Bring your own device

AVG Business

BYOD

One thing is clear: Bring Your Own Device has landed and is here to stay. Employers need to understand what it means, the benefits it could bring and the risks it presents to their entire business, not just their data or a single device. Employees, too, need to understand how this could potentially change the way they work forever.

Introduction

We’ve all been taking our mobile phones to work for quite some time now. Initially they would stay in our coats or bags or rest on our desks until they rang or buzzed. That is, they were purely for personal use and not for work. Oh, how times have changed.

Joanna Brace is Vice President of Marketing & Product Marketing, AVG Business. Her track record spans brand-building, product development and marketing strategy. She joined AVG from Skype.

New research[1] indicates the average amount of devices we carry could reach 4.3 per person by 2020, and they are more powerful than ever. Think smartphones, tablets and laptops. Then add wearables such as smartwatches and wristbands. We can sometimes do just as much work on a smartphone as we can on a laptop. The data they can store is also substantial.

Companies are increasingly adopting a Bring Your Own Device (BYOD) policy whereby employees use their own devices to do their jobs whether at the office, at home or on the train. As long as there is work to be done, data, a device, and a Wi-Fi connection to piece it all together, it sounds like a great idea.

The business benefits are clear: employees can work more flexibly, balancing work and personal life more easily, lessening the impact on absence or downtime for the employer.

The business can offer a more flexible service to its customers outside of the usual 9-5. And, if employees are buying, using and maintaining their own devices, the business may be able to reduce its overheads to some extent.

Data and devices can be lost, stolen, and corrupted. If those devices had access to the company network then they are at risk of being hacked. This is the challenge brought on by technological change but one that can be overcome by clear thinking and decisive action.

JBrace

BYOD is now

Recent research[1] forecasts the number of employee-owned smartphones and tablets to be used in the workplace will exceed 1 billion by 2018. This suggests that BYOD is well on its way from being a trend to becoming the norm.

It's no surprise to see big brands such as Apple and Samsung topping the best-seller rankings but Chinese brands Xiaomi and Huawei are increasingly popular[3]. However, be wary of using popularity as an indicator of which devices are appropriate for your employees to use at work.

Your network and processes will have a certain technological configuration and functional specification. When you're considering a BYOD policy, you should first establish which devices will meet those requirements, which ones won't, and then advise your employees accordingly. Don't just run with the crowd.

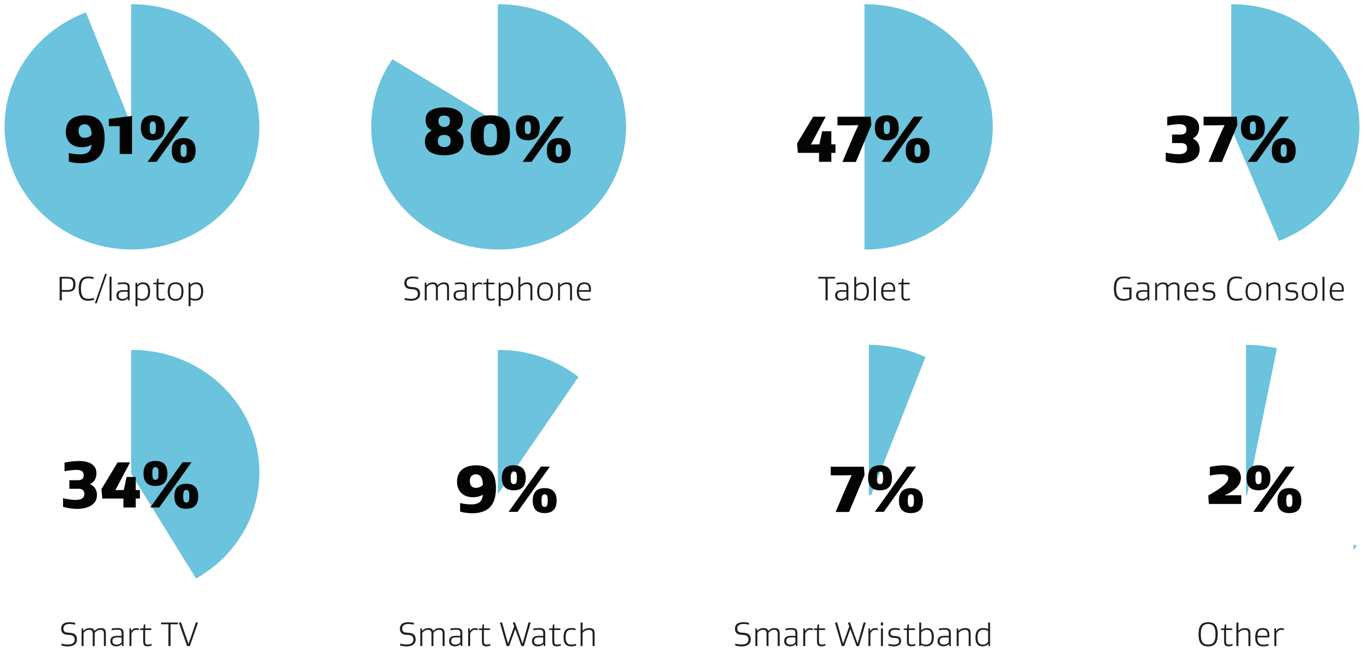


Table: % of internet users who own various technologies

The opportunity

Adopting a Bring Your Own Device policy is a great opportunity to rethink how you do business with your customers and how your employees get things done.

Being on the frontline and being early adopters themselves, many IT managers already believe BYOD can deliver a competitive edge through an increase in productivity, flexibility and customer service.

That's not to say those opportunities are guaranteed or applicable to each and every company. As ever, the nature of your business will influence what type of opportunity BYOD will present you. The general opportunities open to any business adopting BYOD currently fall into three broad categories:

Flexibility / Productivity
If employees can work with a range of devices in different places then this enables them to work whenever, wherever. Your customers, too, can benefit from this change because your employees may be able to service them at times which are more convenient to them and their lifestyle. The traditional 9–5 no longer applies; the working clock is reset forever.

Time / Cost Savings
If employees use their own devices they will likely be paying for them, at least in part. Similarly, they would be responsible for the time it takes to buy them, configure them, maintain and upgrade them, and train themselves in their use.

There will be a limit of interest in adopting BYOD and the value it can deliver

Employee Expectation
Recent business opinion[1] suggests employees expect to be able to use their own devices at work. Enabling employees in this way can deliver improved productivity and customer service because BYOD can offer more opportunities for staff to collaborate in more flexible and efficient ways. Many countries are also enacting legislation giving employees the right to ask for flexible working too.

The benefits

It’s not just technology companies that can benefit from BYOD. Any company can. Almost every business on the planet captures customer and supplier data of some description, then uses it to deliver a product or service.

There are three key benefits to allowing employees to bring their own devices to work:

Customer Satisfaction

If your team can work more flexibly, thanks to being able to work at different times and locations with their own devices, they can deliver a more flexible service.

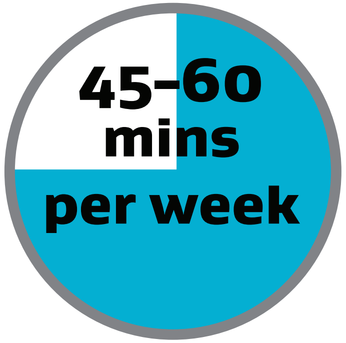
Productivity and Empowerment

If staff can use their own devices to get things done, they’ll be more skilled and faster at using them compared to a third party device or software they might have to be trained on. BYOD can also help people manage their work-life balance more easily, which can translate into less stress, improved productivity and better customer service.

Lower Costs

If employees are using their own devices then the business might be able to lower its IT procurement, maintenance and training costs. Employees who can get their work done wherever they are, are also less likely to leave and ask for pay rises too.

Work is a thing you do, not a place you go[2]



Employee time savings gained from “anytime, anywhere” access[1]

- **16%** of companies worldwide perceived job satisfaction as a benefit of BYOD
- **40%** of employees think they will be more productive using their own device
- **37%** of employees like to work with any device anywhere
- **35%** of employees like to combine work and personal use

The risks

Like any technological innovation - and the cultural and behavioral practices that accompany it - BYOD is no different in that it offers risk as well as reward.

Even though 74% of businesses are adopting BYOD[1] to some extent, not everyone is rushing in. Some have been put off because they see no need; some reject it out of security concerns.

Others are still assessing what the opportunities, benefits and risks are and, wisely, don't want to make a rash decision.

As for the specific risks to your business and your employees using their own devices, they will vary according to the depth and breadth of the adoption.

That said, there are some risks that will apply universally to which you should pay some mind:

Integrating Devices and Interests
If your employees are using a personal device for work then it needs to be integrated into the business network and able to connect to colleagues' devices.

Business data also needs to be partitioned, to keep personal data separate from work data.

The main obstacles to adopting BYOD[1&2]

1. Data security risks
2. Privacy concerns
3. Legal ramifications
4. Hidden costs
5. Compliance issues

there by accident. If a mobile device is hacked then your data is also at risk of being stolen, deleted or corrupted.

Loss of Time or Productivity
A staff member without a device or data will simply not be able to produce good work.

Alternatively, employees could spend too much time using their own device for personal use.

Legal issues

Knowing a little more about some of the most prevalent risks of BYOD from an HR and legal perspective will help you decide how best to counter them.

Conflicts of interest

Who owns, controls and uses the data and intellectual copyright? If the device is being used for work and personal reasons and isn't partitioned i.e. has no technical barrier between where work and personal data is being stored, processed or transmitted, then it can be difficult to prove who owns, created and controls the data in question.

Too much flexibility

Checking work emails on a smartphone on the way home – instead of shutting up shop the minute they leave the office – benefits everyone if it relieves pressure and helps a customer get a quicker reply. But, being technically able to work at any time, is not necessarily healthy or legal. Your employees can burn themselves out or put themselves under undue pressure by working at all hours.

Loss of data

When an employee leaves your company, ideally you'll have a controlled exit where you can determine which data and devices need to be retrieved and/or reviewed. If there is a need to wipe company data from a personal device, then you need to be mindful of deleting personal data (e.g. photos, videos, music). If the device has been partitioned, this may be simple to achieve.

If not, you should seek technical and legal advice before wiping anything. It's also wise, before going ahead with wiping data from a personal device, to speak to your employee and give them the chance of backing up their data. The same advice applies if a device is stolen or lost.

Protection

There's no guaranteed winning formula for protecting your data or devices from theft, corruption or loss other than remaining aware of the risks and mitigating them as best you can.

One thing's for sure, ignoring or vastly underestimating the risks to your devices and data is a potentially disastrous strategy.

For example, don't be fooled into thinking that a hacker won't be interested in stealing your mobile devices or data just because you're a small business. Cybercrime can and does happen to companies, organisations and institutions of all sizes, shape and geographic location. But that doesn't mean you're helpless. There are some basic steps everyone can follow:

Plan ahead: all employees should sign up to your BYOD policy explaining their rights and responsibilities, and allowing you to remotely wipe and monitor the device if needed.

Be practical: find a good Mobile Device Management solution to help you manage the data and devices.

Be proportional: offer BYOD to the employees who will get the most benefit and return out of it. It doesn't have to be company-wide if you don't need it to be.

Build a secure network: if your network is secure to begin with then it becomes much harder to hack.

Limit remote access to your network and data: give permission on a need to know basis and only to relevant data at the appropriate time.

Passwords[1]: change all default passwords, change them regularly, use a unique password for each account and two or three-factor authentication if possible.

Encrypt your data: Use cloud-based services to store data and back it up.

Don't be fooled into thinking a hacker won't be interested in stealing your data just because you're a small business

Lift off

Rolling out a BYOD policy is not something you can launch and leave; technology changes, employees come and go, as does data. Your business will evolve too.

The first step is to identify the business case for BYOD. This means clarifying the benefits, risks, security concerns, legal issues and execution.[1]

What will your business gain by allowing employees to use their own devices for work? How might time savings, greater productivity, and both higher employee and customer satisfaction be achieved?

Create a clear understanding of the benefits, risks and management

Once you've confirmed the business case, identify the following:

- **The TASKS you need to complete**
- **The DEVICES you need to access, process and transmit that data**
- **The DATA needed for those tasks**
- **The PEOPLE who will use control the data and use the devices**

That knowledge builds a picture of your BYOD landscape. Then you can:

1. Create a clear, comprehensive policy around personal devices and the right for your business to track devices, access, and delete all company data. Make sure this policy integrates with your Starters and Leavers Policy too.

2. Deliver an informative briefing where you discuss the policy with your team and require them to sign up. Everyone needs a clear understanding of the benefits and risks of using personal devices for work, especially of theft and the need to remote wipe a device. Offer them training and support.

3. Produce a simple security checklist for your team to follow. This can include aspects like activating passcodes for devices; creating strong passwords; using secure Wi-Fi networks outside the office; and keeping their devices' software up-to-date.

4. Consider buying in a Mobile Application Management solution which will help you manage all the data and devices. Create an Incident Response Plan and train the people concerned, so they know what to do and how to react if the worst does happen.

References

Page 3

1. https://www4.strategyanalytics.com/default.aspx?mod=pressreleaseviewer &a0=5609

Page 4

1. http://www.juniperresearch.com/press-release/mobile-security-pr2
2. https://www.globalwebindex.net/blog/80-of-internet-users-own-a-smartphone
3. https://www.strategyanalytics.com/strategy-analytics/news/strategy-analytics-press-releases/strategy-analytics-press-release/2015/07/30/huawei-becomes-world's-3rd-largest-mobile-phone-vendor-in-q2-2015#.VfLn8PlVikp

Page 5

1. http://www.techradar.com/news/world-of-tech/business-trends-for-2015-the-mobile-workforce-and-byod-maturing-1279975

Page 6

1. http://www.ibm.com/mobilefirst/us/en/bring-your-own-device/byod.html
2. http://www.newstatesman.com/2014/10/work-thing-you-do-not-place-you-go

Page 7

1. http://www.solar.co.uk/byod-statistics-74-organisations-using-adopting-byod/
2. http://betanews.com/2015/05/13/the-main-obstacles-to-byod-mass-adoption/

Page 9

1. https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/458857/Password_guidance_-_simplifying_your_approach.pdf

Page 10

1. https://www.gov.uk/government/publications/byod-guidance-executive-summary/byod-guidance-executive-summary#understand-the-legal-issue

Bring it on

BYOD is here to stay and offers many potential opportunities and benefits for small and large businesses alike: flexibility, reduced costs, happier workers. However, it's not risk-free: data and devices can be lost, hacked or stolen. Employers need to add and manage another policy to their list.

Take your time and think through the full consequences of what this technological change means for you and your business.

Learn more about internet security at www.avg.com/business-security
*** Small Business IT Security Health Check**
www.avg.com/small-business-it-security-healthcheck