The Connected Business

Wednesday 26 September 2012   www.ft.com/connectedbusiness | twitter.com/ftreports

Lines blur in era of the digital native

More companies allow staff to use personal devices for their work, but they need to have proper policies in place, reports *Paul Taylor*

Illustration: FT Graphic

Consumers today have more choice than ever before about the technology that they use – from powerful smartphones and ultrabooks – lightweight, slim computers – to the social networks they use to stay in touch with each other, and the cloud-based services on which they increasingly rely.

As this technology spills over into their professional lives, the line between the personal and the professional, the consumer and enterprise, is blurring. Welcome to a process that is reshaping business computing through a process dubbed the consumerisation of corporate IT.

"People want to use the same technology at work as they use at home," says Microsoft, the US software company. But while consumer technology offers some important potential benefits for the business it also represents added risk in terms of security, privacy, and compliance. "For [corporate] IT, it's about striking a balance between user expectations and [company] requirements," says Microsoft.

These issues have come to the fore particularly in companies that have embraced the BYOD (bring your own device) and CYOD (choose your own device) trends and allow or actively encourage employees to bring to work the devices they use at home – including smartphones, tablets and lightweight laptops.

Vincent Geake, director of secure mobility at BAE Systems Detica, argues that BYOD's success or failure hinges on a company's ability to develop a policy and implement measures properly in advance. The introduction of these devices is disrupting established security practices and services, and organisations must start with a proper risk assessment to determine where policy limits should be set for different user groups.

Just as a corporate car allowance policy sets limits on the type of vehicles staff can use and requires them to purchase appropriate insurance, Mr Geake notes that to be effective a BYOD policy must identify any requirements or limitations in device use and set out the split of responsibilities between employer and employee.

For example, although the employee will provide the device, the employer may need to provide security

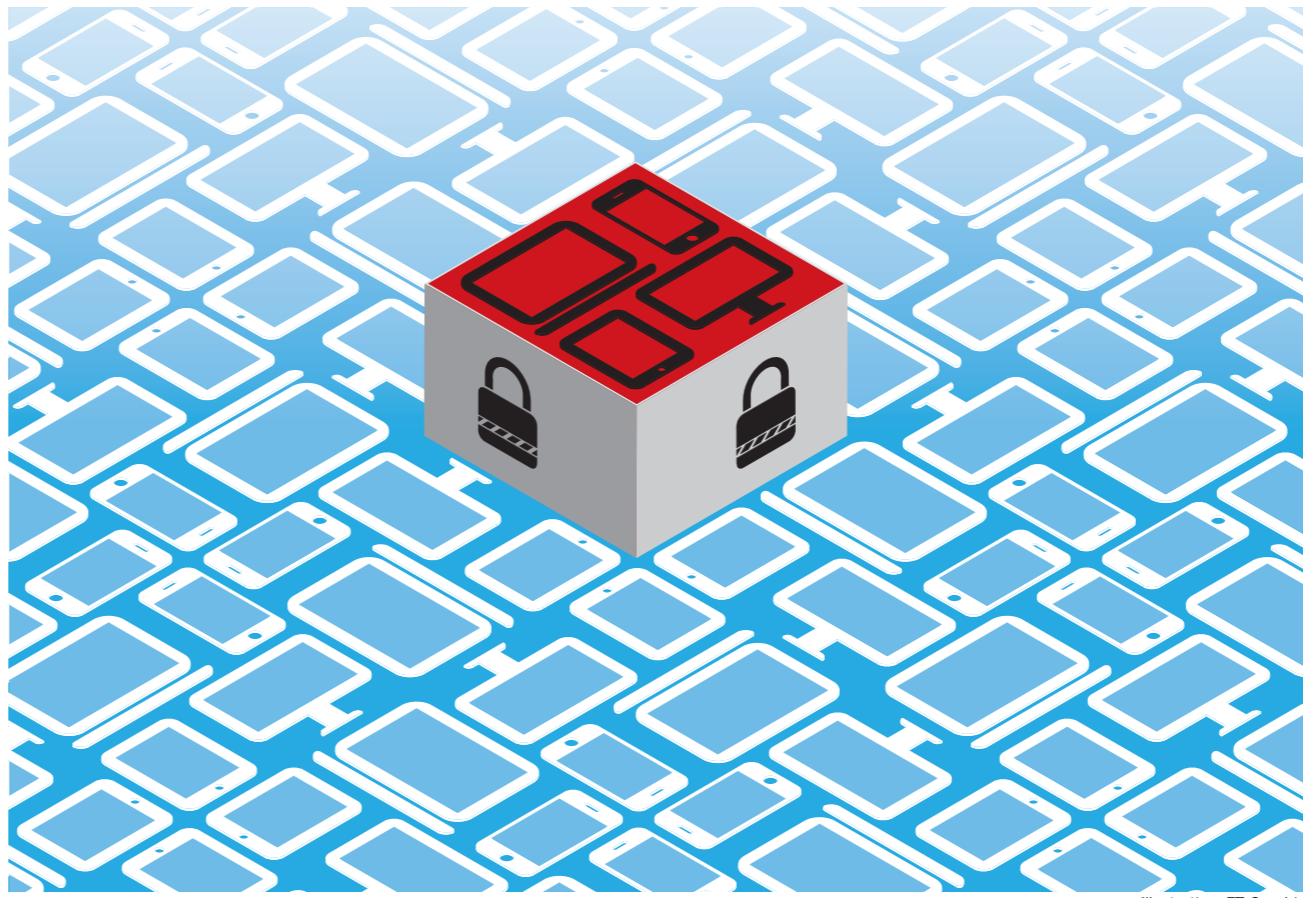> 'People want to use the same technology at work as they use at home'

services the employee must adopt.

"BYOD can't just mean bring any device on your own terms," says Mr Geake. "While there are many advantage to companies incentivising employees to use their own devices, there must be a clearly defined policy in place – for example, restrictions on certain apps and tools they can use on the device. It may also mean employees agreeing to give the corporate IT department the ability to manage the device remotely, and potentially even enable 'remote wipe' should the device be lost while containing valuable corporate data."

The evidence from a broad swath of companies that have already launched formal BYOD programmes suggests the type of policies advocated by Mr Geake are indeed being adopted. Most companies embracing BYOD or CYOD say they are doing it not because it saves money – often it does not – but because studies suggest it improves productivity and helps attract and retain a new generation of so-called "digital natives" as employees. Understandably perhaps, many of the companies in the vanguard of the BYOD movement are technology companies themselves.

Some encourage employees to bring to work personal devices and connect them to corporate IT resources including the main computer network.

Others, such as Germany's SAP, the enterprise software market leader, have increased their purchases of devices, including iPads and iPhones initially targeted at the consumer market, for employee use. "The consumerisation of IT is a corporate reality," says Oliver Bussmann, SAP's chief information officer. Under Mr Bussmann's guidance, SAP has emerged as one of

---

Increase in handsets raises risks

The use of personal items has put IT departments on the back foot, reports *Chris Nuttall*

There are cautionary tales for both employers and employees when it comes to the practice of bringing your own personal device (BYOD) to work.

Take the example of the man who forgot he had signed a waiver months earlier with his company, allowing it to wipe his personal phone of data if he left the company.

On his last day, the phone was wiped clean at 5pm as he left the office. At 5.01pm, he called in to complain that vital personal data were missing – photos and texts he needed for a child custody battle – only to be told there was no way of recovering this. Then there was the investment banker who left his iPhone 4S on a table, allowing someone to pick it up and use voice capabilities on the device to dictate an email to make an illicit transaction.

Alan Dabbiere, chairman of AirWatch, a provider of mobile device, content and applications management services for businesses, cites both cases as examples of the way in which concerns about managing and securing mobile devices have escalated well beyond the requirement to ensure that corporate email is made safe with a standard BlackBerry Enterprise Server (BES). He says: "[BES] was the gold standard in the same way as a lockbox in a bank, but in modern mobile, the task is like trying to secure the Olympics – the BlackBerry model has fallen apart and it's become about securing much richer applications and wider-use cases."

AirWatch says it has grown from 100 employees to 750 in the past 18 months. The company has also been acquiring 500 customers a month as the scale of the problem dawns on companies. Mr Dabbiere also quotes research from Microsoft's Trustworthy Computing Campaign, which says 67 per cent of employees use a personal device for work whether it is authorised to or not.

Geoff Glave, senior product manager for endpoint security with Absolute Software, says companies have to create a policy on users bringing their own devices to work, analyse the risks and decide whether and how to restrict their use in the workplace.

"So we have customers where the only requirement is you must have up-to-date anti-malware software on your device, to the other end of the spectrum where you have customers who are saying you can bring in your iPhone but you've got to turn off YouTube and the camera, using our software," he says.

Such third-party software is needed when users are shunning corporate-friendly devices from companies such as Lenovo or Research In Motion in favour of Apple's products.

"There is no means on an iOS [Apple's operating software] device to block a user from using iTunes and putting what they want on it because Apple's mantra is the user is the owner of the device, not the corporate IT department, and it's in Apple's interest to keep everyone within that iTunes world," says Mr Glave.

James Alexander, a partner in Deloitte's security and resilience practice, says BYOD has put IT departments on the back foot, as it is normally they that are setting company policy and issuing devices themselves. "Early adopters of tablets and smartphones tend to be the executive management team, so IT departments are having to respond very rapidly."

Virus attacks and hackers stealing data are still among the top concerns, according to Pat Calhoun.

67%

Number of staff using a personal device for work, authorised or not, according to Microsoft research

head of network security for McAfee, the antivirus software and solutions company owned by Intel.

"Hackers are really leveraging personal devices to get access to information within the enterprise; this is the weak link in the chain," he says.

"Sometimes they've identified the person within an organisation that they actually want to go after to get what they want, and they can send a highly targeted personal email where an attachment can be opened and create a vulnerability."

Jason Hart, vice-president of Cloud Solutions at data protection company SafeNet, says the information that people provide about themselves on social networks, and the availability of such networks on mobile devices, make the hacker's job easier.

"People are always connected to social media via their device, so the attack vector is broader and wider. It makes getting an individual's username and password such an easy target."

A quarterly McAfee Threats Report published this month said a mobile malware explosion recorded in the first quarter showed no signs of slowing down in the second. Virtually all new mobile malware detected was aimed at the Android platform, often sent through text messages.

"My description of Android is 'insecure with a multiple-personality disorder,'" says Eric Maiwald, infrastructure security analyst with Gartner, the research firm. He refers to the multiple versions of the operating system on employees' own phones and the viruses and data-gathering trojans spread by apps and other entry methods.

"As a result, most enterprises are saying they will not support Android."

Suppliers of desktop PCs to the corporate market are responding to the consumerisation of IT with touch-screen all-in-one PCs, light ultrabook laptops and appealing tablets or hybrid convertible machines, which will feature the new Windows 8 touch-optimised operating system. But Mr Maiwald says these devices are unlikely to reverse the trend: "Consumers have got a taste for their own choice of device, and they're not going to give it up."

The flipside could be an unexpected benefit to business in reducing costs. "Enterprises have started to see that, because of this trend, they don't have to manage and maintain all these devices, and maybe won't have to refresh all their corporate machines every three to five years," Mr Maiwald says.

Alan Dabbiere: 'Task is like trying to secure the Olympics'

The Connected Business

Producers try to bring consumer feel to corporate wares

Manufacturers

Hybrids with a Jekyll and Hyde persona for office and private use are on the way, writes *Jane Bird*

However much we may love electronic devices, who wants to carry several at once? "Some organisations have staff carrying four machines," says Craig Parker, head of product marketing for Fujitsu's Technology Products Group. "Personal and business smartphones, a personal tablet and a business laptop."

While personal smartphones and tablets are convenient, people often need business PCs to access corporate applications and data. Now manufacturers are beginning to develop hybrids that aim to combine the convenience of personal devices with the functionality of corporate PCs.

These hybrids have a "Jekyll and Hyde" persona that lets them transform from ultra-portable tablets to a machine that can be used in a different way in the workplace, says Mr Parker. "These single devices, which can be adapted for different situations, appeal to enterprise [corporate] customers because they get the best of both worlds."

Fujitsu's lightweight Stylistic tablets, for example, come with a range of accessories including mouse, keyboard and Bluetooth wireless communications technology to connect to a screen or projector. They also have a detachable pen that can be used, for example, to let the person confirm a delivery or a sales contract with an electronic signature.

Hardware convertibility is matched with software that gives people contacts, a calendar, email, apps and a window on to the corporate network for work-related data and applications. Security is built into the software and hardware, and includes a fingerprint scanner. If an employee leaves, company data can be remotely and securely removed from the device without touching personal apps and data.

Viruses can also be remotely killed, and if tablets are lost or stolen when employees are working on important documents, the IT department can connect and retrieve them before wiping the device.

"The hybrid approach creates a single device that can be used in a dual personal and business role, so organisations can have their cake and eat it," says Mr Parker. "That is a big hook for the [corporate] market. People get something that is lightweight and small from a physical and software side, but which lets them access what they need and doesn't require them to carry around a lot of unnecessary information when they are on the move."

People will even be able to leave battery chargers and their cables at home thanks to technology that Intel, the chipmaker, is developing, which lets a device draw power wirelessly from another placed alongside it.

Global Positioning System technology is also being exploited by manufacturers to make devices more enterprise friendly. On Fujitsu's Stylistic table, for example, an application or file can be set to only function within a geographical region, time or on a particular network.

Someone might only be able to access "super secret internal data and applications" when they are at work or during office hours; as soon as they leave, or are in the wrong place, the application will not function.

Using GPS, an investment bank might ensure corporate treasurer clients are located with their phones somewhere they are expected to be to authorise a large funds transfer, says Ted Bissell, mobile business expert at PA Consulting.

Access can even be restricted within a building, depending on whether the employee is in specific areas such as research and development, manufacturing, storage or administration.

Engineers working in the field can be equipped with an application that reads the tablet computer's current location to deliver just the detailed installation drawings relevant for a particular valve repair as well as verifying its exact location on a geographical information system.

Near-field communications (NFC), the technology used for contactless travel cards and mobile payments, also has corporate applications, says Mr Bissell. It could turn tablets and smartphones into electronic keys to get people in and out of buildings, or activate control consoles on equipment they are allowed to operate.

NFC is proving popular as it enables people to exchange business cards electronically by tapping two mobile phones together, says Tim Hodkinson, Research In Motion's director of enterprise marketing. With BlackBerrys, it is as easy as shaking hands, he says, though industry s t a n d a r d s have not evolved to the point where it works easily for all phones.

RIM is also encouraging companies to use social networking technology to improve staff collaboration. "With BlackBerry Messenger, people can share ideas and information within a controlled network of colleagues on the move," says Mr Hodkinson.

This can speed up processes such as those of recruitment and retention in human resources departments, for example, by enabling managers to send quick responses at important stages rather than having to use classic corporate resource planning applications, he says.

The irony, says Simon Robinson, an expert at PTS Consulting, is that while manufacturers are trying to respond to business demands by making mobile devices more business-friendly, small "smart" devices developed specifically for the enterprise market, such as the Cisco Cius, have failed.

He says: "This happened because they were not 'consumer-friendly' enough, although they were attempting to enter a market already dominated by iPads, Samsung Galaxies and iPhones."

New breed: the Fujitsu Stylistic Q550

'Organisations can have their cake and eat it, that is a big hook for the corporate market'

Too late to dam river of information

Access *Michael Dempsey* says executives need to stop trying to separate workers' social and career lives

The debate around consumerisation and bring your own device (BYOD) breaks down into a series of opposites, such as agility versus control or security versus flexibility.

It is a controversy of the sort that the IT industry loves to use to dramatise its products. However, if software companies are true to their word, these dilemmas should not prevent any business from letting employees make the most of powerful personal devices.

Lisa Hammond believes that the line between personal and business use of devices is now so hopelessly blurred as to be a distraction. Ms Hammond is the chief executive of Centrix, a UK software house that has been wrestling with the challenge of how to create a flexible digital workspace.

Fresh from a US conference addressing mobile technology she is passionate about this question. "There were 2,000 senior people in San Diego, all facing the same problem," she says. "They were talking about separating social and work use of technology. But it is almost impossible to do this. You cannot stop people sharing information."

Ms Hammond sees digital information as "a river with thousands of tributaries". This means that trying to disentangle the different ways an employee might access data are pointless. The trick, she argues, is to create a space where work takes place under agreed rules.

Centrix sells software that constitutes a safe environment that lets individuals log in via an encrypted connection. They can then access whatever applications their work requires.

The objective, Ms Hammond says, "is to bring everything on to a single pane of glass for the end-user".

Centrix aims to create a zone that keeps working practices secure while freeing staff to employ whatever piece of equipment suits them.

This approach recognises that people are increasingly prone to keep their digital content in different locations and mix the mobile and office-based domains. Ms Hammond describes her company's product, Centrix Workspace, as a secure shell that staff can resort to without a sense of hard barriers.

The Centrix philosophy is to recognise the reality of how people dip in and out of mobile devices, cloud environments and a social media

Wrestling with change: 'You cannot stop people sharing information,' says Lisa Hammond, CEO of software house Centrix

milieu that mixes work and personal contacts.

But how can they be prevented from removing sensitive work material from the secure shell of Centrix? The software meters individual usage, flagging up an alarm if someone suddenly uploads a huge file to an external destination such as Dropbox.

The metering and analysis function is vital, says Ms Hammond, and bad behaviour by one user can rapidly become evident.

Each client for Centrix Workspace can set their own thresholds for access to – and for extraction of – data.

Extremely sensitive information can be restricted to a core of appropriate staff or special conditions of access. This brings the whole area of company policy into focus.

"Accept that you can't control people's own devices." says Ms Hammond, "and accept that there has to be a level of trust here as well. You've got to trust employees not to abuse their access and, if they do abuse it, then metering highlights the failing. You cannot lock people out of

information just because they are on a personal device. End-users will find a way around restrictions unless you have a sensible policy that creates a workspace they can get to."

At Damovo, a UK-based technology group that unifies information feeds and telecoms products, there is agreement that the argument has moved on.

"Two or three years ago, corporates wanted control of devices they were looking for a blunt instrument," says Glyn Owen, the company's portfolio manager.

But it became evident that excessive interference and control created an unwelcoming environment that deterred employees from carrying out work on the road. The fact is that a control-driven mobile device policy completely undermines any productivity gains from staff owning smartphones and tablet PCs.

Mr Owen says the new approach is much more subtle. "Companies want to control part, not all, of the device usage." He cites a common policy whereby if a mobile device is reported stolen the company retains the right to remotely delete only the segmented corporate information on that device. This approach fits the client into the mobile device management (MDM) arena where tight integration of multiple devices is the objective.

Damovo does not restrict itself to MDM operations and has relationships with diverse suppliers. It can install a Cisco programme known as Identity Services Engine (ISE). This works from the centre outwards, spotting where a user is and what device is being used and then allowing access that conforms to a policy based on the status (such as frequency of antivirus updates) of that device.

Above all, effective device management starts with accepting reality. "This mass use of mobile devices is happening so you cannot ignore it," says Mr Owen. "Employees will be using their devices either with or without the company's knowledge."

He warns every business to prepare a security policy with provisions for what Damovo calls a "jailbreak".

This lively term describes how staff can inadvertently damage security by downloading third-party software that opens up a vulnerability in the corporate security fence.

So, for example, a good policy may involve spelling out to employees exactly why downloading an exciting smartphone app while at work is not a good idea.

Hard balancing act for CIOs

Challenges ahead

Maija Palmer finds risk management and saying 'yes' are vital requirements for the role today

Running a company's computer department used to be about buying a bunch of servers, putting them behind a firewall and making sure the budget was not overspent.

In 2002, the number one concern, revealed in an annual survey of chief information officers from around the world by Gartner, the technology research company, was how to keep the costs of hardware down.

Ten years on a lot has changed. For example, it is no longer necessary to have much hardware at all to run a business.

Cloud computing enables corporate software to be hosted on a remote data centre run by another company. About 37 per cent of companies are using cloud computing, according to a survey of US, European and Asian companies last year by Advanced Micro Devices, the US chipmaker.

In addition, employees are bringing their own hardware into the office in the form of tablets and smartphones.

The question of whether a chief information officer – in the traditional sense – is needed any more also keeps cropping up from time to time.

"Consumerisation and cloud computing will potentially slim down the CIO role," says David Aron, analyst at Gartner. "But the digitisation of the world, and development of the internet, for example, will create opportunities. What consumerisation takes away, digitisation gives back," he says.

Mike Wright, head of technology at Man Group, the alternative asset management company, says: "The job is fragmenting. There is still the day-to-day, business as usual of keeping the company running, but that's a smaller part – maybe 5 per cent of the job."

Instead, CIOs are having to evolve into business strategists who can advise companies on how they can best harness all the new ways of reaching customers. These range from smartphone applications to ensuring that all the company's systems are benefitting from real-time data analytics, the capacity to use all available corporate data and resources when needed.

"There is more activity in being an agent of change, helping deliver programmes that change the current business model," says Mr Wright. "My job is to get the computer to say 'yes'."

"Before, the IT directors would secure their boundaries with firewalls, and

dictate what devices people had. Now it is much less fortress IT."

Saying "yes" has brought in a huge added set of difficulties in terms of security, however. "The more connected you are, the more risk you have," says Mr Wright. "How do you marry the need for people to have an iPhone or iPad with the need for regulators to be able to monitor everything that employees are doing on their corporate supplied devices?"

Richard Absalom, analyst at Ovum, a technology consultancy, says: "If company data are lost it is the company's responsibility, whatever device they are lost on. But in protecting the data you can't breach the employees' privacy rights."

He says CIOs now have a difficult balance between data protection rules and employment law, with the line between personal and corporate computer use becoming increasingly difficult to identify.

It has led to companies almost panic-buying ways that allow them to remotely lock down and wipe employees' mobile devices. According to Mr Absalom,

'If data are lost it is the company's responsibility, whatever device they are lost on'

companies such as Good Technology, AirWatch and Zenprise can barely keep up with demand for the corporate mobile management systems. "The role of the IT department now is really to risk manage," he says.

The strong security requirements aside, the CIO role is becoming less technical. According to Gartner, about 25 per cent of chief information officers now come from a non-technical background.

And as tacticians rather than technicians, they are having a louder say in the boardroom, and increasing the status of the job. Only about 4 per cent of chief executives were formerly chief information officers, according to a survey last year by Vanson Bourne, the research company, but this is slowly changing. Companies such as American Express and Starbucks have hired Silicon Valley entrepreneurial types and put them in charge of highly strategic parts of their businesses, where they are conceivably in line for the succession.

"We do see the CIO role becoming more of a leadership role and part of the fast-track for top-level executives, says Mr Aron.

"It used to be that an executive who was being groomed for the top would have a posting in marketing and a posting in Asia on his way. Now it might also include being CIO."

Lines blur in era of the digital native

the largest buyers of iPads, deploying 18,000 in the company.

It has also provided staff with 8,000 iPhones and is now preparing to give out Android devices including Samsung's Galaxy Note and Galaxy SIII smartphones.

In addition SAP supports 10 different CYOD devices and enables employees to choose from 50 mobile apps from its corporate application store.

Similarly, Kim Stevenson, Intel's chief information officer, has helped ensure that the semiconductor maker has embraced BYOD.

"We had provided some

segment of our population with cellphones for many years, probably since cellphones were invented," she says. "But it never was something that was available to the entire population, very consistent with how other big companies work. As the world changed, our employees all have cellphones as part of their daily life."

Next she says, employees wanted to use their handsets not just for voice calls, but to receive data. "They wanted to get their email, contacts and calendar on their device, because even our office dwellers don't really sit in our offices. We

go to conference rooms, we go to the cafeteria – we're mobile in the workplace.

"So, we had this push and then came the richness of consumer applications," she explains. Instead of a casual "I'd like to have this if you got around to it" request to the IT department, Ms Stevenson says employees began saying: "I must have this because I've got these rich applications that actually make my work life easier and more productive."

Intel calculates employees using their own devices save up to 50 minutes a day and productivity gains will be worth $177m this year.

To minimise the possibil-

ity of data loss and other risks associated with BYOD, Intel asks programme participants to sign an end user agreement that requires them to protect company data stored on the device, report it if it is lost and agree that Intel can remotely wipe the device.

Social media services such as Facebook and Twitter have already changed the lives of consumers, helping them connect with each other in new ways. Now a shift is under way in companies as leaders look to generate real value through the use of social technologies to evolve their operations.

As companies begin to adopt versions of social media collaboration and communication tools for their own use, company software suppliers have responded with a series of key strategic acquisitions designed to ensure they can meet customers' needs.

Microsoft's recent purchases of Skype and Yammer, the cloud-based social media service provider, and IBM's purchase last month of Kenexa, the recruitment specialist, are examples. They reflect an acknowledgement among enterprise software suppliers that they need to position themselves for this emerging market.

Similarly, employees have become familiar with consumer-based cloud services such as webmail, storage and streaming music, and are now demanding access to similar services on their computers at work and when they are on the road.

Hugh Thompson, a security expert, says: "As an industry, our first reaction was to block unsanctioned consumerisation.

"We need to rethink our attitude and look at the shift towards consumerisation as an opportunity to defend these applications and devices instead of maintaining the illusion of exclusion."

The Connected Business

Dictating to staff no longer works

Choices Letting workers use their own devices may seem an easy decision, but it needs planning, says *Jessica Twentyman*

Default option: many CIOs admit they have little choice but to let employees bring in technology from home
Dreamstime

At the US-based drinks firm Pabst Brewing Company, Ben Haines, the chief information officer, has announced an end to smartphones provided by the company. "I'm not going to be buying any new phones for staff and I won't have my admins worrying about phone contracts, which frankly has become a total pain for us," he says.

Such has been the success of the company's BYOD (bring your own device) policy, rolled out earlier this year, that Mr Haines is now set on making employee-owned devices the company's default approach to mobility, rather than an optional employee perk. Each new staff member will be given $200 towards the purchase of the device of their choice, and all employees will be paid a subsidy towards their monthly phone bill.

Not every company has embraced the BYOD trend so enthusiastically, but most are being forced to decide whether or not to allow employee-owned smartphones and tablets to access their enterprise networks and information, according to analysts at research company Gartner.

The company's survey of CIOs, conducted at conferences held in the US and Europe during 2012, suggests that, by 2014, 80 per cent of the global workforce will be likely to participate in a BYOD programme.

That figure seems high, but many CIOs now acknowledge that dictating to employees what mobile device they may use no longer works.

The consumerisation of IT, they say, means staff will probably protest against such a policy, and some may seek to circumvent it, in order to use their iPhone 5, for example, or their Windows tablet or Android handset at work.

Against this backdrop of employee demand, however, IT teams face the requirement to keep corporate data safe, even when it is on employee-owned devices, and even if those devices are lost or stolen.

Their best hope is probably mobile device management (MDM) software, back-end platforms that offer IT teams a way to secure, manage and monitor mobile devices, in much the same way that they have previously used Research In Motion's BlackBerry Enterprise Server (BES) to manage corporate BlackBerrys.

The difference with MDM software is that, unlike BES, these products can typically support a wide range of devices, regardless of manufacturer or mobile operating system.

Such capabilities come at a cost: in a May 2012 evaluation of 20 MDM vendors conducted by Gartner, the average price of these platforms worked out at $60 per user per year, although the firm's analysts expect that price to drop to $40. What CIOs and their teams get for that price is security and peace of mind. These products support a number of vital security functions including enforcement of passwords, remote wiping of data and devices locking, and provide a centralised audit trail for tracking logins and configuration changes.

Of the 20 MDM products that Gartner's analysts evaluated, five vendors were ranked as leaders: MobileIron, AirWatch, Fiberlink, Zenprise and Good Technology.

For example, at Pabst, Mr Haines has deployed Fiberlink's MaaS360 MDM product to support employee devices.

When his team is presented with a new device to support, he says, they can get it up and running in about 10 minutes and, because MaaS360 is a cloud-based platform, they have not needed to procure and manage hardware to host it.

Ojas Rege, vice-president of strategy at MDM company MobileIron, says deploying MDM software is perhaps the easiest challenge faced by companies implementing BYOD, because there will be a huge amount of decision-making first. "It's a question of philosophy first, policy second, and only then technology," says Mr Rege.

"You'll need to identify your basic stance as a company on BYOD. You'll need to identify eligible candidates in the workforce for BYOD. You'll need to understand the applications and data they need to access on the move: is it just email, for example, or documents, or field applications?"

They will also need to establish a cost structure, outlining how BYOD will be financed. Some companies make employees responsible for all costs related to devices they own. Others make a contribution towards initial handset cost or monthly bills.

Paying some sort of stipend, say Gartner analysts, "gives a corporation some extra control and makes the employee more beholden to the corporation for a device's use".

Graham Hann, head of technology at law firm Taylor Wessing, says the biggest hurdle, for multinational companies at least, may lie in navigating a tricky landscape of differing data protection and employment laws to implement BYOD.

Even in Europe, "a confusing patchwork of out-of-date national laws and lack of harmonisation make it very difficult for businesses to implement pan-European BYOD policies".

Mr Hann's view is echoed by Quentyn Taylor, Europe, Middle East and Africa director of security, governance and risk at electronics company Canon. "When someone tells me their company has a multinational BYOD policy, my first question to them is 'How?' They'll often admit that, in certain countries, it simply wasn't possible to enforce it."

'It's a question of philosophy first, policy second, and only then, technology'

Shell 'Consumerisation will force more change than any other trend'

The advice to other IT leaders from Jay Crotts, vice-president of IT services and operations at Royal Dutch Shell, is: "Don't ignore the bring your own device (BYOD) trend. Embrace it."

Mr Crotts says: "Consumerisation will force more [corporate] change than any other trend in the coming few years, and employees will use their own devices in the workplace, whether authorised or not."

Security risks aside, he says: "There are significant benefits for both the business and employees to be gained by supporting BYOD – increased flexibility, choice and a more engaged workforce."

In keeping with that philosophy, since July this year Shell has made BYOD available to users right across the company – including its contractors and employees in joint ventures – following its six-month rollout of a mobile device management (MDM) software-as-a-service (SaaS) platform from AirWatch.

The implementation was preceded by a pilot project, in which corporate email was extended to around 2,000 users to test demand.

"It proved extremely popular, and quickly became oversubscribed, with a waiting list," says Mr Crotts.
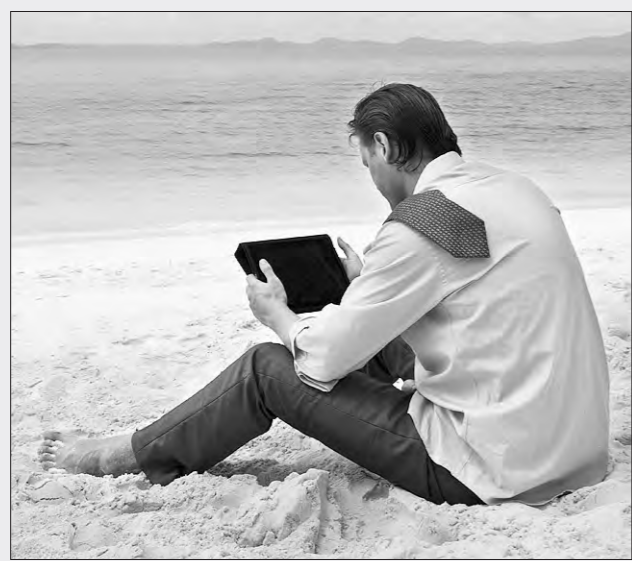
Today, Shell's AirWatch MDM platform supports some 6,000 individual devices. The company supports any employee-owned Apple and Android phones, and tablets that meet its minimum operating system requirements.

2,000
Users in Shell's pilot corporate email programme

Meanwhile, Mr Crotts and his team are keeping an eye on the market: "We'll aim to support devices that are winning in the consumer market and meet Shell's minimum security standards." For example, it is likely that they will support Windows Phone 8 when it is released later this year.

Shell's BYOD model means that employees bring to work devices they have purchased themselves and they cover their own mobile bills.

With many consumer rate plans now offering "all you can eat" data plans, as well as the ready availability of WiFi, there should be no increase in costs for using the service. That said, the company is improving in-office WiFi, so employee mobile devices automatically connect to this, rather than their mobile network – a benefit that is particularly attractive to employees travelling between Shell offices, who might otherwise incur hefty roaming charges.

The introduction of BYOD represented the first manifestation of consumerisation at Shell, says Mr Crotts, so beyond the need to introduce an MDM platform, the project required significant non-technical work with other stakeholders in the business to ensure the company was ready for a new way of working. These included representatives from the HR, legal and tax departments, among others.

"We also engaged with our employees to get their input on what they would like to see in place, and also ensured we were engaged with our employee staff councils, to address any concerns – such as what a new 'always on' way of working might mean for staff," he adds.

There are some restrictions to Shell's BYOD policy, based on geographic challenges, and some legal and regulatory constraints. But, says Mr Crotts: "We continue to review the status [in these territories] and will enable BYOD when and where we can."
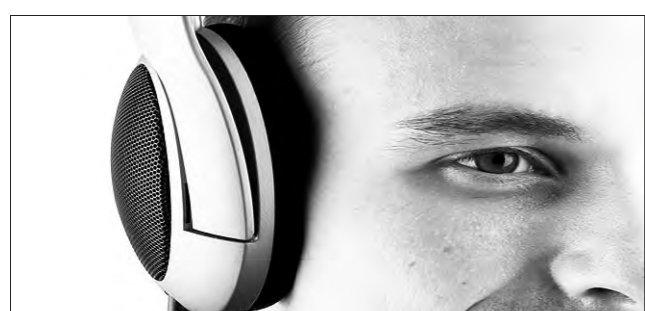
Jessica Twentyman

Life's a device: consumerisation will force change *Dreamstime*

On FT.com »

Podcast
Market forces
Gartner analyst David Willis, Eversheds' CIO Paul Caris, and Hamilton Bradshaw's Daniel Steeves talk about the consumerisation of IT
http://podcast.ft.com

Contributors »

Paul Taylor
The Connected Business Editor

Jane Bird
Jessica Twentyman
Michael Dempsey
Stephen Pritchard
FT Contributors

Richard Gibson
David Scholefield
Elizabeth Durno
Sub-editors

Adam Jezard
Commissioning Editor

Steven Bird
Chris Tosic
Designers

Andy Mears
Picture Editor

The Connected Business

Watch this space: advisers say that businesses will do themselves few favours if they cut staff off from using consumer tools such as Twitter, Facebook or LinkedIn   PA

Pay attention to who is using social media

Networking sites Weight of numbers – and the influence such services have – make it impossible to ignore them, says *Stephen Pritchard*

Facebook claimed 995m active users, as of June 2012. Twitter has about 500m users, and YouTube, owned by Google, says it has 800m visitors each month, watching 4bn hours of video. Renren, a Chinese social media site, claims 157m active accounts.

For marketing purposes alone, social media sites – designed for consumers to stay in touch with friends, publish photographs or share information about hobbies and interests – are an attractive platform.

And they are also economical: a standard Facebook page is free, even to the largest businesses.

Companies are also finding that social media services can provide more than just an alternative to a static web page. Social media, through services such as Twitter's firehose – its full data feed – provide a rich source of information to companies about how their brands or products are perceived.

Handled correctly, social media can serve a valuable customer services function, and also a way to create and follow groups of customers, suppliers or "influencers" who might be useful to the business.

LinkedIn, which styles itself as a business social network, is also a useful recruiting tool.

But it is the way in which social media services allow businesses to interact with their customers, and especially harder to reach groups such as young adults, that appeals to marketers.

Mark McDonald, head of executive programmes research at Gartner, the research company, says: "The economy we are now in places a higher value on participation, and consumers want to connect with each other and demonstrate their knowledge. That changes their association with the product, or the brand."

Used in the right way, Mr McDonald says, social media can persuade customers to become unpaid advocates for a brand.

And research shows that consumers trust and value recommendations on social media more than they do conventional advertising.

At the same time, simply spending money on social media does not always deliver the right results.

Ford, for example, has run successful social media campaigns around car launches such as the latest model Fiesta. Its rival General Motors, though, very publicly pulled advertising worth $10m from Facebook, saying they had not seen a sufficient return on their investment.

Other smaller-scale projects sometimes work better. British Airways, for example, began its recent "Aviators" brand advertising campaign, not in the cinemas, but on Facebook. Sony's broadcast division has also run a series of online chats for filmmakers about its latest video cameras on the same site.

One advantage of social media over conventional advertising is flexibility. However, Nathan Sage, a social intelligence expert at PA Consulting Group suggests that very flexibility can also be social media's weakness.

"You can spend quite a lot of time having a conversation about whether social media is internally or externally focused, whether it is PR or marketing or customer service.

He adds: "There is a disconnect between brands and their understanding of what social is."

There have been faux pas, such as interns tweeting office gossip to thousands of followers, or companies seriously misjudging the mood of their customers.

> Even tightly controlled industries such as retail banking can use Twitter, if they do so with care

McLaren Formula One driver Lewis Hamilton is just one celebrity to have fallen foul of Twitter's ease of use, for sharing a telemetry sheet showing data of car set-up information that could have been useful to rival teams.

Businesses also have to pay more attention to who uses their social media tools, especially in regulated industries such as financial services or legal services.

"We've used social media a lot," says Paul Caris, chief information officer at Eversheds, the law firm. "We've used Twitter for some of our vertical specialisms, such as in our food practice, and our partners in those areas have created small but very active communities.

"Obviously, Twitter is not a brilliant area for collaboration, as it is basically a broadcast medium. But we've introduced policies to ensure that the way we communicate over social media platforms is consistent and that we all understand that what you put on there is public facing.

"And we do also take activity that starts on Twitter offline, either to LinkedIn, or to a private collaboration area, owned by Eversheds."

David Hodgkinson, an adviser on customer and channel management at KPMG, the professional services firm, agrees that even tightly controlled industries such as retail banking can use Twitter, if they do so with care.

"It is a way of capturing customer dissatisfaction that might not be picked up through person-to-person contact," Mr Hodgkinson says.

PA Consulting's Mr Sage says dealing with complaints has to be done correctly: social media users wield enormous collective power.

"Organisations have to have the ability to deal with that. If they don't react, it can damage the brand.

But there is a further, important element to how organisations use social media. Jason Breed, social media practice lead at Accenture, the management consultants, argues that although business-specific tools such as Yammer – which provides internal social networks – businesses will do themselves few favours if they cut staff off from consumer tools such as Twitter, Facebook or LinkedIn.

"Used correctly, social media will help companies to recruit and retain the best employees," says Mr Breed. "For some time, that's given the best companies an edge over those that ask candidates to fax a résumé. No cool kid at college wants to do that."

Conferencing makes way for video chat

Online meetings

Web discussions are moving out of fixed spaces and becoming more common, says *Stephen Pritchard*

Video calling has a long history – at least, in science fiction. Fritz Lang's 1927 film, *Metropolis*, featured an early impression of a video phone and was made just a year after John Logie Baird's first successful TV transmission.

But if the notion of video calls remained a staple of films and TV, the technology itself lagged behind. Industry statistics suggest one in four US adults have tried video calls but there is a long way to go.

Technologies such as Apple's FaceTime, 3G mobile video calls and, especially, Skype, have popularised the idea of video, but most people still seem to prefer voice calling.

However, with easier-to-use equipment and better bandwidth connections, this is starting to change.

User-friendly options, such as being able to use Apple's FaceTime technology over cellular networks, and tablets and laptop PCs with video cameras built in, are attracting new users.

Barbara Nelson, chief technology officer at iPass, a network services provider for businesses. says: "We've seen a significant increase in people using video. Two-thirds are now using video conferencing or video chat, more than a year ago.

"Before, video conferencing was very scheduled, something that was conducive to two or three people talking to each other, but there was not the flexibility the mobile workforce was looking for. They don't want to drive into the office and book a [video conference] room. So consumer solutions such as Skype provide more flexibility."

The trend, she says, is away from conferencing in a room towards simpler, more frequent, ad hoc communications. This is driven by consumer rather than company services, such as Skype, and unified communications (UC) software – which offers real-time communications such as instant messaging, with support for video. There are also browser-based services such as Google+ Hangouts.

"The nomenclature is changing from video conferencing to video chat," Ms Nelson says.

In business, the pressures on companies to cut travel costs and support flexible working, underpin the

> Consumer services have advantages beyond low cost

deployment of fixed-video and "telepresence" systems – which allow staff to feel as if they are in the office.

But the idea of a single set-up – with the ease of use and compatibility of a voice call, on any device from any manufacturer – remains as fictional as Lang's vision.

Companies are also investing in "gateways", usually hardware, that connects consumer video calls from services such as Skype or 3G and 4G mobile networks to their room-based video conferencing systems.

Mr Mason cautions quality and reliability issues mean these systems remain something of a trade off.

But there is another factor limiting the take up of either desktop video phones or video calling from smartphones or laptops: bandwidth. IT managers worry that unfettered use of video

Screen test: video conferencing is now more ad hoc   Cisco

these one-off situations, ease of use trumps quality."

Jason Kane, IT operations manager at BuroHappold, an engineering consultancy, says: "We use Skype for recruitment and where the client or external party requires it. We use 3G with our Polycom system on an ad hoc basis, where an alternative network is not available or when we are on the move."

The company is looking at integrating video calls from devices such as tablets. This is typical of how companies use the technology. Analysts such as Mr Mason say the market is less about a single technology or service, but a range of tools for different jobs.

"For a three-hour to four-hour meeting, you need high-quality video and sound, and that lends itself to the traditional enterprise conference technology," he says. "Employees on the road are also likely to use consumer technology."

calling between staff will clog up networks and slow down access to other business-critical applications.

Mark Lewis, vice-president for enterprise solutions at Interoute, a networking services provider, says: "Video has been a push market [where products are marketed rather than consumers demand them], a luxury purchased for C-level executives, but clients are now saying this needs to be controlled.

"But services such as Skype have led the way for consumers, by using a camera and microphone in the laptop. Samsung has TVs with Skype. The consumer push makes [use of this type of service] unavoidable."

Consumer services have advantages beyond low cost. Some companies that had problems with desktop video phones found consumer technology – designed for lower-speed broadband or WiFi networks – performs better.

The disadvantage is consumer technologies lack the security measures and controls of business-grade software. "We tell enterprise customers to 'anchor and extend': start with highest quality – or the most demanding users and use that as the anchor," says Mr Mason. "But don't be afraid of having tiers: managed services for execs and consumer or UC services lower down is perfectly acceptable, as long as you understand the impact on network resources."

Internal systems offer a better way of managing messages

Control Businesses may need to be in charge, says *Michael Dempsey*

When Iain Elliott founded Canford Audio in 1976 he was determined to retain a collegiate atmosphere, even as the manufacturer and distributor of broadcasting equipment expanded and developed an international customer base.

But Canford's headquarters in the North East of England is bisected by a road, with administration on one side of the carriageway and manufacturing and design on the other side of the road.

With another UK site at the far end of the country, and with offices in France and Dubai, Canford struggled to maintain a sense of common identity.

Technology could provide part of the answer, but Dave Holloway, marketing director at the company, had no illusions about its limitations. "We could share information across the internet, but that tended to result in something I hate with a passion – a long thread of emails!"

It was Canford's technology partner, Manchester IT integrator m-hence that suggested that an internal social media product might open up new avenues of co-operation.

Social Business, as m-hence calls this product, runs in the background on users' PCs or other devices. The user can join a common company group and offer their experience and advice when they spot a relevant subject under discussion.

But why could Canford not use established collaborative software tools from big names such as IBM or Microsoft to connect its staff?

Mr Holloway notes that ease of use and privacy are what mark Social Business out. "To be honest, I haven't come across those other products, which indicates to me they are not as easy to use as they could be. And this is internal, it sits entirely within our network. It personalises the company."

He regards popular social media tools with suspicion. "Facebook is a dangerous weapon. We have a strict policy about what staff can say relating to the company when they are on Facebook."

The Social Business environment is one where Canford sets the rules and everything that passes between the company's 170 staff is regarded as company confidential.

"We are safe in the knowledge that this information never leaves our network," says Mr Holloway.

The internal social media community has uncovered hidden talents at Canford. "There's a lot of skill sharing going on," Mr Holloway observes. "People share knowledge on minor PC problems so they don't have to bother the IT department with their questions."

Mark Thompson, chief executive at m-hence, Mark Thompson says Social Business emerged from the company's own needs. "We grew by acquiring businesses. We found we had eight offices and each one had a different culture. Social Business gave us the ability to bring all these people into one place and tell them what was going on.

"The product name is misleading. What is relevant is not social media, but engagement. It's all about communicating across the organisation."

He does warn prospective users that this kind of application produces a frank picture, and they should be prepared for the naked truth. "It gives you a real raw view of what's going on in your business. You may not like this."

This degree of honesty is not something anyone wants to risk sharing with outside eyes.

So, although Social Business could be deployed via the cloud, Mr Thompson says there is no appetite for this. "People are concerned about privacy. They get nervous about not having complete control, and all of our users want to keep it hosted on their own system."

But this truthful picture comes at a cost-effective price, £3.50 per user per month for m-hance's existing integration clients.

Daniel Kraft, chief executive of Denver-based NewsGator, shares the opinion that social media tools for business are all about the ability to engage employees and get them opening up to each other. He talks about "the social workplace" but stresses the workplace component is the crucial element in how NewsGator's clients, including Barclays Bank and JPMorgan Chase,

use its social media tool.

"Social is a big competitive advantage," Mr Kraft says. "It gives you the ability to share critical and confidential information with colleagues."

Regulatory requirements ensure that these exchanges are recorded in the same way as emails or other internal feeds. This also reflects the fact that internal social exchanges only work when set in a genuine business context, including the same rules and regulations that apply to every other aspect of the organisation's work.

Kelly Dempski, research and development director at business adviser Accenture's Silicon Valley technology lab, has been studying how social media is spreading, and he warns against getting too fixated by a vogue term.

"The word social is like innovation, it means whatever people want it to mean. I don't get too caught up in definitions. People use these internet services in different ways, what matters is the influence of social media."

Mr Dempski reckons there are some 200 social media tools jostling for the attention of tech-savvy customers. With such a bewildering choice, what is a business to do? He says: "You should stop and ask yourself what it is that you want to do. What should the social media product do for your business?"

Getting everyone to reveal their thoughts means confronting the beating heart of your company, and also learning a lot about its true purpose.

Daniel Kraft: 'Social gives you the ability to share critical and confidential information with colleagues'