Managing applications in the age of BYOA:

Reclaiming IT's strategic role

Part of the IT Management Research Series

LogMeIn

Managing applications in the age of BYOA:
Reclaiming IT's strategic role.

Many IT organizations stand at an important crossroads that will define whether they become a part of the important strategic conversations of our time, or become relegated to the sidelines. Several forces have come together to create this pivotal moment including: the exponential use of personal devices for business purposes, rising levels of business data rapidly flowing into the cloud, and applications brought in and managed by employees themselves in ever-increasing numbers. All of these forces have combined to create an environment where IT professionals feel the reins slipping out of their hands.

The rise of devices, data and apps represent a fundamental shift in consumer behavior that is fueling this "Consumerization" of IT. Consumers are now independent, universally connected users of technology who no longer feel the need to ask permission to introduce new technologies into business environments. We first saw evidence of this with the sweeping trend of BYOD or "Bring Your Own Device." Employees brought their personal smartphones or tablets into work for business use and IT had to adapt their infrastructure to accommodate this trend.

We are also seeing another wave of challenges for IT professionals in the form of BYOA or "Bring Your Own Application." Non-IT employees are now driving the adoption and management of applications, often leaving IT out of the equation altogether. So while BYOD was the first sign that the lines between personal and business technology were beginning to blur, BYOA has made those lines almost indistinguishable.

It is essential if IT professionals are to reclaim their strategic relevance to understand the significance of these trends and collaboratively work with business partners to provide the capability to manage their devices, data and apps while maintaining the integrity and security of their IT environment. In this spirit, LogMeIn set out to understand these trends in a major three part IT Management Research Series. The studies will provide guidance for IT professionals on how they can reclaim their seat at the strategy table in three key ways; by effectively managing applications, devices and data.

This first study focuses on applications, and how BYOA has become both a challenge and a blind spot for many IT professionals. It addresses important questions related to how IT professionals should manage apps in this new age of BYOA. Specifically, should BYOA be viewed as a passing, short-lived trend and ignored, or accept that BYOA is only the start of much larger IT challenges and invest now to find the best way to manage it?

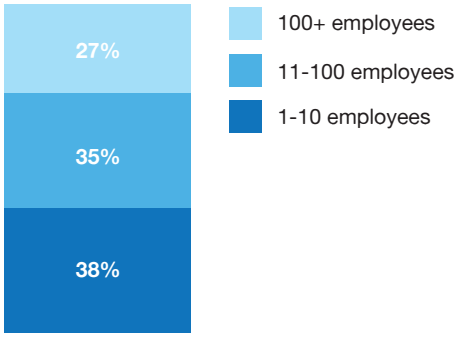
Methodology

This survey is part of a series of major research studies conducted by LogMeIn that focus on the state of IT management in today's world of independent, "BYO" consumers. The series focus on three key areas: managing applications, managing devices and managing data.

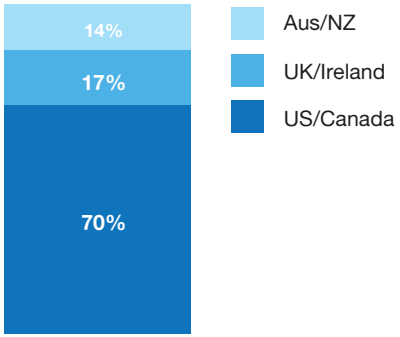
For this study, we explore usage and adoption of employee-introduced applications within companies worldwide and how this has led to a loss of control for IT managers. We partnered with Edge Strategies to survey IT and non-IT professionals across the world in various-sized organizations.

Field Dates: November–December 2013
Method: Online Survey
Segment profile: This part of the series focuses on Internal IT and Non-IT respondents across the globe (419 total respondents)
Total Survey Base: 1,390 IIT, OIT, and Non-IT respondents in six countries: US, Canada, UK, Ireland, Australia and New Zealand.

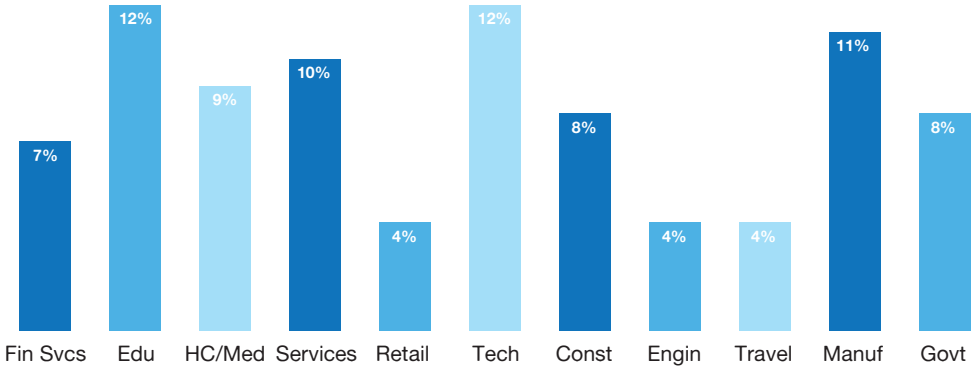
Company Size



Region



Industries (IIT Only)



Summary

BYOA is here to stay.

70% of organizations have some presence of BYOA and it's a trend that is only going to increase.

IT significantly underestimates the scale of BYOA.

IT professionals in this global survey estimated they have, on average, 2.8 applications that were brought into the organization by employees. But LogMeIn data based on companies analyzed in the past 6 months shows the average to be closer to 21 apps—more than 7X what IT estimates.

Consumerization of Apps is accelerating.

Employees are bringing in their own applications in the first place because they're unhappy with solutions provided by IT. More than 64% of the time, applications are brought in by employees when a solution already exists.

IT is out of the loop.

More importantly, employees are consulting IT less than half the time when choosing these applications. Then, even after IT endorses these employee-introduced applications, IT is rarely involved in provisioning or managing them.

Security risks are inconsistently managed—if at all.

IT professionals acknowledge that BYOA poses huge security risks, and takes some of the control for technology out of their hands, but many are not actively working to address the problem; only 38% currently have a policy in place.

Active employee engagement can help.

There are many positive things that can come out of allowing employees to introduce applications if properly managed. Apps brought in by employees tend to be more user-friendly, mobile-friendly, and better suited for collaboration.

IT has the ability to choose its role.

IT professionals can decide what role they want to play. They can act as gatekeepers and restrict app adoption, act as passive observers and let the adoption happen without their involvement—or IT can act as strategic facilitators, managing and shaping the adoption and direction of the growing BYOA trend.


The realities
of BYOA

IT severely underestimates the impact of BYOA.

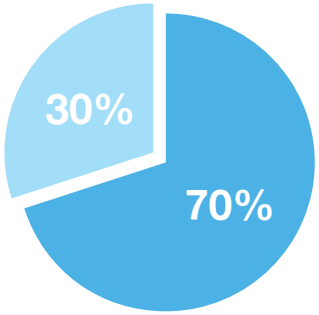
7X more apps coming into the workplace than IT estimates.

When asked about the presence of apps that were brought into their organization by users, 70% of IT professionals indicated there was a least one example of BYOA. But because IT is not always aware of BYOA, the number of organizations with some presence of employee-introduced apps is likely even higher—meaning it's basically everywhere now.

This trend is particularly pronounced in SMBs (11-100 employees)—81% said they have a BYOA presence. And it's not just an issue for the U.S. as organizations worldwide have indicated they're experiencing this trend too, with over 60% of organizations in UK/Ireland and over 70% in Australia/New Zealand having some presence of BYOA.

One area we're seeing a huge hole is IT's lack of awareness to the sheer volume of apps being brought in. IT professionals in this study indicated that on average they estimate 2.8 apps per organization are brought in by employees. However, based on data LogMeIn has collected through app discovery with customers, this number is far closer to 21 apps—a staggering 7X more.

There is an enormous IT disconnect around the scale of BYOA



Percentage of organizations with presence of BYOA

Percentage of organizations without presence of BYOA

Average # of apps IT estimates to be brought in by employees

Actual # of apps non-IT users bring into organizations[1]

takeaway:

If you don't believe BYOA is happening at your organization, than you're either tragically unaware of what's really going on, or you're part of the very rare organization that's in the minority.

Base: IIT only
LogMeIn App Discovery usage data[1]

People are not consulting IT anymore. They are just bringing in a device and expecting us to support it. This is something organizations do need to adapt to and be more agile.

— IT manager, Services industry, 2,500+ employees

Why IT needs to pay attention now.

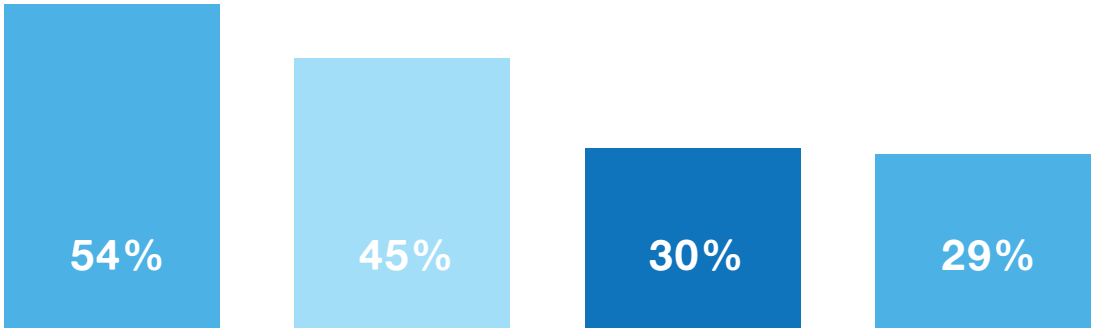
BYOA can pose huge security threats if not properly managed.

So why does it even matter if BYOA is so widespread? Because most IT professionals know that bringing apps into the workplace without consulting IT exponentially increases your security risks.

When asked which issues limit their company's adoption or support of BYOA, more than half (54%) point to concerns around data security, and 45% cite a lack of control/management of apps.

When IT loses management control of apps, they can no longer monitor which apps pose security threats, or appropriately integrate new apps with existing ones. Some IT professionals also point to data compliance requirements as a potential issue that can arise when BYOA goes unchecked.

Top issues limiting adoption and support of BYOA



takeaway:

IT pros who know about employee-introduced apps but don't take steps to manage them may face huge security and other threats that could ultimately damage their organization.

Which of the following (if any) limit your company's adoption of – or support for – employee introduced applications?
Base: IIT only

The reliance on such BYO apps makes me a bit nervous as the office IT pro because important company information is held in such apps and IT has no control over the security of that information.

— IT manager, Non-profit, 10-25 employees

Things are only going to get worse.

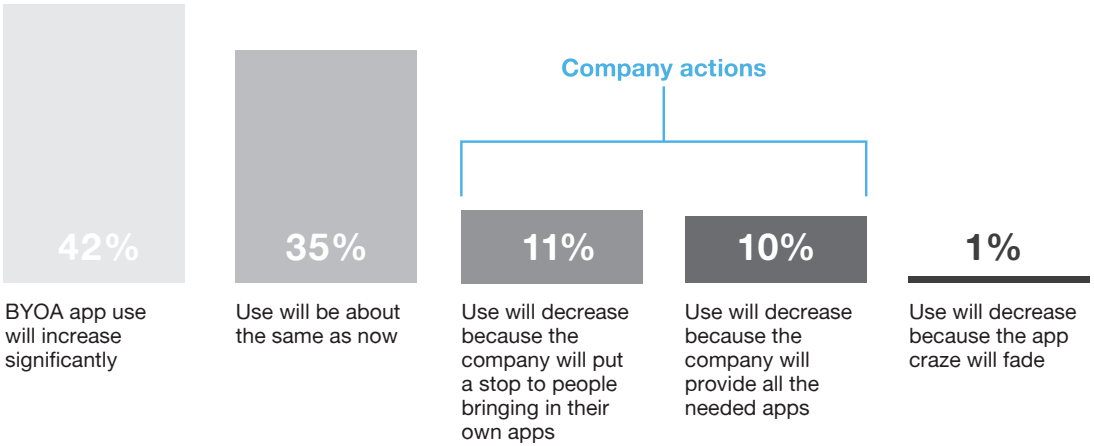
Over 40% say BYOA will significantly increase.

If we knew for sure that BYOA was going to wind down a year from now, it wouldn't be much cause for concern. But the fact is, IT professionals see this as a trend that will, at the bare minimum, stay the same (35%), but more likely significantly increase (42%).

On the flip side, those who feel the trend will go away only think that will happen based on a company's actions. 21% see BYOA decreasing because a company puts a stop to outside apps or provides all the apps needed. Just a small fraction (1%) see a decrease coming because the app craze fades away.

In short, no one sees anything stopping users from bringing in the apps they want to use other than companies taking major actions.

Changes in BYOA trend over next 5 years



takeaway:

Ignoring BYOA will not make it go away. IT pros need to make the shift now to the tools and processes that help manage this new way of doing business.

How do you believe that employee use of BYO apps will change over the next five years?
Base: IIT only

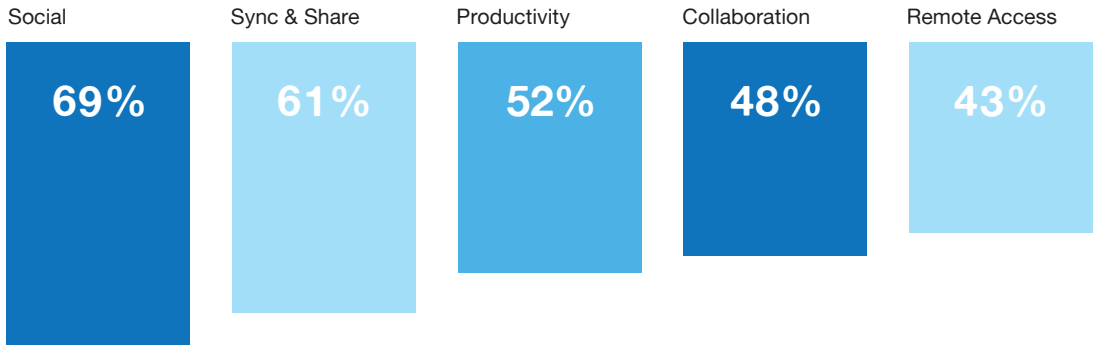
BYOA is happening across all application types.

What's worse, the "Dropbox problem" is spreading.

This study found that for all of the major types of applications being used by employees, many were originally employee-introduced.

We've all heard horror stories related to Dropbox usage in the workplace, but what's most troubling is that the influx of employee-introduced sync and share apps isn't shrinking. And with many employees using Dropbox for personal reasons on company-owned devices, the security risks are even greater.

Percentage of times applications were brought in by employees



takeaway:

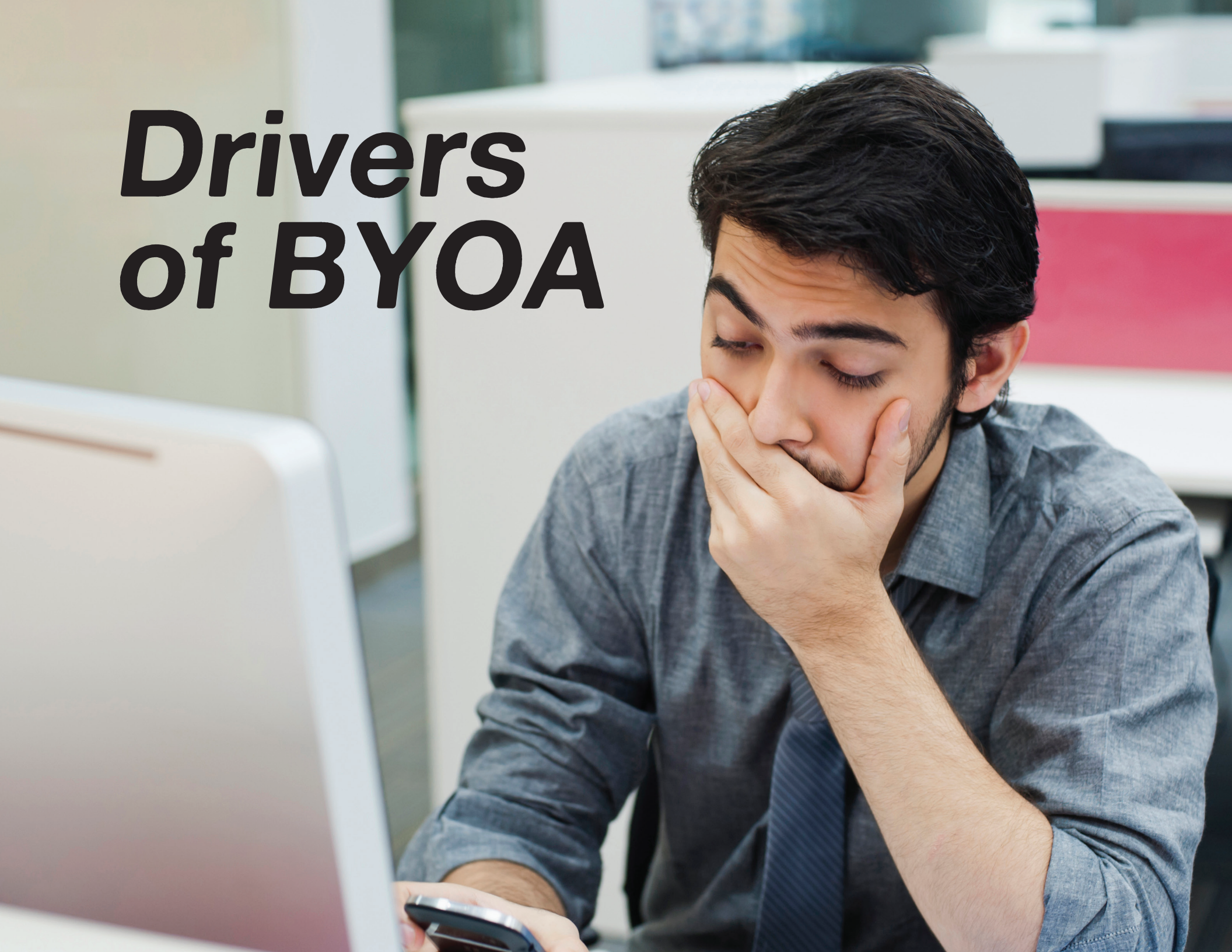
IT can't afford to sit idly by, and needs to pay serious attention to employee-introduced sync and share apps.

How were each of these applications brought into your company?
Base = IIT only Companies with employees using BYO application; DK answers excluded

It’s become a bit of the ‘wild west’ with regards to everyone using a different application, and application provider.

— IT manager, Construction, 501-1000 employees

Drivers of BYOA

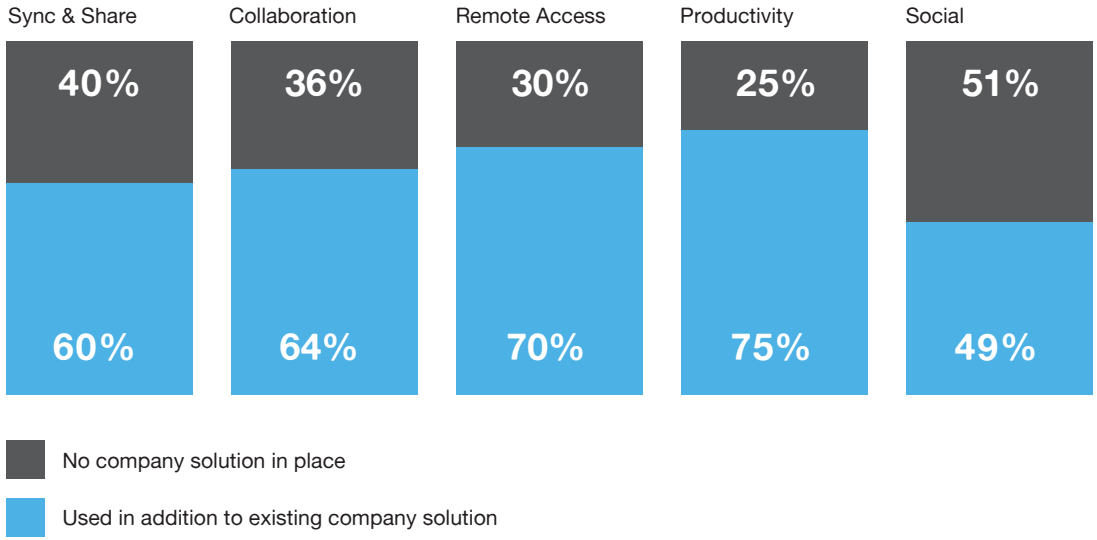


Employees just aren't happy with what they're given.

More than half of the time, BYOA duplicates an existing solution.

One of the harsh realities of BYOA is that many of the apps employees are bringing into the workplace already have a similar solution available. That means they simply don't like the tools IT provided—for productivity apps in particular, this happens 75% of the time. Only 25% of the time do employees bring in a productivity app because there wasn't already a solution in place.

These numbers send a clear message to IT pros about how empowered employees feel. IT can implement what they believe to be high-quality solutions, but that won't stop their employees from bringing in the apps they prefer.



takeaway:

Whether or not IT has provided apps for sync & share, collaboration, remote access and other functions, employees will always find and bring in a solutions they like more.

Are the BYO apps filling a gap (i.e., there was no solution in place) or being used in addition to existing tech/apps?
Base = IIT only, Companies with employees using BYO application; DK answers excluded

There is more need for solutions that can be used on an ad-hoc basis, quick to set up, low cost, etc., so that BYO solutions become more attractive especially where IT solutions become a roadblock.

— IT manager, Internet/web business, 5 employees

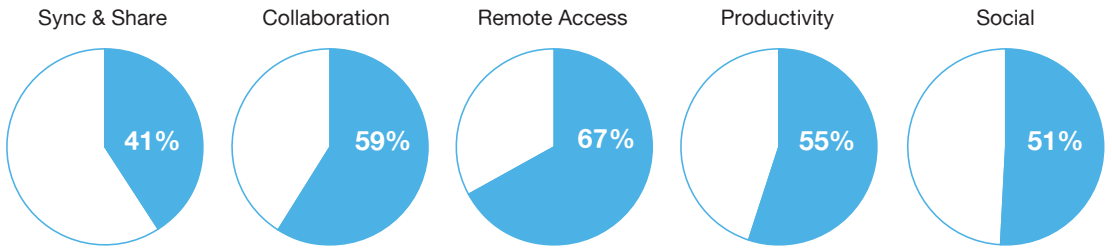
Employees lead, IT follows.

Of the apps introduced by employees, half the time they are later adopted by IT.

While apps brought in by employees can pose problems if not properly managed, these apps are often better than the original solution provided by the organization. In many cases, IT pros evaluate employee-introduced apps and then decide they're worth implementing company-wide. In fact, these BYO apps are often embraced and implemented more than a quarter of the time, including 67% of remote access apps and 59% of collaboration apps.

What these numbers point to is a significant shift in the app adoption process. We're no longer seeing IT as the sole decision-makers—the process is now driven by employees, with IT following their lead.

Originally introduced by individual employees, but now adopted/endorsed by the company



takeaway:

IT is already embracing employee-introduced apps but they need the flexibility to more openly adopt apps they didn't choose.

How were each of these applications brought into your company?
Base = IIT only Companies with employees using BYO application; DK answers excluded

BYO is both an asset and a liability. The liability part comes from company IP being on systems that the company can't directly manage. The asset part comes from employees organically self-discovering and introducing apps and use cases that might not have otherwise come onto the radar of the IT team.

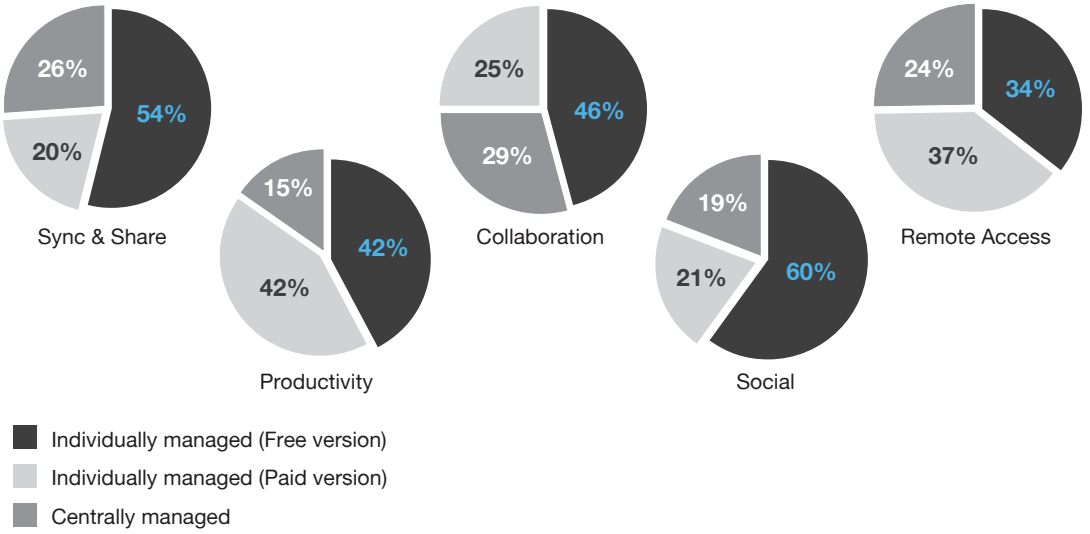
— IT manager, Marketing/advertising, 51-100 employees

Even after adoption, IT isn't fully in control.

Only 15-26% of apps are being centrally managed.

Even after IT pros endorse employee-introduced apps they're not always in complete control after they've been adopted. As shown here, only a very small percentage of apps brought into organizations become centrally managed. Only 26% of sync and share apps are centrally managed, with the rest being managed by individual employees, often as part of a free account.

So what does this mean? Major management problems for IT. While free versions alleviate some of the cost, the flood of individual versions (both free and paid) prevent IT from managing these apps. That makes the previously mentioned "Dropbox problem" that much more problematic, and the potential for security risks to grow by leaps and bounds.



takeaway:

Individually managed free and paid apps can be great for employees but a nightmare for IT.

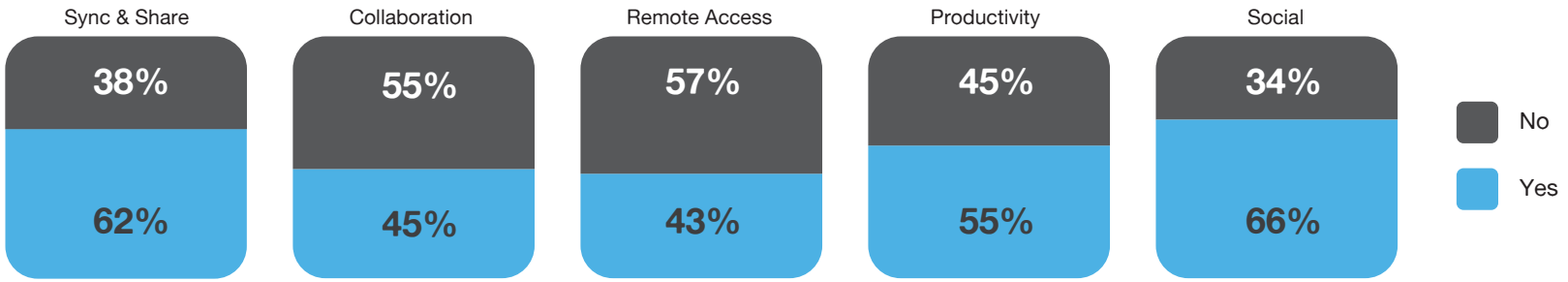
Since it is now endorsed by the company, are your employees primarily using the free, paid or business versions?
Base = IIT only Companies that have adopted BYO application; DK answers excluded

Employees won’t stop bringing in new apps.

More than half the time they continue to bring in more.

Adopting an employee-introduced app ends any struggles with BYOA, right? Wrong. IT pros admit that even after implementing the apps employees want, it won’t stop them from bringing in even more apps to meet their needs. Then it becomes a never-ending cycle of employees finding new apps, IT adopting some of them, and then employees finding a better, newer app, and so on and so on.

Do employees continue to use their own apps in addition to the IT-provided solution?



takeaway:

IT pros need a clear plan on how to continually manage BYOA.

For those categories where your company has either adopted an employee-introduced app or provided the app/solution itself, do employees continue to use their own apps in addition to the established solution?
Base = IIT Only Companies that have adopted BYO application or provided a company solution; DK answers excluded

Generally, the more options that are available, the more the employees turn to the various options. The PROBLEM is the fragmentation. One employee will insist on trying something via 1 app, and another employee will use another app entirely. It's become a nightmare.

— IT manager, Construction, 500-1000 employees

The diminishing role of IT

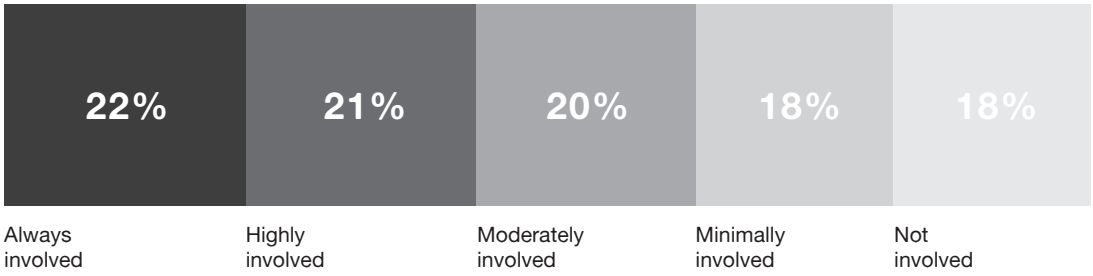
IT admits they are not focused on apps.

56% of the time they are moderately, minimally or not involved.

No IT professional wants to admit they're not controlling the technology decisions within their organization. When asked how involved they are in certain IT activities, they often overstate their roles.

But what's more surprising is how openly IT pros admit their lack of involvement in selecting apps. They claim to be involved only 43% of the time, not involved at all 18% of the time and minimally or moderately involved 38% of the time.

How involved are you or the others in your IT department in the selection of new cloud or SaaS apps today?



takeaway:

IT accepts the fact that employees are driving app decisions. But now they need to figure out how to manage those apps.

How involved are you or others in your IT department in the selection of new cloud or SaaS apps today?
Base = IIT only

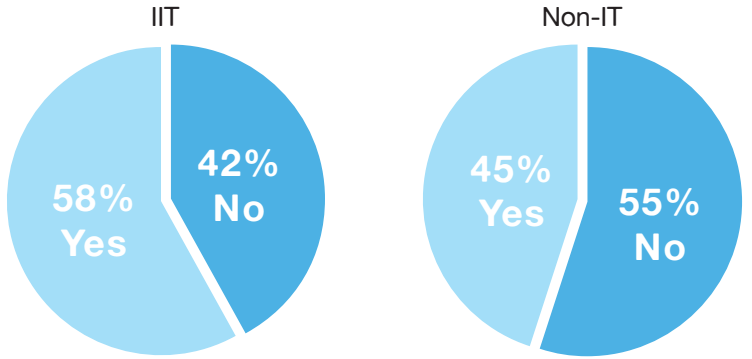
Non-IT employees are going rogue.

They only consult IT 45% of the time.

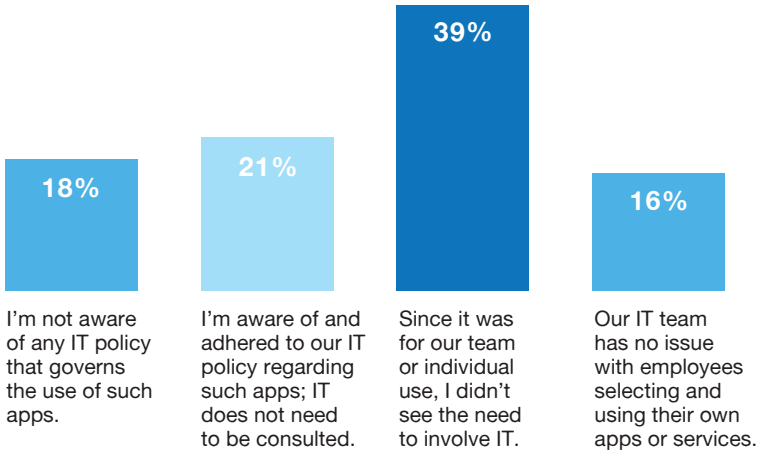
When asked if they're consulted on the decision to use sync and share apps, IT admits they're only consulted 58% of the time. When you ask the actual people who would do the "consulting" (i.e.: non-IT professionals), the real number shows to be even smaller—just 45%. This shows a disconnect between the two groups, but more importantly, points out that no matter who you ask, IT is involved only roughly half of the time.

The number 1 reason they don't involve IT? 39% don't see a reason to consult IT if they're using an app for individual or team use.

Was IT consulted on the decision to use BYO sync & share apps?



Which statement best describes why you did not involve IT in your decision to use sync & share apps?



takeaway:

It's impossible for IT to insert themselves into the entire process, but they can learn to manage the influx of apps brought in by non-IT employees.

Base = IIT and Non-IT users sync & share only

The main factor against BYOA is the fragmentation and loss of company records. Main attractors seem to be the cool factor and desire to do it differently for the sake of it.

— IT manager, Government, 250-500 employees

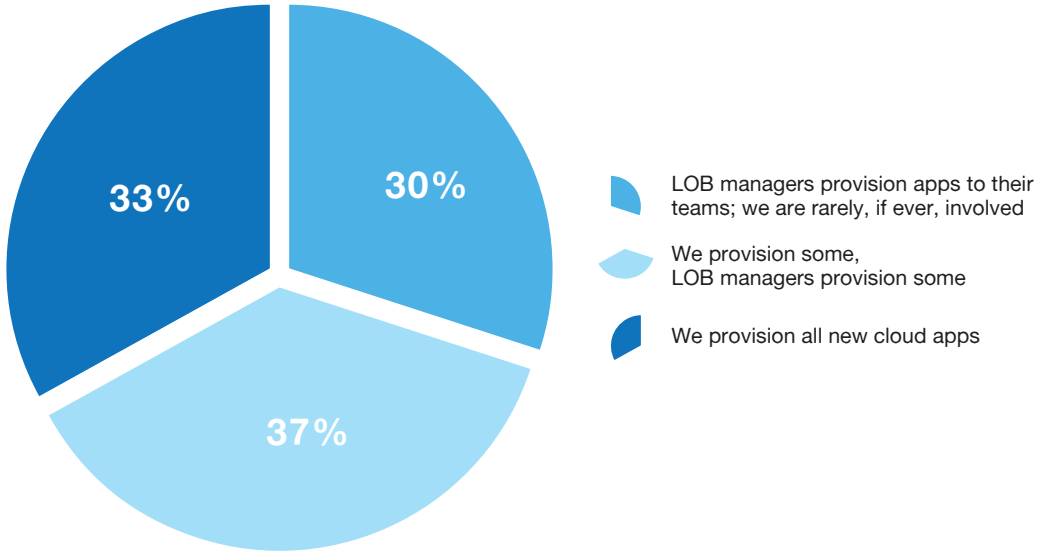
IT isn't even always involved with provisioning.

30% of the time LOB provisions on their own.

Even if IT was ok with employees bringing apps into an organization, you'd think they would want to be involved in provisioning the apps. That's not always the case. The bold truth is that line of business (LOB) managers are involved more often than IT managers in the process—67% of the time. What's more, 30% of the time LOB managers provision apps on their own, with zero involvement from IT.

The really scary part? While the IT department may know an app exists, they don't know who has the app or how they're using it. Which only worsens the major security risks and lack of control for IT.

What is IT's role in provisioning new cloud apps?



takeaway:

IT pros need to seek out tools that aid in the management and provisioning of apps so they're always in control.

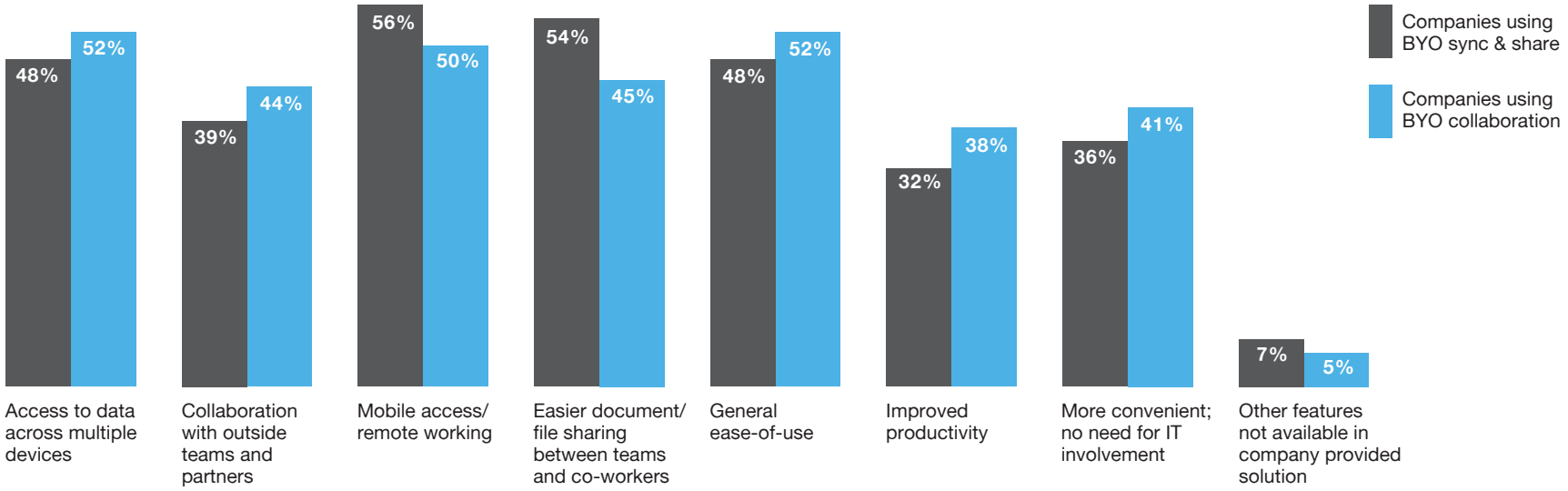
Base = IIT pros only, DK excluded

Reclaiming IT control

IT can see the positive side of BYOA.

Helps employees find easy-to-use and mobile-friendly apps.

Surprisingly, IT pros can point to many factors that drive employees to bring in their own apps. These vary by type of application, but the most important tend to be ease of use and greater mobile access/remote working capabilities. The fact that these are major drivers of BYOA tells us that many IT departments aren't delivering easy-to-use solutions, or ones that are mobile-friendly for today's on-the-go employees.



takeaway:

BYOA has many positive benefits for employees but IT needs to properly manage it to avoid the negatives.

Which of the following describes why employees have introduced cloud storage/file sync and share and collaboration apps into the workplace?
Base = IIT only in companies with employees using BYO sync & share and/or collaboration apps

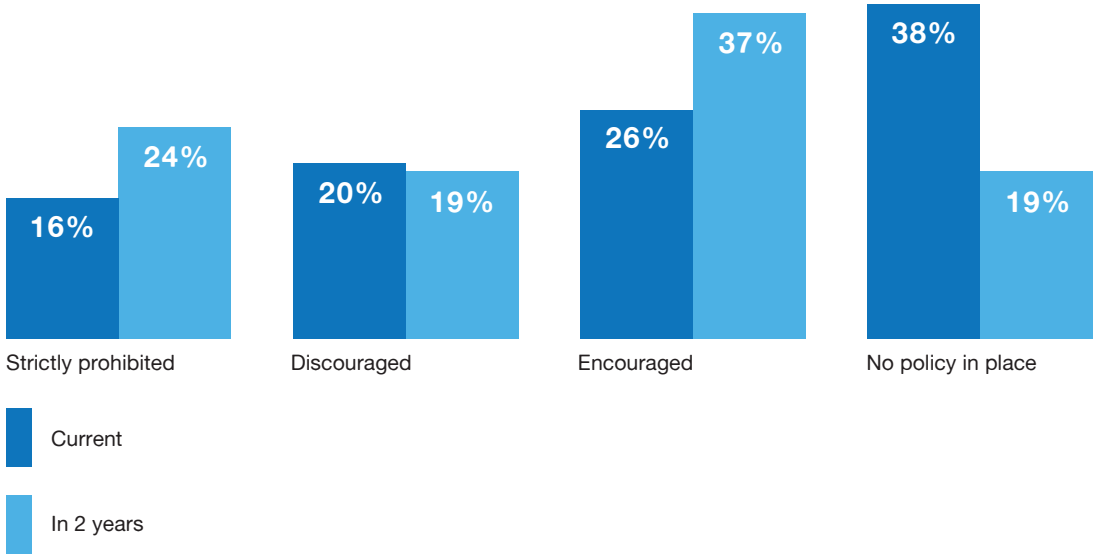
IT needs to focus on BYOA.

38% do not have policies in place now, 81% will within 2 years.

If you look at how IT professionals are dealing with the issue of BYOA, we see wildly disparate approaches, with many not even having a formal policy in place (38%).

More interesting is a closer look at the approach IT departments are making. Among those who have policies, we see a very even distribution of those who strictly prohibit (16%), those who discourage (24%), and those who encourage (26%). These are three very different approaches, and not one is the clear preferred choice.

What we do see is a general trend towards openness to BYOA coming in the future where the number who encourage it will grow from 26% to 37%.



takeaway:

IT pros are all over the map in how they're approaching the BYOA issue, with no clear consensus on the best path.

What is your current policy on the use of BYO apps for work purposes?
Base = IIT only

We don’t currently have a policy. IT should make it a priority to sit down with company CEO, CFO and IT supervisors to create a policy.

— IT manager, Non-profit, 11-25 employees

Strategic facilitators will be most successful.

Gatekeepers face an uphill battle, and observers will fall victim to perils of BYOA.

When asked how they're currently monitoring BYOA at their organization, IT pros again came back with three vastly different approaches.

The first was to act as a gatekeeper and restrict apps (30%). This is the role IT has traditionally taken—one of continually saying "no" to users and policing what they do.

Another way is to act as a passive observer, and let the BYOA trend wash over them without monitoring app usage. About 39% of IT professionals are currently employing this sit-back-and-take-it approach.

The third is to be more of a strategic facilitator by allowing apps to be brought in by employees, but actively monitoring and managing them. This promises to be the best suited as it embraces the BYOA trend as a reality, but doesn't try to stop it in its path with strict, gatekeeping policies.

Active gatekeeper:
Restrict BYOA
by blocking apps

Strategic facilitator:
Manage BYOA through analyzing web traffic logs, packet sniffing, and/or monitoring devices

Passive observer:
Ignoring BYOA
(not monitoring)

takeaway:

IT pros who act as gatekeepers will prevent app adoption at the expense of continuous improvement.

How are you monitoring the use of BYO apps?

The technology is advancing so rapidly IT departments have two choices: (1) Lock down all apps and control everything, hamstringing the productivity of 100% of their employees, or (2) Do their best to educate employees on security and trust them. I believe #2 is the only option.
I have seen IT departments cost their companies hundreds of thousands of dollars because they are so rigid about the network security that it is nearly impossible to get things done.

— Non-IT executive, Engineering firm, 10 employees

Conclusion: Reclaiming IT's strategic role

The BYOA trend is accelerating, as more users are introducing their own applications into the workplace, often without consulting IT. So, IT professionals have an important decision to make: are they going to sit back and let this trend wash over them, or take action and claim their rightful seat at the strategic table?

Here are four ways that IT pros can use the findings from this study to help guide them down the right path.

1: Understand the scale and reality of BYOA.

70% of IT organizations recognize that the BYOA trend exists, but they underestimate the scale; they assume that, on average, 2.8 applications are brought into their organization by employees when the number is closer to 21. They need to first understand the true scale at their organization before they decide how to address it.

2: Embrace the Consumerization of Apps as a positive that will make workers more productive.

IT recognizes the value of adopting employee-initiated applications so they shouldn't look at BYOA as a bad thing. Employees are choosing apps that enable better mobile access and remote working, and more intuitive, multi-device user experiences.

3: Acknowledge that their peers are still figuring out the best route to take with BYOA.

Across the board there are disparate approaches to BYOA. Some (38%) do not have policies in place, others (40%) are not monitoring it at all—but 81% say they will have a policy within 2 years.

4: Seize the opportunity to define their strategic role within their organization.

IT can map out their path to facilitate continuous, secure policies for their organizations now.

About LogMeIn

LogMeIn (Nasdaq:LOGM) transforms the way people work and live through secure connections to the computers, devices, data and people that make up their digital world. Serving over 90,000 customers, LogMeIn's solution portfolio of cloud services free millions of people to work from anywhere, empower IT professionals to securely embrace the modern cloud-centric workplace, give companies new ways to reach and support today's connected customer, and help businesses bring the next generation of connected products to market. Founded in 2003, LogMeIn is headquartered in Boston's Innovation District with offices in Australia, Hungary, India, Ireland and the UK.

IT management solutions:

LogMeIn's portfolio of intuitive IT management solutions enable organizations to effectively manage applications, data and devices in the cloud. Our solutions are purpose-built to help IT address the changing needs brought about by the Consumerization of IT, and the accelerating trends of BYOA and BYOD.

Manage applications:

AppGuru by LogMeIn

Learn more

Manage data:

cubby by LogMeIn

Learn more

Manage devices:

Central by LogMeIn

Learn more

Manage remote access:

Pro by LogMeIn

Learn more