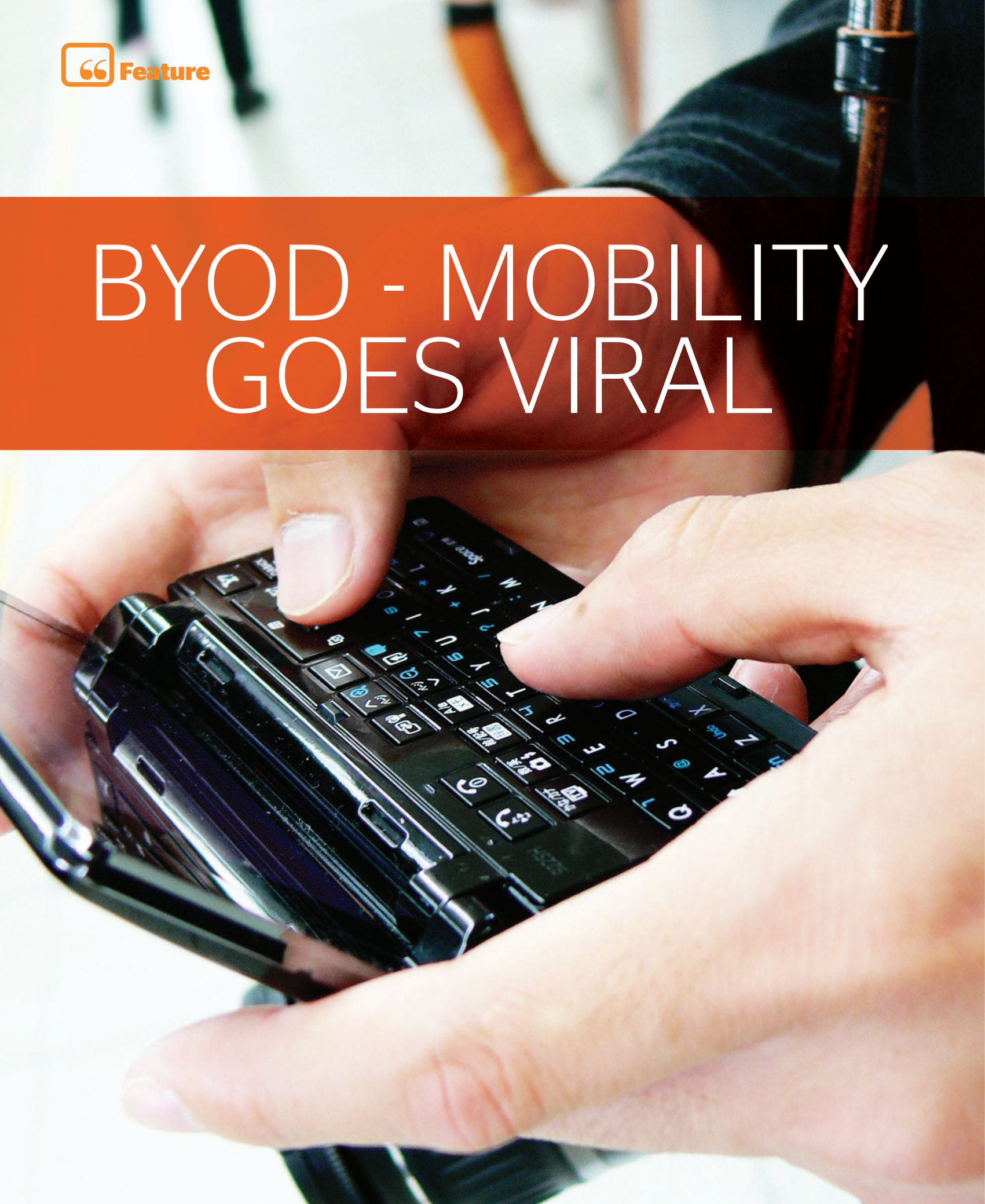
Feature

BYOD - MOBILITY GOES VIRAL



A year ago it was the development no employer wanted to know about; now, it's the movement every employer has to deal with. Bring-your-own-device (BYOD) computing is the trend du jour, but is it really the Holy Grail of increased productivity, customer engagement and happy employees? Or are we just nearing the peak of inflated expectations before the inevitable trough of disillusionment?

If there was one technology that was currently being touted as the next big disruptor, it would have to be BYOD.

Sitting at the centre of a perfect storm of mobile, cloud and virtualisation technologies, BYOD may be in its infancy, but its potential is huge. Although often characterised as a Generation Y-driven phenomenon, CEOs and other mobile device savvy executives are making their wishes known – they want to bring their own devices into the workplace.

But while many are predicting huge productivity gains for businesses that manage to implement BYOD successfully, there's no denying that the fast moving growth of BYOD brings along with it threats to sensitive and confidential information.

Nevertheless, some very heavy hitters are already adopting BYOD as their modus operandi. IBM recently announced that by the start of 2012, 100,000 IBM employees will be able to connect handheld devices of their choosing to IBM's internal networks. One study found nearly 50 per cent of firms say they're currently focusing on how to support more mobile applications for employees to accommodate the trend.

So is a consumer mobile device strategy just a 'nice to have'? Or is it approaching the point of being an outright necessity?

What's the attraction?

The 2011 US Enterprise Mobility: Employee Survey found that the number one reason employees use consumer applications at work is familiarity. This phenomenon, dubbed 'the Apple effect', promotes the idea that the king of consumer electronics has affected the way we interact with technology to such a degree that mobile devices 'just feel like home' for employees – a home where their productivity measurably improves. (And surely it's a curious fact, given that Apple, a company that has never targeted enterprise, has had more impact on enterprise IT departments than any other technology vendor.)

Essentially, employees like their devices a lot, and they want to use them in the workplace.

"Typically it's been the IT manager or the technology department decides what device you're allowed to bring into the workplace," says Sean Kopelke, director, security and compliance solutions, Symantec.

"The big shift we're seeing is that the end users – the employees – are beginning to bring in their own devices. They don't want to be limited to a device that's been forced upon them.

"When you look at what cloud technology has done to the market, it's allowed our files and documents to be easily accessed on tablet devices, notebooks, desktop machine or phone devices from anywhere. The technology has enabled us to move between devices very effectively and easily. People aren't working a nine to five job sitting at their desk in front of a large computer screen or desktop computer - those days are well and truly past us - and they want to be able to access their corporate information where they are."

But there's more to it than just mobility. In many work environments, the employees' own device is *superior* to the outdated systems operating in-house. Many employees simply feel they can do their jobs better on their smart-phone or tablet than they can on their aging PC or under-performing laptop.

For these reasons, among others, employees aren't waiting for an invite. They're diving in.

The future is here

According to George Hamilton, principal analyst in Yankee Group's Enterprise Research group, the employee consumerisation experience is being driven by three interrelated trends:

1. Enterprise mobility – Employee-owned smart-phones and tablets are becoming the norm, and the users of these devices are bringing apps and content with them into the enterprise.

2. Cloud computing - Public and private cloud-based infrastructure and applications are driving down capital expenditure »

QUICK STATS:

- 60 per cent of all corporate employees share, access and manage content outside the office – be it via their iPhone, iPad, Blackberry, Android or other device, with indications given that that number is only going to increase.
- 73 per cent of business leaders surveyed currently allow mobile devices or tablets to connect to their corporate networks.
- 50 per cent of firms say they're currently focusing on how to support more mobile applications for employees to accommodate the trend.

and IT operational costs. Those same applications are giving users instant access to cloud-based alternatives to IT-controlled applications. And they're using them—with or without IT's involvement.

3. Social media - Businesses around the globe are on the cusp of a generational shift in how their workers communicate that is directly tied to consumer communications.

"These are not three independent developments," says Hamilton, "there is a synergistic relationship.... This new era of consumerisation and mobility is changing the relationship between users and the enterprise IT department. For enterprise IT to actually lead and embrace the consumerisation and mobility revolution, it needs to adapt IT processes and user support to this new norm."

And it seems that it is, indeed, the "new norm".

A US 2011 enterprise mobility survey, found that thirty per cent of employee respondents said they had installed consumer applications on their work device, even though 49 per cent admitted that their IT department does not grant them permission to do so. Long story short, employees aren't waiting for business policies to change. With or without policies in place, offers of reimbursement or even permission, employees are driving forward, causing headaches and real-world security issues for management and IT departments alike.

"More and more employees are coming along," says Todd Cassie, manager of technology solutions at Christchurch Airport, "and saying 'I've got an iPhone, I've got an Android, I don't want to use your standard phone, I want to use this phone', and we have to actively try to figure out the best way to deal with that....because if someone's got an Android or an iPhone or a Windows phone and they can make that work for them, then that's going to work for us ultimately. We've fully bought into that. The concern is now 'how do we manage that?'"

The, problem, he says, is "fundamentally about security and control".

"It's about [IT departments] not being able to have their hand on their hearts and say to the board and to the business 'we feel safe and we feel secure that these machines on the network aren't going to cause us any issues or cause us any concern'."

New layers of complexity

Companies that have already embraced Blackberry's mobile business platforms are perhaps less intimidated by the consumer device shift than others. Enterprises working with Blackberry already have the appropriate tools to manage mobile devices – high visibility, remote locking and remote wiping.

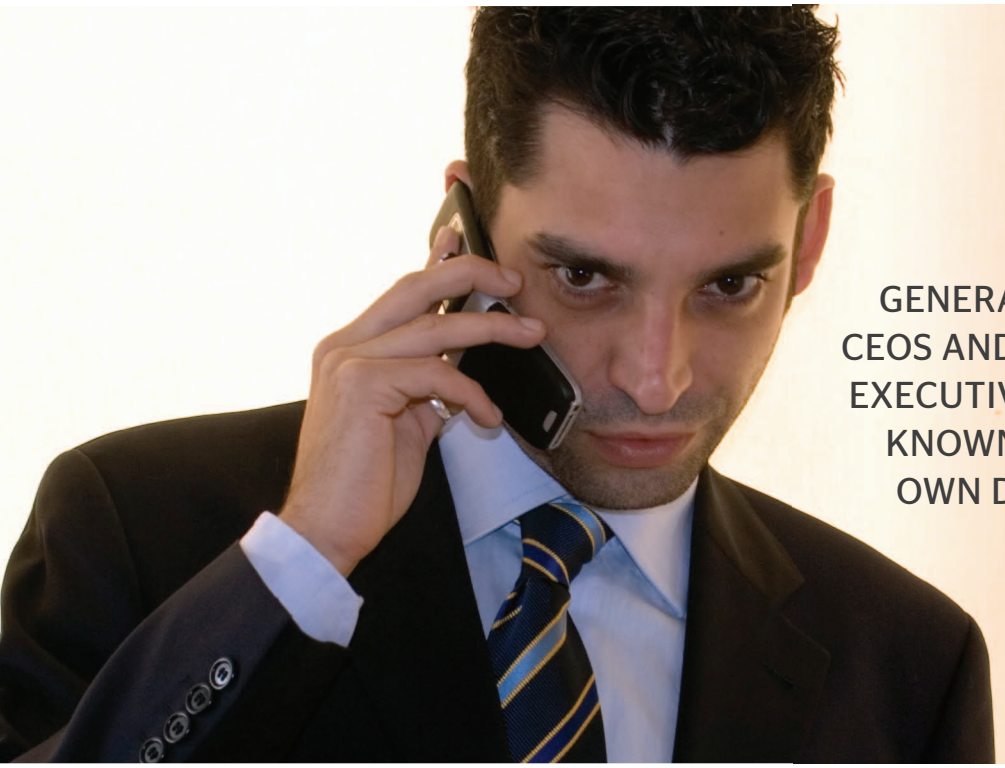
Blackberry, however, does not rule the mobile world, Apple does, with Android rapidly closing the gap. And it's the presence of these varying devices in the workplace that's wrestling control from the hands of IT departments and putting it into the hands of employees.

"I think IT departments have really been put in a difficult position," says Kopelke. "[BYOD has] lead them into this spot where they're no longer in this position where they can say 'no, we're not going to allow that'. They're being forced into it and they have to figure that out how to move forward."

And with multiple new layers of complexity it's not a case of 'one policy for all'. Different devices present different risks and the challenge is to produce policies with sufficient sweep and detail.

But while security companies and mobile device management vendors may have an interest in promoting the complexity of security issues BYOD-curious businesses are facing, the risks can in fact be characterised as 'IT business as usual', just with a mobile twist:

- The employee who ignores company policy with, or without, ill intent
- The employee who intentionally or unintentionally stores sensitive data on an unsecured device or in an unsecured place (e.g. in a personal cloud application)
- The employee who broadcasts sensitive information via to social networks, blogs, chatrooms, wikis, YouTube or IM.
- The fired employee who has access to sensitive/valuable data (risking intellectual property, financial integrity, corporate reputation, the control of our individual and corporate identities, privacy)
- An increased risk of infection from malicious programs from contaminated devices
- Lost/stolen devices



OFTEN CHARACTERISED AS A GENERATION Y-DRIVEN PHENOMENON, CEOS AND OTHER MOBILE DEVICE SAVVY EXECUTIVES ARE MAKING THEIR WISHES KNOWN – THEY WANT TO BRING THEIR OWN DEVICES INTO THE WORKPLACE.

While the risks posed by BYOD don't break new ground, the proposed solutions to these problems are where things get interesting.

Safety first

"Security and control is the big challenge," says Cassie. "There's a lot of talk out there that 'you just need to do this' and 'you just need to do that', but actually doing the 'this and that' is really hard to do. It's hard enough trying to get an access control scenario on your network working with your own equipment, let alone trying to get the whole working with others as well. There are a lot of glossy brochures out there that tell you how easy it can be, but that's not necessarily the case."

"We believe these tools will give us gains that we haven't thought of yet; we just need, from an IT point of view, to be comfortable that by doing that we're not trading productivity gains for a security hole."

So just how does a company get its approach to consumer devices from 'disruptive' to 'productive'?

The key is in developing a strategy for consumer device use; deciding how best to manage devices and support users; making expectations clear company-wide and then backing up those expectations with real-world responses in the event of non-compliance.

1. Developing a strategy

The rise of BYOD computing poses real challenges for IT departments. These challenges demand a strategic approach to managing risks, threats and vulnerabilities without negatively impacting user convenience or productivity. Accepting the fact of BYOD computing, rather than attempting to needlessly limit the use of these devices, allows businesses to get on with the business of increasing efficiency, worker flexibility, end-user convenience, and decreasing operating costs.

Consider conducting an audit to see what devices are being used, and where, in your operation. This will help you to understand the risk posed by the new technology, what behaviours are being enabled and where sensitive or confidential information might be at risk.

Classifying what data is allowed on what device allows a company to communicate with staff about what behaviours are appropriate or inappropriate, but also to be crystal clear with employees about their accountability with the data. Research organisation, the Ponemon Institute, suggests that such data be classified as: regulated data (such as credit cards, health data, SSN and driver's license number), non-regulated customer data (such as purchase history, email address list, shipping information), non-regulated confidential business data (such as IP, business plans and financial records) and employee data.

Conduct a risk assessment to determine what possible scenarios could compromise data and decide on the appropriate response in their event. Devise appropriate security measures for both the data and the device.

2. Create a comprehensive policy

Your policy should include specific guidelines for employees, addressing the risks associated with each device – such as

»

MANY EMPLOYEES SIMPLY FEEL THEY CAN DO THEIR JOBS BETTER ON THEIR SMART-PHONE OR TABLET THAN THEY CAN ON THEIR AGING PC OR UNDER-PERFORMING LAPTOP.

what type of data cannot be stored on the device - and the security procedures that should be followed, such as how to download an application securely and what to do in the event of a lost or stolen device. While obvious security threats, such as 'jail-breaking' of devices, should be prohibited, policy-makers should understand that it is near-on impossible to prevent employees from using devices for both personal and business purposes. Guidelines should take this into account and establish clear rules for specific non-work-related activity.

A rigorous monitoring process should also be established to ensure that employees are complying with policy. The penalties for non-compliance – including the punishments for malicious or negligent activity – should be made clear.

3. Conduct training

Companies should conduct training sessions to make sure that employees are aware of the risks and emerging threats created by BYOD computing. Training should stress the need for care when transmitting confidential information.

Employees should also be trained to recognise traditional threats that are exacerbated by BYOD – such as phishing threats. Inform them that phishing threats often appear to come from established and well-known organisations and request personal information, and often arrive via email, social media and social networking sites.

Urge employees to treat texts, system messages or events on their mobile devices that they did not ask for, initiate or expect, with caution, and to never assume that voice calls, especially international ones, are confidential.

4. Use remote control

The downloading of unproductive or risky applications must be blocked on company-owned devices.

Furthermore, given the wide-range of applications available to the consumer, blacklisting methods are perhaps not sufficient to prevent targeted attacks against specific vulnerabilities. Application control should be used, if possible, to ensure that applications such as browsers, PDF readers and flash players are patched and up-to-date.

Monitor and control the data that travels on your network and make sure you have controls in place to inform you about third party transfers.

To reduce the risk of data breaches, use remote wipe, remote data encryption and anti-theft technologies that allow you to locate stolen devices and prevent their unauthorised use. Many smart-phones come with the ability to remotely wipe data in the event of their theft, and this technology is widely available for purchase.

Employees should be educated about what the response will be if devices are lost or compromised.

5. Reinforce the basics

Making sure systems are up to date, making sure passwords are in place and ensuring employees follow basic best practice (not clicking on links or responding to requests that could be malicious for example) need to be reinforced. Familiarity with a device can lead to a slackening of attitude towards security. Reiterate general rules of thumb.