Bring Your Own Device: The Results and the Future

Published: 5 May 2014

Analyst(s): David A. Willis

Bring-your-own-device strategies are creating new opportunities and challenges for business and IT leaders. This document shows the results of mature BYOD programs and identifies best practices.

Impacts

- BYOD creates new opportunities for CIOs and the business by increasing the number of mobile-application users in the workforce.

- BYOD drives employee satisfaction, productivity and new applications.

- BYOD requires IT and business units to invest in ongoing policy creation, enterprise mobility management, security and infrastructure expansion.

- BYOD increases risks for CIOs and CISOs and changes expectations for workforce enablement.

Recommendations

- Examine opportunities for new applications that assume personally owned devices in the workplace at all levels.

- Pursue platform-agnostic management tools and application platforms.

- Establish clear goals and policies for your BYO program. Periodically benchmark stipends, reimbursements and allowances.

Analysis

"Bring your own device" (BYOD) strategies are maturing. Early adopters are showing results and getting some hard-earned lessons. This research summarizes the results of several Gartner primary research studies and provides guidance for IT leaders and CIOs (see Figure 1).

Figure 1. Impacts and Top Recommendations for BYOD Strategies for IT Leaders

Impacts	Top Recommendations
BYOD creates new workplace engagement opportunities for CIOs and the business.	• Examine new applications that assume personal devices in the workplace. • Pursue multiplatform management tools and device-agnostic application platforms.
BYOD drives employee satisfaction, productivity and new applications.	• Set goals for your program, and measure success accordingly.
BYOD requires IT and business units to invest in policy, security, management and infrastructure expansion.	• Invest in technologies to manage applications, devices, security policy and infrastructure. • Periodically benchmark stipends, reimbursements and allowances.
BYOD increases risks for CIOs and CISOs and changes expectations for workforce enablement.	• Establish clear geography-specific policies for BYOD, addressing business unit and other concerns. • Clearly set support expectations for diverse device platforms.

CISO = chief information security officer

Source: Gartner (May 2014)

Gartner defines a BYOD strategy as "an alternative endpoint deployment strategy that allows employees, business partners and other users to use a personally selected and purchased client device to execute enterprise applications and access data. It typically spans smartphones and tablets, but the strategy may also be used for PCs. It may or may not include a subsidy."

Current and Future Landscape

Half of enterprises say they intend to move exclusively to BYOD for smartphones in 2017, eliminating their employer-supplied option (see Figure 2). A slightly smaller percentage expect this policy for tablets, while very few anticipate going all-BYOD for their PCs.

Almost 40% of organizations worldwide are actively encouraging "bring your own" (BYO), while about 20% are actively discouraging it. There is a wide variation by country and region. In general, employers in EMEA tend to be less aggressive with BYO than other parts of the world, especially as compared with the United States.

Figure 2. In 2017, BYO Smartphone Will Be the Preferred Option for Half of Enterprises

Do you anticipate your organization moving to all-BYOD for each of the following devices within the next three years, eliminating the enterprise-supplied option?
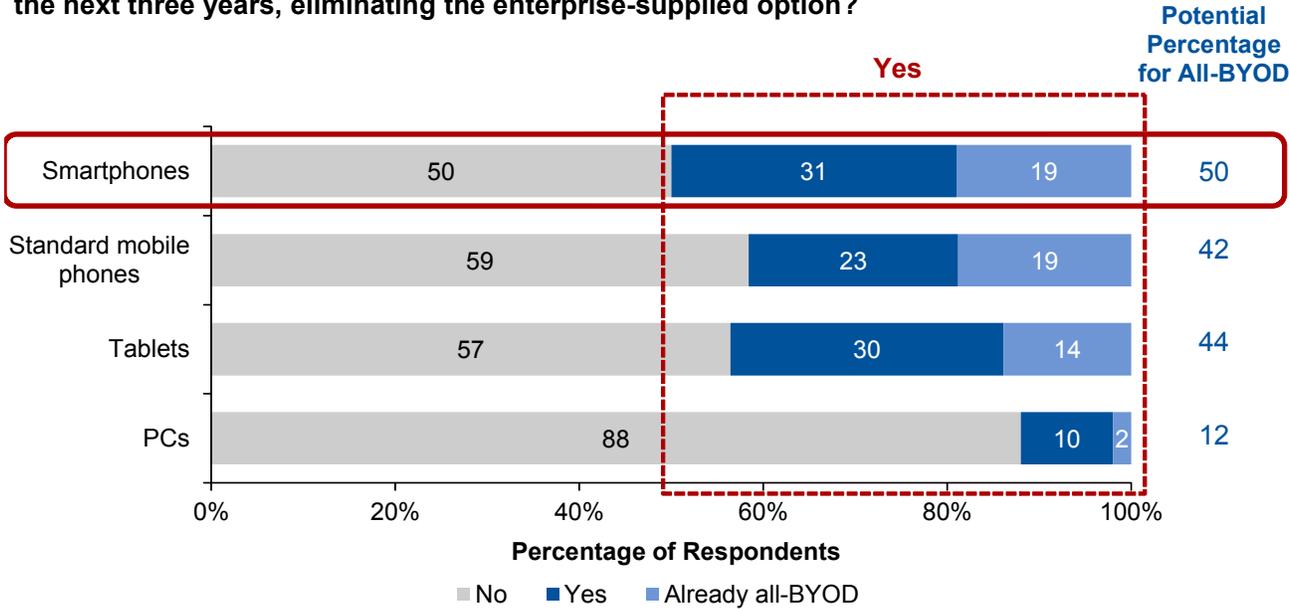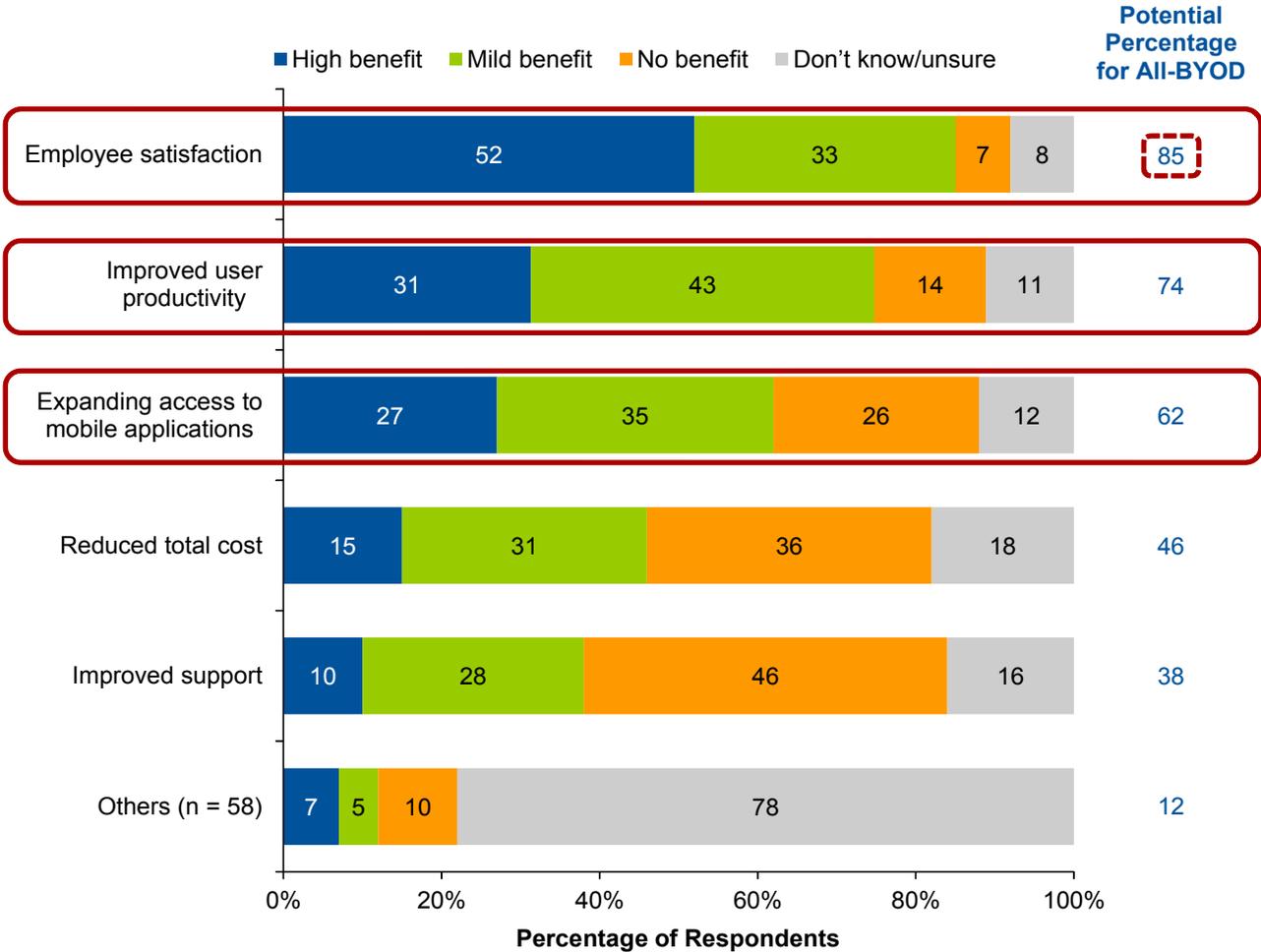

n = 355

Source: Gartner (May 2014)

Impacts and Recommendations

BYOD Creates New Opportunities for CIOs and the Business by Increasing the Number of Mobile-Application Users in the Workforce

Early-adopter organizations see breakaway benefits in employee satisfaction and report increased user productivity as a result of their BYO programs (see Figure 3). Employees prefer using a single device of their personal preference, and they believe this makes them better workers.

Figure 3. Benefits Realized From Current BYOD Programs

What level of benefit has your organization seen as a result of its BYOD program in each of the following areas?

■ High benefit ■ Mild benefit ■ No benefit ■ Don't know/unsure

Potential Percentage for All-BYOD

Category	High benefit	Mild benefit	No benefit	Don't know/unsure	Potential Percentage for All-BYOD
Employee satisfaction	52	33	7	8	85
Improved user productivity	31	43	14	11	74
Expanding access to mobile applications	27	35	26	12	62
Reduced total cost	15	31	36	18	46
Improved support	10	28	46	16	38
Others (n = 58)	7	5	10	78	12

Percentage of Respondents (0% – 100%)

n = 271

Source: Gartner (May 2014)

Other studies that focus specifically on the employee also show this perceived benefit. A survey of 995 BYOD employees in the United States conducted in December 2013 indicated that BYO workers notionally add up to 32 work hours per month (see "Survey Analysis: What IT Leaders Need to Know About Employee BYOD Attitudes in the U.S."). However, satisfaction and productivity are generally subjective benefits that are difficult to correlate to revenue growth or any specific efficiency, especially for knowledge workers. We are skeptical that these hours are effectively recaptured: It is just as likely that employees are mixing work and personal activities during the working day. We remain neutral on the productivity gains, but recognize that perception is often what drives investment.

The real payoff lies in the fact that over 60% of early adopters see providing broader access to mobile applications as a benefit. Not only has BYO created an option for employees who were already eligible for an enterprise-supplied device, but 18% of organizations say it has already allowed them to expand beyond that base, effectively creating a new class of mobile worker. Through expanding the number of workers who can use mobile applications, while not having to supply them with a device, it is possible to capture new opportunities in the moment, at any point during the day. Workers can get crew assignments, take training, complete internal forms, communicate, collaborate and do other tasks on their personal devices.

Organizations expect to simultaneously grow BYO *and reduce the span of their enterprise-supplied programs.* Key inflection points will occur around 2017, when more employees will qualify for BYO programs than will qualify for enterprise-supplied devices.

These inflection points vary substantially by device, as noted in the following figures. Once again, smartphones have the highest adoption rates (see Figure 4).

Figure 4. Employee Access to Smartphones Hits a Key Inflection Point by 2017

What percentage of your organization's total employees are currently participating in your BYOD program and enterprise-supplied programs, by device, and what do you expect this to look like in 2017 and then in 2020?

Percentage of Respondents
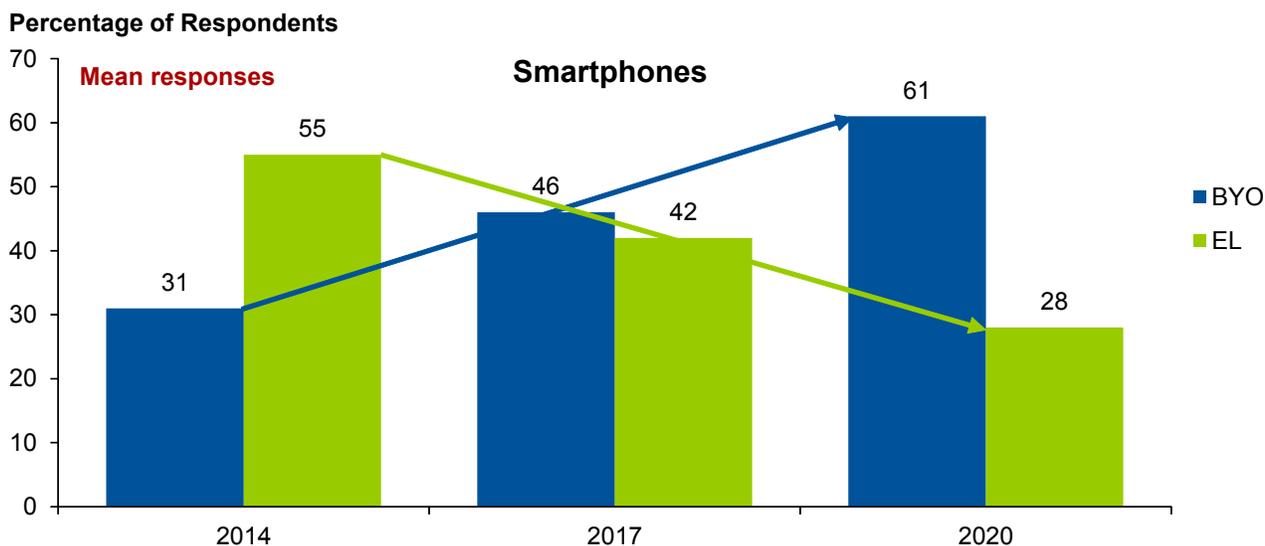
EL = enterprise-liable

Source: Gartner (May 2014)

Tablets will follow a similar but slightly slower trajectory, and are expected to be adopted by fewer workers than with smartphones (see Figure 5). This is because tablets are currently optional, adjunct devices and not the principal device seen in the broader workforce. But their popularity among executives and managers, sales and field service organizations will continue to rise.

Figure 5. More Employees Will Have Access to BYO Tablets Around 2017

What percentage of your organization's total employees are currently participating in your BYOD program and enterprise-supplied programs, by device, and what do you expect this to look like in 2017 and then in 2020?

Percentage of Respondents
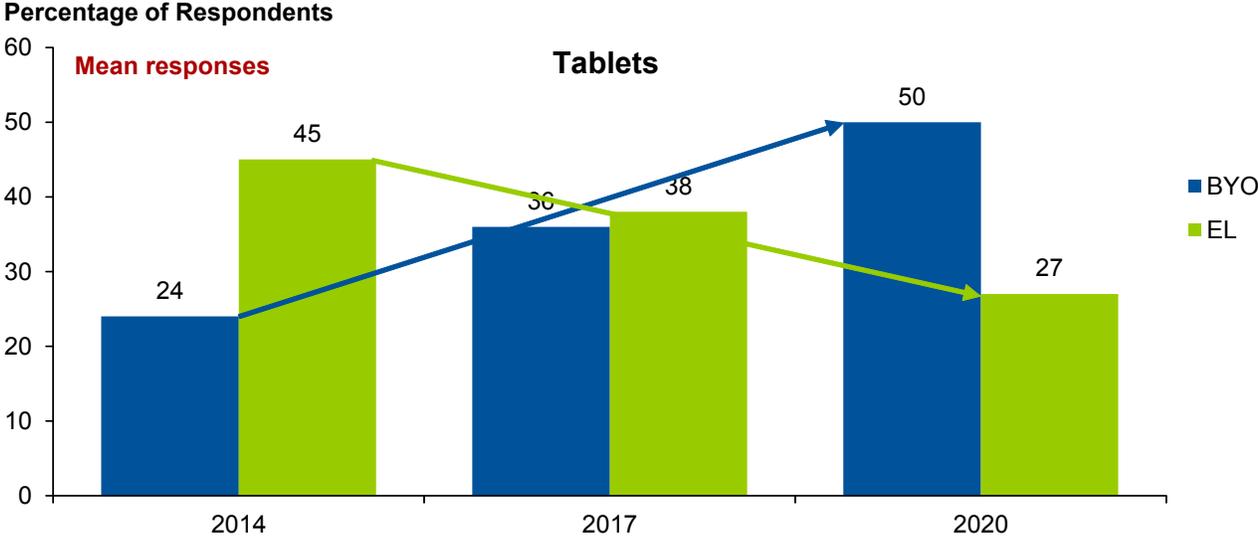
Source: Gartner (May 2014)

Meanwhile, employers still expect to maintain control of the *primary* personal computer (PC) that an employee uses (see Figure 6). The economics of BYO PC are not particularly attractive, especially if any stipend, reimbursement or allowance is provided to the employee. *Note that this does not count supplemental use of a personally-owned PC for nonessential applications like casual access to email over the Web.*

Figure 6. Employers Retain Control of PCs

What percentage of your organization's total employees are currently participating in your BYOD program and enterprise-supplied programs, by device, and what do you expect this to look like in 2017 and then in 2020?

Percentage of Respondents
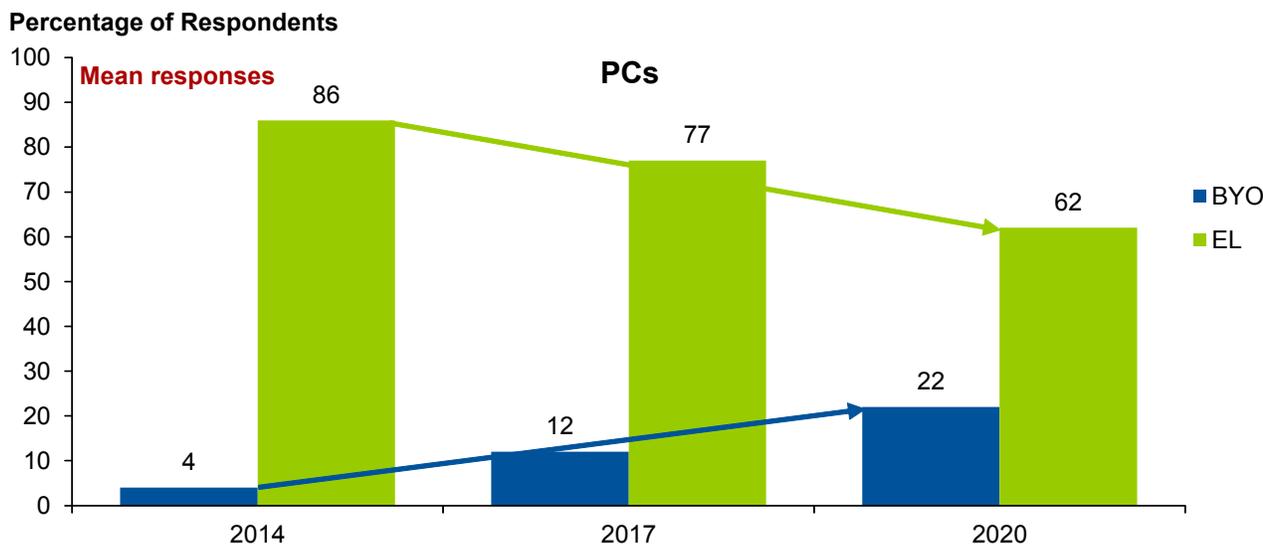
Source: Gartner (May 2014)

Resistance to BYO PC is especially high in government and banking organizations, with roughly one-quarter of organizations banning BYO PC altogether.

Most Organizations Will Mix BYO and Enterprise-Supplied Devices

The rise of BYO does not mean that highly sensitive tasks or those that require special hardware will suddenly be replaced by whatever device a worker happens to have, especially in highly regulated industries like government/defense, financial services and healthcare. In fact, many organizations will support both BYO and enterprise-supplied models simultaneously. For example, pilots may carry airline-issued devices for their electronic flight bags but still be able to use their personal phones to bid on routes, take training courses or file expenses.
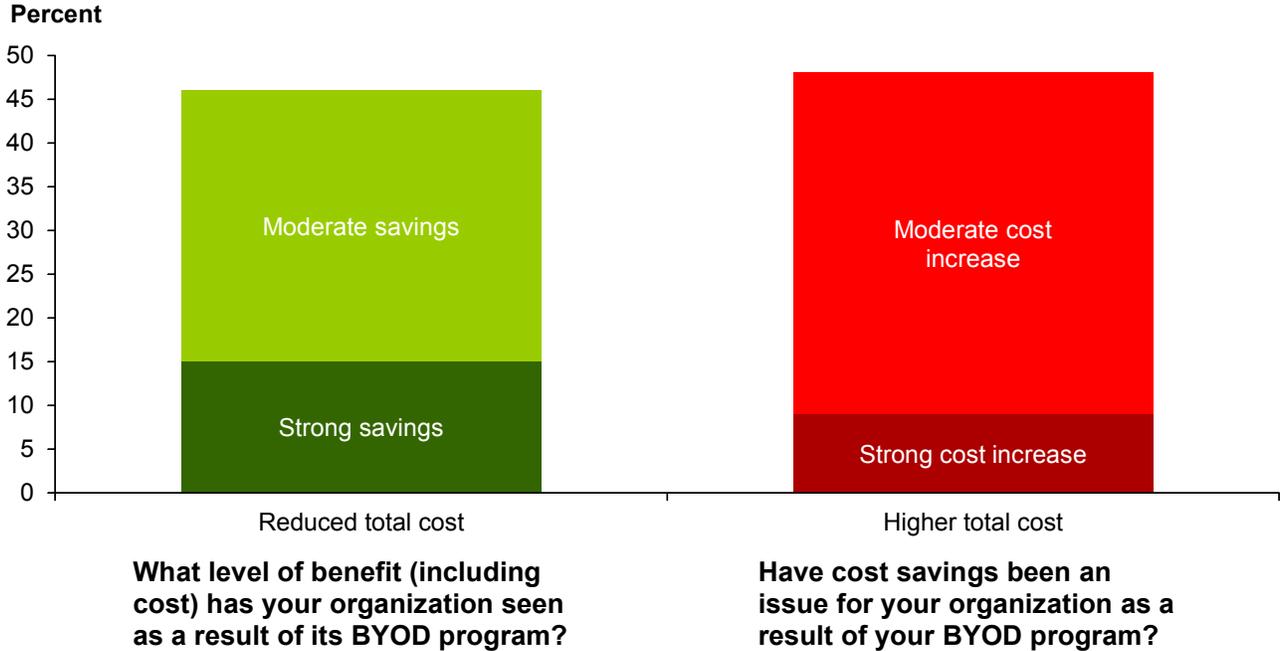
CIOs and IT leaders should use this as an opportunity to identify applications that might be delivered to every type of worker in their organization, not just the traditional mobile executives, field sales and field force. Use a cross-functional mobile center of excellence to generate ideas for the newly mobilized workforce created by BYOD. First movers that can manage and develop applications for the entire workforce will often gain a competitive advantage.

BYOD Drives Employee Satisfaction, Productivity and New Applications

Cost reduction is not universally achievable with BYOD. A roughly equal number of organizations say they are spending *more* money as a result of BYO as those that are spending less (see Figure

7). We also expect most respondents are not taking hidden costs into account, such as employees' time spent managing their own devices. But even though the savings potential is lackluster, organizations often see other benefits, which are driving investments in BYO.

Figure 7. BYO Doesn't Assure Cost Savings

Percent

What level of benefit (including cost) has your organization seen as a result of its BYOD program?

Have cost savings been an issue for your organization as a result of your BYOD program?

Source: Gartner (May 2014)

As noted above, the payoff is more in soft benefits like employee satisfaction and productivity, or in opening up new opportunities for applications to the broader workforce. Therefore, the goals of a BYO program, as well as the ways success is measured, vary in more ways than cost savings (see Figure 8). Communicate your goals clearly to management, and identify metrics that you will use as a yardstick for success.

Figure 8. Goals Drive Different Strategies and Metrics

	Mobile Expansion	Employee Satisfaction	Cost Reduction
Device choice	Wide	Modest	Narrow
App controls	Tiered	Minimal	Heavy
Subsidy	None	Fair and none	Limited, declining
Communications	Enterprisewide	Marketing to existing users	Management mandate
Management support	Modest	Light	Heavy
Measure by	Take rates	Perception	Total cost
Effect on EL program	Limited	Attrition	Rapid drawdown
Focus on	Workforce enablement apps	Choice	Cost controls, limited subsidy

Source: Gartner (May 2014)

The strategies and measures of success for BYO vary substantially based on the goals of the program. When an expanded mobile workforce is the goal, providing the right tools to enable new capabilities should be a priority, and adoption of those new capabilities (measured by take rate) should be a key metric. If employee satisfaction is the major driver, then employee sentiment about the organization's attractiveness as a place to work, as well as the perceptions of its policies, must be measured. If cost reduction is the goal, then tight cost controls, standardization and restrictions on usage apply.
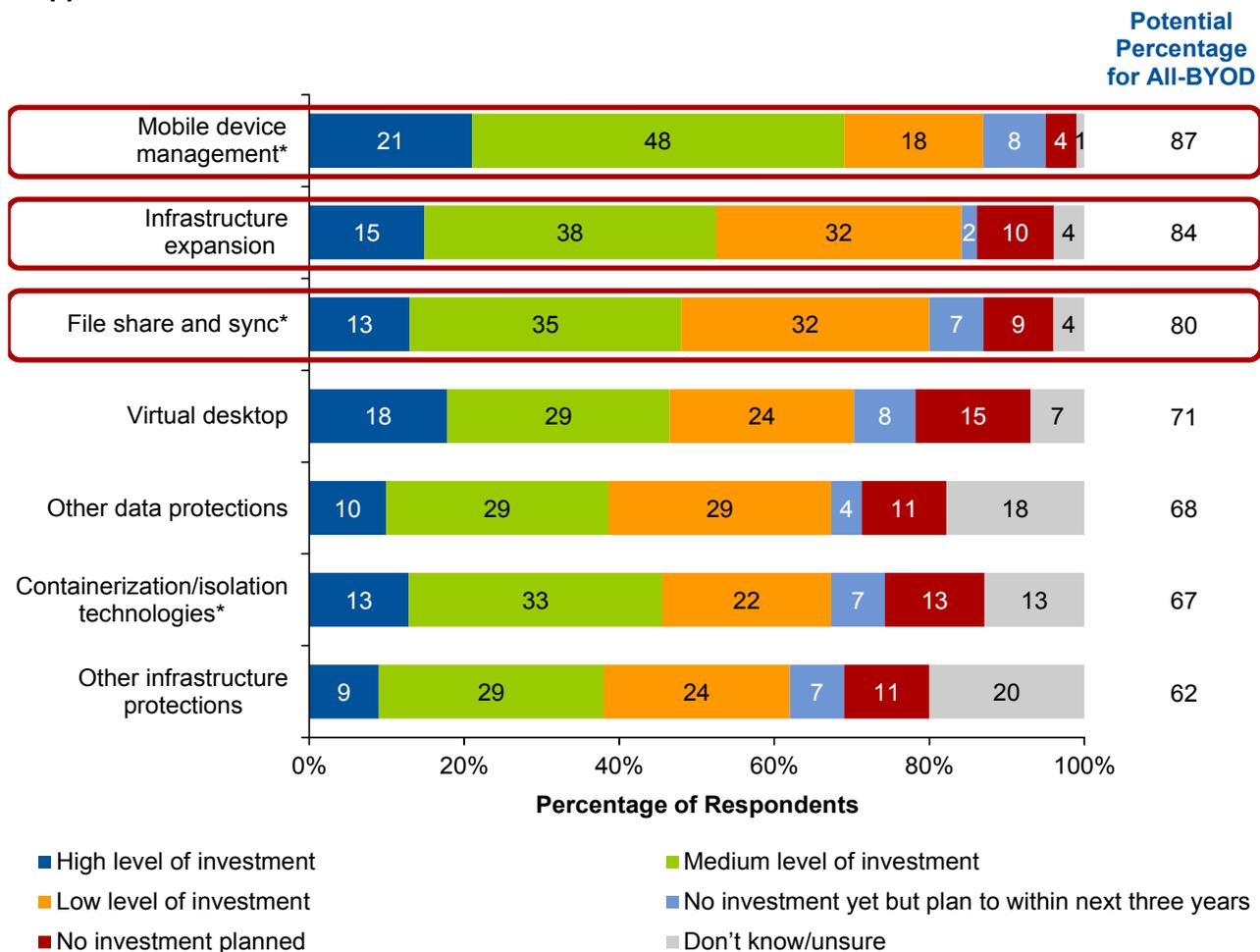
BYOD Requires IT and Business Units to Invest in Ongoing Policy Creation, Enterprise Mobility Management, Security and Infrastructure Expansion

One of the key reasons that BYO is not a simple cost reduction strategy is the fact that the costs of implementing a BYO program are substantial. Policies require continual vigilance and must be owned by a cross-functional team representing HR, the legal and risk departments and IT, with input from a variety of business units. Figure 9 shows that aggressive early adopters also report escalated investments in mobile device management/enterprise mobility management systems, as well as in intelligent infrastructure to support higher volumes of users and the higher load that new devices place on networks, all the while providing enhanced security protections (such as Wi-Fi expansion, authentication systems and network access control). For a discussion of this phenomenon, see "Solving BYOD's Impact on Communications Infrastructure."

Overall investments across all industries are strong, with the notable exception of government organizations, which currently tend to invest only in basic mobile device management capabilities.

Figure 9. Investments Made by Organizations That Actively Encourage BYOD (38% of Enterprises)

What level of investment is your organization making in the following key technologies to support BYO?

	High level of investment	Medium level of investment	Low level of investment	No investment yet but plan to within next three years	No investment planned	Don't know/unsure	Potential Percentage for All-BYOD
Mobile device management*	21	48	18	8	4	1	87
Infrastructure expansion	15	38	32	2	10	4	84
File share and sync*	13	35	32	7	9	4	80
Virtual desktop	18	29	24	8	15	7	71
Other data protections	10	29	29	4	11	18	68
Containerization/isolation technologies*	13	33	22	7	13	13	67
Other infrastructure protections	9	29	24	7	11	20	62

Percentage of Respondents

- ■ High level of investment
- ■ Medium level of investment
- ■ Low level of investment
- ■ No investment yet but plan to within next three years
- ■ No investment planned
- ■ Don't know/unsure

*elements of enterprise mobility management (EMM)
n = 135 who said their organization actively encourages BYOD

Source: Gartner (May 2014)

Enterprise file share and sync capabilities are an increasingly essential element of an overall mobile portfolio, as are containerization solutions that allow for enterprise-managed data and applications to be kept separate in various ways (see "Learn the Taxonomy of Mobile and Endpoint Management Architectures"). These two capabilities are increasingly considered part of the overall EMM function, extending beyond traditional mobile device management (MDM). Banks tend to invest at higher than average levels in these technologies.

Even though users report mixed results with virtual desktops on smaller handheld devices, organizations see this as a core part of the portfolio. Virtual desktops are a way to deliver a wide range of applications to remote devices in a secure fashion. However, organizations also report

issues with usability, application fidelity and offline use that make this solution less than ideal. In addition, it often drives higher costs in infrastructure and software, and forces a close look at application licensing (see "Minimize Licensing Costs for BYOD When Windows Client Is Included Under Microsoft Enterprise Agreement").

In the next several years, this suite of capabilities will rapidly converge into a more consistent approach for all endpoint devices via unified endpoint management (UEM). UEM is a consolidation of independent technologies formerly employed to manage mobile devices such as smartphones and tablet computers (on non-Windows x86 OS platforms), ruggedized devices and PC devices, such as laptops and desktops. UEM includes the technologies of MDM, EMM, hosted virtual desktop/virtual client management and client management tools.

This trend implies that over time, all devices will be managed more like smartphones than like traditional PCs. In this model, IT will assume that devices are untrusted and that the networks they operate over are untrusted, making even enterprise-owned devices appear more like BYO devices. So the investment in BYOD is a precursor for a greater change that is occurring in management strategies; early adopters are likely to be better prepared for this eventuality.

A Deeper Analysis of Cost Buckets

Hard, direct costs for BYOD can be broken down into the major categories shown in Table 1.

Table 1. Hard, Direct Costs for BYOD

SRAs	Application Costs	Management Tools and Infrastructure
Voice/data/text usage SRAs* Device SRAs Warranty plans Spare inventory	General-purpose tools* (e.g., file sharing and sync, office productivity tools, collaboration software and services) Organizational-specific applications*	Management, operations and security tools* (EMM/containers/app shielding) Virtual hosting infrastructure* Network coverage and capacity Network security protections User self-service and support systems Managed-service fees, if applicable
* Largest cost drivers SRAs = stipends, reimbursements and allowances		

Source: Gartner (May 2014)

Soft, indirect costs for BYOD can be broken down into the major categories shown in Table 2.

Table 2. Soft, Indirect Costs for BYOD

Administration	IT Operational Support	User Costs
Policy development and maintenance IT support training Enterprise awareness and communications	Service desk Level 2 support Planning and architecture	User training Personal administration Peer support Self-support Downtime

Source: Gartner (May 2014)

The costs listed above form the basis of a total-cost-of-ownership analysis for BYOD programs. There is overhead associated with every device, whether it is enterprise-supplied or BYO, and even if the company provides no cost offset to an individual user. Overheads often run between $100 and $200 in the United States, but costs vary widely. Organizations should use this model to produce a fully loaded cost for mobile devices, spanning both direct and indirect costs.

For smartphones in particular, carrier service fees are a substantial part of the cost. Globally, 22% of companies provide SRAs for business use of personal phones — but there are notable differences by region: 31% of Asia/Pacific companies and 26% of U.S. companies surveyed provide such SRAs, but only 14% of EMEA-based organizations do so. Partial allowances are typical: Under 10% of companies cover 100% of an employee's cost for a personal phone. As noted in "How to Manage Stipends, Reimbursements and Allowances for Employee-Owned Mobility," organizations have a mix of flat-rate — where all qualified users get the same amount — and multitiered plans that vary by organizational role.
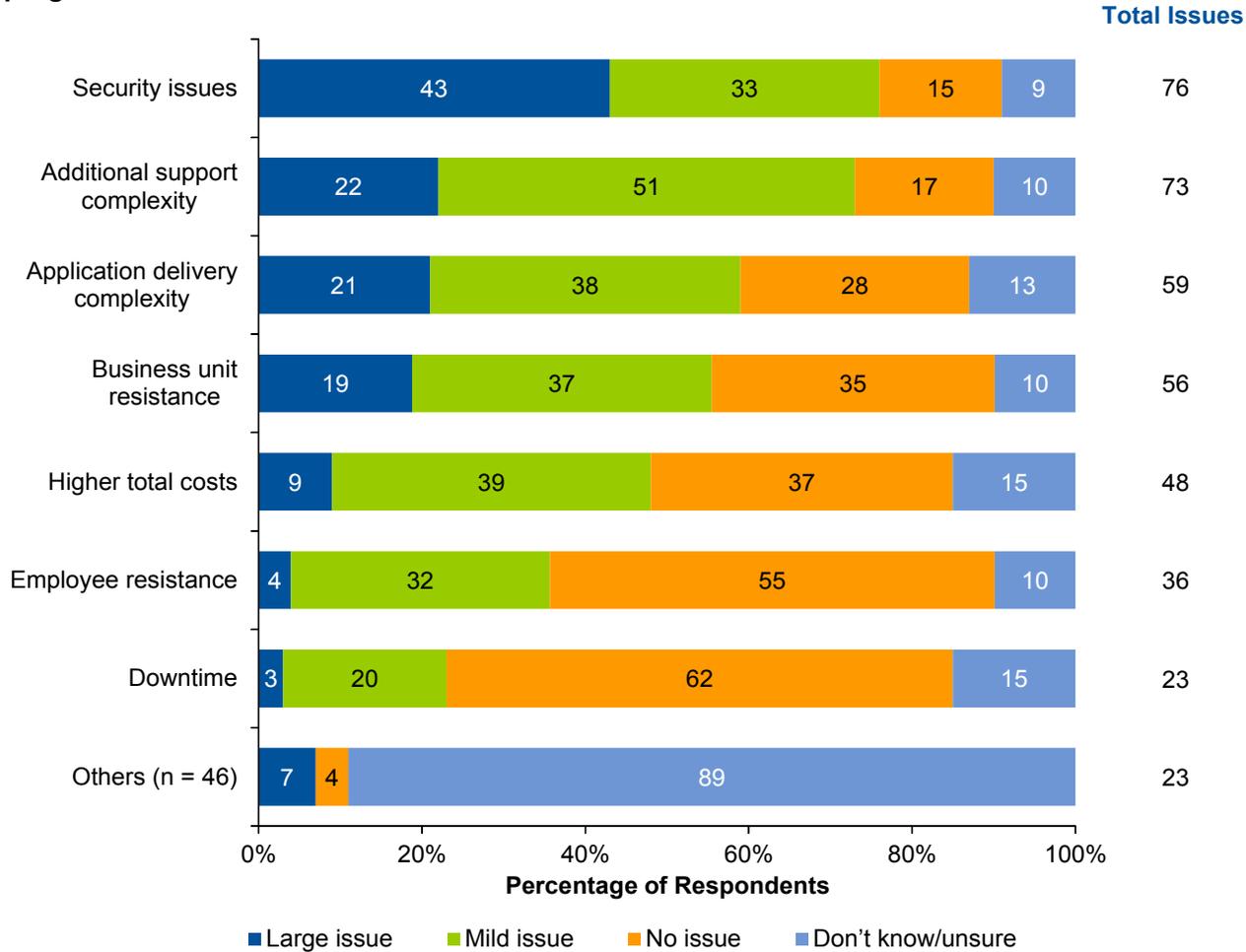
Many employees in the new class of mobile worker being enabled for the first time may have not used an app on their phones before. A substantial number of smartphone users, especially those using Android, use email and the mobile Web but do not download or use apps from the consumer app stores. This is one example of the communication and education challenge facing organizations looking to engage the broader workforce.

BYOD Increases Risks for CIOs and CISOs and Changes Expectations for Workforce Enablement

Security, support and application delivery complexity are the overarching issues for BYOD programs (see Figure 10). Over three-fourths of organizations cite security issues as the biggest concern, and with good reason: 23% of U.S.-based employees say they have experienced some compromise on their personal device in the past year (mostly with PC-based malware or hardware failures, but at least 5% of smartphone and tablet users report compromised credentials, device failure, and/or lost or stolen devices). The biggest risks for tablets and smartphones lie in data loss and theft, rather than malware. Investments in containerization and file sync and share are wise.

Figure 10. Issues With BYO Programs

**Have any of the following been an issue for your organization as a result of your BYOD program?**

Total Issues

Issue	Total Issues
Security issues	76
Additional support complexity	73
Application delivery complexity	59
Business unit resistance	56
Higher total costs	48
Employee resistance	36
Downtime	23
Others (n = 46)	23

Percentage of Respondents

■ Large issue ■ Mild issue ■ No issue ■ Don't know/unsure

n = 271

Source: Gartner (May 2014)

Beyond those factors, resistance from specific business units, most notably the legal and risk departments, HR, and line-of-business leaders, dominate the objections to BYOD (see Figure 11). Business units often object when the goals are not clearly understood or they see unwarranted risk. Gartner inquiries show a high concern among HR departments that are concerned about hourly or union workers being expected to respond at all hours, even when not technically on the clock. This is generally addressed by clearly issuing guidance to workers and their managers that employees are not expected to respond or even monitor enterprise systems after hours. A few explicitly shut down systems after hours to prevent it.

Figure 11. Business Units Show Most Resistance to BYO, Especially Legal/Risk and HR

**Has there been any resistance to the BYOD program at each of the following levels?**
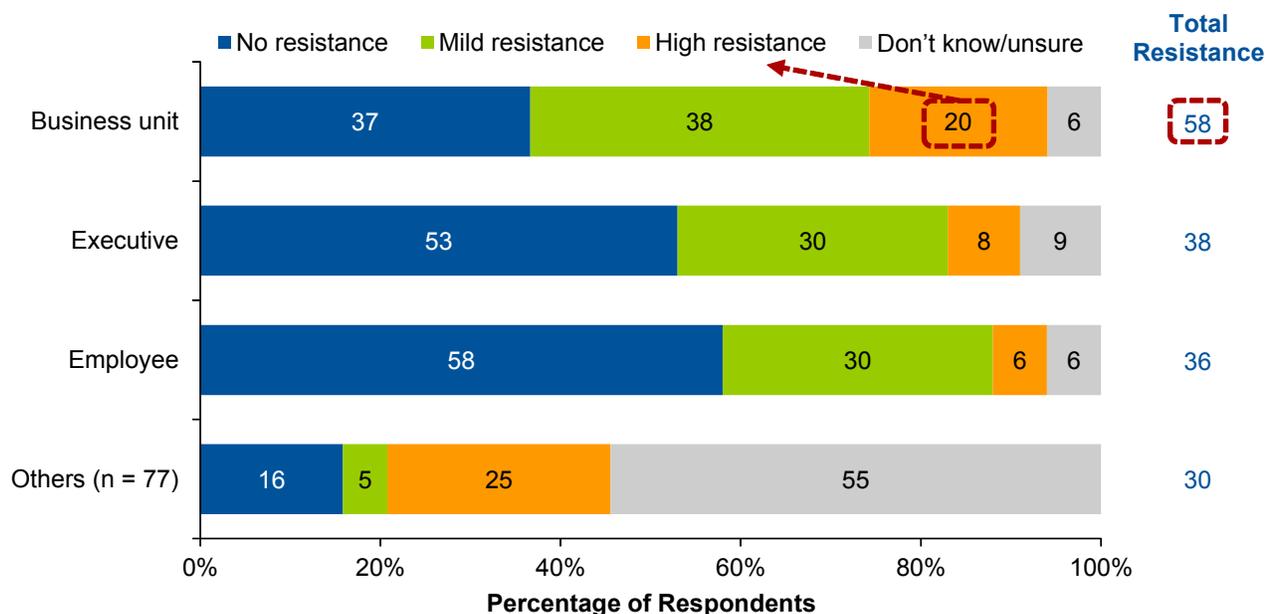
n = 271; base: has BOYD employees currently or in 2017 or in 2020

Source: Gartner (May 2014)

Likewise, legal and risk departments are concerned about the liabilities associated with data loss and theft that often occur on cloud-connected mobile devices. Some are concerned about the implied access to employee location and personal information. Organizations in Europe often cite regulatory or works council barriers to BYOD. Many, but not all, of these issues may be addressed through an explicit policy stating the employee's rights versus those of the employer. Technology solutions such as enterprise mobility management, secure enterprise file share and sync, and containerization play a role, as does periodic auditing, in mitigating these objections.

Surprisingly, we found only moderate objections from employees from the average organization. Those with highly mature programs acknowledge that there is a small percentage of employees who do not want to use a personal device in business, for whom they take other measures (such as low-cost EL devices or providing traditional PC-only access to applications). The top objection from employees, when it exists, is the perception of cost shifting; the second concern is how their personal privacy will be protected (see Figure 12).

What are the main reasons for the issues around employee resistance?
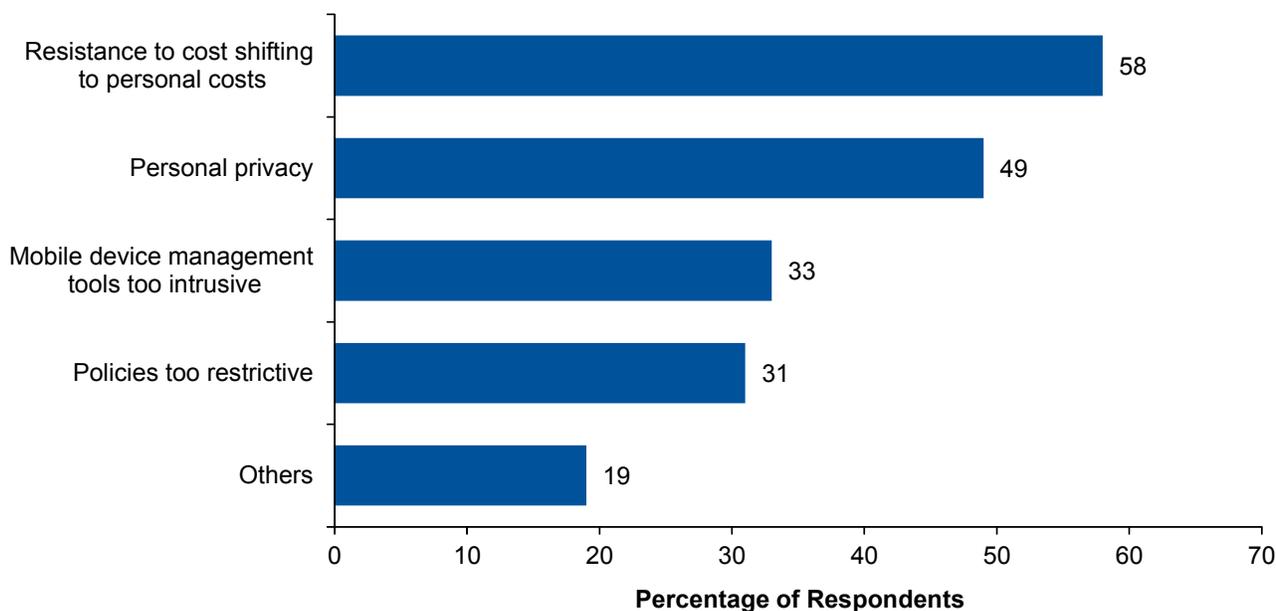
n = 84; base: high resistance to BYOD program
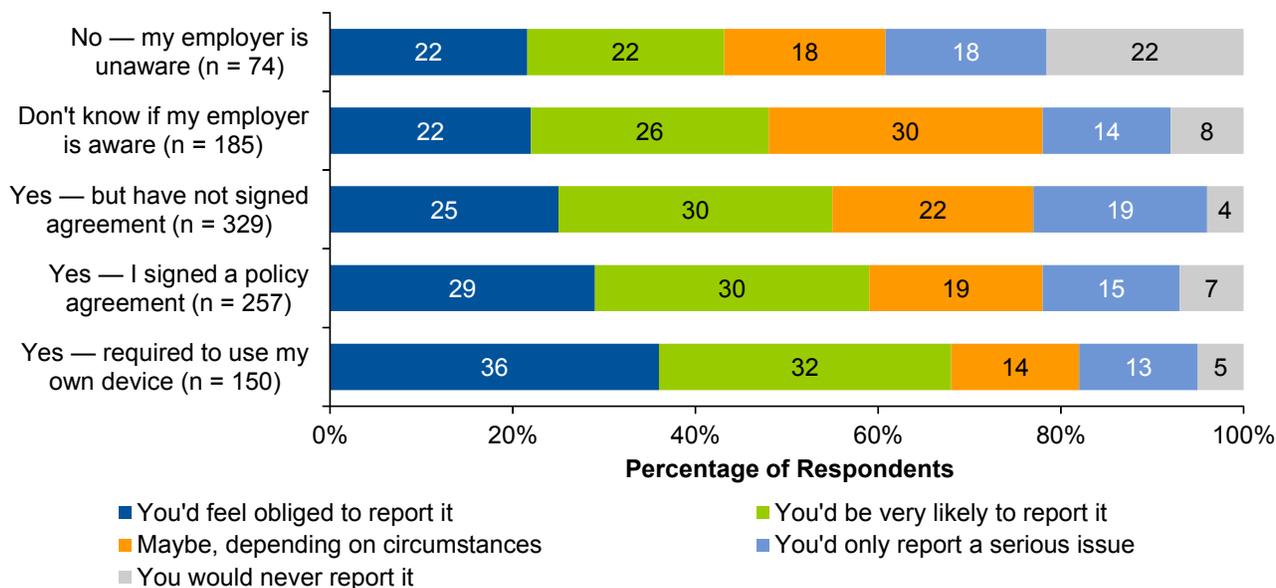
Source: Gartner (May 2014)

Employers see some resistance from certain employees, mostly mild; only 6% of organizations report strong objections from staff. Those objections center around cost shifting, personal privacy, and invasive tools and policies. The highest rate of employee resistance is found in the Asia/Pacific region, where 17% of companies report high employee concerns. Organizations in any geography should provide fair SRAs, at least in line with common practices in the region, and should be explicit in their protections of employee privacy (or directly assert their rights to personal information, such as location). For more on employee objections to BYOD, see "Employee Attitudes Toward Bring Your Own Device."

Policy Awareness Is Crucial

As shown in Figure 13, when the employer is unaware of business use of a personal device, the employee is much less likely to report problems.

Figure 13. Employees Who Know the Policy Are Most Likely to Report Issues

Would you tell your employer if a personal device you used for work purposes was hacked or lost or had a virus?

n = 995
Data is from "Survey Analysis: What IT Leaders Need to Know About Employee BYOD Attitudes in the U.S."

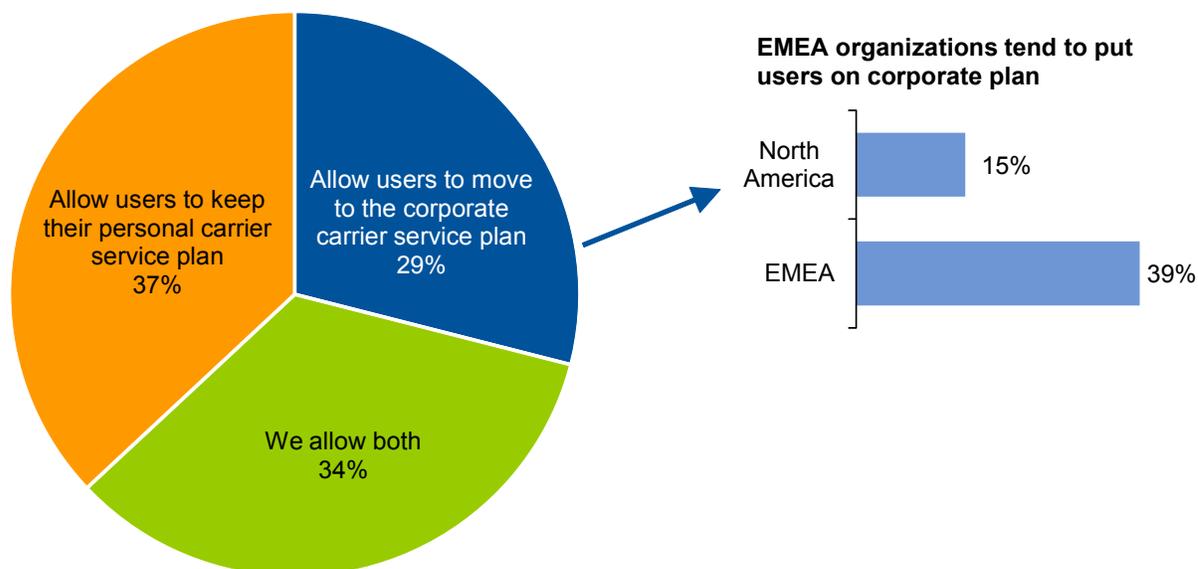Source: Gartner (May 2014)

Guiding User Device Choices

Over half of organizations that have BYO programs for smartphones or tablets provide a recommended/supported list to the employee. We see this as a key best practice, following Gartner's managed-diversity model (see "Managed Diversity Defines Best Practices for BYOD and Endpoint Management Policies").

Carrier Service Plan or Employee Plan?

A consideration is whether the BYO smartphone users are allowed to use their own plans, for which the organization typically provides only a partial cost offset, or whether they are put on the corporate plan (see Figure 14). In many cases, using the corporate plan increases the organization's purchasing power, allowing it to get better rates than an individual consumer. However, it typically means the organization will cover all service fees for the individual, whereas BYO allows cost sharing with the employee. Another complicating factor is ownership of the business number. Very few organizations, and few individuals for that matter, want to put their personal number on a company business card; corporate plans make this easier. However, enterprise-issued virtual numbers can be applied to a personally owned number when the employee holds the carrier contract.

Figure 14. Carrier Service Plan Ownership Strategies Are Mixed, but Regional Differences Are Strong

For your BYOD phone users, which of the following does your organization allow?

n = 111; base: provide reimbursement for standard mobile phone/smartphone
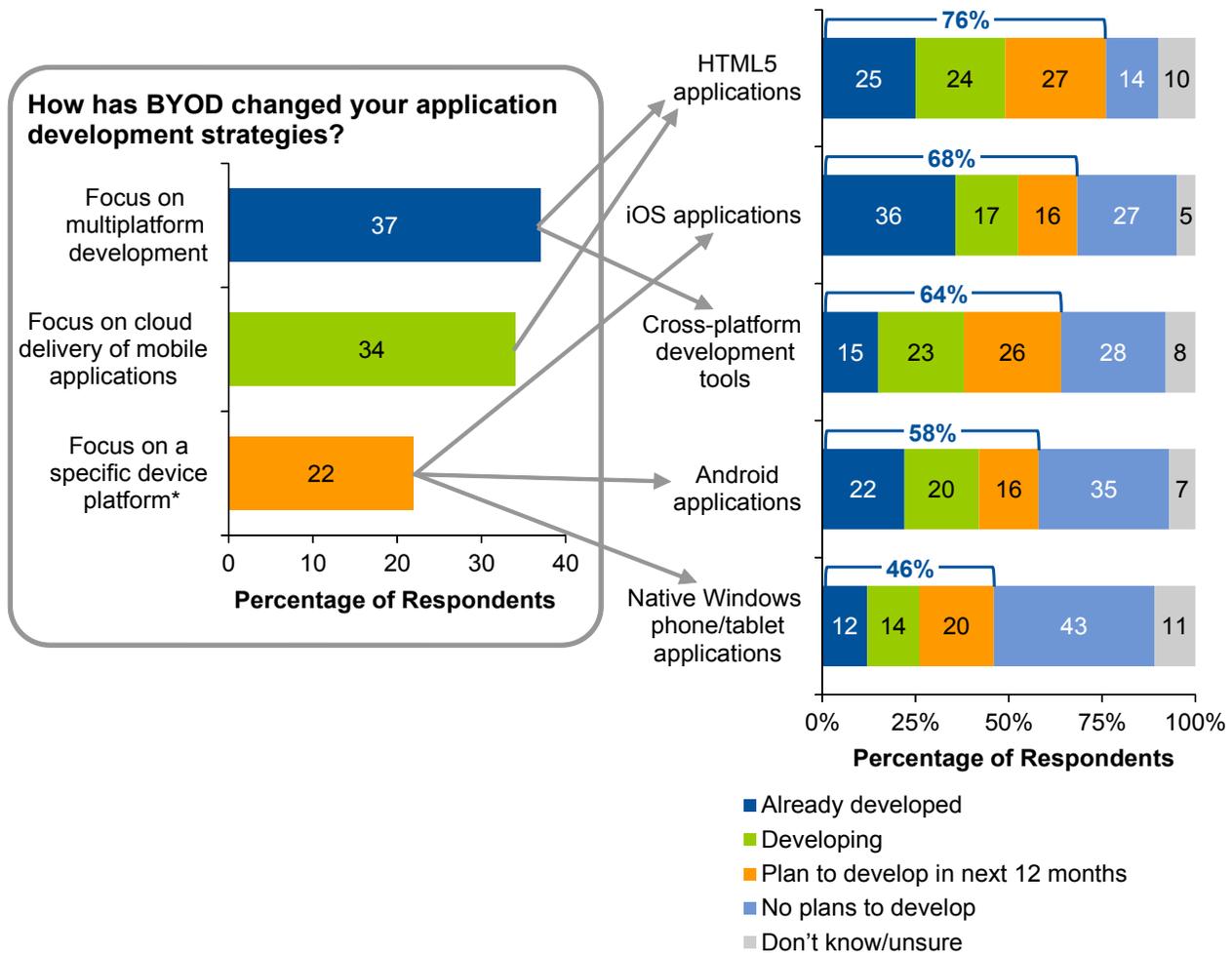
Source: Gartner (May 2014)

Organizations are fairly evenly split on their approach to carrier service plans, according to worldwide averages. However, regional differences are notable: 85% of U.S. organizations either use the employee's plan by default or give the employee the option; in contrast, nearly 40% of EMEA organizations keep the user on the corporate plan. We believe that global carriers are generally unprepared in their billing systems to deal with BYOD as many enterprises would like to see them structured. More has to be done by the carrier community to support increased billing flexibility.

Application Development Choices

Application developers have a different set of concerns with aggressive BYO organizations than with traditional development: more users and more device types. BYO simultaneously increases the number of employees who have access via mobile devices *and* increases the number of platforms likely to be seen in the enterprise (see Figure 15). The payoff for taking on this complexity is in more application opportunities to leverage mobility across the broader workforce.

Figure 15. Device Diversity With BYO Changes App Development and Procurement Strategies

What stage of development is your organization in for each environment below?

How has BYOD changed your application development strategies?

Focus on multiplatform development: 37

Focus on cloud delivery of mobile applications: 34

Focus on a specific device platform*: 22

Percentage of Respondents

HTML5 applications — 76% — 25 / 24 / 27 / 14 / 10

iOS applications — 68% — 36 / 17 / 16 / 27 / 5

Cross-platform development tools — 64% — 15 / 23 / 26 / 28 / 8

Android applications — 58% — 22 / 20 / 16 / 35 / 7

Native Windows phone/tablet applications — 46% — 12 / 14 / 20 / 43 / 11

Percentage of Respondents

- Already developed
- Developing
- Plan to develop in next 12 months
- No plans to develop
- Don't know/unsure

* If using a specific platform, it is most likely to be iOS, but Android gap is narrowing
n = 271

Source: Gartner (May 2014)

In general, the strategic answer lies in a focus on multiplatform development. In specifics, however, we see different tactics in play. If organizations choose a single platform to serve natively, it is most likely to be iOS; however, the gap with Android is closing, and we have seen an uptick in native Windows phone and tablet development, especially among very large organizations. Organizations are investing for the longer term in HTML5 for employee-facing applications, a trend that is especially strong in the Asia/Pacific region.

It is notable that this change toward device-agnostic and/or multiplatform development strategies also applies to commercial apps used by the enterprise; increasingly, we believe that buyers will seek apps that work on multiple device families.

Device Choice Is Here to Stay

Even among organizations that resist or outright ban the use of personal devices in the workplace, the trend toward offering a wider device choice remains strong. Employees expect to have a greater say in the equipment they use at work. Today, the discussion is about smartphones and tablets; tomorrow, the focus may be on personal wearables, an employee's connected objects and other emerging smart technologies. Those that can overcome the complexities will see greater opportunities to enable the mobile workforce.

Acronym Key and Glossary Terms

BYOD	bring your own device
EL	enterprise-liable
EMM	enterprise mobility management
MDM	mobile device management
SRAs	stipends, reimbursements and allowances
UEM	unified endpoint management

Gartner Recommended Reading

Some documents may not be available as part of your current Gartner subscription.

"Managed Diversity Defines Best Practices for BYOD and Endpoint Management Policies"

"Employee Attitudes Toward Bring Your Own Device"

"Survey Analysis: What IT Leaders Need to Know About Employee BYOD Attitudes in the U.S."

"How to Manage Stipends, Reimbursements and Allowances for Employee-Owned Mobility"

"Magic Quadrant for Mobile Device Management Software"

"MarketScope for Enterprise File Synchronization and Sharing"

"Learn the Taxonomy of Mobile and Endpoint Management Architectures"

"BYOD Mobile Device Policy Template"

"Magic Quadrant for Mobile Application Development Platforms"

"Solving BYOD's Impact on Communications Infrastructure"

Evidence

A majority of the data cited was gathered in February 2014 from 355 members of the Gartner Research Circle, who represent IT leaders in a wide variety of companies and governments worldwide. Several supplemental studies were also used, including: "Survey Analysis: What IT Leaders Need to Know About Employee BYOD Attitudes in the U.S.," a research survey conducted in December 2013 involving a representative sample of 995 self-reported BYOD users in the United States; and "Employee Attitudes Toward Bring Your Own Device," a survey in August 2013 of 1,088 knowledge workers who use personal computing devices for work-related purposes.

GARTNER HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
USA
+1 203 964 0096

Regional Headquarters
AUSTRALIA
BRAZIL
JAPAN
UNITED KINGDOM

For a complete list of worldwide locations,
visit http://www.gartner.com/technology/about.jsp