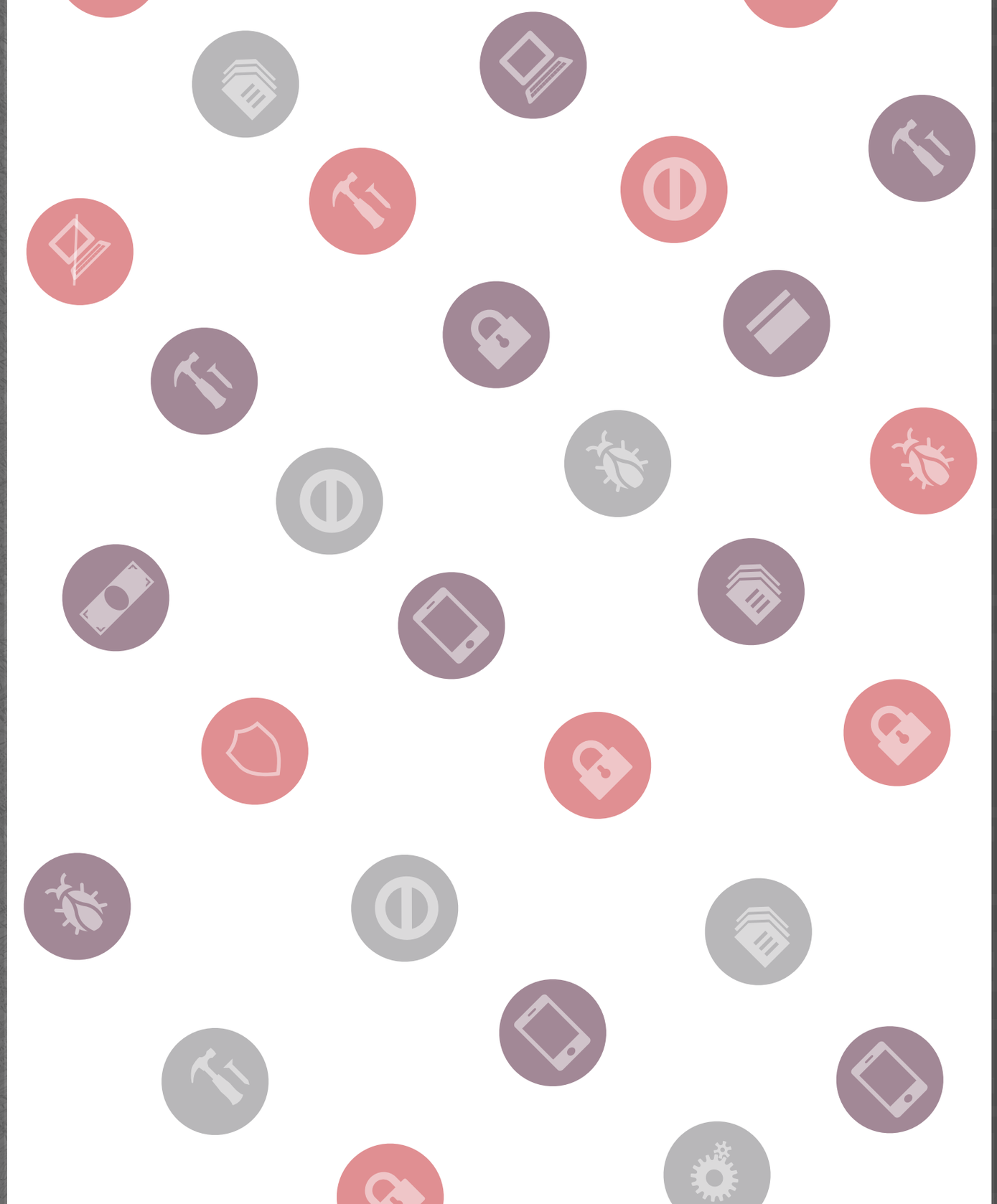
FUJITSU

in association with IDG CONNECT

# Does BYOD Hold the Keys to Building a Better, Happier Workforce?

A White Paper on the Bring Your Own Device phenomenon, based on research conducted by IDG Connect on behalf of Fujitsu





IDG Connect is the demand generation division of International Data Group (IDG), the world's largest technology media company. Established in 2006, it utilises access to 38 million business decision makers' details to unite technology marketers with relevant targets from 137 countries around the world. Committed to engaging a disparate global IT audience with truly localised messaging, IDG Connect also publishes market specific thought leadership papers on behalf of its clients, and produces research for B2B marketers worldwide.

FUJITSU

in association with IDG CONNECT

# Introduction

# BYOD Works: Now You Have to Deal With it



The Bring Your Own Device (BYOD) phenomenon has been much discussed over recent years as employees delighted by consumer technology experiences (and sometimes underwhelmed by the workplace equivalents) have stepped up their use of favoured products and services in their professional lives.

That in turn has seen a flood of PCs, Macs, tablets, smartphones, software and web-based services enter offices and anywhere else work is done. To better understand what's happening under the BYOD umbrella, IDG Connect, on behalf of Fujitsu, researched 250 IT decision makers across the US, Middle East, UK, Germany, France and Sweden. About a third were at companies with 100 to 999 staff, a third had 1000 to 4,999 staff and a third had more than 5,000 staff.

In particular, we sought to understand how enterprises were dealing with BYOD, the benefits they were seeing and the challenges they were facing.

The findings were remarkable. First of all, we shouldn't think of BYOD as remotely futuristic or 'bleeding edge' but rather as a phenomenon that is a fixed part of the working landscape.

Some level of usage of employee-owned devices exists at 99% of the companies surveyed. As for the backdrop to BYOD, when asked a broad question about essential technology goals today at the organizations surveyed, the answers proved to be broad, with an almost equal number of answers for protecting corporate assets and data, developing flexibility of IT device choices, meeting new rules for data protection and security, improving collaboration/communications processes and modernising ICT to attract and/or retain talented people.

BYOD is a good match for some of these goals because - and this is perhaps the most striking discovery of the research - staff feel markedly more satisfied and productive when they can select their own devices.

And, despite what sceptics might think, relatively few of those surveyed see the chance to cut costs as being among the more appealing aspects of instituting a BYOD strategy.

These findings should be noted by anybody who doubts the potential benefits of letting users have more control over choice of ICT tools.

Security and data governance are major issues, however. Accidental disclosure of company information is the number-one concern and many fear a growing threat from malware when BYOD takes effect.

To secure working practices, password protection is the dominant first point of control with VPNs and encryption also popular. But, in some countries more than others, a 'soft' approach is also being used with written codes of conduct on appropriate usage being introduced.

The ways in which companies deploy and manage BYOD are also interesting. Pre-approving devices where the process is a two-way interaction between user and organization is preferred and this is twice as popular as a laissez-faire approach where the end-user calls the shots.

There is also significant variation in payment models. In some cases, the organization pays for the device, in some there's a subsidy provided and in others the employee is responsible for payment.

In what may be a sign of maturity and an attempt to regain control, employees are increasingly not being asked to pay for their devices.

The research also unveiled some fascinating side notes.

The devices users are asking for indicate the way computer architectures and preferences are changing. While Windows has been the dominant client-side platform for 25 years, more of the devices being brought in via BYOD are Apple or Android-based.

This reflects the fact that Microsoft is still aspiring to the same success in the tablet or smartphone spaces as it has enjoyed on the PC. In desktops and laptops, Apple and, to a lesser extent, Google offer alternatives.

Finally, not all the regions are moving at the same pace or doing things the same way. The US appears to be most advanced in recognizing the value of BYOD and the Middle East is the least receptive.

The loud message from the research is clear: there are big advantages to BYOD and staff want it. The challenge is to manage this trend so productivity and creativity are enabled — but not at the cost of reduced security or governance.

FUJITSU

in association with IDG CONNECT

## Lots of Goals

# IT's Balancing Act: Security With Innovation



Organizations we interviewed are keeping lots of plates spinning when it comes to IT objectives today.

Not one answer stood out but, taken together, keeping data safe and meeting laws and other rules covering data is front of mind for many.

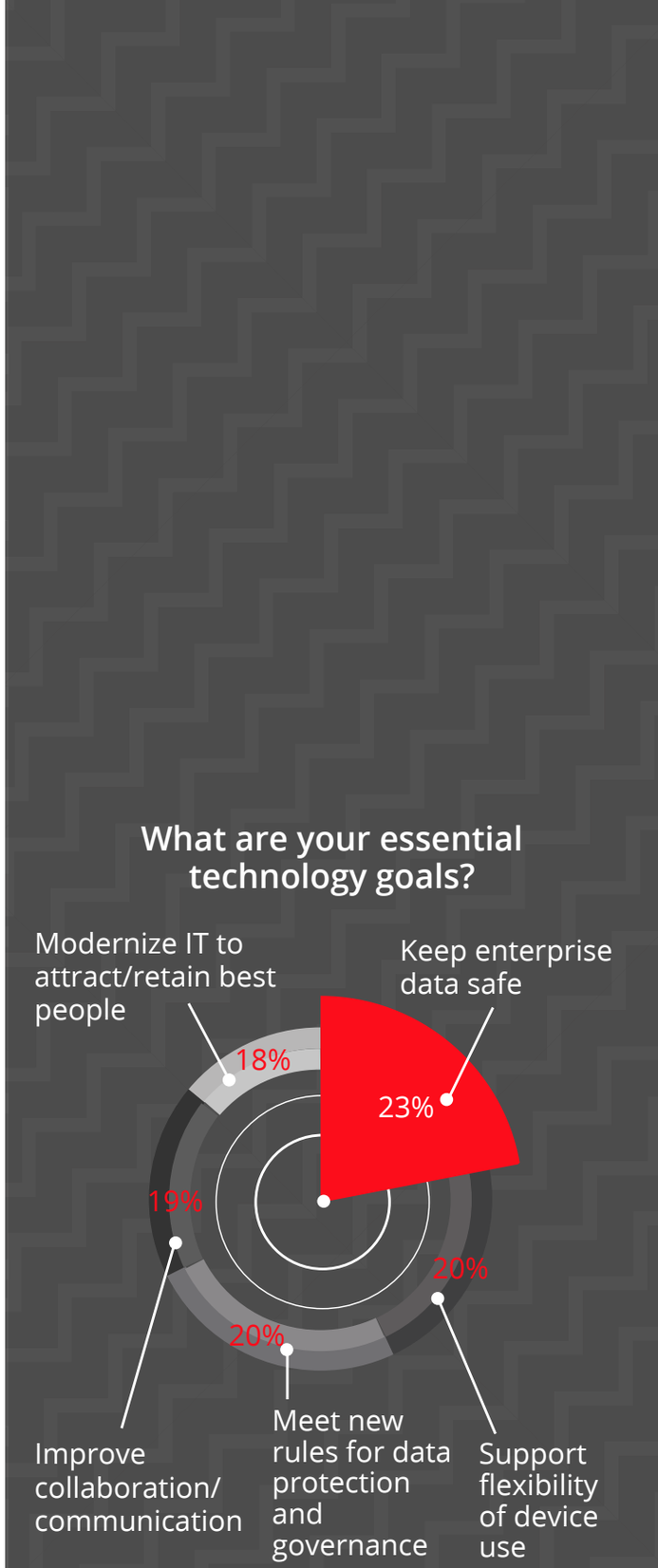
The traditional balance between 'keeping the lights on' by maintaining operations and doing more innovative creative work is observed here with the need for security and governance balanced by a desire to improve collaborative processes and create an IT environment that is modern and capable of playing a role in attracting and keeping top talent.

Effectively, CIOs today need a two-track focus.

On the one hand they must strictly observe the various laws, rules and codes that apply to them, especially in the light of the media attention trained on data breaches, loss of individual privacy and post-Enron corporate malfeasance.

On the other, they need to modernize processes and systems to compete in a world where companies rise and fall faster than ever.

Improvements to collaboration and communications are highly prized as ways to generate ideas and take advantage of a globalizing economy. It's also critical that organizations improve the attractiveness of their brands by having up-to-date ICT tools and processes that attract the brightest and best people to join and stay.



FUJITSU

in association with IDG CONNECT

# BYOD Everywhere

# BYOD is Saturating Organizations Today



There's no going back when it comes to non-corporate devices entering the workplace. Windows remains dominant in laptops but, otherwise, very often it's Apple or Android devices (almost 7 times out of 10) that are entering the enterprise in this way.

Just 1% of those polled said none of the above could be brought into the workplace.

Of course, not all these organizations will have a rigorous, formal approach to BYOD but, whether it's organically evolved or pre-planned, the trend of bringing in user-selected or user-owned devices appears to be in full flow.

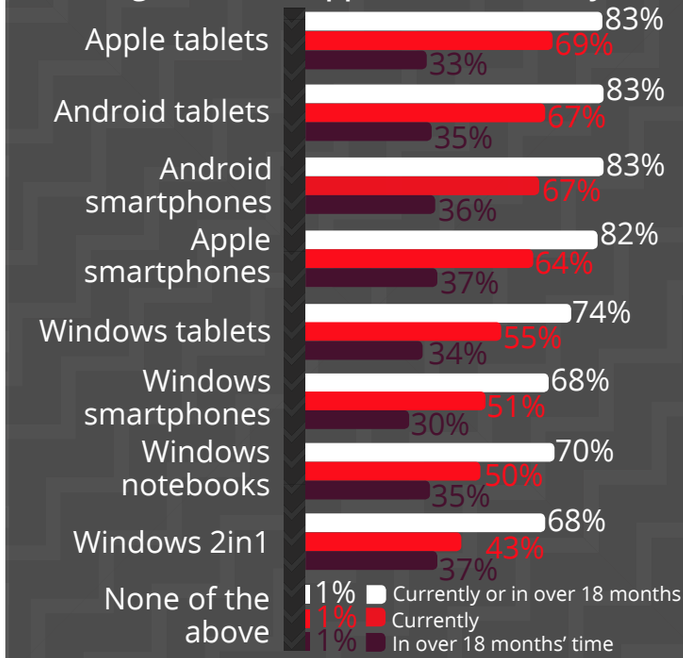
And it's not stopping. When asked about future plans, the overwhelming verdict was that BYOD levels would rise over the next 18 months.

Although BYOD is sometimes depicted as a 'Wild West' or anarchic scenario, two-thirds of those polled said schemes were corporate-approved. However, and unsurprisingly, smaller companies tend to have fewer formal controls over BYOD schemes than their larger counterparts.

For IT departments who once enjoyed 'command and control' dominance of IT equipment, this new world will require a cultural change. CIOs might need to adopt a more 'softly, softly' approach that sees them working more closely with users to understand their needs. It is also likely to stretch capabilities. Where once, domain knowledge of the 'Wintel' world of PCs running Windows would suffice, IT admins in future will need to expand their interests and have at least a working knowledge of other computing platforms in order to control and secure the influx of new hardware and software entering their organizations. However, Microsoft remains the default choice for most office tasks and that is unlikely to change in the near future.

As is often the case, the US is leading the way in this trend. The Middle East is a relative laggard in this sense.

**Which of the following non-corporate mobile devices are employees currently bringing into work where the organization supports connectivity?**



FUJITSU

in association with IDG CONNECT

## Pay to Play?

# BYOD Procurement is a Mixed Bag



The way organizations are operating BYOD schemes varies markedly, with three main models emerging. In 35% of cases the employer pays outright, in 29% of cases the employee pays for and owns the device, and in about a quarter of cases there is some form of subsidy for a pre-selected range of tools.

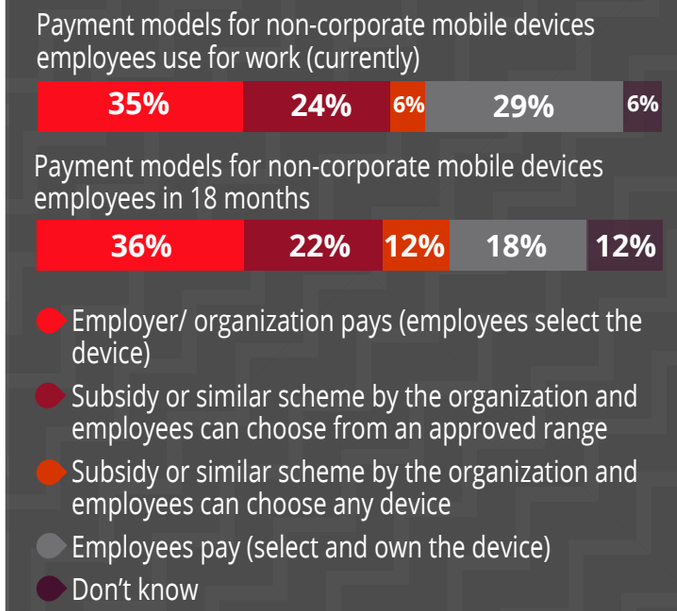
However, things are changing. In 18 months' time, respondents said that the least popular option (where an employee chooses the device and the employer subsidizes that selection) will be far more popular, moving from 6% today to 12% later.

This is most likely because BYOD will mature and firms will seek improved governance without losing the advantages of such schemes.

There are also notable differences across countries and regions. For example, in Sweden, 67% run schemes under which the employer pays outright.

This variability is the sign of a market that is still youthful. As BYOD matures and as best practices emerge, it is likely that payment and procurement approaches will coalesce and the default model may become corporate procurement and user selection. In this way, the CFO and the business will gain good visibility into costs without sacrificing the benefits achieved by such schemes.

**Which best describes the current payment and selection of non-corporate mobile devices that employees bring into work, and that the organization supports (rather than provides)?**



FUJITSU

in association with IDG CONNECT

## Controls

# Controlling Access: More Than Passwords



While passwords are unsurprisingly the most commonly cited form of protection, virtual private networks and encryption are being used in almost half of cases while a formal mobile device management (MDM) suite is being used by a third of those polled.

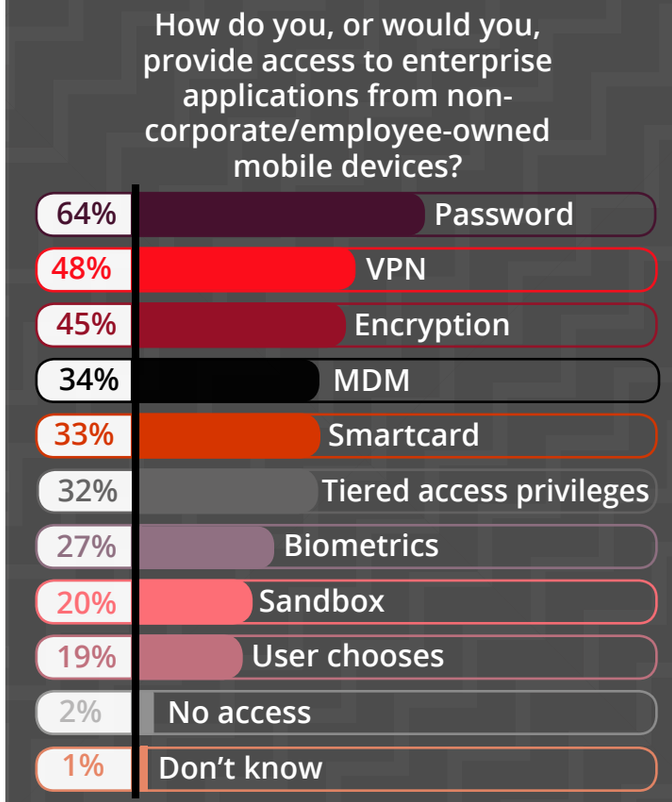
MDM is a field to watch. By providing tools to quarantine systems and by offering services such as remote wiping or the ability to find lost systems, MDM suites are rapidly winning favor among CIOs.

In an age of paranoia about data loss, they are likely to become an essential part of the IT stack in enterprises.

Biometrics is another area that is worth watching as fingerprint, retina and other identification criteria provide another tier for protection.

Also 'security by obscurity' might have a big role to play, even if it's just a case of making sure users only have access to data and systems they need to access.

Clearly, firms need to ensure that the freedom of ubiquitous access afforded by non-corporate mobile devices does not lead to compromises and, just as obviously a wide range of defense tactics are being put in place to control who gets access to what. This is especially the case among larger organizations with the most resources... and, perhaps, the most to fear.



FUJITSU

in association with IDG CONNECT

## Risks

# Risk Management Steps Include 'Soft' Approaches



While much media discussion focuses on technological approaches to ensuring security in the BYOD world, over half of those surveyed said they have, or will have, an employee code of conduct.

Another 'soft' approach, user training, is also popular.

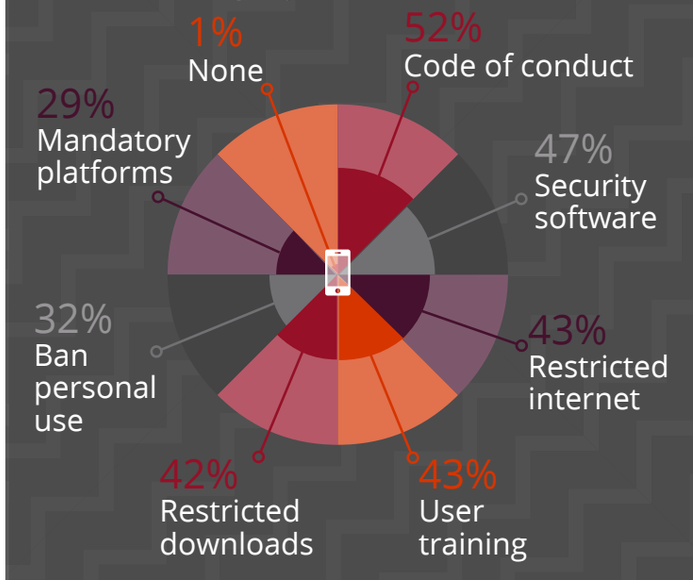
This is analogous to the early days of corporate email and internet usage and provides not only a way to encourage users to follow guidelines but also some form of defence if data does go missing.

As with email and the internet, it is likely that a standard approach will arise that outlines the basics of what users should do to protect against data loss or security threats.

However, trust and guidance only go so far in many cases and restrictions on internet usage and downloading apps are common. Also, security programs designed to find lost devices and wipe data are in place with half of respondents. Specifying brands and operating systems is another approach by which IT seeks to maintain control. In the Middle East, tougher approaches are more common than elsewhere.

Fairly draconian policies are also in place with many: almost a third say they ban use of devices for personal purposes. However, these harder lines of action are unlikely to be popular with users and could lead to a backlash as more users demand work-life balance from their employers.

**Which of these steps do you/ would you take to reduce or control risk from non-corporate mobile devices brought in and used by employees for work?**



in association with IDG CONNECT

## Tasks

# Users Want BYOD Across The Board



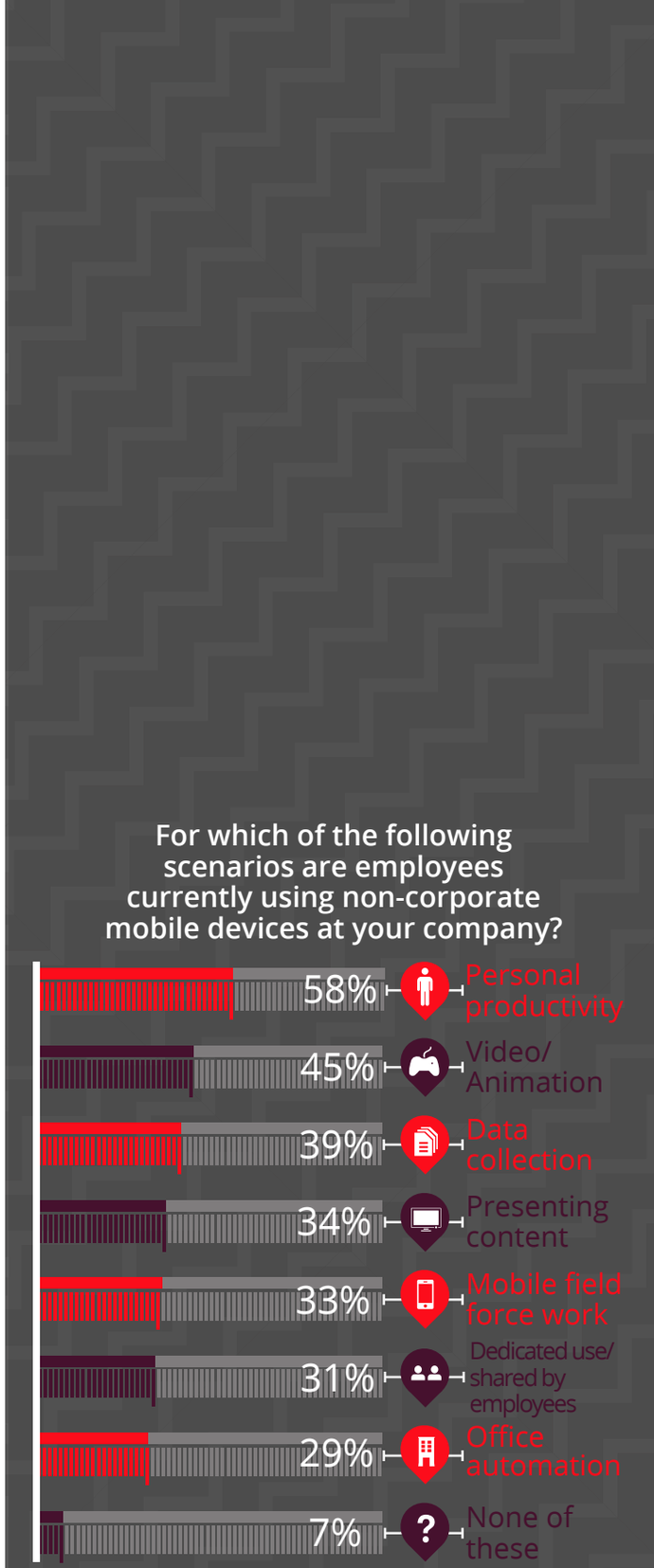
The short answer to how BYOD is being used is 'to get the job done'. In other words these devices are being used for the full gamut of productivity tasks employees are asked to do.

Video and animation, for example in training or conferencing, are clearly a good fit with tablets as these devices are easy to share, have good screens and are lightweight and highly portable. Similarly, these highly mobile systems are excellent for collecting information such as inventory checklists and for staff working in the field. Ruggedized and semi-ruggedized tablets would be an obvious development trend, based on this usage model.

Office automation might appear less applicable as tablets and smartphones are often seen as a bad fit for office productivity

tasks like word processing, presentations, database work or spreadsheets. However, this may change as vendors target business audiences more specifically and new apps are being delivered to improve the experience of tasks such as word processing. Also, Microsoft is clearly stepping up its efforts with tablets and optimized software for these devices.

One interesting data point is that shared usage is common. This suggests that users might be dipping in and out of using devices that are pooled, in the same way that in the early days of mobile computing there would be an office laptop available for workers traveling.



in association with IDG CONNECT

## Benefits

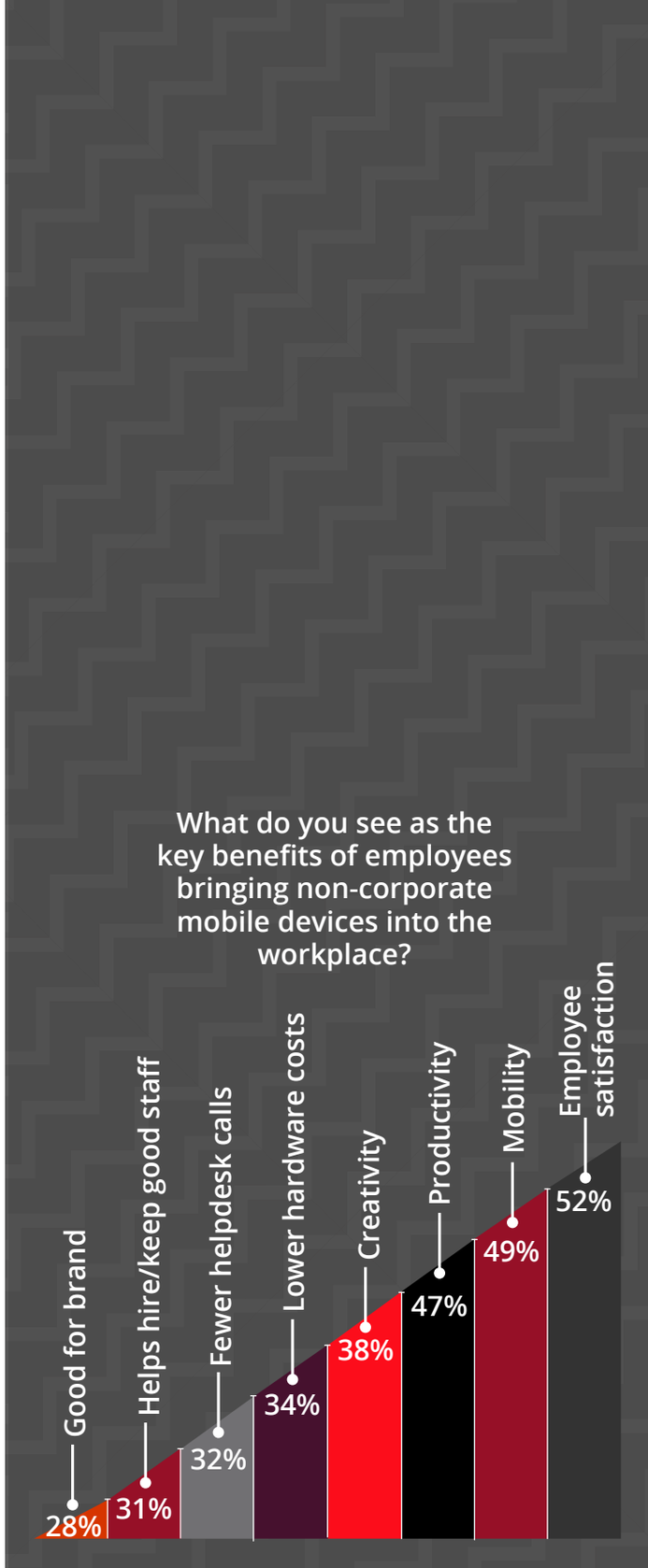
# Big Benefits and Bonuses Observed



Over half of those polled said they thought staff were happier in their work with a BYOD approach. For many, BYOD also means the ability to work from anywhere and be more productive and innovative. This is highly significant given the intense competition in the knowledge economy for the smartest people. Hiring and retaining staff will clearly be boosted when staff are satisfied in their work and granting good tools and user choice is an effective way to achieve this. But also business unit managers (for example, sales directors) appreciate the benefits of more flexible work styles, as it directly translates into increased workforce productivity.

There are also some welcome surprises. BYOD schemes might actually translate into lower hardware costs but also a lighter burden for service desks.

And there are softer advantages to BYOD as well as making it easier for HR to hire good people. A BYOD policy sends out the message that the company is modern in its outlook and presents a strong brand image for the company.



FUJITSU

in association with IDG CONNECT

## Productivity

# BYOD Means More Productive People



This is a powerful finding, perhaps the most powerful of all discovered in this research: IT decision-makers in general feel strongly that a BYOD scheme translates into more productive people.

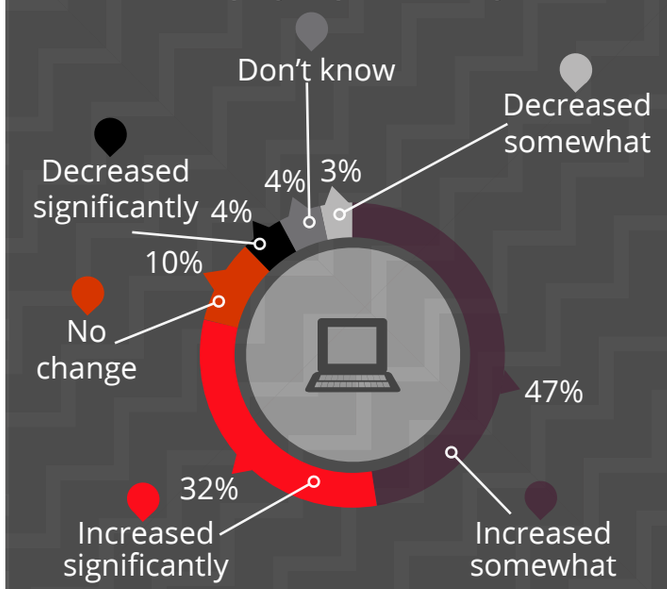
Even allowing for a little 'boosterism' this is a finding that should make the laggards sit up and take notice. And, taken in tandem with the previous page, it represents a potent argument for giving employees more largesse and control in their choice of tools.

It probably shouldn't be too surprising either. The employee who is happy with his or her tools is likely to make better use of them and the company benefits from the resulting uptick in work completed.

Even the small numbers who detect declining productivity in the BYOD era might

be negatively prejudiced as there are bound to be some who fear and dislike the more liberal model of IT deployment. But almost four in five see an increase in productivity and that alone makes for a very strong argument in favor of the BYOD model.

**And from a business perspective, what is the impact of personal devices on employee productivity?**



FUJITSU

in association with IDG CONNECT

## Secured Fears

# Security Tops BYOD Concerns



It's not surprising that in these days of constant threats, security is top of mind among respondents, alongside fears of virus proliferation and susceptibility to malware. Any significant change in the way IT is deployed is bound to spark concerns and it's understandable that IT leaders will have fears about users behaving irresponsibly then bringing malware back into the office. But the tools are available to control user activity and curb risks in the BYOD world; already, many organizations have a 'quarantine' system whereby systems are security-checked in isolation before they access the corporate network.

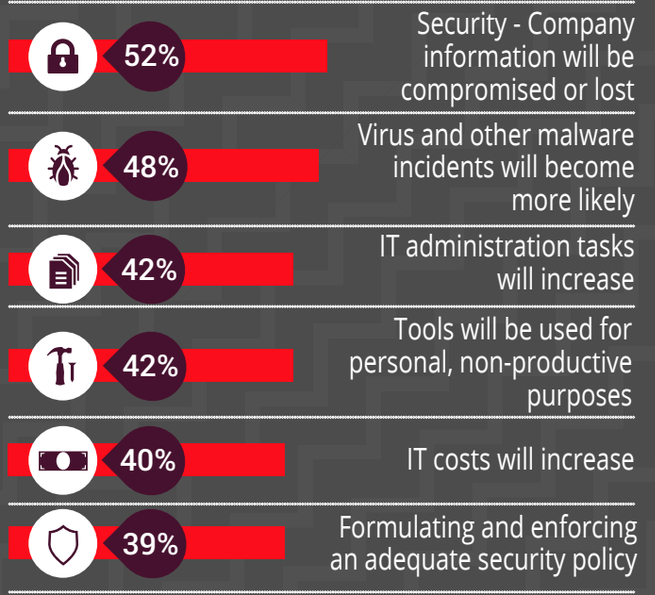
Given the obvious upside of the BYOD model, IT's job will be to deal with the new risks in a sensible fashion through usage policies, training, retraining and technological controls.

Worries of escalating admin and costs and the need for revised security policies are also common but, with improvements to best practices, these should be mitigated. The notion that users will use their shiny new tools for personal usage and therefore enlarge the corporate risk profile might appear to be something of a 'dinosaur' concern but, certainly, controls and policies need to be in place.

Some respondents note that highly regulated industries make BYOD inappropriate. However, outside the most sensitive areas (defence, for example) these will form a small minority.

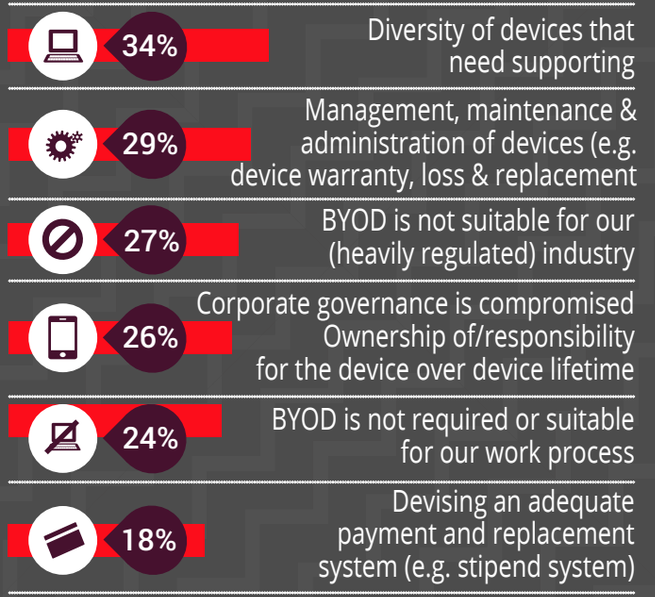
**What are your concerns over employees bringing non-corporate mobile computing devices into the workplace?**

1-6 of top 12 concerns | 7-12




**What are your concerns over employees bringing non-corporate mobile computing devices into the workplace?**

7-12 of top 12 concerns | 1-6



in association with IDG CONNECT

## Challenges

# BYOD has an Impact on IT Security and Admin Challenges



The waves of governance and 'bad news' stories in the media, as well as the very real threat landscape, all point to companies having to carry out their due diligence over security. In total, 83% said there had been an increase in challenges to IT security. However, just one in three say their security challenges have grown 'significantly'.

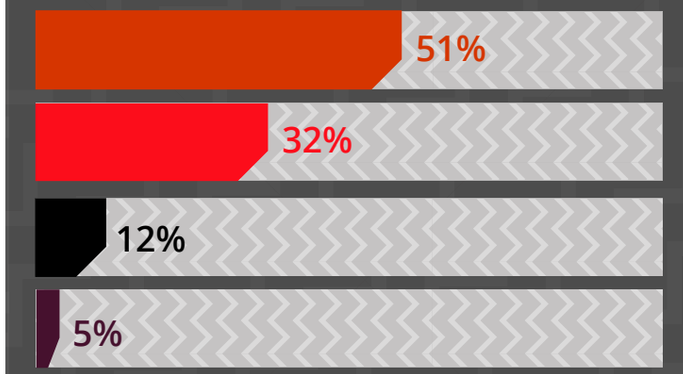
Drilling down into the numbers, Swedish, German and Middle Eastern companies have the most concerns but the numbers are stable across company size.

IT administration overheads have also been impacted by the advent and proliferation of employee-owned devices that are used for work purposes and over a fifth of companies surveyed estimate a "significant increase" with over half saying that their overheads "somewhat increased".

Swedish organizations report the largest IT overhead increase with 94% seeing 'some' or a 'significant' increase. Generally, large companies with over 5,000 employees see the 'significant' IT admin overhead increases.

Of course, the need for security and essential administration will always be with us but, judging by earlier answers, the price for that extra work appears to be worth paying.

**How has your organization's IT security been impacted through employees using non-corporate devices in the workplace?**



FUJITSU

in association with IDG CONNECT

## Conclusion

# Challenges are Worth Addressing Given BYOD Upside



Even the strongest proponents of BYOD should realize that the model is no 'free ride'. There are challenges along the way, most notably in security and increased administration and organizations will have to reformulate codes of conduct and prepare for a cultural change.

However, the positive aspects of BYOD are so obvious and startling that the price is worth paying. Already, organizations are having to adapt to users having more say over their choice of systems and the reward is more engaged, happy and productive employees. IT will need to meet these users halfway and provide the underpinning and controls necessary to ensure good governance. The tools are there for them to address challenges, however. Now is time to get on with optimizing for the BYOD era.