The Economist Intelligence Unit

A report from the Economist Intelligence Unit

The personalisation challenge

Business culture and mobile security

Sponsored by hp

Contents

About the report

An influx of powerful mobile devices is transforming workplace culture and how we do our jobs, upending our sense of "work-life" balance and fanning anxieties about security and privacy. *The personalisation challenge: business culture and mobile security* explores the cultural shifts, security issues and policy changes that will enable companies to grab the full benefits of the mobile revolution. As the basis for this research, the Economist Intelligence Unit surveyed 316 senior executives in January 2013 and conducted in-depth interviews with mobility experts. The findings and views expressed in this report do not necessarily reflect the views of the sponsor. The author was Rik Fairlie. Riva Richmond edited the report, and Mike Kenny was responsible for the layout. We would like to thank all of the executives who participated, whether on record or anonymously, for their valuable insights.

Interviewees

Andrew Borg, research director for enterprise mobility and collaboration at Aberdeen Group

Jeanine M. De Guzman, IT manager of Ford Motor Company's Digital Worker initiative

Nancy Flynn, executive director of the ePolicy Institute

Dan Guido, co-founder and chief executive of Trail of Bits

Rich Mogull, chief executive of Securosis

Eric Openshaw, vice chairman and US technology, media and telecom leader at Deloitte

Roel Schouwenberg, senior researcher at Kaspersky Labs

Ed Stroz, co-president of Stroz Friedberg

David Willis, chief of research for mobility at Gartner

Executive summary

People are obsessed with their mobile gadgets. Millions breathlessly follow launch events for new smartphones and tablets, which are now international spectacles, met by a surge of live tweets and blog posts. Once in hand, they want to use their devices everywhere, including on the job to perform work tasks.

Employers, too, are seizing the windfall that always-connected mobile workers offer their businesses. In the past, corporate IT departments would have quashed employee requests to access company data, applications and networks using their own devices. That has all changed. Today, 62% of companies around the globe allow employees to use personal devices on the job, according to a January 2013 global survey of 316 senior executives by the Economist Intelligence Unit, sponsored by HP. Of those that do not, most provide many of the same coveted gadgets, thus ensuring the workday need never be constrained by time or presence in the office.

Yet our research exploring the impact of mobility on the workplace also found continued impediments that must be addressed if businesses are to realise the full benefits of the mobile revolution. The principal research findings are as follows:

- **Employees and employers alike are embracing the benefits of a highly connected work style**. Almost one-half (49%) of respondents say that using mobile devices boosts innovation, and many feel they are more on top of their jobs (39%) and more efficient (37%). They also say mobility is making their companies more dynamic and innovative (49%) and improving communications (42%). Organisational structures are becoming flatter and less hierarchical.

- **Yet personal and work lives continue to blur—for good and ill**. While today's workers are embracing the flexibility, freedom and productivity improvements that come with mobility, many struggle with the increased intrusion of work into personal time. Only 33% of respondents say that their work-life balance has improved and only 29% believe that they set effective boundaries.

- **Security remains a top concern, but security knowledge is lacking**. Executives express considerable anxiety about data security. Yet they lack knowledge of true mobile risks and seem unaware of security incidents that occur inside virtually all firms today. This is likely to be because workplace training is quite limited, communication about company policies is often passive, and enforcement of policies anaemic. This situation—combined with a widespread belief that corporate security policies more often reflect compliance needs than actual risks—could explain why one in four executives admit to skirting their company's security rules.

- **Many companies offer mobile apps, but IT support for personal devices is limited.** Many firms are enthusiastically embracing mobility. Some 58% of respondents say that their company provides mobile applications to help them perform job-related tasks and 51% say that their company provides custom-designed applications. Yet only 51% rate IT support for mobile devices owned by employees, but used for work purposes, as "strong" or "very strong". As personal technology advances and becomes ubiquitous in the workplace, companies must put in place effective security safeguards, awareness programs and IT support for disparate devices. ■

Who took the survey?

The survey drew on 316 responses from executives around the world, with nearly equal numbers in North America (29%), Asia-Pacific (29%) and Western Europe (27%). Of the 57 countries represented, the most responses came from the US, India, the UK and Canada. Almost half of respondents (49%) are C-level executives or equivalent, 20% are vice presidents or equivalent and 13% are senior managers. Nearly two-thirds (64%) represent very large companies, with annual revenues of US$1bn or more. A wide range of industries is represented, with the top three being financial services (16%), energy and natural resources (10%) and manufacturing (9%). Please see the appendix for full survey demographics. ■

Introduction

Employees and employers alike must balance the benefits mobile devices provide with the challenges they pose.

The proliferation of mobile devices is significantly and swiftly transforming the work environment. As the ground shifts, employees and employers alike must balance the benefits mobile devices provide with the challenges they pose, especially to data security and privacy.

Pervasive use of smartphones and tablets is making businesses flatter, more dynamic and more productive. But security and privacy anxieties are running high among executives and employees alike. Electronically tethered employees are spending more time on the job after-hours, on weekends and even on vacation. Not surprisingly, their "work-life" balance has tilted towards work, and their personal lives are taking a hit. Yet they remain deeply connected to their gadgets.

Employee demand to use the powerful, familiar consumer devices they love has created a conundrum for employers, who are rightly concerned about the security of corporate data.

Should businesses allow employees to use their own devices for work, even though they can be more difficult to secure and manage? Or should they provide company devices? How much choice should they give employees in the types of devices they use and how freely they mix their work and personal lives on them? These are the security questions that matter, especially as more companies encourage employees to "bring your own device" (BYOD) to the office.

The BYOD trend was sparked by employee demand to use their own, often superior, devices, but was later appropriated by companies as an opportunity for cost savings and productivity gains. Regardless of the impetus, the IT department has often been left with little choice but to support BYOD, since employees often use their own devices whether their employers like it or not.

In fact, the majority of organisations around the globe (62%) now permit their employees to use personal mobile devices for work purposes, according to a January 2013 global survey of 316 senior executives by the Economist Intelligence Unit, sponsored by HP. Yet a solid minority of respondents (34%) insist on supplying company-owned devices that they can control. And these holdouts indicate that they are unlikely to embrace BYOD in the next few years.

Regardless of who owns the hardware, our research shows that mobility has made the workplace more productive and efficient, and organisational structures flatter—both of which are advantageous to corporate vitality.

As for cost savings, no company will realise them without an effective, well-implemented security strategy that enables the organisation to avoid costly security breaches. The growing hazards include threats to corporate intellectual property (IP), loss of customer and employee data, missteps owing to the complexity of managing multiple types of devices, misuse by rule-bending employees, and a raft of potential legal pitfalls.

Despite these well-known risks, our survey suggests that many companies have not yet implemented robust mobile-security safeguards, comprehensive employee-awareness programs or strong IT support services for employee-owned devices. By failing to act, they are putting their business in peril and jeopardising the opportunity to realise the full benefits of mobility. ■

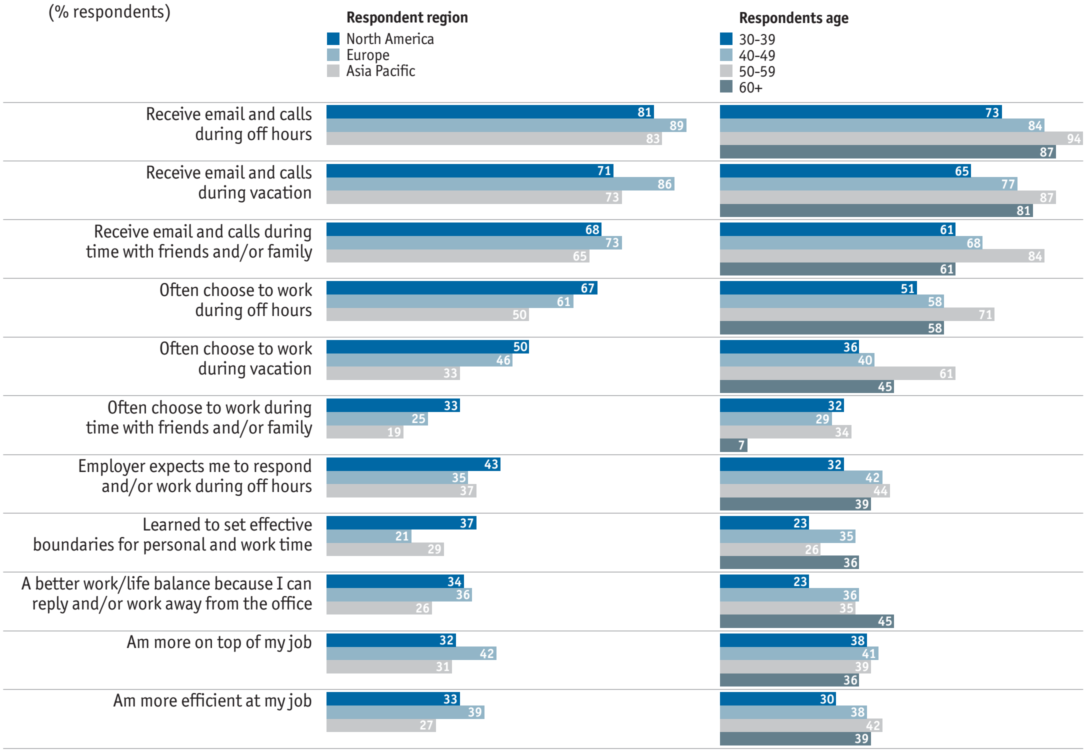
1 A personal trade-off: Empowered or enslaved?

Our survey shines a bright light on a key fact: the use of employee-owned devices has created tightly drawn battle lines between the flexibility of "work-anywhere" freedom and the burden of 24/7 attachment to the job.

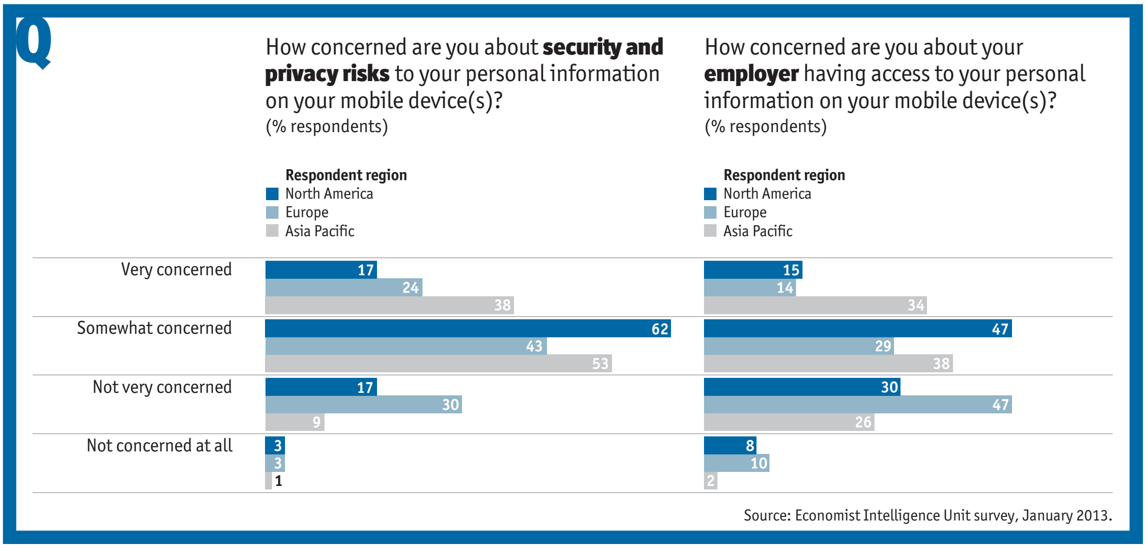
Across industries and around the world, people are increasingly working around the clock, thanks to mobile devices. Most survey respondents say that they read e-mail and take work calls out of office hours (84%) and while on vacation (76%), while 60% often choose to work during off-hours and 43% on vacation. As a result, many people feel that the quality of their personal lives is eroding.

Globally, Europeans are considerably more likely to work out of office hours. So are older employees. These decisions are not always a choice. In fact,

Q How has the use of consumer devices at work impacted you personally and at work?
Select all that apply.
(% respondents)



Source: Economist Intelligence Unit survey, January 2013.



How concerned are you about **security and privacy risks** to your personal information on your mobile device(s)?
(% respondents)

How concerned are you about your **employer** having access to your personal information on your mobile device(s)?
(% respondents)

Source: Economist Intelligence Unit survey, January 2013.

39% of respondents say that their employer expects them to respond to messages or work during off-hours. This expectation is particularly high in Latin America, the Middle East and Africa.

Despite the long hours and incursion into workers' personal lives, many appreciate the benefits of mobility. Some 39% of respondents say that they are more on top of their jobs, and 37% say that they are more efficient. "There are a lot of people that really like being constantly connected," says Rich Mogull, chief executive of Securosis, a US security research firm. "In exchange for that, they get freedom to work when and where they want."

In today's "do more with less" zeitgeist, a willingness to work longer hours and while on the move can be a productivity boon for companies. "The reality is that for most enterprises, the connected worker enabled by BYOD extends the workday significantly," says Eric Openshaw, vice chairman and US technology, media and telecom leader at Deloitte, a consulting firm. "It's recognised that employees deliver more, and the return is pretty good for the company."

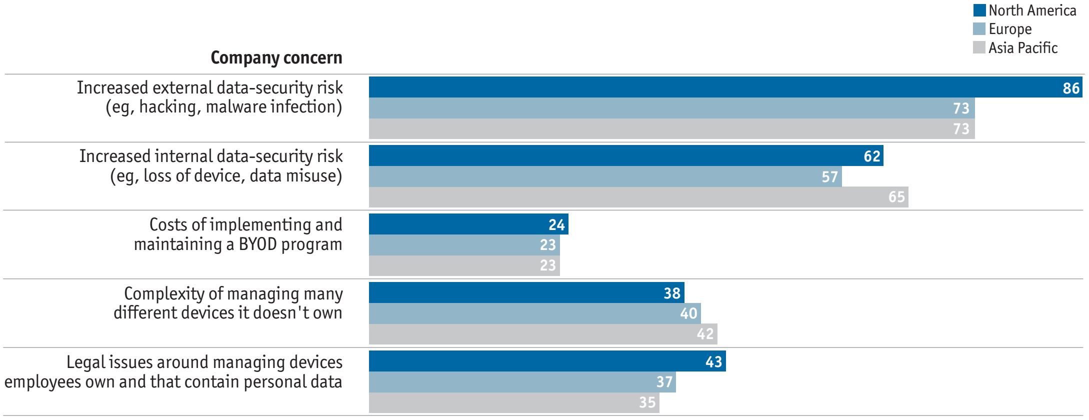
But the return may not be so good for employees—and that could catch up with companies. Only 33% of respondents say that their "work-life" balance has improved because mobile devices help them to work away from the office. Fewer still (29%) say that they have learned to set effective boundaries between work and personal time. Interestingly, the older the respondent, the more sanguine, with 45% of those over the age of 60 saying that mobility has improved their "work-life" balance, compared with 23% of thirty-somethings.

Companies that push too hard run a risk. "Employees may eventually come to resent their supervisors or suffer from burnout," says Nancy Flynn, executive director of the ePolicy Institute, a US consulting firm that advises companies on workplace technology policies. "All companies should have introspective discussions at the executive level on corporate culture and the expectations of employees."

There is also a risk that the fabric of the corporate community could fray. One in four survey respondents say that their company's workforce is becoming disconnected, a sentiment most strongly felt among European respondents. About one-quarter say that employees are preoccupied with checking devices and lose the ability to concentrate and innovate (26%).

Benefits and drawbacks aside, it is clear that easy access to information for individual workers is driving a fundamental change in the way we work. Employees increasingly expect to be able to work anywhere and everywhere using the devices they

Q Why do you believe your company resists facilitating access to data using personal devices?
(% respondents)



Source: Economist Intelligence Unit survey, January 2013.

want to use. In this new "culture of convenience," says David Willis, chief of research for mobility at Gartner, a US research firm, "employees simply want IT and security to get out of the way so they can get their jobs done".

But for remote work to serve both companies and employees well, the modern workplace must foster a culture of personal responsibility and mutual trust—which does not appear to be broadly in place today.

For remote work to serve both companies and employees well, the modern workplace must foster a culture of personal responsibility and mutual trust.

More than one-half (59%) of survey respondents say that they are "very" or "somewhat" concerned about their employers having access to the personal information stored on their mobile devices. They also lack confidence in the security of the devices themselves and in corporate policies governing them. Asian respondents were especially concerned about security and privacy risks to their personal data, while European respondents were considerably less worried, perhaps because of the continent's strong privacy laws.

Likewise, employers appear to be distrustful of their employees. Almost two-thirds (64%) of respondents say that their firms are concerned about risks to data security from loss of devices or misuse of data. Their firms also worry about workers using mobile devices for personal tasks (39%) and either restrict or do not allow the use of social media such as Facebook and Twitter (39%), despite the limited security risks, the growing role of social media in the workplace and the potential damage to employee trust and goodwill, particularly with younger workers.

At the same time, mobile devices are empowering workers, and perhaps even helping to modernise the very structure of the organisation. Survey respondents indicate that the corporate structure is becoming flatter and less top-down thanks to these devices, especially in North America and, to a slightly lesser extent, Asia-Pacific.

This would be progress. A corporate structure with fewer management layers, which empowers workers to make more decisions on operational processes, products and services, is typically a more effective organisation.

The implications of these shifts are hard to overstate. The tug of war between employee freedom and information security—combined with the increasing sophistication of mobile devices and services—is fundamentally reshaping the workplace. ■

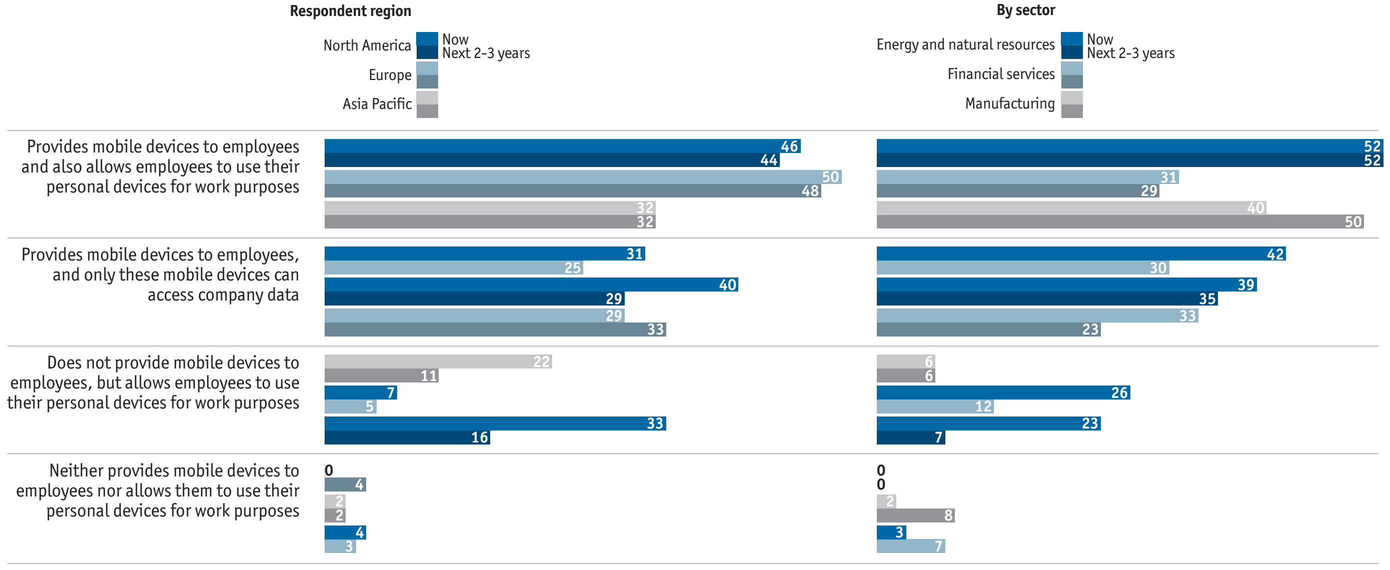
2 The mainstreaming of mobility: Rewards and risks

Powerful mobile devices at work are now mainstream, but companies are still struggling with management and security issues that need to be addressed to enable them to reap the full benefits of mobility.

While most companies still provide devices (stated by 77% of respondents), many also allow employees to use their own (43%). North America (68%) and Asia Pacific (66%) have the highest adoption of BYOD. Yet about one-third (34%) of respondents say that their companies provide mobile devices and that only these devices may be used to access company data. Energy and financial services companies are more likely to fall into this anti-BYOD camp (42% and 39%, respectively). This is likely to be because data security is at the forefront of people's minds in these highly regulated industries, and ownership gives companies clearer legal rights to manage devices and the content on them.

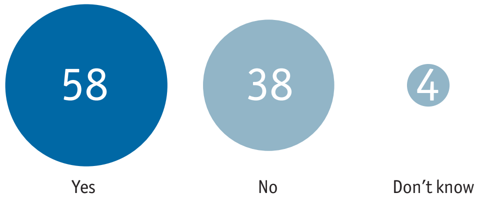
Companies that do provide smartphones and tablets typically ask workers to choose among a select group of devices. In fact, we found that only 8% of respondents say that their company allows employees their full pick of gadgets. That is undoubtedly because managing many hardware

Q What best describes your company's policy on company vs employee mobile-device ownership?
(% respondents)



Source: Economist Intelligence Unit survey, January 2013.

Q Does your company provide mobile applications for use in performing your job duties?
(% respondents)



Source: Economist Intelligence Unit survey, January 2013.

models can be costly and complex, although it may also reflect an effort to lead employees towards more secure models.

Companies are keen to grab the benefits mobility offers the workplace. Almost one-half (49%) of survey respondents say that the use of mobile devices is boosting innovation at their company—a key to developing competitive advantage. Mobile devices can also bring improved productivity, greater process efficiency, a happier work environment and lower operating costs.

Take Ford Motor Company, a major US auto manufacturer. Currently, 9,000 of the company's employees are participating in a BYOD initiative that enables them to use their own Android, Apple iOS and BlackBerry devices for corporate e-mail, calendars and contacts. Ford launched the program in 2007, after realising that company-provided technology was not cutting it with their staff.

"We wanted to embrace the fact that people are more and more into technology," says Jeanine M. De Guzman, IT manager of the company's Digital Worker initiative. "And we realised the technology employees used outside of work was better than what we provided."

Twice-yearly surveys show that participants are highly satisfied with the program, Ms De Guzman says. "The two most cited benefits are increased flexibility and use of the devices to help balance work and life," she says. "And it's also an employee value proposition, because the program helps us attract, attain and keep employees."

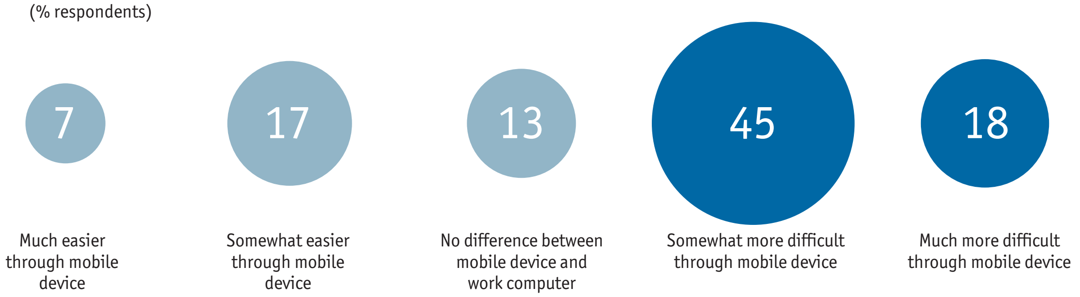
Efficiency is another bottom-line benefit. "What has risen to the top this year for the first time is that BYOD can increase operational efficiency," says Andrew Borg, research director for enterprise mobility and collaboration at Aberdeen Group, a research firm. "The best practice around mobility is not just to mobilise existing processes but to look at mobility as a way to streamline processes and identify new ways for collaboration. It's an enabler of change."

Many companies are turning to mobile apps to make working and accessing company data easier and more efficient. Some 58% of survey respondents say that their company provides mobile applications to help them to perform specific job-related tasks, and one-half (51%) say that these apps are custom-designed for the individual business.

"If you can expand the number of workers who have access to mobile apps, you can redesign a lot of business processes and increase productivity," Mr Willis of Gartner says.

> “If you can expand the number of workers who have access to mobile apps, you can redesign a lot of business processes and increase productivity.”
>
> David Willis of Gartner

Q To what extent do you find it easier or more difficult to access company information on a mobile device compared with your work computer?
(% respondents)



Source: Economist Intelligence Unit survey, January 2013.

Yet companies are grappling with a broad spectrum of risks. Employers are concerned about malware and theft of data when passwords are filched via "phishing" scams, according to our survey. While malware targeting mobile platforms is still rare compared with desktop computers, the number of attacks, particularly on Android devices, is growing quickly, according to Kaspersky Lab, a provider of anti-malware software. Prior to 2012, Kaspersky Lab had identified a total of 6,356 instances of mobile malware, says Roel Schouwenberg, a senior researcher for the company. But in 2012 alone, Kaspersky Lab recorded an astonishing 40,059 new instances, 99% of which targeted the Android operating system.

A key to battling mobile malware, which have primarily appeared as rogue apps, is keeping device operating systems free of known security flaws. Yet vendors and carriers have been very slow to provide security patches, says Dan Guido, co-founder and CEO of Trail of Bits, a New York IT-security firm. He says that Apple devices and Android models offered directly by Google receive patches most frequently.

Companies are also worried about data breaches caused by device loss or theft and employee misuse. Misuse may, indeed, be a significant risk. Alarmingly, almost one in four survey respondents skirt mobile-device security policies. Younger workers are even more likely to disregard policies; 29% of respondents in their 30s bend the rules, compared with only 17% of workers aged 60 and over.

At the same time, businesses face a raft of potential legal issues, says Ms Flynn of ePolicy Institute. For instance, in the US, if an employee who drives uses a mobile device and causes an accident in which someone is injured or killed, "the company can be held liable, regardless of whether the employee is using a company-owned phone or a personal device," she says, citing a US$18m judgment against a trucking company. Emerging risks include lawsuits filed by employees who claim that they were not paid the overtime due to them and a co-worker accused of using their mobile device to send inappropriate content.

One liability that companies are dodging is the cost of devices. While they increasingly allow workers to use personal handsets, they typically do not buy them, nor do they reimburse monthly service fees. For employee-owned devices, 37% of respondents say that their company pays some of the monthly cost, while 52% say none is reimbursed. Our research found that most companies (70%) pay the entire monthly service fee for company-provided mobile devices.

Nevertheless, Aberdeen research shows that companies often spend more on BYOD programs. "If not implemented and managed properly, BYOD can actually increase costs by as much as 33%," Mr Borg says. Consider monthly service fees. Company-provided phones cost organisations an average of US$60 per device for voice and data services under volume discounts, he says. But the average employee reimbursement in a BYOD environment is US$70 a month. And companies must still pay for software to manage and secure the devices, as well as some level of IT support—expenditures that Mr Willis of Gartner estimates cost between US$100 and US$200 per device per year. ■

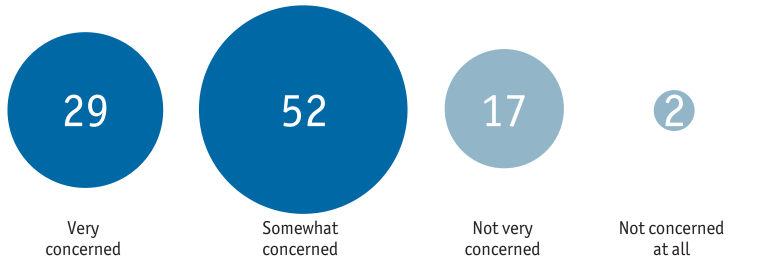
3 What's missing: Security policies, technologies, enforcement and education

If our survey is any guide, executives do not seem to have a visceral understanding of today's heightened security risks. Perhaps consequently, security policies and technologies often fall short of best practice, are poorly communicated to employees and are feebly enforced.

Many respondents seem to underestimate the frequency of actual security incidents, perhaps because companies tend to keep them quiet. Only one in four say they are aware of an IT security breach at their firm in the past year, though security experts and law enforcement agencies say that attacks are rampant. Indeed, the frequency of attacks has led to a new axiom. There are two types of companies: those that have been hacked and those that have been hacked but don't know it yet.

However, one-quarter of respondents say that they have personally experienced a security incident on their mobile device, perhaps explaining their anxiety level. Alarmingly, C-suite executives, often stewards of sensitive company data, are more likely to report a breach or a lost mobile device.

Q How concerned are you about security and privacy risks to your personal information on your mobile device(s)?
(% respondents)



Source: Economist Intelligence Unit survey, January 2013.

Security policies and policy awareness are both often deficient. Overall, executives are divided over whether companies' polices are becoming more permissive and open (43%) or growing stricter (39%) owing to mobility, which may reflect the scramble to react to rapid change. They also question the legitimacy of company policies—58% believe that their company's policies aim to satisfy compliance and legal concerns, while fewer (49%) believe that security is driven by actual risks.

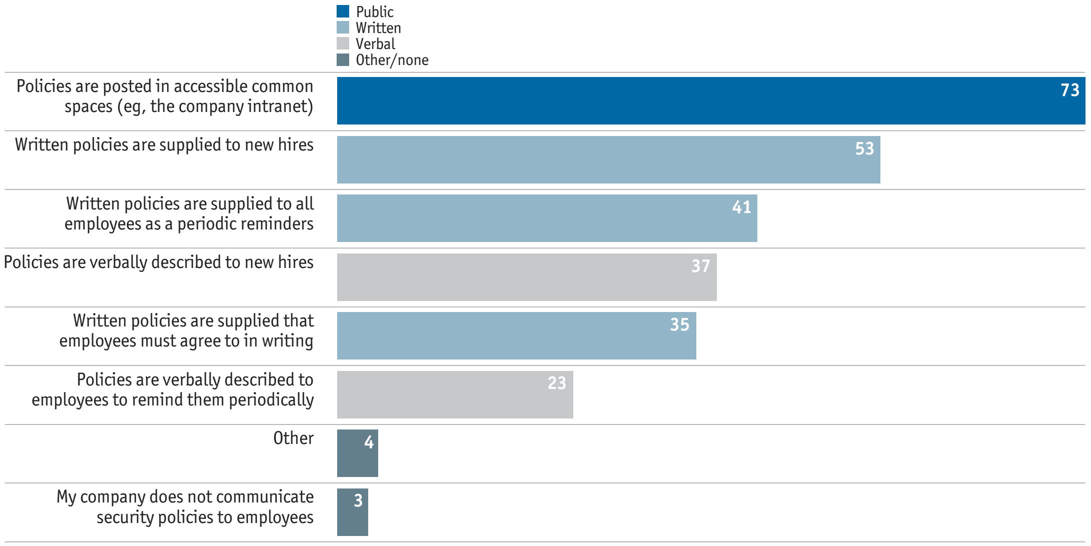
They may be right. Mobile malware is usually a rogue application, yet only 23% of respondents say that their company tracks applications installed on mobile devices. While security software is widely used (77%), only 32% of respondents say that their company employs applications for locating and deleting data from lost or stolen devices, and fewer (31%) say that their company has data back-up and replication processes for mobile devices. This, at a time when valuable intellectual property and other sensitive content have become key targets.

"Companies must start by considering risk," says Ed Stroz, co-president of Stroz Friedberg, a US investigations firm. "You have to think out a strategic approach based on risk tolerance and goals."

Risk of data theft by outside attackers or unscrupulous insiders can be mitigated by technologies that allow companies to manage

How does your company communicate its security policies and usage restrictions?

(% respondents)



Source: Economist Intelligence Unit survey, January 2013.

devices based on set policies and provide secure file-sharing, data encryption (also known as containerisation) and virtualisation, according to Mr Willis of Gartner. Companies also use technologies for user authentication—such as personal identification numbers (PINs)—malware blocking and to track and control company data.

"Data loss prevention is becoming more important for mobile security, and more companies are realising that it's the missing piece to secure and manage content," Mr Borg says. "Can documents be e-mailed to a third party or posted to [online storage services such as] iCloud or Dropbox? Locking down access to devices, networks and applications isn't enough. You have to lock down important data."

> "Locking down access to devices, networks and applications isn't enough. You have to lock down important data"
>
> Andrew Borg of Aberdeen Group

Even if companies do implement effective policies and deploy sophisticated technology safeguards, mobile security will remain elusive if employees are not comprehensively and continuously trained. Again, many companies fall short of this mark. Only 27% of respondents say that their company's security education program is comprehensive.

Moreover, policies are not aggressively communicated to employees and enforcement is anaemic at best. Most firms lean on more passive methods of communication, such as posting security policies in common areas (73%), rather than employing more muscular methods, such as supplying written policies that employees must sign (35%).

"You cannot expect an uninformed workforce to be a compliant workforce," Ms Flynn of ePolicy Institute says. "Once you put policies in place—policies with teeth—you need to do some training. Employees must understand the policy, the rules, and that they must adhere to the rules." Companies ought to invest in formal, in-person education, which gives participants the opportunity to ask questions, she says, arguing that webinars and online modules are less effective.

In light of changing worker expectations about the efficacy of the technologies they use, it seems clear that companies must rethink their approach to support if they are to ensure that employees adopt and use mobile technologies securely and efficiently.

Usability, in fact, is ripe for improvement. Overall, 63% of survey respondents say that accessing company data on a mobile device is more difficult than on a work computer.

A major challenge comes from the smaller screen and more difficult to use keyboards, which may not be very compatible with applications designed to be used on desktop machines. People "expect that mobile applications should be easy to use and are designed to work specifically for the new environment," Mr Willis says. "Simply giving people access to information isn't enough. You have to adapt it to the context."

But adapting can be tricky. The new environment is actually made up of many new environments, because of the multiplicity of mobile operating systems, says Mr Borg. Logging onto a network with a mobile device can require multiple steps and awkward typing of complicated passwords. A lack of file-storage systems can cause confusion. Server instability and inferior network connectivity can also cause frustration.

The human learning curve may also be a factor. Older employees report difficulty more frequently. For instance, 76% of those 60 years or older say that accessing data is more difficult on mobile devices, as opposed to 58% of those in their 30s.

Ford has come face-to-face with this age-related comfort gap. The automotive company expects workers to turn to their device's maker or seller for help, although it does offer an IT-monitored online forum for troubleshooting. That approach has not gone over well with everyone.

"People who are just out of college don't tend to have issues with support," says Ms De Guzman. "We are hearing from some of the more senior people that they don't want to have to post in a forum."

Overall, executives are lukewarm about IT support for personal devices. Just over one-half (51%) say that support is "strong" or "very strong", a finding that was not influenced by age. A significant number (28%) say that IT is of limited or no help in gaining access to company data via their personal device, with older workers being more critical. ■

4 Conclusion

The continued proliferation of powerful, easy-to-use mobile devices inside organisations is inevitable, as employers and employees alike seize the opportunity to stay connected and work anywhere, anytime.

In this context, the BYOD trend is destined to continue apace. Gartner predicts that almost 40% of businesses globally will be totally BYOD by 2016.

"In the future, the company attitude may be, if you're going to work here, we expect that you have appropriate work clothes, that you drive yourself to work and that you to provide your own devices," Mr Willis says.

That trend may morph into a more encompassing BYOT—"bring your own technology"—in which workers are given a stipend to purchase the technology they believe will make them most productive. A few companies, primarily small firms with tech-savvy workers, such as Securosis, have already adopted this approach.

"Bring your own technology doesn't make sense for every organisation—it will work best for knowledge workers," Mr Mogull says. "And we don't expect BYOT to happen overnight. It will be a ten to 20-year change."

Will people continue to work longer hours, out of office hours and on vacations and weekends? Undoubtedly. While workers may privately grumble about being on-call day and night, there is no evidence that they want to become any less connected to each other or to the workplace.

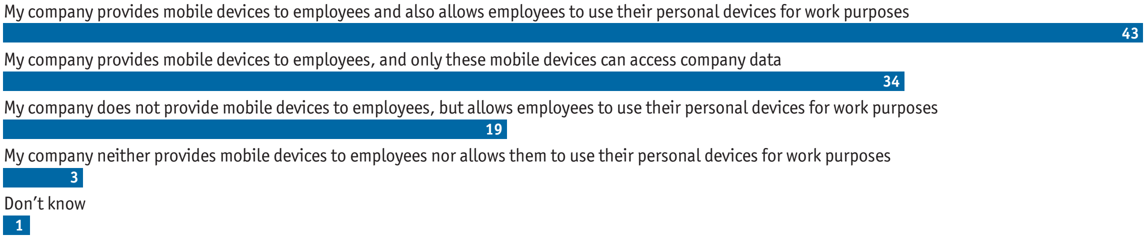
In fact, workers around the world are increasingly embracing job flexibility and the ability to customise the traditional office and work week. As more young people—those who have grown up with mobile devices and expect to be able to use them everywhere—join the work force, the "work-life" balance issue may resolve itself, says Mr Mogull. "We'll find new balances," he says. "Part of this is a generational change."

But to realise the full benefits of the mobile revolution—wherever it may lead—companies ought to examine their mobile work expectations and their approach to addressing security risks. They must also involve their silicon-empowered workers as allies and participants in securing the organisation and ensuring its future success. ■

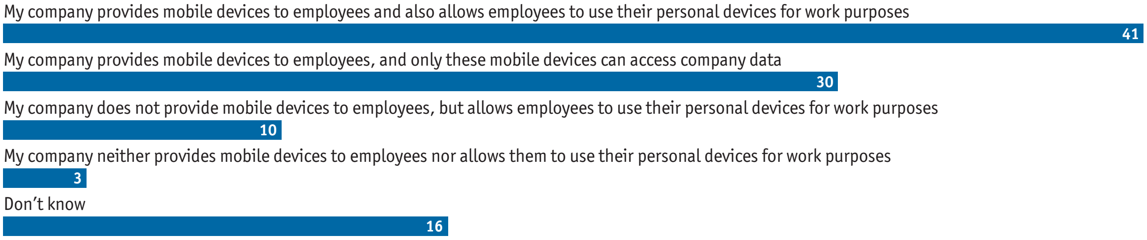
Appendix: survey results

Percentages may not add to 100% owing to rounding or the ability of respondents to choose multiple responses.

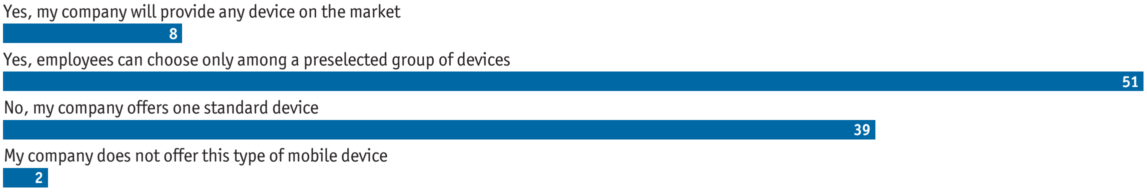
What best describes your company's policy on company vs employee mobile-device ownership? Now
(% respondents)



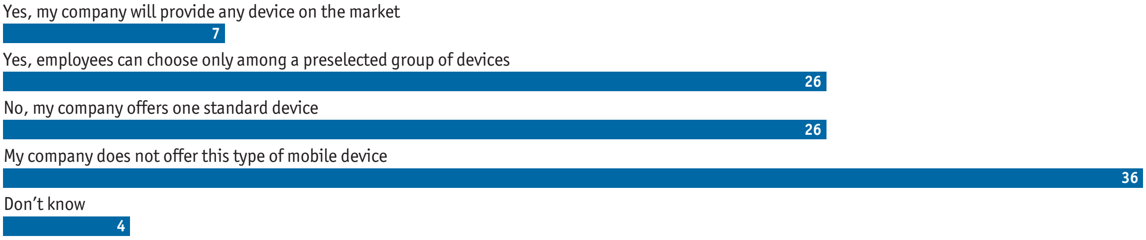
What best describes your company's policy on company vs employee mobile-device ownership? Next 2-3 years
(% respondents)



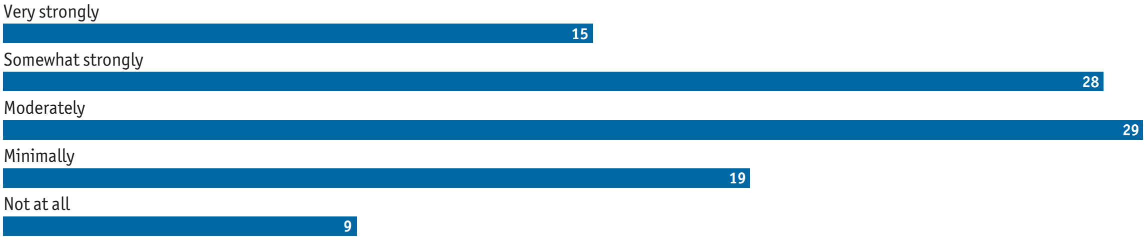
If your company provides employees with mobile device(s), does it let them choose the device(s) they want or does it provide a standard device(s)? Mobile phones
(% respondents)



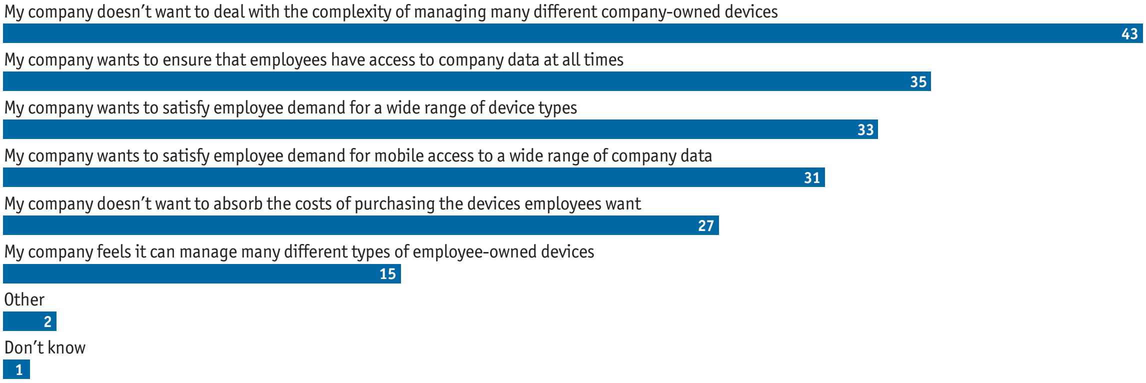
If your company provides employees with mobile device(s), does it let them choose the device(s) they want or does it provide a standard device(s)? Tablets
(% respondents)



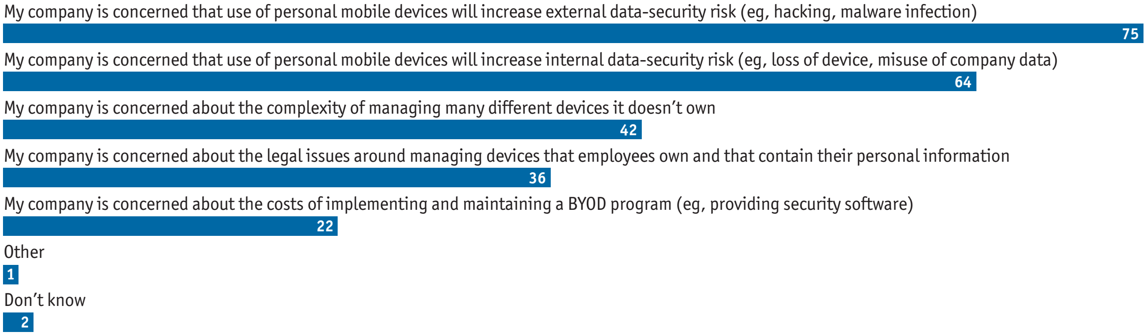
To what extent does your IT department facilitate full access to the company information you need for your job via your personal mobile device(s)?
(% respondents)



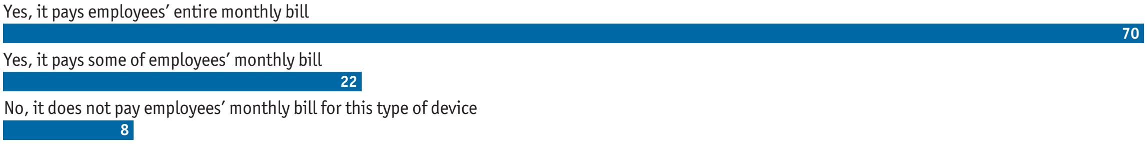
If your company facilitates access, why do you believe this is the case?
Select all that apply.
(% respondents)



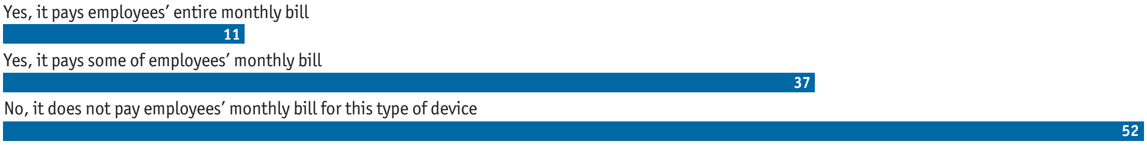
If your company only minimally or does not facilitate access, why do you believe this is the case?
Select all that apply.
(% respondents)



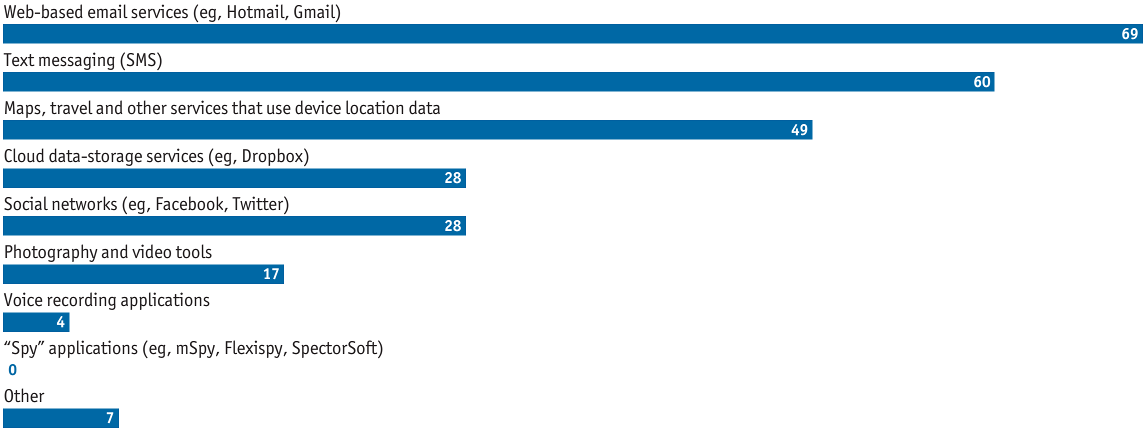
Does your company pay employees' monthly device services bill? Company owned mobile devices
(% respondents)



Does your company pay employees' monthly device services bill? Personal mobile devices used for company data access
(% respondents)

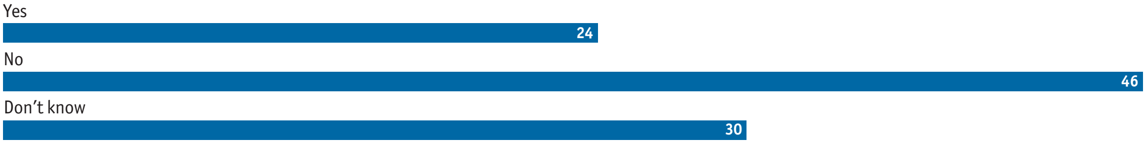


Which of the following consumer digital services do you use most on your mobile device(s)?
Please select top three.
(% respondents)



Has your company experienced an IT security breach in the past 12 months?

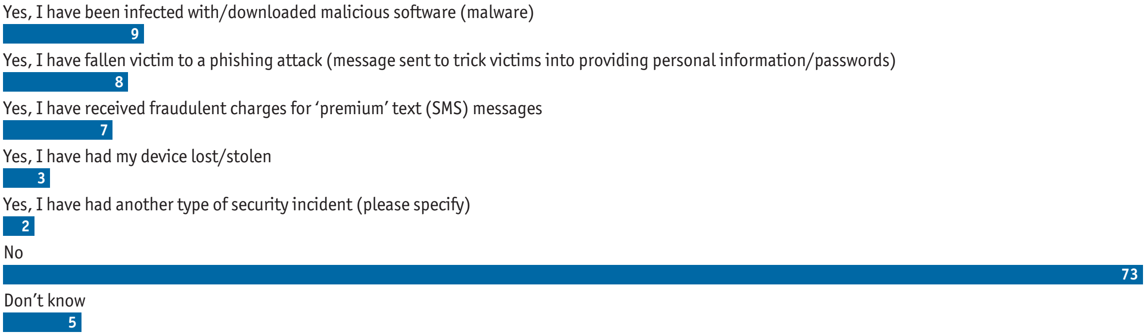
(% respondents)



Have you experienced a security incident related to any of your mobile devices in the past 12 months?

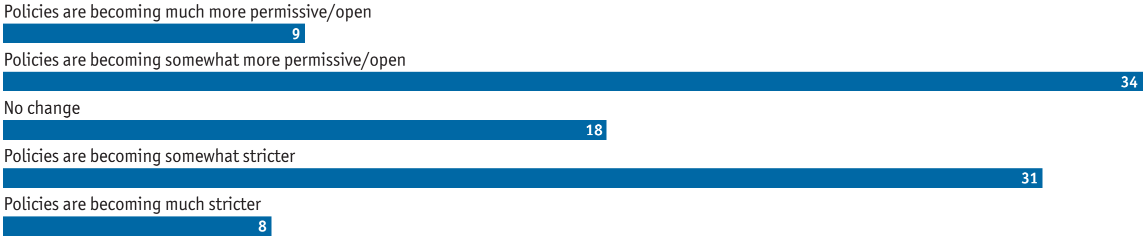
Select all that apply.

(% respondents)

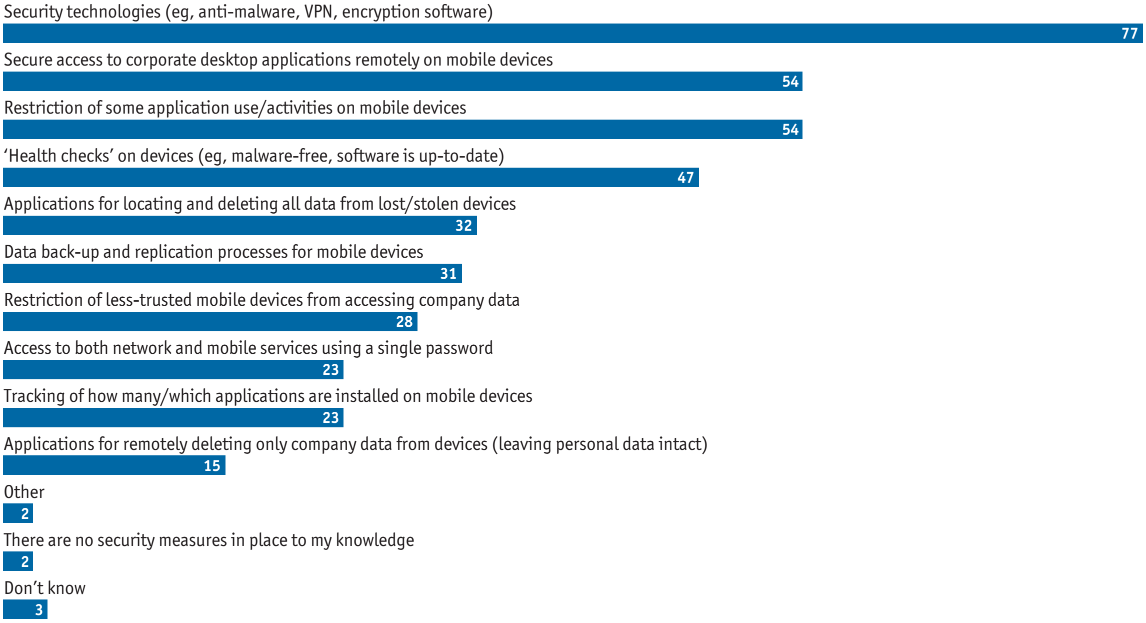


How do you think popular consumer devices are changing overall security policies at your company?

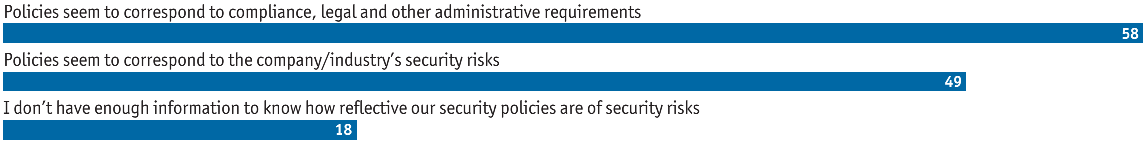
(% respondents)



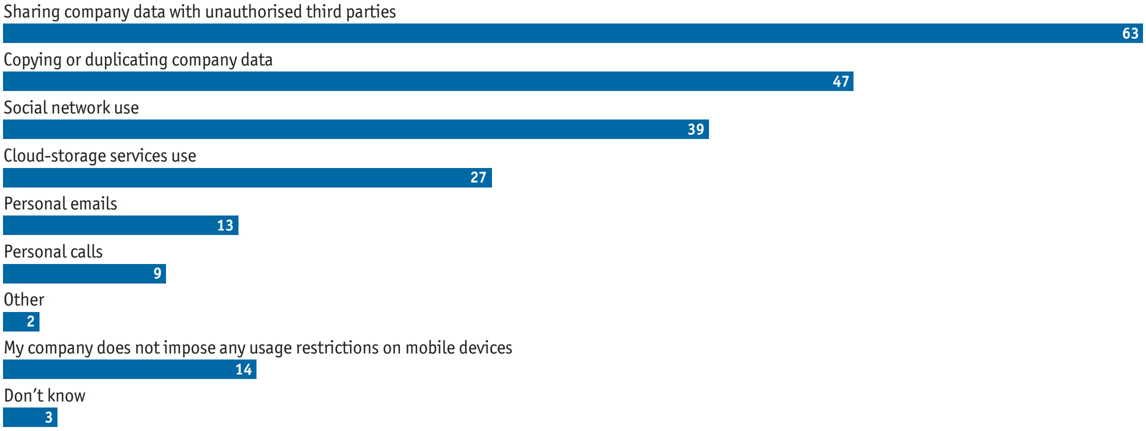
What kinds of mobile-device security measures are in place at your company?
Select all that apply.
(% respondents)



Which statements describe the nature of mobile-security policies and understanding of risks at your company?
Select all that apply.
(% respondents)

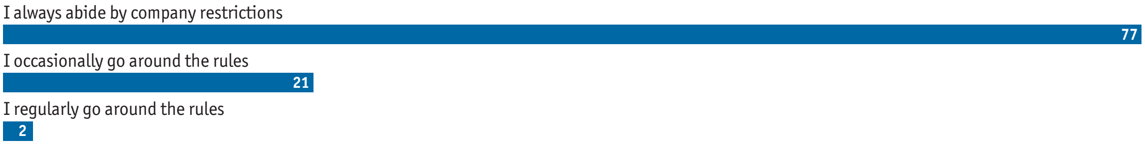


To your knowledge, which of the following types of mobile usage activity are restricted or disallowed by your company?
(% respondents)



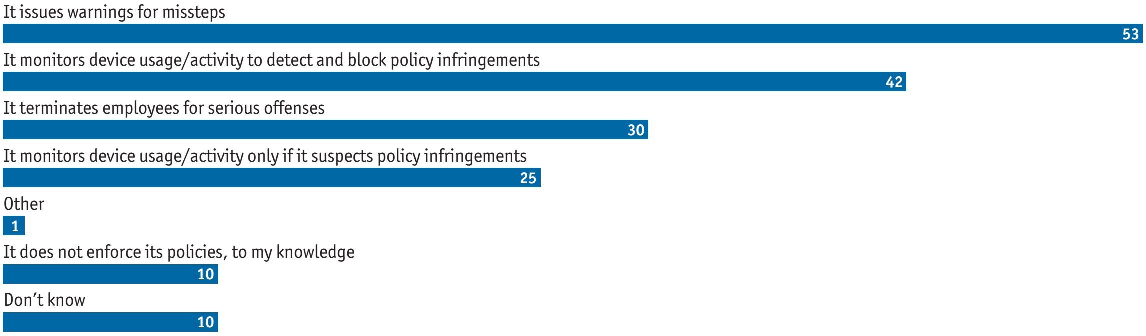
To what extent do you follow company mobile usage rules/restrictions?

(% respondents)



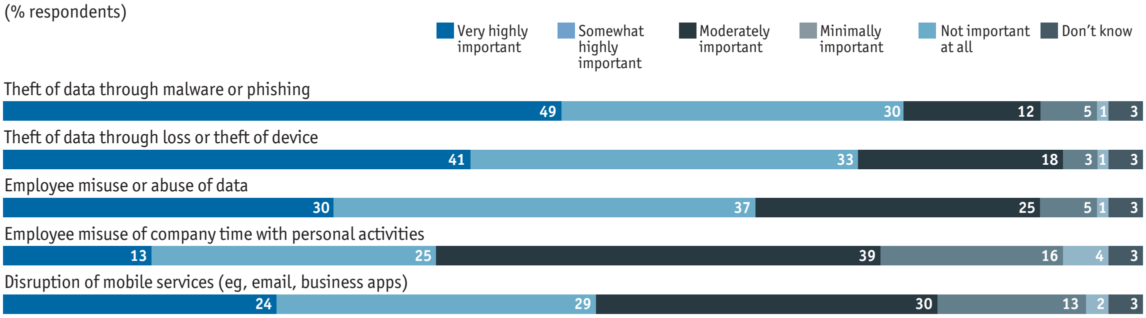
How does your company enforce its mobile device policies?

Select all that apply.
(% respondents)



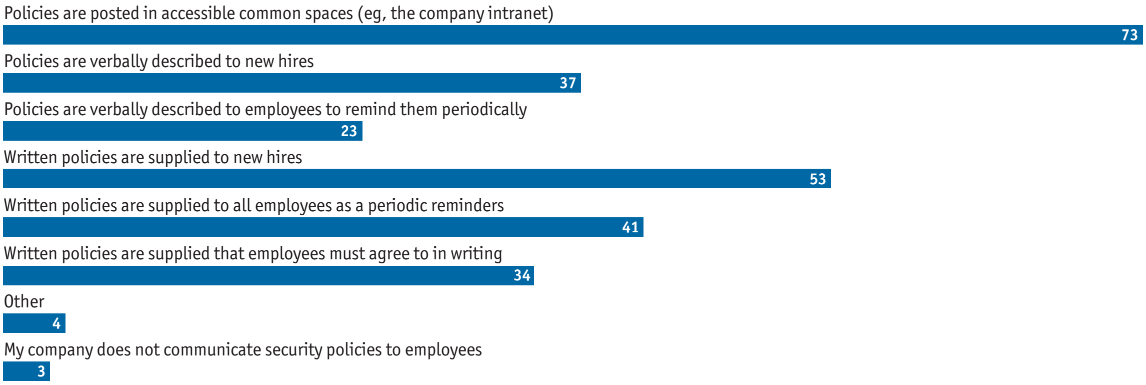
Which mobile security threats and risks does your company communicate as being of greatest concern?

(% respondents)



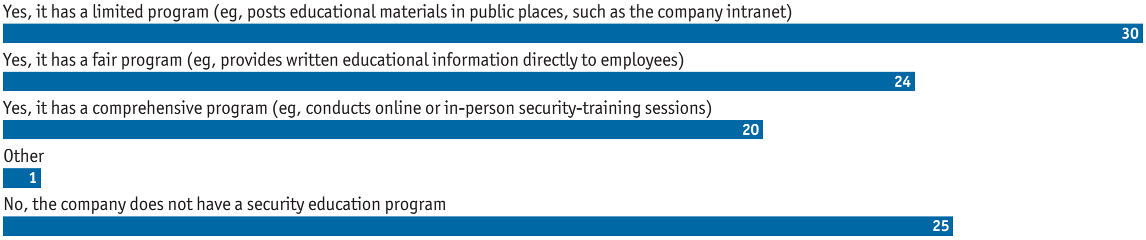
How does your company communicate its security policies and usage restrictions?

Select all that apply.
(% respondents)



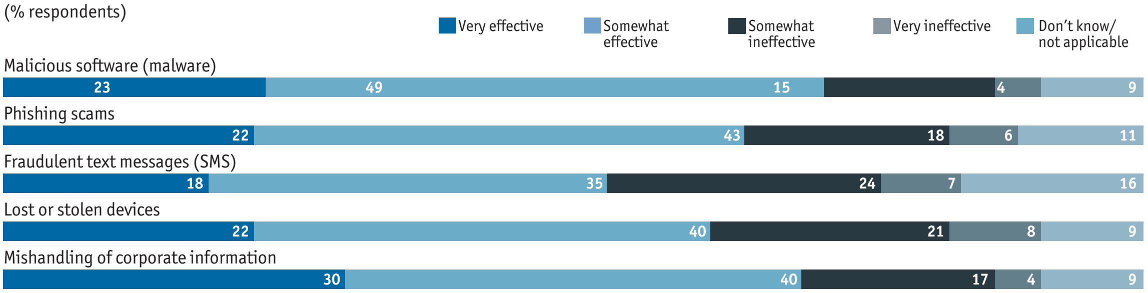
Does your company have a program to educate employees about specific security threats (eg, malware, phishing)?

Select the response that best reflects your view.
(% respondents)



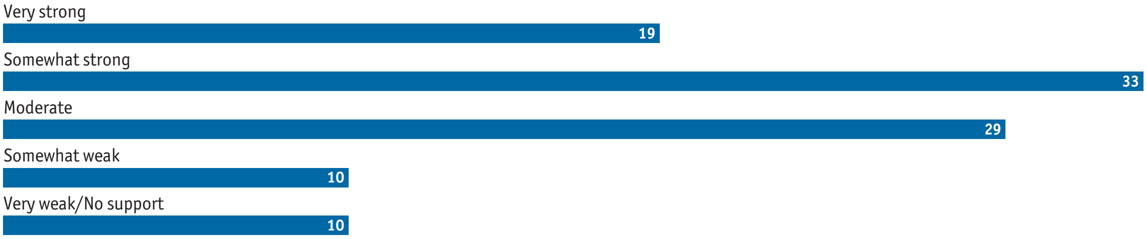
In your opinion, how effective are your company's educational programs at promoting safe practices in relation to the following risks?

Select one in each row.
(% respondents)



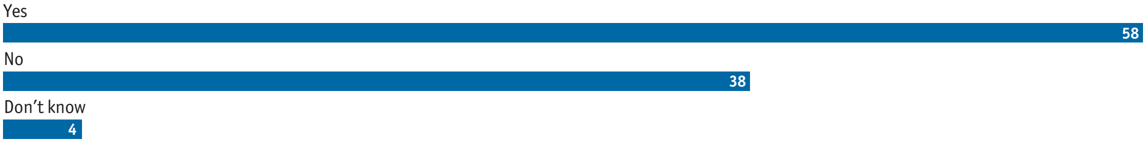
How would you rate your IT department's support services for your personal mobile device(s)?

(% respondents)



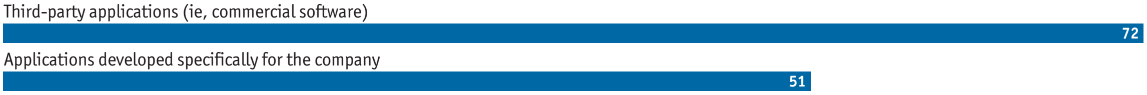
Does your company provide mobile applications for use in performing your job duties?

(% respondents)

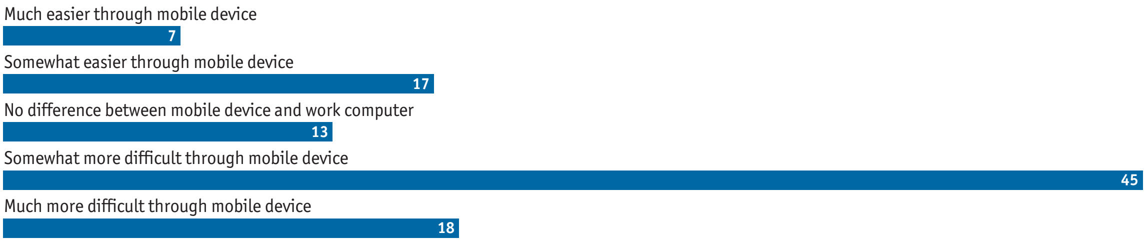


If yes, does your company provide the following application types?

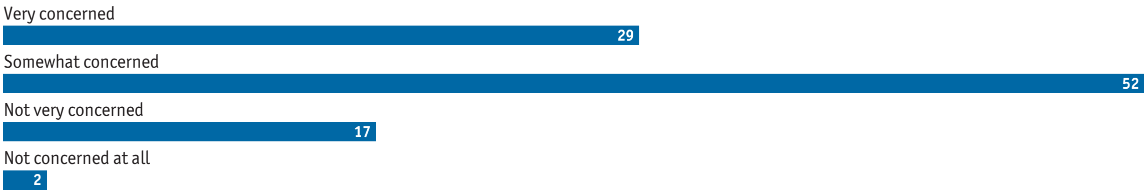
Select all that apply.
(% respondents)



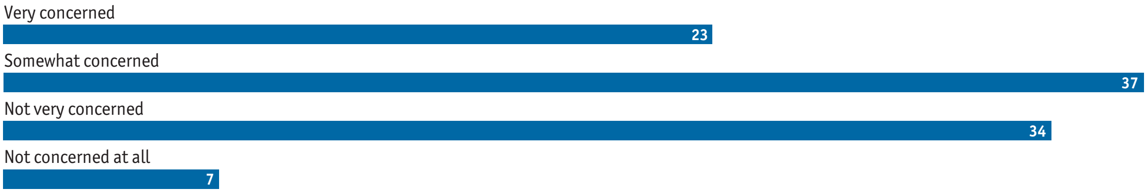
To what extent do you find it easier or more difficult to access company information on a mobile device compared to your work computer?
(% respondents)



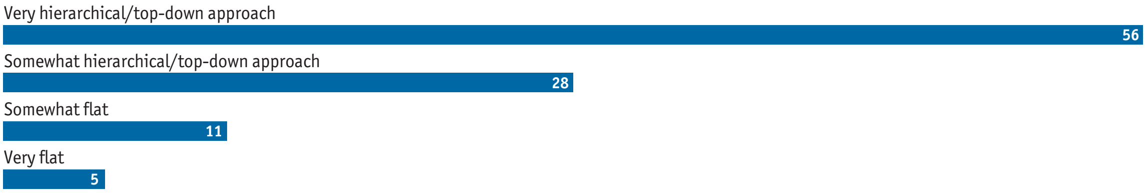
How concerned are you about security and privacy risks to your personal information on your mobile device(s)?
(% respondents)



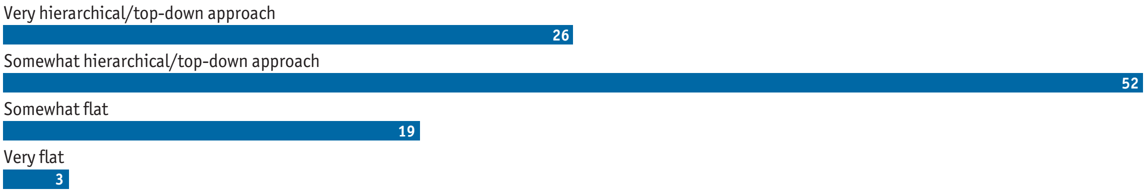
How concerned are you about your employer having access to your personal information on your mobile device(s)?
(% respondents)



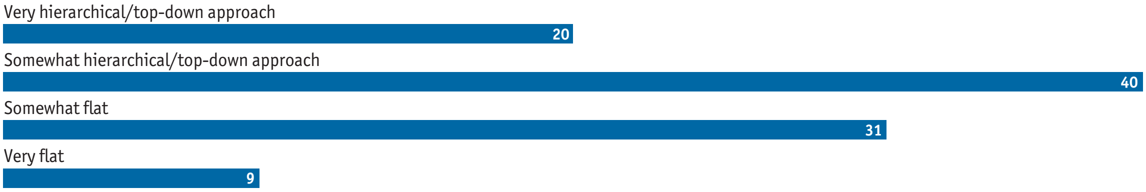
Based on what you know about your current company, how would you describe its structure? 5 years ago
(% respondents)



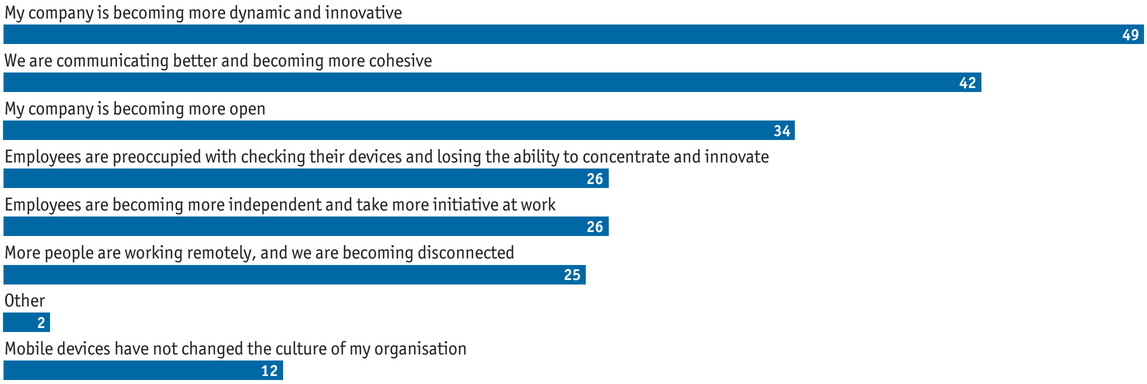
Based on what you know about your current company, how would you describe its structure? Now
(% respondents)



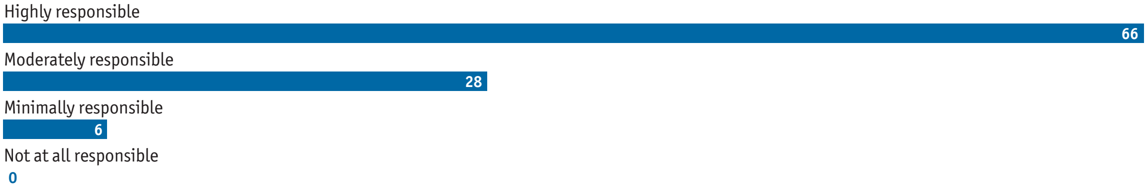
Based on what you know about your current company, how would you describe its structure? 5 years from now
(% respondents)



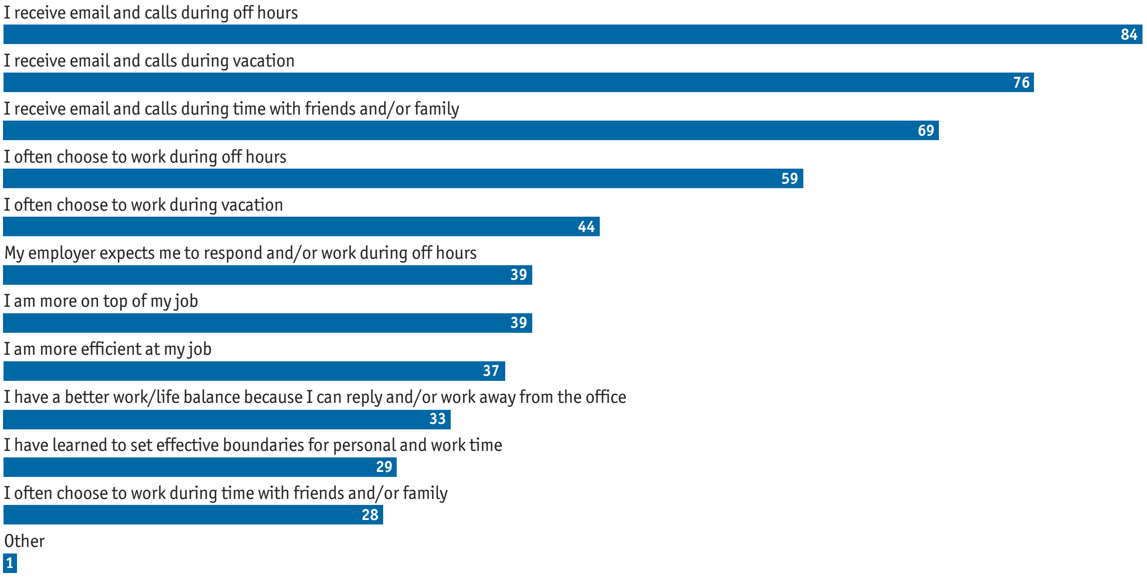
How do you think popular consumer devices are changing your company's culture?
Select all that apply, and explain.
(% respondents)



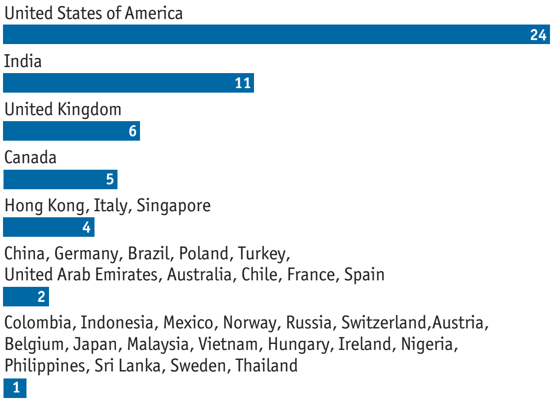
To what extent do you feel responsible for the safety of company data on the devices you use?
(% respondents)



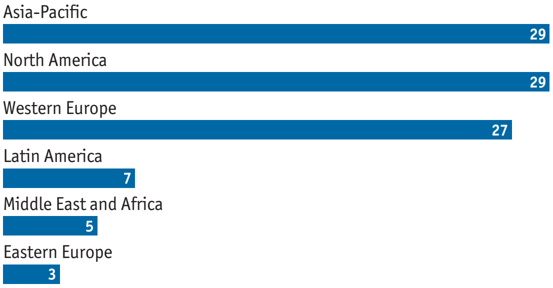
How has the use of consumer devices at work impacted you personally and at work?
Select all that apply.
(% respondents)



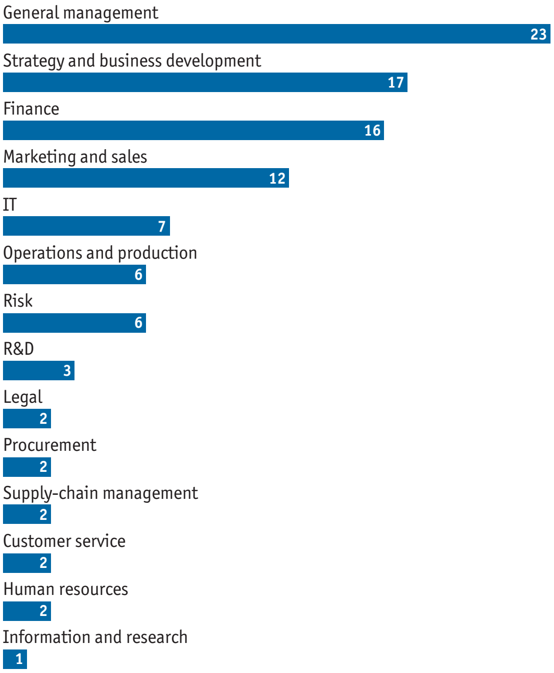
In which country are you personally located?
(% respondents)



In which region are you personally located?
(% respondents)

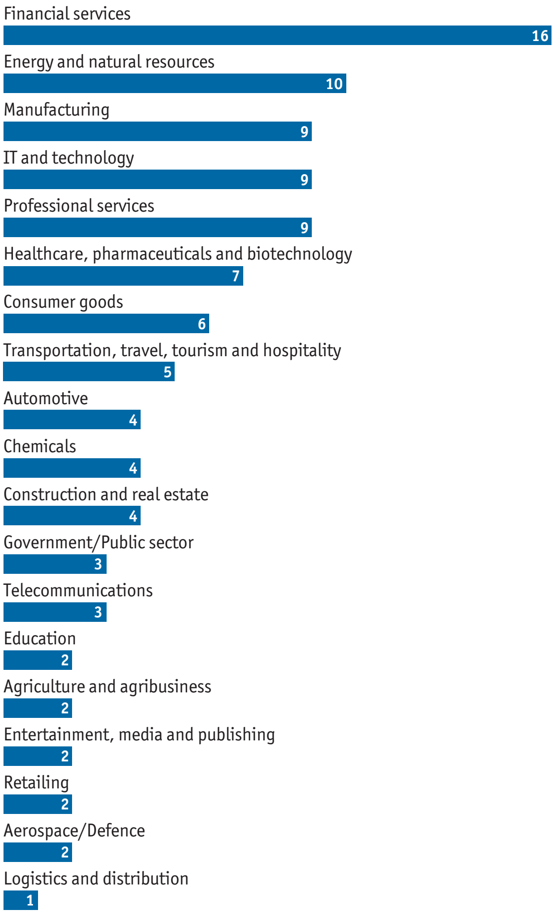


What is your main functional role?
(% respondents)



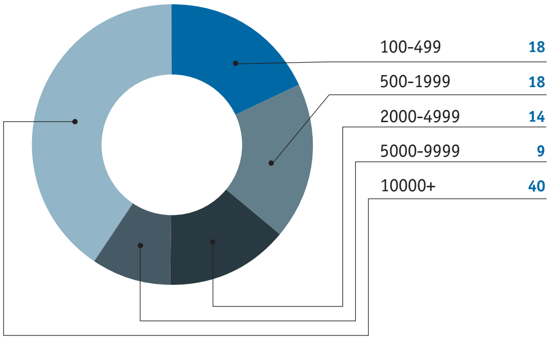
What is your primary industry?

(% respondents)



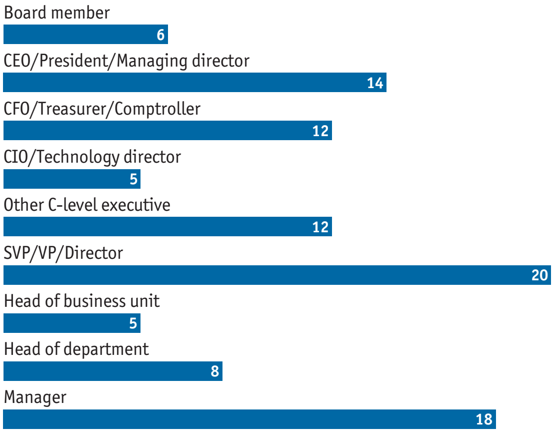
Approximately how many employees does your company have?

(% respondents)



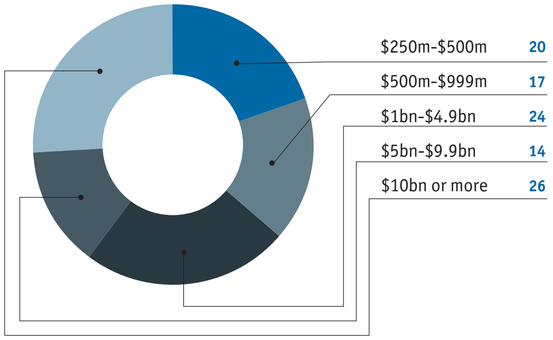
Which of the following best describes your title?

(% respondents)



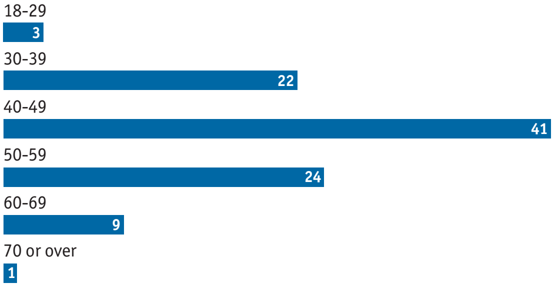
What are your organisation's global annual revenues in US dollars?

(% respondents)



What is your age group?

(% respondents)



Whilst every effort has been taken to verify the accuracy of this information, neither The Economist Intelligence Unit Ltd. nor the sponsor of this report can accept any responsibility or liability for reliance by any person on this white paper or any of the information, opinions or conclusions set out in the white paper.

Cover: Shutterstock

London
20 Cabot Square
London
E14 4QW
United Kingdom
Tel: (44.20) 7576 8000
Fax: (44.20) 7576 8476
E-mail: london@eiu.com

New York
750 Third Avenue
5th Floor
New York, NY 10017
United States
Tel: (1.212) 554 0600
Fax: (1.212) 586 0248
E-mail: newyork@eiu.com

Hong Kong
6001, Central Plaza
18 Harbour Road
Wanchai
Hong Kong
Tel: (852) 2585 3888
Fax: (852) 2802 7638
E-mail: hongkong@eiu.com

Geneva
Boulevard des
Tranchées 16
1206 Geneva
Switzerland
Tel: (41) 22 566 2470
Fax: (41) 22 346 93 47
E-mail: geneva@eiu.com