WHITE PAPER

Putting IT Back in Control of BYOD

An Osterman Research White Paper

Published June 2012

SPONSORED BY

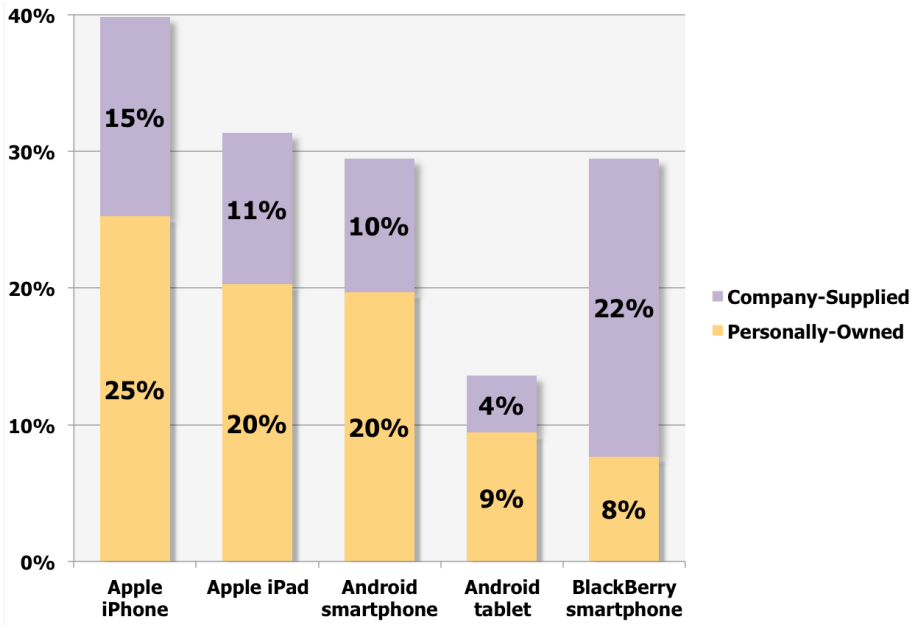
Osterman Research, Inc.
P.O. Box 1058 • Black Diamond, Washington • 98010-1058 • USA
Tel: +1 253 630 5839 • Fax: +1 253 458 0934 • info@ostermanresearch.com
www.ostermanresearch.com • twitter.com/mosterman

EXECUTIVE SUMMARY

Over the past several years, one of the most important trends to impact organizations of all sizes – but particularly mid-sized and large organizations – is for employees to use their own smartphones and tablets in the course of their work. The so-called Bring Your Own Device (BYOD) trend was initiated several years ago, often by senior executives who had purchased an Apple iPhone or an Android device and then requested their IT department to support it instead of, or in addition to, the mobile device that the company had supplied to them. Osterman Research includes as a key element of the BYOD trend the various applications that employees use as part of their work, such as personal file sync services.

To understand just how pervasive this trend has become, Osterman Research conducted a survey of 760 individuals with regard to the BYOD issues they face in their organizations. We found, as shown in the following figure, that unlike RIM BlackBerry smartphones – the traditional mainstay among corporate smartphone users – personally owned Apple iPhone and iPads, as well as Android smartphones and tablets, are more common than their company-supplied counterparts.

Penetration of Mobile Devices by Ownership *(As a % of Users)*



Our research also found widespread use of third party, cloud-based storage and file synchronization offerings that are sometimes used with IT's blessing, but more often not: Dropbox, for example, is used in 14% of 1,000+ employee organizations with IT's blessing – and in 44% of them without approval.

KEY TAKEAWAYS

- The BYOD trend for both mobile devices and employee-managed applications is pervasive and growing. Although most common in smaller organizations, even very large enterprises are experiencing the impact of BYOD.
- BYOD offers various benefits, including more efficient work by employees, *possibly* lower IT costs and improved corporate morale.
- At the same time, BYOD is fraught with risks that include reduced protection from malware and data breaches, various legal and regulatory problems, more

The so-called Bring Your Own Device (BYOD) trend was initiated several years ago, often by senior executives who had purchased an Apple iPhone or an Android device and then requested their IT department to support it instead of, or in addition to, the mobile device that the company had supplied to them.

difficult management of content for activities like eDiscovery or regulatory compliance, corporate governance obligations that are more difficult to satisfy, and often higher costs.

- A large proportion of organizations have not fully embraced the impact of BYOD. For example, our research found that even among organizations with 1,000 or more employees, only 54% have a formal IT policy for supporting personally owned mobile devices used for work purposes; the proportion of smaller organizations that have such an IT policy is even lower.

- A failure to put IT in control of BYOD is having a negative impact: between 12% and 33% of organizations (depending on the number of employees) report that the use of smartphones is being hindered or slowed because IT cannot manage them to the extent they would like; 20% to 42% of organizations report the same for the use of tablets.

- There is also concern about corporate data that is stored by third party, cloud-based providers: between 43% and 62% of organizations are concerned or very concerned about this issue.

- Organizations should implement policies and technologies that will channel the BYOD trend into appropriate management of corporate data and assets instead of banning the use of personal devices and applications outright.

ABOUT THIS WHITE PAPER

This white paper discusses the BYOD trend and provides data from an extensive survey conducted specifically for this document. The white paper also provides a brief overview of its sponsor – McAfee – and the company's relevant offerings.

THE GROWING TREND TOWARD BYOD

WHAT EXACTLY IS "BYOD"?

Bring Your Own Device (BYOD) is exactly what its moniker implies: the growing trend for employees to use personally-owned smartphones, tablets, laptops and other platforms to access corporate applications like email and databases; and to create, store and manage corporate data using these devices. For example, our research found that business email and Web browsing are the most commonly used business tasks for which mobile devices are used (employed by 99% and 93% of users, respectively), but use of personal social media, corporate social media and storage of business-related documents are also commonly used.

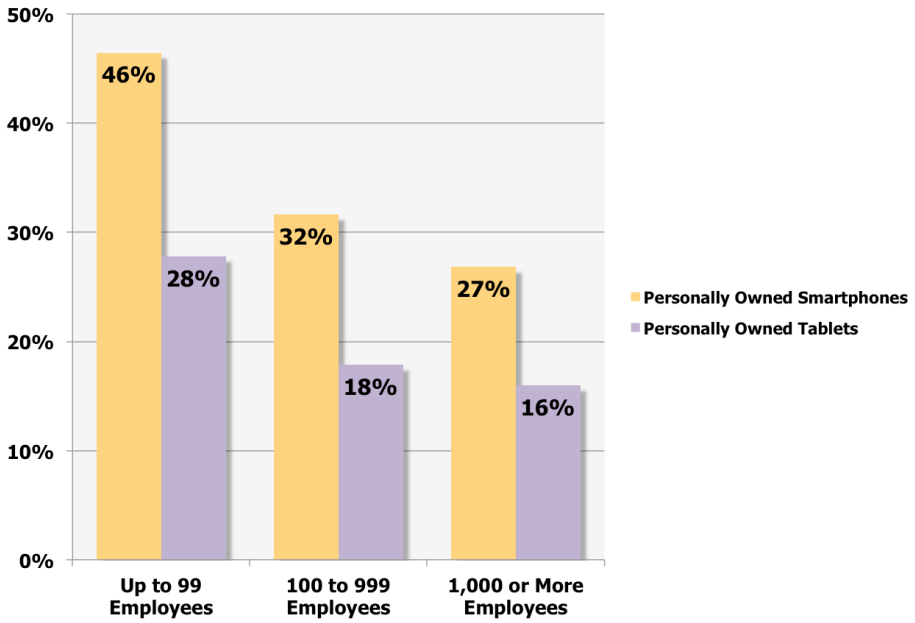
Osterman Research actually takes a somewhat broader approach to BYOD to include applications like personal file sync services and Skype as part of this trend, since the implications from the use of these tools – which are typically downloaded by individual users for their personal use – are identical: corporate data is accessed, created, stored and managed using tools that are under the direct control of employees, more or less independently of corporate IT departments and most often without their blessing and often without their knowledge.

BYOD IS PERVASIVE

Just how pervasive is the BYOD trend? The research we conducted for this white paper, and presented in the following figure and table, demonstrates that BYOD is quite common across organizations of all sizes.

Organizations should implement policies and technologies that will channel the BYOD trend into appropriate management of corporate data and assets instead of banning the use of personal devices and applications outright.

Use of Personally Owned Mobile Devices for Work-Related Purposes by Organization Size *(As a % of Organizations)*



Penetration of Cloud-Based Applications by Organization Size
As a % of Organizations

		Up to 99 Employees	100-999 Employees	1,000+ Employees
Dropbox	Used w/IT's blessing	40%	21%	14%
	Used w/o IT's blessing	32%	49%	44%
	Not used	28%	30%	42%
Google Docs	Used w/IT's blessing	24%	12%	10%
	Used w/o IT's blessing	19%	39%	42%
	Not used	57%	48%	48%
YouSendIt	Used w/IT's blessing	18%	8%	4%
	Used w/o IT's blessing	14%	17%	22%
	Not used	67%	75%	73%

The pervasiveness of BYOD is also borne out by other research. For example:

- A Research and Markets study found that 65% of enterprises worldwide will adopt BYOD to some extent by the end of 2012[i].
- An Aberdeen Group study found that 75% of companies permit BYOD[ii].
- Equanet reports that 71% of tablets used in a business setting are employee-owned[iii].
- Some companies are migrating to a completely BYOD approach, such as Cisco, where 100% of mobile devices are provided by employees and not the company itself[iv].

EMPLOYEES ARE DRIVING BYOD BECAUSE…

There are several drivers for BYOD. For example, employees often want newer, faster and overall higher performance hardware than what their employer provides

Individuals are generally freer to make impulse purchases in response to the latest and greatest hardware announcements – IT departments typically make more well-informed, more well thought-out decisions about purchasing capital equip-ment.

for them across a variety of platforms: desktop PCs, smartphones, tablets, etc. This is due in part to the fact that decisions about personal devices are not constrained by the return-on-investment and limited budget considerations that often limit IT decision making. Moreover, individuals are generally freer to make impulse purchases in response to the latest and greatest hardware announcements – IT departments typically make more well-informed, more well thought-out decisions about purchasing capital equipment and do so during normal hardware refresh cycles. In short, individuals who buy new hardware for themselves are not constrained by the need to make a business case for their purchases.

With regard to the widespread use of applications like personal file sync services or Skype, or the hundreds of thousands of other applications available via the Apple or Android apps stores, there are somewhat different drivers involved. For example:

- A growing proportion of employees work at home as part of formal or informal telework programs and so are not as constrained by their IT department about downloading and installing applications that may or may not have been vetted for use on the corporate network.

- Many IT departments impose file-size limits or prevent the sending of certain types of content in the corporate email system to maintain acceptable network or application performance or to protect against malware.

- Many users have multiple workplaces: their cubicle, their home office, Starbucks, airplanes, etc., and so need to have access to all of their files – and the latest versions of their files – on their laptop, their tablet and their smartphone.

- IT departments often cannot afford to deploy all the tools that users need, the vetting process for these applications is too slow to meet users' expectations, or the IT department simply does not allow certain tools to be used because of concerns over corporate security, the potential for data breaches, etc.

- Finally, many employees are happy to accommodate – or are at least willing to accept – a blurring of the distinction between work and personal life and so need access to critical applications and data on every platform, whether supplied by their employer or not.

Many employees are happy to accommodate – or are at least willing to accept – a blurring of the distinction between work and personal life and so need access to critical applications and data on every platform.

THE BENEFITS OF BYOD

There are three fundamental benefits that the trend toward BYOD can provide:

- **Users are more efficient**
  One of the primary ways in which BYOD helps users is by making them more efficient. Having access to every file and every email from any hardware platform or Web browser enables users to get more work done. For good or bad, numerous surveys have found that a large proportion of employees check email and do other work after hours on weekdays, on weekends and on vacation. BYOD is a key enabler of this phenomenon.

- **Corporate costs can be reduced**
  At least in the short term, corporate costs can be reduced by having employees fund some or all of their mobile device and cloud-based application requirements. For example, while many employers will pay for employees' mobile devices outright, some provide only partial reimbursement, if that. A comScore MobiLens study of BlackBerry users in late 2011 found that 22% of employers provide only partial reimbursement for users' devices[v]. Moreover, an Aberdeen Group study found that carrier costs for employee-owned devices are $10 per month per device lower than if the company owns the device[vi].

- **Employee retention and satisfaction can be improved**
  There is also some evidence to suggest that when employees are permitted to choose their own mobile device their job satisfaction is higher. For example, an Aberdeen Group study found that 61% of companies that permit employees to use their own mobile device experience higher employee satisfaction[vii].

THE DANGERS OF BYOD

SECURITY

One of the fundamental dangers of BYOD is that personally owned and managed devices used to create, access and store corporate data will typically bypass inbound content filtering systems that have been deployed by IT. One result of this is a potentially greater likelihood for malware intrusion, particularly for Android devices. For example, F-Secure found that for the 12-month period ending in the first quarter of 2012, the number of new Android-focused malware families and variants had increased from 10 to 37, and the number of malicious Android-focused application package files had increased from 139 to 3,063[viii]. Moreover, personally owned devices will normally bypass outbound content filtering systems, resulting in potentially more violations of corporate and regulatory policies focused on encrypting sensitive content or preventing disclosure of confidential information. Add to this the fact most personally owned devices cannot be remotely wiped if they are lost, leading to a much greater likelihood of data breaches and loss of intellectual property.

One of the fundamental dangers of BYOD is that personally owned and managed devices that are used to create, access and store corporate data will typically bypass inbound content filtering systems that have been deployed by IT.

The greater security risk posed by the use of personally owned devices was borne out in the research conducted for this white paper. For example, in organizations with at least 100 employees, we found that:

- 69% of company-owned smartphones can be remotely wiped if they are lost compared to only 24% of personally owned smartphones. Similarly, 54% of company-owned tablets can be remotely wiped versus only 21% of personally owned tablets.

- 44% of company-owned smartphones and 38% of company-owned tablets can be scanned for malware; the figures for personally owned smartphones and tablets are 10% and 9%, respectively.

Moreover, BYOD can increase the likelihood that sensitive or confidential corporate information will be breached. For example, researchers in a UK-based study acquired 49 mobile devices that had been resold through secondary markets; forensic examination of the devices resulted in the discovery of information on every device and a total of more than 11,000 pieces of information collectively from all of the devices[ix].

LEGAL AND REGULATORY PROBLEMS

Another danger of BYOD – and one that also affects employers who provide mobile devices themselves – is that non-exempt employees may have to be paid for their after-hours work using mobile devices. This applies to employers who require this work, as well as to those that are simply aware of it. For example, companies including T-Mobile and Black & Decker have been sued by employees for their unpaid overtime as a result of doing work with their smartphones after hours[x]. In the case of *Scheinder v. Landvest Corporation*[xi], the court ruled that "an employer is obligated to pay an employee for all hours worked, even those in addition to his or her pre-scribed schedule, if the employer knows or has reason to know that the employee is working additional hours". Terremark Worldwide was sued in a 2008 class action because Data Return LLC, a company that it had acquired, allegedly required employees to respond to phone calls and emails after hours from their mobile devices[xii].

It is also important to note that firms registered with FINRA and the SEC are required to archive and monitor communications via smartphone. For example, FINRA

Regulatory Notice 07-59[xiii] states "…a firm should consider, prior to implementing new or different methods of communication, the impact on the firm's supervisory system, particularly any updates or changes to the firm's supervisory policies and procedures that might be necessary. In this way, firms can identify and timely address any issues that may accompany the adoption of new electronic communications technologies."

CONTENT RETENTION AND MANAGEMENT

Smartphones and tablets contain a significant proportion of corporate data. Osterman Research has found that more than five percent of corporate data is stored just on users' smartphones – we expect this figure to soar during the next 24 months as iPads and other tablets are employed in much larger numbers. Employee-owned and controlled devices make access to this data by corporate IT or compliance departments much more difficult, such as during an eDiscovery exercise. This is not only because of the difficulty that might be encountered in physically accessing these devices, but also because of the potential privacy and other legal issues that are raised by companies accessing their employees' personal property.

From a purely practical standpoint, knowing what data is available on mobile devices becomes more difficult. This is particularly problematic for legal counsel and others that must assess the information that the organization has available to it during eDiscovery, early case assessments, legal holds and similar types of litigation-related activities. Moreover, the likelihood of spoliation of content stored on personally owned devices is much greater simply because it is not controlled by the IT or compliance department.

With regard to just the legal hold issue, when data that might be required in a legal action must be held back from the normal deletion cycle or from users' arbitrary deletion, it is imperative that an organization immediately be able to retain all relevant data, such as emails sent from senior managers to specific individuals or clients. Placing a hold on mobile data may be more difficult than it is for traditional systems – and much more difficult when it is located on devices that are under the control and ownership of individual employees.

Placing a hold on mobile data may be more difficult than it is for traditional systems – and much more difficult when it is located on devices that are under the control and ownership of individual employees.

CORPORATE GOVERNANCE

There are a growing number of corporate governance obligations with which virtually every organization must comply, but particularly those in heavily regulated industries. These obligations, which are focused primarily on the archiving, encryption and monitoring of certain types of communications, include the following:

- The **Payment Card Industry Data Security Standard** is a set of requirements for protecting the security of consumers' and others' payment account information. It includes requirements for building and maintaining a secure network, encrypting cardholder data when it is sent over public networks and assigning unique IDs to each individual that has access to cardholder information.

- The **Gramm-Leach-Bliley Act** requires financial institutions to protect sensitive information about individuals, including their names, addresses, and phone numbers; bank and credit card account numbers; income and credit histories; and Social Security numbers.

- The **Health Insurance Portability and Accountability Act (HIPAA)** requires healthcare and other organizations to protect sensitive health records of patients and others. However, the "new" HIPAA that took effect during the first quarter of 2010 greatly expands the impact of the law. For example, while HIPAA previously applied mostly to physicians, medical practices, hospitals and the like, now the business associates of these entities will be required to comply with HIPAA's rules about the security and privacy of protected health information (PHI). That means that accountants, benefits providers, attorneys and others

that are given access to PHI will now be fully obligated to comply with HIPAA.

- Electronic recordkeeping rules established by the **SEC, FINRA, FSA** and other regulatory bodies are focused on financial services organizations' obligations to monitor and archive communications between registered firms and their customers.

- The **Federal Rules of Civil Procedure** obligate organizations to manage their data in such a way that it can be produced in a timely and complete manner when necessary, such as during legal discovery proceedings.

- The **Sarbanes-Oxley Act of 2002** obligates all public companies and their auditors to retain relevant records like audit workpapers, memoranda, correspondence and electronic records – including email -- for a period of seven years.

- **Federal Energy Regulatory Commission** Order No. 717 imposes various rules on regulated and vertically integrated utilities so that transmission providers do not give preferential treatment to their affiliated customers. The purpose of this order is to create an ethical wall between the marketing and transmission functions of vertically integrated companies that distribute electricity and natural gas between states.

These governance requirements apply to any platform in use by an organization, including those that are owned by and under the control of employees, if they are used to access or store corporate information.

POTENTIALLY HIGHER COSTS

An Aberdeen Group analysis found that a 1,000-seat organization will spend an additional $170 per user per year when using BYOD as compared to providing smartphones themselves[xiv]. This makes sense given that support for a wide range of mobile platforms, operating systems, operating system versions and firmware versions will typically be more expensive than supporting just one or two IT-approved and company-funded platforms.

However, BYOD can lead to other, potentially enormous costs. For example if a company-owned smartphone that contains consumer data is lost and it cannot be remotely wiped, in most cases an organization will be obligated to report this data breach to all of the affected parties. If we assume, as discussed above, that 69% of company-owned devices can be remotely wiped compared to only 24% of personally owned devices, then the likelihood of losing data for the latter – and the cost of the data breach – will be 2.9 times greater.

If a company-owned smartphone that contains consumer data is lost and it cannot be remotely wiped, in most cases an organization will be obligated to report this data breach to all of the affected parties.

STEPS TO MANAGING BYOD

There are five steps that Osterman Research recommends for any organization as it attempts to manage the growth of BYOD:

- **Management must understand the benefits and risks**
  The key to dealing with the BYOD phenomenon is first to understand just how pervasive it is in most organizations. While most senior managers will surmise that some of their employees are using personally owned smartphones and tablets (given that senior managers often were the instigators of the trend after the introduction of the iPhone), they may not appreciate just how widespread this use has become. Senior managers need to understand how personally-owned smartphones and tablets, as well as tools like personal file sync services or Skype, are used throughout the organization, what types of data they are used to access and store, and the reasons for their use.

- **Evaluate the options**
  Decision makers in IT, HR, compliance, etc. should then consider the options for managing BYOD. The available options will range from doing nothing to implementing draconian controls that will all but eliminate – or at least attempt to eliminate – the use of personally owned devices and employee-managed applications for work-related purposes. While some decision makers may opt for the latter as a sort of knee-jerk reaction to protect corporate data assets or reduce the potential for malware infiltration, there are two reasons to opt for more open, rather than more restrictive, BYOD-related attitudes:

  - ***Draconian controls are unlikely to work***
    Faced with a requirement to eliminate use of personal devices or applications, many employees will do so secretly, particularly the growing proportion of employees who work from home at least one day per week. For organizations that need to lean in this direction, if eliminating consumer-grade options, an easy-to-use, secure and sanctioned alternative must be provided.

  - ***Employee productivity will suffer***
    It is important to understand that the vast majority of employees do not use their own devices or applications simply for the fun of it – they are doing so to be more productive, to bypass IT restrictions (e.g., email file-size limits) that prevent them from being effective in their work, or because they have found a way to be more efficient at no charge to their employer. To issue an edict that prevents employees from using these tools will likely be counterproductive to the interests of both management and employees.

- **Implement policies to protect the organization**
  It is critically important that organizations faced with the BYOD problem implement policies about acceptable use of devices and applications, perhaps creating a list of approved devices, operating systems, applications and other personally owned or managed solutions. These policies should be detailed and thorough, and should be included as part of an organization's overall acceptable use policies that are focused on use of corporate computing resources.

  A key element of these policies as they apply to mobile devices should be that any mobile device must be wipe-able by the IT department in the event of its loss, and that all devices that contain corporate content should be encrypted to prevent the loss of sensitive data or intellectual property. 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 on best practices**
  It is also important to educate users on best practices with regard to accessing and managing corporate data on personally-owned devices or when using specific applications. An important reason for doing so is not only to make employees aware of the dangers that can ensue if corporate data is not adequately protected, but also to achieve employee buy-in and cooperation with corporate policies.

- **Deploy the appropriate technologies**
  Finally, it is imperative that organizations deploy technologies, such as mobile device management solutions, that will enable their policies to be satisfied and for overall corporate risk to be managed at an appropriate level. For example, an organization in which a consumer-focused file-sharing application is used should deploy an alternative that is just as easy to use, but one that provides IT control over how content is shared (expiration dates for content, tracking managing and reporting of files downloads and sharing, control over file types that can be sent, automatic encryption of content sent beyond the corporate firewall, etc.). Similarly, an organization that allows employees to use personal tablets should deploy a solution that enables full disk encryption, under IT's

It is critically important that organizations faced with the BYOD problem implement policies about acceptable use of devices and applications, perhaps creating a list of approved devices, operating systems, applications and other personally owned or managed solutions.

control, that will protect sensitive data if the device is lost. Other technologies that should be on the short list of those deployed include anti-virus, malware detection and remediation, role-based access, content inspection and archiving – these apply to both personally owned devices, as well as to employee-managed applications.

SPONSOR OF THIS WHITE PAPER

McAfee is the world's largest dedicated security technology company. Delivering proactive and proven solutions and services that help secure systems and networks around the world, McAfee protects consumers and businesses of all sizes from the latest malware and emerging online threats. Our solutions are designed to work together, integrating antimalware, antispyware, and antivirus software with security management features that deliver unsurpassed real-time visibility and analytics, reduce risk, ensure compliance, improve Internet security, and help businesses achieve operational efficiencies.

Backed by an award-winning research team, McAfee security technologies use a unique, predictive capability that is powered by McAfee Global Threat Intelligence — enabling home users and businesses to stay one step ahead of online threats. McAfee's security products and solutions span the following areas:

- Data Protection
- Database Security
- Email & Web Security
- Endpoint Protection
- Mobile Security
- Network Security
- Risk & Compliance
- Security-as-a-Service (Security SaaS)
- Security Management
- Security Information and Event Management (SIEM)

McAfee solutions deliver the highest levels of threat visibility and antimalware protection, including comprehensive system and endpoint protection, network security, cloud security, database security, and data protection. McAfee's complete security solutions extend beyond virus software. Backed by McAfee Global Threat Intelligence, our solutions help companies enhance visibility into their security postures, allowing business to embrace Web 2.0 technology, virtualization, cloud computing, and personal and mobile devices, while protecting critical assets and sensitive data.

www.mcafee.com
twitter.com/mcafee
sales@mcafee.com

+1 888 847 8766
+1 408 988 3832

---

[i] http://www.researchandmarkets.com/research/pwsr9h/bring_your_own_dev

[ii] http://www.xigo.com/byod/

[iii] http://www.equanet.co.uk/cms/apple/ipad-in-business/bring-your-own-device.html

[iv] http://www.zdnet.com/blog/sybase/cisco-the-biggest-mobile-byod-deployment-around-slides/2671

[v] http://www.bgr.com/2012/01/27/blackberry-users-are-older-and-wealthier-than-average-smartphone-users-study-suggests/

[vi] http://www.xigo.com/byod/

[vii] http://www.xigo.com/byod/

[viii] Source: *Mobile Threat Report Q1/2012*, F-Secure

[ix] *Electronic Retention: What Does Your Mobile Phone Reveal About You?* http://EzineArticles.com/7068075

[x] http://cspalaw.com/pdf/Smartphones.pdf

[xi] *Schneider v. Landvest Corp.*, 2006 WL 322590 (D. Col. Feb. 9, 2006)

[xii] http://www.munckwilson.com/media-center/in-the-news/audrey-mross-quoted-in-dallas-business-journal-article-employee-smartphone-

[xiii] http://www.finra.org/web/groups/industry/@ip/@reg/@notice/documents/notices/p037553.pdf

[xiv] http://www.vcinsight.com/116/ExecutiveIntervierws/807/ToBYODornottoBYOD–thatisthequestion!