that the security measures being adopted by organisations should reflect the sensitivities of the information that is being accessed.

Employers should make sure that they understand the protection mechanisms available in the personal devices they allow to connect to their networks and make sure that they are being used correctly. For example, most modern devices will offer some sort of password access to the device and support encrypting some or all of the data on the device. Organisations will also need to know where the weaknesses are in these devices. It is important that employers are not reducing the level of security afforded to their information by allowing additional devices to access the network.

Another feature on most personal devices is the ability to lock the device, or delete all of the data stored on it, if the password is entered incorrectly on a number of occasions. In most cases, this can be enabled on a device at little or no additional cost, but could make all the difference if the device is left at a restaurant or stolen.

Smartphones and tablets can also be registered and managed remotely using specialist software, commonly referred to as a Mobile Device Management (MDM) solution. An MDM solution can provide a remote wiping facility that locks or deletes all of the information held on a device if it is reported lost or stolen by the owner.

The majority of these measures cost very little and take a small amount of time to introduce, but will help to keep the personal information that employees are accessing secure and ensure compliance with the Data Protection Act.

We are not expecting a revolution in organisations’ existing data protection practices, but an evolution to reflect the way the modern workforce is using and storing people’s details is a must.

Simon Rice, is group manager for technology at the Information Commissioner’s Office (ICO)

**Data protection dos and don’ts**

The ICO’s guidance on BYOD recommends the following:

- Public cloud-based sharing and public backup services, which have not been fully assessed, present many risks. Use with extreme caution, if at all.
- A remote locate and wipe facility should be registered to all devices. This will maintain confidentiality of data in the event of a loss or theft.
- BYOD may lead to increased usage of social media channels. In this instance, a social media policy that includes clear information about data protection laws could be appropriate.
- A clear separation between the personal data processed on behalf of the data controller and that processed for the device owner’s own purposes should be maintained. For example, different apps for business and personal use.
- The choice of devices should be limited to those which have been assessed as providing appropriate security for the personal data being processed.
- BYOD users should be given guidance on the risks of downloading from the web.
Despite the many obvious benefits that bring-your-own-devices afford employees and employers alike, it is only natural that with new practices come new security challenges.

People are far more mobile than ever before,” says Malcolm Hay, enterprise technology specialist at Intel EMEA, the world’s leading maker of the semiconductor chips that live in any desktop, laptop or mobile device. “Security is a hot topic right now. We’re collaborating more, and there are many excellent tools that companies and individuals can now use to share items. Most of these growing trends, BYOD included, mean higher security threats – whatever makes people more productive tends to makes risks worse.”

With increased flexibility comes increased responsibility, and anyone engaged in BYOD should learn how to keep individual devices safe or company data free from loss or intrusion. With ultra-mobility on the rise, the two main questions people are seeking answers to are how to make security more bulletproof and how to make security work better on increasingly smaller and lower-power devices.

So, be it personal laptops, tablets or smartphones, what are the key areas of concern, what security features should individuals be aware of, and what developments does the future hold?

**Encryption**

How to keep data secure is frequently the top concern for companies allowing employees to access corporate information via personal devices. Often the go-to solution is an encryption programme, which can be used to encode anything from messages to data to passwords.

“Data protection takes us immediately to encryption,” explains Hay. “The danger of unencrypted data is that if I steal your device, I can read anything I like. Encryption uses mathematical algorithms to scramble information up, so that if an intruder looks at it, they can only see hieroglyphic gobbledygook that would need to be unscrambled to read.”

This encryption and decryption process is done via a cypher key which belongs to the authenticated user and/or receiver. Historically used by governments and the military, encryption is now an incredibly popular security tool when exchanging or storing digital information. Encryption is considered a simple and effective way to keep both standing and in-transit data safe. However, the main concern is that it takes a lot of resources. “The scrambling process uses intense mathematics that can make a device run slower – particularly when moving down to the tablet and smartphone level where processing power is reduced,” says Hay.

One solution is to embed encryption technology into the hardware of a device’s central processing unit (CPU) which, by its nature, is faster and less susceptible to hacking than software. Intel implements several encryption-related security capabilities in hardware, including engines which are capable of much faster encryption and decryption than traditional software algorithms, and random number generators, which are used for cipher key
generation and deliver more secure keys than before. “You need both soft and hardware capabilities. No solution is 100 per cent foolproof, but by focusing on increasing hardware capability we can get 99.99 per cent assurance,” explains Hay.

**PASSWORDS**
A password is often the first line of defence between the outside world and the data on a device. Password and pin codes are one of the most everyday tools used to access private spaces on computers, phones, files or emails. Passwords can be strengthened by unusual characters, cryptographic scrambling or by programmes that request randomly generated pieces of the password rather than the whole thing. Passwords, however, are often controlled by software rather than hardware, which can leave devices vulnerable to prying eyes.

“Whenever you put a pin code into a device you always run the risk that there is keyboard logger malware [malicious software] in the system,” says Hay. “The malware can get hold of your password because it can see the keystrokes being sent across the network.”

Password safety falls under the umbrella of “identity protection” and can be strengthened, like most other IP features, by embedding password recognition into the hardware of a device.

“Putting password capability into a device’s hardware completely locks the malware out,” says Hay. “It becomes a user-to-silicone-chip interaction — no memory, no software, no chance to see what is going on. It is important to keep passwords as an interaction exclusively between the user and the back end — a person-to-hardware bubble.”

**VIRUSES**
Viruses are self-replicating malicious software that hamper a device’s ability to function. Viruses can steal hardware space, access private information, corrupt data, spam contacts or log keystrokes when entering passwords. Having robust anti-virus software is a must when bringing personal devices into work.

Intel warns particularly about a growing threat, the “something you know and something you possess” attack. “Some-thing should really give users confidence is the future?” asks Hay. “Absolutely.”

**DIGITAL CERTIFICATES**
When it comes to security, what should really give users confidence is possessing two things, says Hay, “something you know and something you have.” This “something you know” tends to be a password, pin code or encryption key. The “something you have” is called a digital certificate, and it works a bit like a virtual fingerprint — a proof of authenticity that devices (and by default, you) are who they say they are.

“When you show up in a foreign country, your passport implies you are trusted to let in. A digital certificate does this in computer-speak. It verifies your device’s identity and allows you to make connection with other computers, share data, or join a network.”

Digital certificates can be obtained from a certification authority and used to ensure a device’s legitimacy. Certificates can also be used to encrypt information or messages so that only the recipient with the correct digital ID can read it. Once verified, this exchange of certificates happens implicitly at software level, leaving users blissfully unaware. However, there is always the worry that certificates can be forged or stolen, thus allowing an individual to pretend to be someone else. Burying a digital certificate at hardware level can make them much more difficult for anyone to impersonate.

**LOOKING AHEAD**
The future of device security looks promising, with increasing focus on user-friendly and adaptable solutions. Biometric recognition — with Apple’s new fingerprint login for iPhones a key example. It is a trend Hay thinks is set to continue.

“From a user-experience point of view, it is a pain to remember lots of passwords,” he explains. “You end up using the same password for everything: emails, banking, logins, etc, which isn’t very safe. Our directional thinking is about improving the user experience, which will ultimately get rid of passwords entirely. We are looking at 3D facial recognition which, like other biometric technologies, will be more convenient and harder to steal.”

In the future we could also see more “location-sensitive” devices which allow certain privileges based on where they are. Imagine a device that granted access to corporate data during in-office use, but adjusted its security settings or access levels if taken to the local Starbucks. “Could this make sense for BYOD in the future?” asks Hay. “Absolutely.”
BYOD is not a panacea for all business pains

As Sage UKI’s chief technology officer I’ve looked long and hard to see if BYOD is appropriate for our 2,500 staff, and have concluded that, at this stage, a full implementation will not be made due to a number of hidden costs and challenges.

Take, for example, the influx of additional devices on the company’s infrastructure. Network performance (speed) can suffer and ultimately mean you need to buy network kit to manage the change in access type (Wi-Fi from wired) and usage.

Equally, many enterprise applications (the software tools used to do the job) aren’t yet configured for BYOD, resulting in frustrations for staff. For example, the need to use a webmail version of email instead of a native client that pushes messages seamlessly to mobile devices.

And who pays for the device usage? If a business only wants to pay for work-related calls and data, it puts a large burden on the finance team to validate claims. This makes it much more challenging to forecast and manage cash flow, particularly for companies with large numbers of employees, such as ours.

By shifting the hardware cost to the user, the BYOD model allows firms to significantly reduce technology costs. However, it is very important for staff to have the right tools to do their jobs effectively and in some cases this can only really be achieved if the IT department fully manages the devices used to ensure uptime, security and compliance. Businesses need to ensure they consider every facet of the issue before making a disruptive decision.

Stuart Lynn is CIO at Sage UKI

Data security is the prime concern

Given the ever increasing memory and storage afforded by the current generation of devices, it is becoming increasingly easy for people to carry huge amounts of sensitive data around with them. No wonder, then, that the loss of confidential company data is a major concern for employers.

The train is still the number one hotspot for laptop loss and theft, with homes and airports coming second and third respectively, according to the 2013 VAIO Digital Business report. And just 28 per cent of businesses have security features on laptops as standard, while nearly half spend less than £1,000 a year on security.

There are readily available security solutions that are not only easily implemented regardless of IT infrastructure, but that act as a ready-made safety net for those firms transitioning to BYOD. Security features such remote lockdown and location tracking are available on many models, including the VAIO range, right out of the box. With data security the primary concern for businesses, these are as important as the decision to go mobile itself.

BYOD should be rationalised on a case-by-case basis, with employee demands balanced against the pros and cons. For example, the need for education on how to utilise available mobile security measures is just as critical as having quality, light weight machines, with strong battery life. Simple steps like these go a long way to defusing the time bomb represented by the UK’s one million missing laptops.

Ruth Storey is category marketing manager at Sony, VAIO

A necessary part of a digital government

In the past, the performance of workplace computers was well ahead of what the average person could realistically aspire to own. Now, with nearly 80 per cent of households online and over half of UK adults owning a smartphone, this is no longer the case, as our report Smaller, Better, Faster, Stronger: Remaking government for the digital age, which surveyed over 2,000 public-sector employees’ attitudes to technology, highlighted.

When asked to think about how the technology available to them at work compares to what they have at home, 37 per cent felt their workplace technology was worse. Furthermore, 36 per cent said their organisation’s leadership didn’t understand what tools they needed to do their job well. Considering the need for a truly digital government, ignoring the potential of BYOD is ignoring the realities of how people work in today’s world. BYOD presents the opportunity for public-sector workers to make the best use of technology, increasing productivity while allowing for personal choice of device, thus raising workplace satisfaction.

Sarah Fink is a research fellow in the Digital Government Unit at Policy Exchange
1 in 4 UK businesses has either lost a laptop or had one stolen. Of laptops do not feature anti-theft security as standard. 72% of laptops do not feature anti-theft security as standard. 42% of laptop owners use data encryption as a security tool.

£1,000 is the amount 69% of UK businesses spend (or less) on IT security. £500,000 is the amount businesses could be fined by the ICO for loss of personal data.

The global view: percentage of companies citing security as the biggest BYOD risk.

82% of people don’t change their password monthly, as recommended. 20% of respondents never change their password. 17% only change it when prompted. 5% of people still use the word “password” as their password.

26% of companies globally say “security” is the biggest BYOD challenge.

Source: Sony; Cisco; AppSense.
Carry your office anywhere with the award winning VAIO® Pro 13
Crafted in tough carbon fibre, it’s our lightest Ultrabook™ ever

- Durable and lightweight
- Up to 18 hours of battery life (with the extended battery)
- TCG ver.1.2 compliant
- Intel® Anti-Theft Service 90 day trial

For the best offers in the market visit www.vaio.eu