BRING YOUR OWN DEVICE

Personal devices enter the workplace

Companies are looking at the benefits of allowing employees to access corporate systems using their own smartphones, laptops and tablets, but the strategy does not come without challenges

ELIOT BEER

The ability to access business emails and other systems on the go has become the norm in recent years. The rise of smartphones with email, a calendar and even sales-system capabilities, including the once-ubiquitous Blackberry, allows employees to keep up with their work using company-supplied devices, reducing response times and improving productivity.

The boom in popularity of smartphones, however, has moved them from being the preserve of corporate employees to becoming mass-market devices, with lower prices and easier-to-use handsets putting them within reach of many. This trend has been accompanied by a dramatic fragmentation of the smartphone market, with former market leaders Nokia and Blackberry usurped by Apple's iPhone and the vast range of handsets running Google's Android software.

Corporates turn personal

As a result, organisations have been faced with not only many more choice of mobile device, but also a wider demands from informed users on their preferred makes and models.

For growing numbers of enterprises, the solution has been to allow employees the ability to access corporate systems on their personal devices; a practice known as bring your own device (BYOD). This includes not just mobile phones, but also tablets and laptops, and can have significant advantages for both the user and their employer.

Adriana Rangel, research director for systems and infrastructure solutions at research firm IDC, says moving to a BYOD model can result in significant increases in productivity and profits. "This increase in productivity comes from enhancing portability in the work environment, as well as making it possible for workers to perform more tasks remotely," she says. "This, in turn, tends to improve field service response time and has a direct impact on the company's revenue."

Another advantage, at least for employers, is the savings that come from having employees use their own devices. While this remains optional at many organisations, there is a shift towards making BYOD mandatory: a March 2013 survey by California-based network systems provider Aruba Networks revealed 40 per cent of Middle East businesses provide no mobile devices for their employees.

KEY FACT

Eighty per cent of organisations in the Middle East allow some form of personal device access to corporate systems

Source: Aruba Networks

"A BYOD strategy also presents IT departments with an opportunity to reduce their IT spending costs"
Jatin Sahni, Du

"A BYOD strategy also presents IT [information technology] departments with an opportunity to reduce their IT spending costs and, in particular, costs associated with hardware expenditure," says Jatin Sahni, vice-president for large enterprise and business solutions marketing at Dubai-based telecoms operator Du. "Employee-owned devices are also likely to have their own warranty or service agreement in place. This could further reduce the volume of support contracts IT departments have with manufacturers."

While this is clearly a benefit for employers, there has not been a backlash by employees at this transfer of costs. "You might expect users to revolt against paying for the devices and technology they use at work," says Manish Bhardwaj, regional marketing manager, Middle East and Turkey, at US-based Aruba Networks. "Not so. Users have the laptops and smartphones they have for a reason: those are the devices they prefer, and they like them so much they invested their hard-earned money in them. Of course, they'd rather use the devices they love than be stuck with laptops and mobile devices that are selected and issued by the IT department."

As a result, increasing numbers of employees are using personal devices to access corporate systems, with 80 per cent of organisations in the Middle East allowing some form of personal device access, the highest of any region in the world, according to a 2012 survey by Aruba Networks. This can be seen as part of a broader trend towards increasing mobility in the region. In a 2013 survey of chief information officers from the Middle East by IDC, 41 per cent said mobilisation was a priority.

But while the top-line benefits are clear, adopting BYOD policies comes with a significant amount of overheads for IT departments and potentially large security risks. Organisations have to do their homework when setting policies and educating users, and make calculated decisions about how much data can be accessed by employees' personal devices.

Company policy

"The important thing is that it's driven by policy, and policy leads to investment" says Arthur Dell, director of technology sales and services for Europe, the Middle East and Africa at Symantec, a California-based IT security and services firm. "What do you want to achieve, how do you drive that, and what are the specific considerations around implementation? To manage or not to manage users' devices, what to manage, what kinds of corporate resources do you want to provide, and securing corporate resources once delivered: those are the fundamentals of driving the strategy."

For many companies, the most significant shifts may not be in security or infrastructure, but around policies and corporate culture. Megha Kumar, research manager for software

"BYOD policies need to be transparent. Such openness requires a rethinking of corporate communications"

Manish Bhardwaj, Aruba Networks

at IDC, says: "Most companies are good at creating policies, but are very poor in increasing user awareness. Some companies in the region do not realise that when you implement new solutions you also need to train users, since change management can be incredibly cumbersome. It is usually left up to the IT department to manage this, when it is really the job of human resources to work with IT to increase policy awareness."

Aruba Networks' Bhardwaj makes a similar point. "BYOD policies need to be transparent. Having parts hidden from employees can cause the policies to backfire," he says. "Such openness requires a rethinking of corporate communications with its traditional need-to-know basis. The trust that this change can foster will, in turn, fuel the productivity increases that enterprises are hoping to get from BYOD."

Issue of trust

But setting and communicating effective policies is an area where regional organisations are struggling; as is the rest of the world. According to Aruba Networks' 2013 survey, 35 per cent of Middle Eastern respondents claimed their IT department takes no steps to ensure the security of corporate files and applications on their personal devices. And 53 per cent said their employers provide no additional security software for their personal devices.

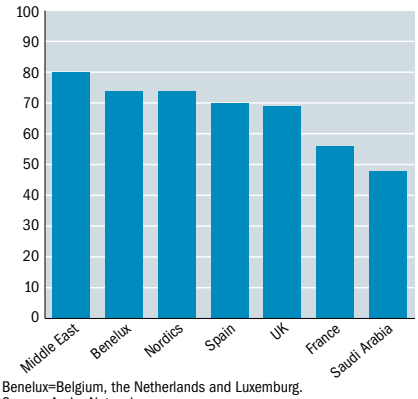
The survey reveals there is also an apparent communication gap between employers and employees on the issue of personal data.

While employees may not mind, or even prefer, using their own devices for work, they are still unsure how their employers will handle their private information. Thirty-one per cent of regional respondents were worried their employers may access personal data, and 24 per cent believed if they were asked to install additional security software, this would give employers' access to their data.

"A company would be required to gain the employee's prior consent to process such personal data, or demonstrate that it is in the firm's lawful interests to do so," says Bhardwaj.

PERSONAL DEVICE ACCESS

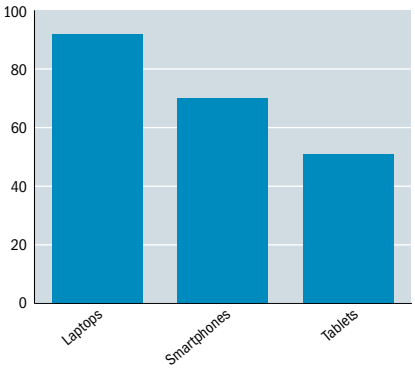
(PERCENTAGE OF FIRMS THAT ALLOW ACCESS)



Benelux=Belgium, the Netherlands and Luxemburg.
Source: Aruba Networks

COMPANY-SUPPLIED DEVICES*

(PERCENTAGE OF FIRMS THAT PROVIDE DEVICES FOR EMPLOYEES)



*=Europe, the Middle East and Africa. Source: Aruba Networks

"Again, it all comes down to the policies a company sets for BYOD. The policy also should provide that the employer might access the device to remotely wipe corporate data when an employee decides to leave."

Du's Sahni suggests there is a trust issue: almost 50 per cent of workers in the UAE claimed data privacy concerns would stop them using personal apps on a corporately provided smartphone and/or tablet. While these problems can be solved to some extent by having clear policies, the issue of trust is not likely to disappear in the near future.

An unfortunate consequence of this is that users are reluctant to report problems or losses, or even the use of corporate systems on personal devices at all. Seventeen per cent of regional respondents failed to tell employers they were using personal devices, and 26 per cent would not report that their personal device had been lost or stolen, according to Aruba Networks.

IDC's Middle East IT End-User Security 2013 survey shows organisations also see users' lack of understanding as a problem. Of organisations in the Middle East, 82 per cent claimed to have proper IT security policies in place, but 57 per cent of the organisations surveyed claimed employees not adhering to security policies was a major challenge to IT security.

Beyond organisational issues, adopting BYOD also means dealing with increased risks of more traditional security threats, such as malware – including viruses or trojans – or phishing attacks.

"A survey found the typical employee uses a number of endpoint devices, which can also be openings through which malware can enter the network. During a typical month, as many as 4 per cent of these employee endpoints become infected, with a growing number of organisations reporting security violations through their use of web and email," says Sahni.

Symantec's Dell says the first step for companies considering BYOD is to identify what applications need to be made available on personal devices. Then organisations need to look at how to protect devices and insulate corporate data from personal data. Next come decisions around specific data and device policies.

Offsetting risk

"What kind of data do you want to send; what data can you forward?" he says. "How can you categorise data internally, and how do you allow what can or cannot be sent to and from that device? Also, how do you protect those devices against traditional malicious threats, and so on? Finally, try to make sure the settings are defined for devices, so if there are risks to changing particular configurations, those configurations can be managed through policy.

"The important thing is what's on the device, versus the device itself. There are many features, such as remote wipe or remote locking that are common as well, so when not in use, the device locks itself. If the device is lost or stolen, the data can be remotely wiped. And, of course, all data on the device is secured; it is not possible to access the corporate data on a device, because it's encrypted."

While it is clear there are risks to implementing BYOD policies, it is becoming easier to manage and mitigate these risks, and the potential benefits for productivity gains and cost savings are significant.

"The key point here is, it is OK to be cautious about mobility," says Dell "Being resistant is probably going to be a penalty, so our guidance would be to start embracing it."