WHITE PAPER

Managing BYOD in Corporate Environments

An Osterman Research White Paper

SPONSORED BY

Osterman Research, Inc.
P.O. Box 1058 • Black Diamond, Washington • 98010-1058 • USA
Tel: +1 253 630 5839 • Fax: +1 253 458 0934 • info@ostermanresearch.com
www.ostermanresearch.com • twitter.com/mosterman

EXECUTIVE SUMMARY

The Bring Your Own Device (BYOD) trend is pervasive today in organizations of all sizes and across all industries. It enables users and IT to improve worker productivity and generate higher employee satisfaction, reduce operational costs, innovate more quickly, and sustain competitive advantage. BYOD reflects the general trend of enabling collaboration anytime, anywhere for workers who expect to be just as productive away from the office as they are when working within their corporate network (e.g., a presentation that is started on a laptop, revised on a tablet and approved by team members on a smartphone). Moreover, BYOD enables workers to achieve a seamless flow of information and access to applications across all of their devices, whether these devices are supplied by their employer or personally owned. At the same time, the BYOD trend is also posing challenges to IT to secure and manage a much more diverse mobile device and application landscape.

More and more employees are bringing their own devices and preferred applications into the enterprise, creating what we call the BYODA (BYOD plus Applications) phenomenon. Workers' behavior and expectations are contributing to the consumerization of IT, where lines of business and users themselves are having an enormous influence on the types of technologies and applications used. While employees expect anytime, anywhere access to their content to get their work done, their CIOs are now expected to support BYOD within their corporate environment.

ARE YOU PREPARED?

Osterman Research has performed extensive research into the BYODA phenomenon and has found that it is viewed in one of two ways:

- For organizations that do not address BYODA properly, it represents an increased risk on a number of fronts, including the possibility of security breaches, malware intrusion and an inability to meet corporate governance, legal, and regulatory obligations.

- However, for organizations that address BYODA effectively, there are tremendous opportunities and benefits that it can provide to organizations of any size and in any industry.

KEY TAKEAWAYS

- Our research found that BYODA is well entrenched across organizations of all sizes, so much so that personally-owned smartphones and tablets are found in a larger proportion of organizations than are employer-supplied and managed devices.

- Moreover, employee-deployed, cloud-based applications are widely used – for example, tools like Dropbox, Apple iCloud and Google Docs are used in more than one-half of organizations.

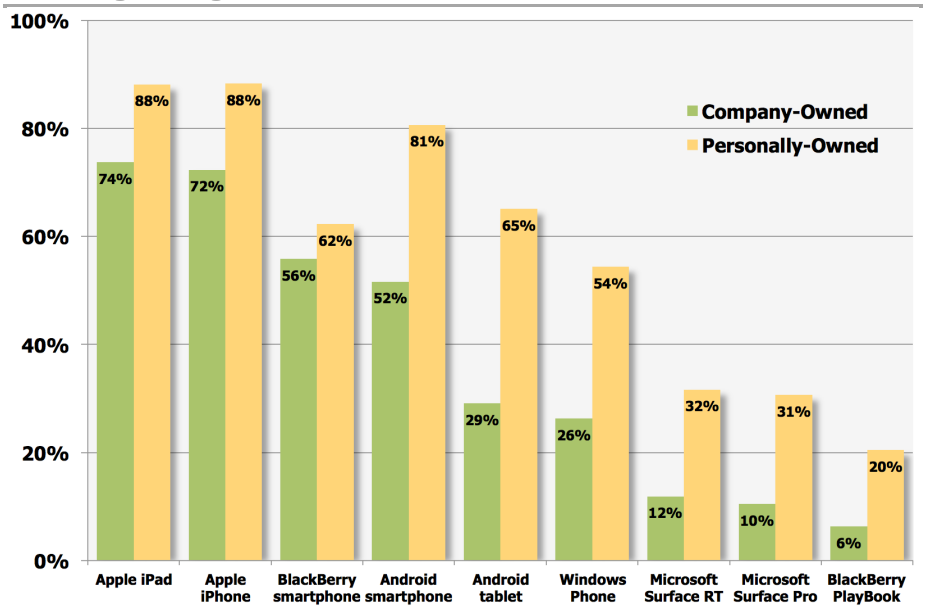
- IT is aware that BYODA creates some risks for an organization if not managed properly. Among these risks are an inability to retain and manage corporate content that may be required for purposes of archiving, regulatory compliance, eDiscovery or knowledge management; an inability to protect against the incursion of malware; and an inability to properly scan inbound and outbound content for sensitive content, inappropriate language and the like.

- BYODA brings many benefits that far outweigh the risks if managed properly. The risks created by BYODA are not inherent to the mobile devices, cloud-based applications or mobile apps themselves. Rather, the risks are introduced by overreliance on managing how the end point devices and applications are permitted to access corporate data and systems. Moreover, our research found that there is a disconnect between the perceived risks of BYODA and how well organizations are addressing them.

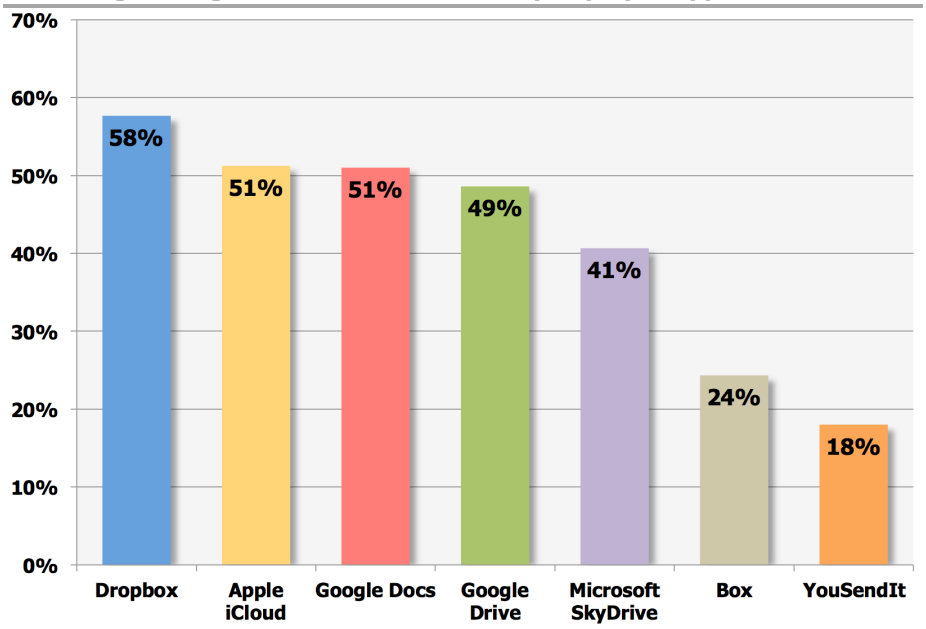
For organizations that address BYODA effectively, there are tremendous opportunities and benefits that it can provide to organizations of any size and in any industry.

- With IT management and controls in place, companies can leverage the productivity benefits that come along with BYODA. Just a few of these benefits include enabling the anytime, anywhere office; improving employee collaboration and communication (to get work done, to close a sales deal, or to move a project along); and reducing corporate costs.

Percentage of Organizations With Mobile Devices in Use



Percentage of Organizations With Personally Deployed Applications



- There are several steps that organizations should take when embracing BYODA, including understanding how personally-owned devices and self-deployed applications are used, creating policies to address their use, educating users about best practices related to these devices and applications, and deploying the appropriate technologies and applications to mitigate any risks.

There are several steps that organizations should take when embracing BYODA, including understanding how personally-owned devices and self-deployed applications are used.

ABOUT THIS WHITE PAPER

Osterman Research conducted two primary research surveys specifically for this white paper: an IT-focused survey with 444 individuals, and an end-user survey with 433 individuals. Our goal in conducting this research was to gauge:

- The pervasiveness of BYODA in small, mid-sized and large organizations across a wide range of industries.
- How well organizations have responded to BYODA in the context of protecting their data and access to corporate resources.
- What organizations are planning to do to manage the growing use of personally owned mobile devices and self-deployed applications.
- Whether organizations are fully leveraging all of the advantages that BYODA offers.

This white paper was sponsored by Micro Focus – information on the company is provided at the end of this document.

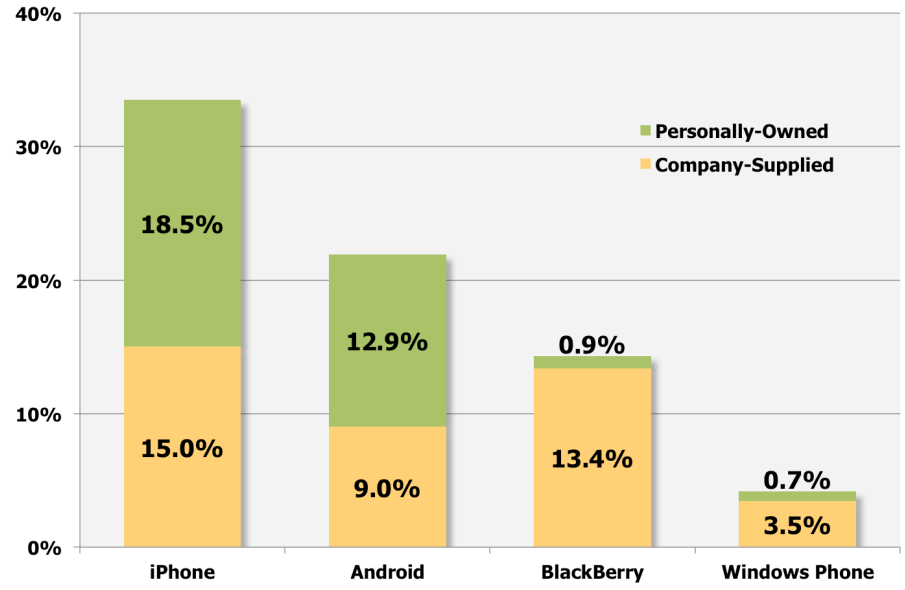
THE INCREASING USE OF PERSONAL TOOLS IN THE WORKPLACE

DEFINING "BYOD" AND "BYODA"

The concept of Bring Your Own Device (BYOD) – which is part of the larger trend toward the consumerization of IT – is a simple one: employees use their own devices to access corporate content and other resources like email, databases and various applications. It is important to note that the consumerization of IT is not just BYOD: it also includes social technologies, cloud-based tools to access content in a faster and easier way, and more consumer-oriented expectations within the workplace. The popularity of the BYOD trend is demonstrated in the following figure that shows the majority of iPhone and Android devices used for work-related purposes are personally owned.

Consumerization of IT is not just BYOD: it also includes social technologies, cloud-based tools for access to content in a faster and easier way, and more consumer-oriented expectations within the workplace.

Primary Mobile Device in Use as Reported by End Users



Osterman Research expands the definition of BYOD to include the growing number of cloud-based applications and mobile apps that are also used by employees in the performance of their work – hence, Bring Your Own Devices *and* Applications (BYODA). As discussed later in this white paper, various cloud-based applications are used extensively, but often without the permission, or sometimes even the knowledge, of IT.

FACTORS DRIVING THE TREND TOWARD BYODA

The growth toward BYODA is being fueled by a number of factors:

- Employees often have better, faster, newer and more fun devices than those supplied to them by their IT department. These include the latest and greatest iPhones and Android devices, iPads and Android tablets, but will increasingly include the new BlackBerry and, possibly, Windows Phone devices. Quite often, employees seek out specific smartphones and tablets that offer features that they desire and are willing to fund themselves. For example, Forrester Research found that more than one-third of workers are willing to use their own funds to employ the computer they want[i].

- The growing trend toward telework (recent developments at Yahoo! notwithstanding) is also fueling the BYODA trend as employees work increasingly from home and employ their own desktop computers, laptops, smartphones, tablets and other infrastructure to do their work. Forrester Research also found that 37% of employees work from more than one location and 53% do so with multiple devices[ii]. Moreover, employees who are working away from the corporate network are not subject to the same level of IT supervision imposed upon them behind the corporate firewall, and so will find it easier to deploy cloud-based applications, mobile apps, etc. However, it is also important to note that employees who are in the office also use the same applications as they do when working remotely.

- Employees increasingly have an expectation of always being connected and of always having access to content, whether work-related or personal. This blurring of the work-life separation makes access to corporate data and resources essential on all devices used by employees.

- IT departments often cannot or will not afford the latest and greatest hardware because of tight IT budgets and/or the need to apply sound financial principles to purchase decisions for hardware and other infrastructure – for example, individuals can swap out their mobile devices in as little as 18 months because of the financial incentives offered to them by mobile carriers, while organizations often do not have this luxury. Where the hardware purchase decision is not the limiting factor, quite often the cost of managing a wide range of different devices and operating system versions is determined to be too costly.

- IT departments sometimes do not provide all of the features and functionality that users want, and so they bringing in their own devices, cloud-based applications, and mobile applications to meet there needs.

- Finally, a growing proportion of organizations are supporting BYOD programs. For example, Gartner, Inc. found that 38% of US-based CIOs were expected to support a BYOD program in 2012[iii] and a Dell Quest-funded, Vanson Bourne report found that three out of four IT leaders believe that BYOD can help employees to be more productive[iv]. Comparing our own survey results with a survey we conducted in Q2/2012, we found the same proportion of organizations supporting BYOD, but a larger proportion that plan to do so.

THE GROWTH OF PERSONALLY DEPLOYED TOOLS

There are literally thousands of cloud-based apps, mobile apps and other tools that employees can use to be more efficient in their work or that can supplement the

Blurring of the work-life separation makes access to corporate data and resources essential on all devices used by employees.

capabilities that IT provides for employee use. These applications include those that provide enhanced email capabilities, file storage, file synchronization, content collaboration, large file transfer and other capabilities that IT departments will not or cannot implement. As shown in the following table of the leading cloud-based file sync and share applications in use, many of these applications have been deployed by IT in some organizations, but quite often they are deployed without IT's knowledge or consent.

Leading Cloud-Based Applications Deployed by Users
Based on % of Organizations

Application	Up to 99 Employees	100-999 Employees	1,000+ Employees
Dropbox			
Deployed by IT	17.3%	12.2%	5.7%
Used with IT's blessing	39.5%	26.3%	13.2%
Used w/o IT's blessing	21.0%	31.4%	43.1%
Not used	22.2%	30.1%	37.9%
Apple iCloud			
Deployed by IT	10.1%	13.5%	7.0%
Used with IT's blessing	34.2%	22.4%	21.1%
Used w/o IT's blessing	20.3%	23.7%	33.3%
Not used	35.4%	40.4%	38.6%
Google Drive			
Deployed by IT	7.7%	6.6%	6.7%
Used with IT's blessing	28.2%	20.5%	11.0%
Used w/o IT's blessing	20.5%	27.8%	37.8%
Not used	43.6%	45.0%	44.5%
Google Docs			
Deployed by IT	7.7%	12.7%	10.6%
Used with IT's blessing	25.6%	26.0%	12.9%
Used w/o IT's blessing	19.2%	27.3%	38.8%
Not used	47.4%	34.0%	37.6%
Microsoft SkyDrive			
Deployed by IT	21.0%	10.7%	10.8%
Used with IT's blessing	33.3%	24.8%	10.8%
Used w/o IT's blessing	7.4%	17.4%	28.3%
Not used	38.3%	47.0%	50.0%

INCREASING USE OF CLOUD-BASED APPLICATIONS

Our research found that many cloud-based applications are increasing in use. For example, comparing this year's survey results (conducted in Q1/2013) with results from a survey we conducted in Q2/2012), we found that:

- Use of Box has increased by 28%
- Use of Google Docs has increased by 24%
- Use of Microsoft SkyDrive has increased by 19%
- Use of Dropbox has increased by 4%

WHY ARE CLOUD-BASED TOOLS SO POPULAR?

Reasons for the use of cloud-based file sync, sharing, storage and other tools are varied and based on a number of factors:

- Many users are simply not satisfied with the status quo of capabilities offered to them by their IT department and so want to provide their own superset of features and functions. For example, users who work from home or when traveling may not want to take files with them on a USB stick and manually synchronize them when back in the office, and so use a cloud-based file synchronization service to do this for them.

- IT will often impose limits on what users can do in email and other tools. For example, most email administrators place a limit on the size of files that can be sent through the corporate email system. While this helps maintain acceptable levels of email server performance, it can prevent users from sending very large files as part of their work. Consequently, many users will opt for a free or low-cost, cloud-based file transfer tool to overcome IT-imposed limits.

- Many users simply prefer the ease of use and optimized interface of cloud-based applications compared to the more traditional capabilities that IT offers to them.

Users, in effect, are greatly influencing the tools that are brought into the enterprise. Employees will be much more satisfied, and in turn more productive at their work, when they have a say in the types of tools and applications that should be used, yet still meeting the security and information governance requirements of IT.

THE RISKS AND REWARDS OF BYODA

THE RISKS

While IT will be expected to manage all these devices, and the corporate content on them, it is important to note that the rewards of BYODA far outweigh the risks, and with a bit of planning in place, IT and the organization as a whole will see the lasting benefits that it brings. That said, there are some risks associated with BYODA for those organizations that do not address and manage them properly.

Employees will be much more satisfied, and in turn more productive at their work, when they have a say in the types of tools and applications that should be used.

- **Content Retention and Management**
  One of the fundamental risks associated with the BYODA phenomenon is that organizations may be less able to manage their content. For example, content that is created and stored on personally owned tablets, stored in a cloud-based file synchronization tool not approved by IT, or sent via personal Webmail systems is less accessible to the organization at large. This makes it more difficult for the organization to know the content it has available for eDiscovery or regulatory audits, makes it more difficult to access this data when required, and makes content retention more difficult. This can lead to a greater risk of evidence spoliation, greater risks in satisfying regulatory obligations, and more difficulty in managing content retention periods.

- **Security and Malware Protection**
  Because personally owned devices and personally managed cloud applications often use non-corporate networks for communication and storage, BYODA can create security-related risks through bypassing of corporate defenses. This means, for example, that inbound content on personally owned devices or applications may not be scanned for malware as vigorously as if the data was sent through the corporate network. Outbound content may bypass corporate policies that will automatically encrypt, scan for inappropriate content leaving the organization or otherwise manage the transmission and storage of sensitive data. This creates a higher level of risk for both data and financial loss.

- **Information Governance**
  Another risk that organizations face from BYODA is the reduced level of governance that comes from IT's loss of control over personally owned devices, corporate data that is sent from and stored on these devices, the loss of control over access to corporate applications, and the potential loss of intellectual property that can result from the physical loss of a device that cannot be wiped.

  Not to be overlooked is the threat of regulatory or legal sanctions due to inadequate recordkeeping or supervision. BYODA content is treated as a form of electronic communication by courts and regulators, so it is subject to the same rules as those for email. Thus, organizations must take into account regulatory rules and eDiscovery guidelines when devising their BYODA policies and procedures.

Moreover, the use of a wide range of devices and operating systems, out-of-date firmware on devices, and protocols limits an organization's ability to properly manage its systems and access to them, simply because IT often does not have the bandwidth or internal expertise available.

THE BENEFITS OF BYODA OUTWEIGH THE RISKS

There are enormous benefits (and enormous return-on-investment for organizations) to be gained from the use of personally owned devices and various employee-managed applications when used for work purposes:

- **Employee Productivity**
  Users can be more efficient and effective in their work if they are enabled with capabilities that give them access to all of their files, communications tools and other services from any platform or any location. 71% find that BYODA increases worker productivity and makes employees much more productive on mobile devices. Because IT often does not have the budget to enable every capability for every user, BYODA helps to fill in the gaps that might exist in the corporate infrastructure. A good case in point is Intel Corporation. The company has embraced BYODA and has realized a productivity increase of 57 minutes per employee per day as a result, giving the company a three-fold return on its consumerization investments[v].

- **Anytime, Anywhere Access**
  Not only will employees be always connected to do their work, but they're able to bring their work to the field. Sales can access their corporate content stored in a cloud-based application to showcase the latest marketing collateral and updated pricing information to prospective clients. Doctors can view videos or review notes before going into a procedure right from their device instead of going to the ER workstation. Construction field engineers can access project drawings, specifications, quality records, and predictive safety analysis all via applications on their tablet while being on the job site.

- **Employee Satisfaction**
  Users want to choose the device they do their work on. They don't have to use a device they're not comfortable with or have to learn another operating device. No longer do they have to carry a separate "work" phone and "personal" phone, but BYOD ensures they're always online and always connected to their work since they're using only one device, and the device they want to do their work on. According to Osterman Research's survey, approximately 68% of employees said they were kept happy by being allowed to bring their own device into work. Employees who are permitted to use their own devices and applications will likely have higher morale and will be less likely to seek employment elsewhere.

- **Decrease in Corporate Costs**
  Corporate smartphone and tablet costs can be reduced because employees are supplying their own devices instead of the company funding them. In fact, 35% of survey respondents whose companies have 1,000+ employees are trying to reduce spend on their telecom bill. This applies even when employees are reimbursed by the company with a monthly stipend to cover their mobile device charges, since the mobile service is managed by the employee, not his or her employer. This is particularly important for employees who leave an organization. Osterman Research found in a recent survey that 11% of organizations are not sure if they are still paying for mobile services for employees who are no longer employed – for organizations with 2,000 or more employees, this figure was 17%[vi].

  BYODA can also reduce the strain on email servers, bandwidth and other elements of the corporate infrastructure, potentially reducing costs by postponing enhancements to or replacements of email servers, storage systems, etc. 35% of surveyors whose companies have 1,000+ employees are committed

Users can be more efficient and effective in their work if they are enabled with capabilities that give them access to all of their files, communications tools and other services from any platform or any location.

to leveraging the cloud for IT services and moving their workloads onto the cloud. Clearly they see the advantages that the cloud brings.

- **Competitive Advantage and Increase in Revenue:**
  Having a permissive BYODA policy can give an organization a competitive advantage and actually improve corporate revenue. This is achieved through:

  - Increase in productivity
  - Enhanced team communication and collaboration
  - Improved work processes and efficiencies
  - Higher customer service rate / faster response times
  - Access to applications based on role
  - Speed of innovation

  Employee communication and collaboration can be improved through the use of social media, text messaging, document sharing, mobile apps and other tools. IT should be improving these capabilities rather than recommending that they should not become involved in the consumerization trend.

- **Innovation**
  Mobile is changing the way we work. It's no longer just an access point; employees are able to get their work done faster and better through accessing the right tools and technologies right in their hands wherever they are (whether at home, in the workplace, at a client visit, or on the job site). 51% of all companies surveyed see mobile as truly transformative, a way to get ahead of the competition and maintain their competitive advantage. It's solving multiple business problems and through the use of BYODA, we're able to reexamine how we engage with our customers, partners and suppliers, and think through the impact of how we can make core critical services available on these devices at a time when the way users interact with technology on their smartphones and tablets are changing everyday.

Our research found that a large proportion of organizations consider several key attributes of BYODA are important or very important reasons to support the use of personally owned devices, as shown in the following table.

Having a permissive BYODA policy can give an organization a competitive advantage and actually improve corporate revenue.

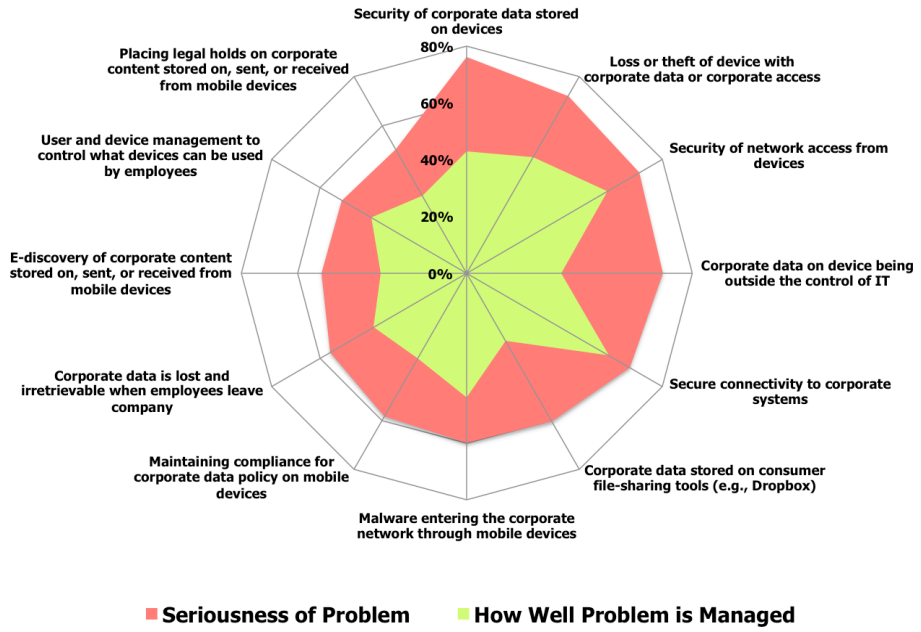
Reasons for Supporting Personally Owned Devices
% Responding Important or Very Important

Driver	Up to 99 Employees	100-999 Employees	1,000+ Employees
Keep employees happy by permitting them to bring their own mobile devices to work	85%	60%	60%
Increasing productivity and making employees more productive on mobile devices	62%	72%	68%
View mobile enablement as way to get ahead of competition and sustain competitive advantage	54%	52%	47%
Trying to reduce spend on our telecom bill	38%	44%	35%
Reexamining how we engage with our customers, partners and suppliers and thinking through the impact of making core critical services available on these devices	31%	42%	48%
We are committed to leveraging the cloud for IT services and enabling enterprise mobility is a critical piece of our journey to moving workloads onto the cloud	31%	32%	35%
Keeping the stress off the file-sharing infrastructure and reducing storage costs	15%	14%	21%
Reducing the strain on our email server	15%	16%	17%

THE CURRENT CORPORATE DISCONNECT

One of the more important findings from our research is that many organizations are not protecting themselves from the risks associated with unmanaged BYODA. We asked respondents to rate the seriousness of problems on a scale of 1 (not serious at all) to 5 (very serious), as well as their management of them on a scale of 1 (not well at all) to 5 (very well). As shown in the following figure, while organizations view a variety of issues in BYODA management as serious or very serious, a much smaller proportion consider that they manage these issues well or very well.

Seriousness of Issues vs. How Well They are Managed



There are significant gaps presented by BYODA that organizations have yet to fill, particularly in the context of data security and content management. Our research found that the problem is even more serious for smaller organizations that often do not have the IT staff, budgets or expertise to match their requirements with the appropriate controls to protect data and other corporate assets.

Another way of looking at this data is in terms of how well organizations manage problems, even those that they do not consider serious. For example, our research found that for the most serious problem – the security of corporate data stored on mobile devices – 57% of respondents believe that their management of the issue is insufficient given the seriousness of the problem, while 43% believe that they are managing the problem well enough. Similarly, 54% believe that their management of lost devices is insufficient to remedy the problem.

ORGANIZATIONS CAN PROTECT THEMSELVES IF THEY MANAGE BYODA PROPERLY

It is important to note, however, that organizations are able to protect themselves from these risks if they have developed the appropriate policies and deployed technology solutions to address the specific risks that they face. In other words, the problems created by BYODA are not inherent in the particular mobile devices or applications that employees own or self-deploy, but rather in organizations' willingness to implement detailed and thorough policies and the right technologies focused on remediating these problems.

There are significant gaps presented by BYODA that organizations have yet to fill, particularly in the context of data security and content management.

RECOMMENDATIONS FOR MANAGING BYOD

UNDERSTAND THE BENEFITS AND RISKS OF BYOD

One of the most important steps in approaching the BYODA phenomenon is to appreciate just how pervasive it is in most organizations, as shown in the table on the next page. While most believe that many of their employees are using personal smartphones and tablets (given that senior managers themselves often were the early adopters of BYODA after the introduction of the iPhone), they may not fully understand just how widespread this phenomenon has become within their organizations. Senior managers must understand:

- How personally-owned smartphones and tablets, as well as personally deployed applications, are used throughout the organization
- What types of data they access and store
- The many (typically good) reasons for their use
- The applications and technologies that are adopted/demanded by users while still meeting the requirements and the needs of IT

It is essential that decision makers consider their options for managing BYODA. While some may opt for restrictive – perhaps draconian – policies that limit or prevent employees from using personally owned smartphones or tablets, or that prohibit the use of cloud-based applications or mobile apps of any kind, Osterman Research recommends the opposite approach: namely embrace BYODA and the overall trend toward the consumerization of IT, realizing that the trend is not going away and that it can provide numerous benefits. In fact, an improving economy that provides employees more choice on where and how they work makes opposing BYODA even more difficult.

As part of the BYODA analysis process, we recommend that decision makers survey employees about what their work requires.

- Do they need particular applications that will enable them to be more productive?
- How does the use of personally owned devices and self-deployed applications impact current business processes?
- How important are various capabilities to end users, such as viewing documents, sharing status updates with others, or collaborating with colleagues?

Ensuring that management understands how BYODA impacts end users will go a long way toward helping them develop the right policies to both protect the organization and enable end users with the tools they need to be efficient and productive.

DEVELOP A PROGRAM AND IMPLEMENT POLICIES TO PROTECT THE ORGANIZATION

It is vital that organizations implement BYODA policies about acceptable use of personally owned devices and self-deployed applications. This might include creating a list of approved devices, operating systems and operating system versions, cloud-based applications, mobile apps, etc. These policies should be as detailed and thorough as necessary, and should be included in an organization's overall set of acceptable use policies that are focused on use of all corporate computing resources and access to them.

An important element of these policies as they apply to mobile devices should be that any mobile device – whether company-supplied or employee-owned – must be wipe-able by the IT department in the event of its loss, that all devices be scannable for

The problems created by BYODA are not inherent in the particular mobile devices or applications that employees own or self-deploy, but rather in organizations' willingness to implement detailed and thorough policies and the right technologies focused on remediating these problems.

malware, that content be scannable for data leakage, and that content be archivable as necessary. However, as shown in the table on the next page, many organizations have not yet implemented these capabilities fully.

Percentage of Organizations in Which Personally Owned Smartphones are Used, by Type

Smartphone	Up to 99 Employees	100-999 Employees	1,000+ Employees
Android smartphone			
Used with IT's blessing	57.7%	57.7%	53.0%
Used, but w/o IT's blessing	17.9%	23.7%	29.2%
Not used	24.4%	18.6%	17.8%
Apple iPhone			
Used with IT's blessing	70.6%	72.0%	75.7%
Used, but w/o IT's blessing	11.8%	15.5%	15.9%
Not used	17.6%	12.4%	8.5%
BlackBerry smartphone			
Used with IT's blessing	32.8%	37.7%	68.4%
Used, but w/o IT's blessing	7.5%	16.7%	8.6%
Not used	59.7%	45.7%	23.0%
Windows Phone			
Used with IT's blessing	43.1%	32.6%	33.9%
Used, but w/o IT's blessing	5.6%	12.6%	30.4%
Not used	51.4%	54.8%	35.7%

Moreover, corporate policies focused on employee-managed applications should include requirements for the encryption of data if stored in a third party's cloud data center. They should also include requirements that mobile devices are encrypted so that corporate data and access to it is not compromised if a device is lost. Policies should also reflect specific regulatory and legal requirements, in addition to industry and corporate best practices.

Corporate policies focused on employee-managed applications should include requirements for the encryption of data if stored in a third party's cloud data center.

EDUCATE USERS ABOUT BEST PRACTICES

Another important step in managing BYODA is educating users about best practices related to the use of personal devices and self-deployed applications. This should include how to properly access and manage corporate data and other resources, which applications represent a risk to corporate security and which are safe to use, the types of communications that are appropriate over various types of cloud-based applications and mobile apps, where it is not appropriate to access sensitive corporate applications or databases (public Wi-Fi or certain countries, for example) if appropriate encryption or VPN capabilities are not in place, etc. The goal is not simply to create a list of do's and don'ts, but rather to help gain employee buy-in and adherence to corporate policies.

Capabilities for Company- and Personally-Owned Devices
Based on % of Organizations

Device	Up to 99 Employees	100-999 Employees	1,000+ Employees
Company-owned smartphones			
Device can be remotely wiped	90.0%	90.5%	93.0%
Device can be scanned for malware	41.7%	33.3%	40.7%
Content can be scanned for language, leakage	15.0%	14.3%	20.9%
Content can be archived	15.0%	21.4%	25.6%
Company-owned iPads and other tablets			
Device can be remotely wiped	86.5%	84.2%	89.1%
Device can be scanned for malware	42.3%	37.5%	42.3%
Content can be scanned for language, leakage	17.3%	18.3%	22.4%
Content can be archived	15.4%	20.0%	26.3%
Personally-owned smartphones			
Device can be remotely wiped	68.3%	78.6%	70.0%
Device can be scanned for malware	34.1%	27.4%	31.0%
Content can be scanned for language, leakage	12.2%	8.3%	15.0%
Content can be archived	7.3%	13.1%	18.0%
Personally -owned iPads and other tablets			
Device can be remotely wiped	71.1%	78.4%	69.6%
Device can be scanned for malware	39.5%	24.3%	34.8%
Content can be scanned for language, leakage	13.2%	8.1%	14.1%
Content can be archived	7.9%	13.5%	18.5%

DEPLOY THE APPROPRIATE TECHNOLOGIES

It is also important to deploy the appropriate technologies that will enable organizations to manage BYODA properly. This includes:

- Systems focused on mobile device management (MDM)
- Malware detection and remediation
- File sharing and collaboration
- Content inspection
- Archiving
- Encryption
- Other tools, as appropriate.

As shown in the table above, the majority of organizations can remotely wipe both company-supplied and personal devices, although far fewer have yet to deploy a variety of other capabilities.

Since access to corporate content plays a huge role in BYODA, organizations should consider a mobile content management (MCM) solution.

OTHER CONSIDERATIONS IN DEPLOYING BYODA-FOCUSED TECHNOLOGIES

- One important aspect of deploying the appropriate technologies should come from information gleaned during the employee survey phase. For example, if the survey reveals that employees have deployed a consumer-focused file-synchronization tool that does not meet IT's requirements for corporate data security, an alternative should be offered that provides the ease of use of the consumer-focused tool, but with the security capabilities that will meet the needs of the organization.

- With regard to MDM, BlackBerry Enterprise Server (BES) continues to be the dominant solution in place today – our research found that 61% of organizations today use BES, although Microsoft Systems Center Mobile Device Manager is gaining traction along with several other solutions. However, in the enterprise

market (1,000+ seats), BES currently has an even more dominant share and is expected to retain its leading role over the next 12 months, largely because of its robust security model.

- Since access to corporate content plays a huge role in BYODA, organizations should consider a mobile content management (MCM) solution, built for enterprises for scale, security and compliance – solution should include integration with Active Directory and Single Sign-On solutions, remote wipe as well as lightweight mobile device management, full encryption at rest and transfer, and integration with leading data loss prevention providers, and relevant certifications such as SSAE 16 Type II SOC 1, SOC 2, Safe Harbor, HIPAA and HITECH among others. Businesses who want to move their employees away from a personal cloud solution should look to Box, who has a strong enterprise, security and mobility focus while still meeting the expected end-user experience enabling users to easily discover, connect to, engage with, and share content more effectively.

- Businesses that want to move their employees away from a personal cloud solution should look to one that has a strong enterprise, security and mobility focus while still meeting the expected end-user experience. This might include cloud-based file-sharing and collaboration solutions or Virtual Desktop Interface (VDI) technology that can allow IT to manage both the user experience and access to corporate applications. However, we believe that the fundamental consideration here should be the deployment of "smart VDI" technologies that provide very high performance, the ability to offer smoother and more fluid collaboration and that negate the need to manage individual devices, but instead any device that might connect to the corporate network.

- In some cases, it may be appropriate to ban specific applications, although we recommend doing this as little as possible. For example, a user of a company-supplied iPhone who implements iCloud can make a backup of all corporate and personal data. If the employee leaves the company and buys a personal iPhone or receives one from his or her next employer, accessing their personal iCloud account will download all of the previous employer's content onto the new device.

- Moreover, decision makers should seriously consider deploying technologies that will segment personal and work data on mobile devices. Our research found that a large proportion of organizations either have plans to do so or they are considering doing so, as shown in the following table. For example, we believe that organizations will increasingly deploy solutions that will allow the management of multiple platforms via a single pane of glass, offering full MDM capabilities. At the client level, we also believe there will be increasing use of solutions that will enable seamless management of personal and work personas on both company-supplied and personal devices. Solutions like BlackBerry Balance or VMware Horizon Workspace permit a single device to contain separate work and personal applications and content, permitting IT to remotely wipe company-managed content without impacting employees' personal content.

In some cases, it may be appropriate to ban specific applications, although we recommend doing this as little as possible.

Plans to Segment Personal and Work Content on Mobile Devices
Based on % of Organizations

Plans	Up to 99 Employees	100-999 Employees	1,000+ Employees
Will deploy technology to do so	5.6%	19.0%	19.6%
No plans to deploy technology, but are considering/evaluating	42.7%	39.9%	49.2%
No plans to deploy technology and not considering/evaluating	51.7%	41.1%	31.2%

THE BENEFITS OF THE CLOUD

Finally, while many decision makers may resist the use of cloud-based applications, fearing that corporate data security or information governance requirements may be compromised, we recommend that decision makers fully embrace the cloud. Reasons for doing so include the ability to improve employee productivity, enable more efficient collaboration and reduce costs, among other benefits. While resistance to the cloud is understandable, particularly in industries that tend to be more staid or that have a significant number of regulatory obligations to satisfy, cloud-based tools can provide enormous benefits.

Key reasons to embrace the cloud include:

- Leading enterprise cloud vendors have invested significantly in making their data centers, staff, product development and release cycles secure via SSAE Type II third-party audits.
- The ability to shift from a capital expense/depreciation (CAPEX) economic model to an operating expense (OPEX) model that permits organizations to pay only for the services they need.
- The ability to avoid the expense related to "shelfware" – IT investments that are not fully used or that take a long time to become used for mission-critical applications.
- The ability to reduce storage, file server, VPN, data replication and email storage costs by shifting functionality away from in-house infrastructure.
- The ability (with the right providers) to implement robust and improved business continuity capabilities for critical corporate systems.
- Finally, the right cloud providers can improve an organization's security, compliance and corporate governance posture.

SUMMARY

The BYODA trend is enormously beneficial for organizations on a number of levels:

- Organizations can leverage mobile applications, including ones that enable employees to get work done anytime, anywhere, as well as collaboration around content that applies to a group project or piece of content that employees need to work on. Developers are increasingly building applications specific to a business' needs to enable their workers to get more work done while remote.
- BYODA fits in nicely with the increasing trend toward multi-platform environments, including the trend toward having applications available on all platforms – desktops, laptops, smartphones and tablets.
- Innovation will continue to take place with mobile devices and cloud-based mobile applications. Those who don't put mobile at the core of their workforce mobile strategy will miss out.

The BYODA trend is here to stay, and so decision makers need to understand the new reality of employees accessing corporate data and other resources with their own devices and via cloud-based applications and mobile apps that they have deployed themselves. Consequently, decision makers must do three things:

- Develop policies that will address the risks associated with unfettered use of BYODA.

The BYODA trend is here to stay, and so decision makers need to understand the new reality of employees accessing corporate data and other resources with their own devices and via cloud-based applications.

- Implement technologies that will prevent data leaks, archive content, encrypt content and devices, prevent data loss, and otherwise mitigate the risks associated with unmanaged use of personally owned devices and self-deployed applications.

- Where appropriate, implement replacements for employees' self-deployed applications that will provide the same ease of use, but that offer better protection of corporate data and other assets.

With the right BYODA program in place, IT will see the huge opportunity it brings as well as being able to become *more secure* by being in control of all corporate content; and how it is accessed, managed and shared.

SPONSOR OF THIS WHITE PAPER

Micro Focus is a global software company with 40 years of experience in delivering and supporting enterprise software solutions that help customers innovate faster with lower risk. By applying proven expertise in software and security, we enable customers to utilize new technology solutions while maximizing the value of their investments in critical IT infrastructure and business applications. As a result, they can build, operate, and secure the IT systems that bring together existing business logic and applications with emerging technologies—in essence, bridging the old and the new—to meet their increasingly complex business demands.

www.microfocus.com
twitter.com/MicroFocus

+1 866 464 9282
+1 646 304 6250

---

[i] Schadler, Ted. *2013 Mobile Workforce Adoption Trends.* Forrester Research. Feb 4, 2013

[ii] Ibid.

[iii] Willis, Davis. *Bring Your Own Device: New Opportunities, New Challenges.* Gartner, Inc. August 16, 2012

[iv] http://www.quest.com/documents/byod-putting-users-first-produces-biggest-gains-fewest-setbacks-datasheet-19142.pdf

[v] http://www.infoworld.com/d/consumerization-of-it/afraid-of-byod-intel-shows-better-way-204123

[vi] Internally funded survey conducted during 2012, Osterman Research, Inc.