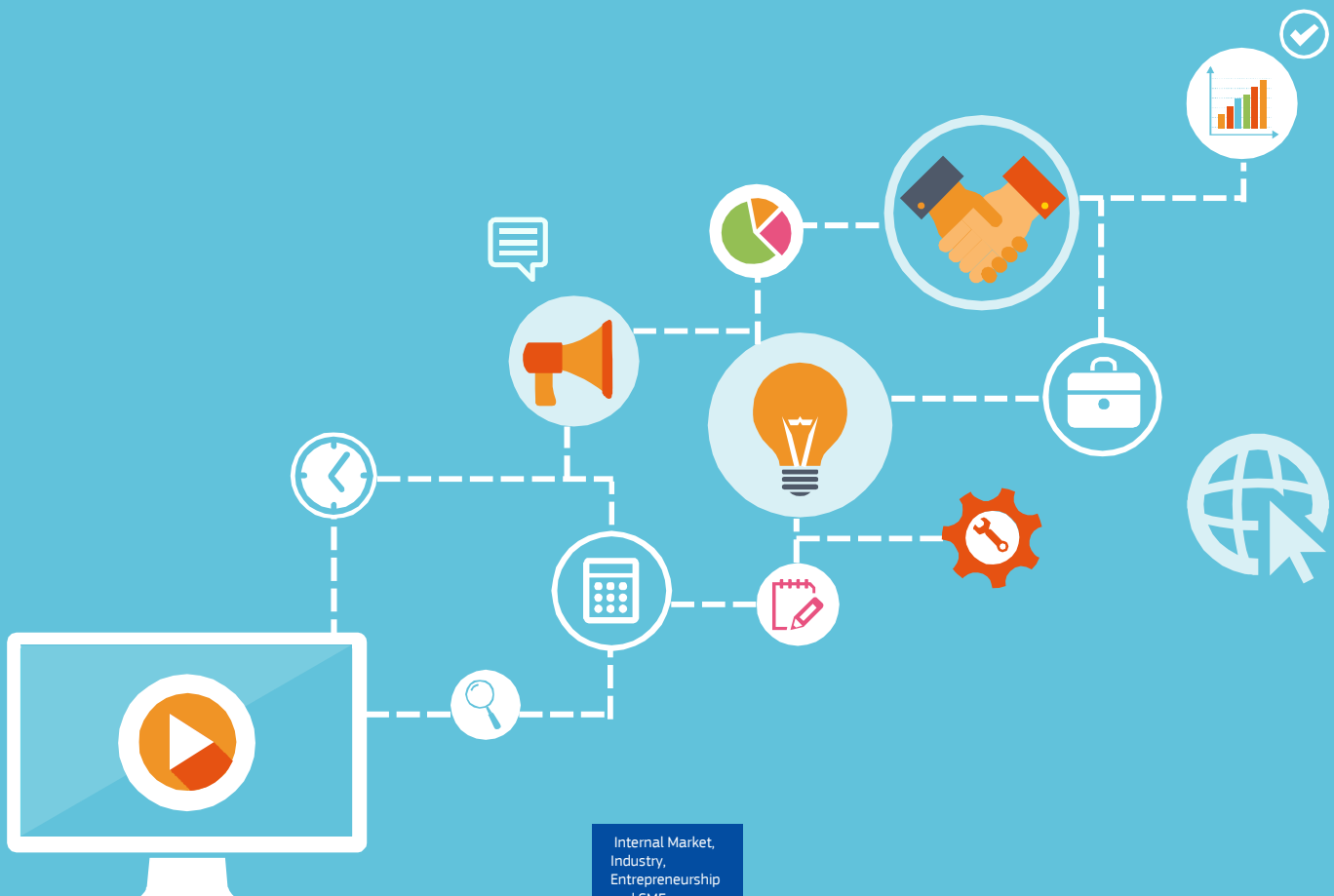
European Commission

Digital Transformation Monitor

Bring your own device: a major security concern

May 2017



Internal Market, Industry, Entrepreneurship and SMEs

© Rawpixel.com/Shutterstock.com

Bring your own device: a major security concern

More and more businesses are introducing Bring Your Own Device (BYOD) programmes believing that by allowing their employees the use of their own familiar devices to work, they will increase productivity while reducing costs. Simultaneously mobile malware reveals to be one of the ten most common attack types[1] making the corporate network vulnerable, and therefore requiring a stronger IT security system.

1

BYODs - gaining traction in the business world

BYOD or Bring Your Own Device refers to an increasingly popular trend in the business world which allows employees to bring their own computing devices including smartphones, tablets, laptops and wearables to their workplace for business use. BYODs might also be referred to as employee-owned devices as opposed to corporate-owned devices, or personal-liable devices as opposed to corporate-liable devices.

BYODs in the office – presence and modes of usage

Typically, personal mobile devices are used to access the corporate network for communication, presentation, databases, download and share documents and files. The LinkedIn Information Security Community reported in their latest survey[2] that for 84% of respondents, email, calendar and contact management are the most common applications used via BYOD followed by document access and editing (45%), access to Intranet (43%) and finally access to SaaS applications such as Salesforce (23%).

Simultaneously, smaller business are more likely than bigger companies to jump on the BYOD trend. According to a TechPro survey[4] led in 2014, 71% of the small businesses were already allowing BYODs, compared to only 54% among big businesses.

It has to be pointed out that European businesses are significantly lagging behind their North American colleagues regarding the overall adoption of BYODs. In North America, over three-quarters of business smartphone users bring their own device to work. In Europe, on the other hand, corporate-liable devices keep dominating the global installed base of business smartphones.

In the first quarter of 2015, 61% of all business smart phones in Western Europe were corporate-liable[3]. In Central and Eastern Europe, the rate of BYOD devices shipped was slightly higher in the same period (41%) while remaining far inferior to the number of BYODs sold in the US. European businesses are thus approaching this trend more cautiously than their American colleagues.

More personal-liable than corporate -liable devices

BYOD smartphones shipments **61%**

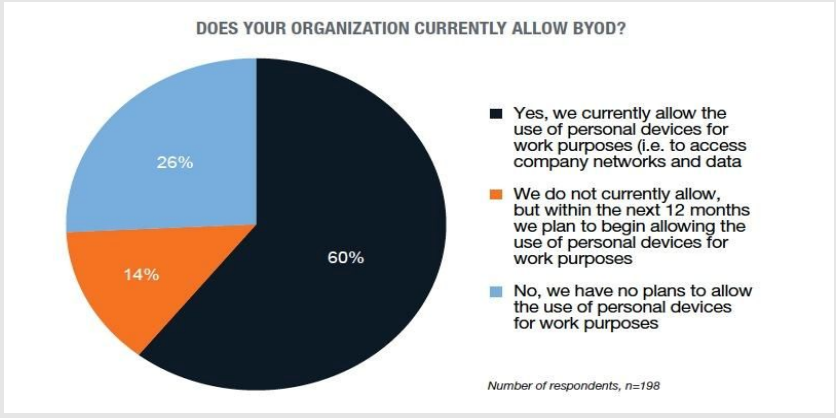
Source: Strategy Analytics[3]

Use of the BYOD concept - driving growth in the mobile business device market

The market for business smartphones has been steadily growing. According to a Strategy Analytics study[3], business smartphone shipments accounted for 27% of the global market in 2015 compared to 22.6% in 2014. This increase in shipments was driven by BYODs that made up for almost two thirds of all business smartphone shipments in this period.

A similar trend can be observed in the tablet market, in which the proportion for business owners is estimated to increase from 14% to 20% in the 2015-2020 period[5].

More and more entreprises allow the use of personal devices



Source: TechPro

2

Advantages of the BYOD concept

Increasing productivity

One of the expected benefits associated with the adoption of the BYOD concept is an increase in the efficiency of employees due to working in a comfortable environment. By adopting BYOD, employees can work in a consistent and flexible mobile environment. At the same time, as they are already familiar with the system used, productivity can be increased.

Studies estimate that employees using the BYOD concept work up to 2 additional hours each day, checking and sending emails as well as making/taking calls[6]. Moreover, employees check their messages 20 times more per day if they have access to their work emails on their personal devices.

Increasing employee satisfaction

Another significant advantage of the BYOD concept is its positive effect on employee satisfaction[2]. The BYOD concept allows employees to use the device of their choice for work even if they have to buy them themselves. Forrester study[5] notes that 55% of tablet users bring their own device to work because their company did not want to purchase them even though they felt they needed them. By adopting the BYOD concept, this problem can be directly solved.

Encouraging mobility

The BYOD concept is naturally linked to the growing mobility of employees that spend most of their time outside the office. However, in some specific markets where mobility is seen as primordial (eg. healthcare) the sensitive nature of the data imposes specific care in the implementation of the BYOD concept and will require enforced security. Governments are also expected to oppose the BYOD concept due to the sensitivity of the information treated[4].

Employees work more with BYOD

2 hours

More per day

Source: BMC[9]

Saving equipment costs

The BYOD concept allows companies to shift their equipement costs to the employee as they have to purchase their own devices. This allows companies to cut costs related to the acquisition of devices and related expenses (voice and data plans, maintenance, repair etc.).

By adopting the BYOD concept IT systems can increase the support they offer as the investments previously used for the acquisition of devices can now be shifted to their maintenance[7].

3

Strong security concerns despite BYOD benefits

The risk of losing corporate data

As the concept of BYOD involves the mix of personal and company data on the same device, security concerns about the safety of corporate data can increase. An attack on an employee's mobile phone can compromise the company's entire security system.

Losing critical company data, and especially customer data represents the major concern for most of the companies not yet having adopted the BYOD concept. 37% of respondents of a TechPro survey[4] ruled out BYOD due to security reasons. Other concerns include unauthorized access to company data and systems, the downloading of unsafe apps or content, the loss of devices, malware and the exploitation of vulnerabilities.

Who is responsible for setting up the BYOD policy in your organization ?

Source: Crowd Research Partners[2]

Enterprises are attacked

every 3 minutes

One attack costs

2730 € per day to recover

Source: Fireeye[10]

The need for a stronger security system

A LinkedIn survey[2] reveals that security breaches are on the rise with BYOD with 39% of respondents having experienced mobile threats using their devices and 37% of respondents not being sure whether they have been breached. At the same time, 35% of respondents needed additional IT resources to manage mobile security. Further investments regarding the development of mobile applications as well as the time spend on managing the internal network might thus be necessary to protect the company's internal IT system.

Box 1: Security failures increased by BYOD

- 51% of companies allowing BYOD experienced a mobile data breach
- 38% reported stolen or lost data
- 31% confidential data stolen
- 7% information destroyed

Source : Ponemon Institutes[8]

4

Steps to limit the risk posed by BYODs

The use of personal devices for business purposes has led entreprises to create dedicated policies especially focusing on security and management concerns. The BYOD security policy aims to guarantee the security of the company's corporate network while giving employees the possibility to use their own devices.

At the same time, BYOD policy needs include a list of the employees eligible to bring their own devices, the identification of those employees that require access to confidential and sensitive information and how they use it.

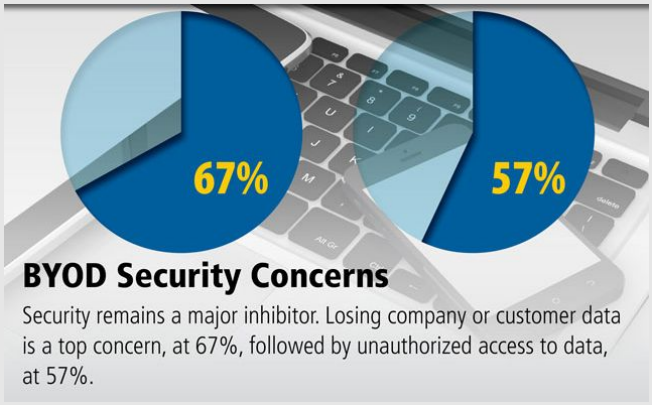
Separation of corporate and personal information on the device

Implementations of antivirus programs or password protections can separate work and personal information on mobile devices.

A further solution to cope with privacy issues has been developed by enterprise mobility management providers such as AirWatch by VMware. Samsung, on the other hand, relies on its Knox offering which provides notably features targeting the BYOD trend with the ability to dynamically switch between a professional and a personal mode on a single device.

Both solutions are based on the separation of corporate and personal data on devices through customisable privacy policies that can be based on device ownership type.

Data security is the main concern with BYOD



Source: Channel insider

5 New trends adapting the BYOD concept

COPE – the Corporate-Owned Personally-Enabled model

The COPE model allowis IT managers greater control over the devices used while not depriving their employees of the devices that make them more productive.

Indeed, with COPE, devices are purchased by the company and thus remain corporate owned devices. This makes it easier for the company to protect its IT system as all the employees use the same device model. This makes it easier for IT managers to manage mobile fleets.

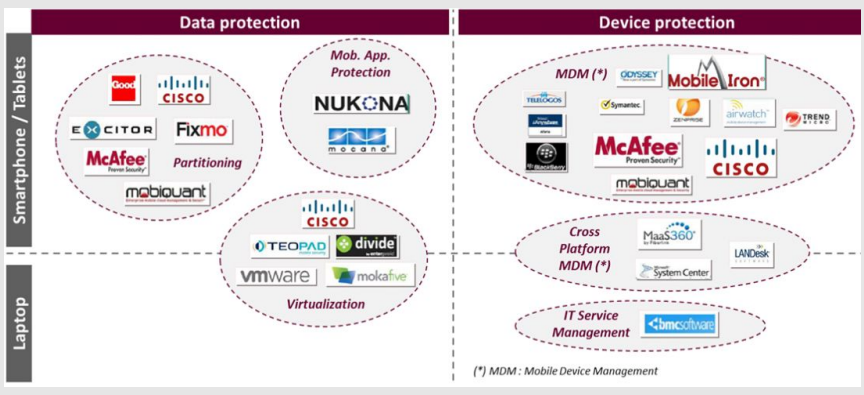
Moreover, employees are allowed to use their corporate devices for personal activities and can select their favorite services and applications. They are thus given a certain amount of freedom while keeping the corporate network secure.

The only disadvantage of the COPE method is that the company might have access to the employees private information, which some might consider a breach of their privacy. To limit any interference in their employees privacy, companies are therefore trying to delimit clear areas solely dedicated to business activities.

CYOD – Choose Your Own Device

The CYOD offers employees a bit more freedom than the COPE model by allowing the employees to choose their business device from a selected list defined by the company. On one hand this allows employees to express their preferences, on the other hand it allows the company's IT department a certain amount of control over the devices used on the company's network.

Large ecosystem to secure BYOD



Source: CIO advisory

References

[1] Threat Research published in July 2016 by Check Point

[2]http://www.slideshare.net/hschulze/byod-and-mobile-security-report-2016-01

[3] https://www.strategyanalytics.com/strategy-analytics/news/strategy-analytics-press-releases/strategy-analytics-press-release/2015/06/17/business-smartphones-shipments-in-q1-up-26-from-last-year-now-27-of-total-smartphone-market#.VmG1kHYve00

[4]http://www.techproresearch.com/article/research-byod-booming-with-74-using-or-planning-to-use/

[5] Tablet market report by Forrester Research at https://www.forrester.com/Apple+Google+Microsoft+Battle+For+EnterpriseOwned+Tablet+Market+Making+Up+20+Of+Gl

[6]http://www.telegraph.co.uk/technology/mobile-phones/9646349/Smartphones-and-tablets-add-two-hours-to-the-working-day.html

obal+Tablet+Market+By+2018/-/E-PRE8124

[7] http://www.gartner.com/newsroom/id/2909217

[8] http://www.websense.com/content/ponemon-institute-research-report-2012.aspx?cmpid=prnr2.29.12

[9]http://www.bmc.com/blogs/is-byod-a-glorious-boost-to-productivity-or-a-gaping-hole-in-your-it-security-plan/

[10]https://www.fireeye.com/platform/overview-of-advanced-cyber-attacks.html

[11] http://www.esg-global.com/mobility-spending-brief

About the Digital Transformation Monitor

The Digital Transformation Monitor aims to foster the knowledge base on the state of play and evolution of digital transformation in Europe. The site provides a monitoring mechanism to examine key trends in digital transformation. It offers a unique insight into statistics and initiatives to support digital transformation, as well as reports on key industrial and technological opportunities, challenges and policy initiatives related to digital transformation.

Web page: https://ec.europa.eu/growth/tools-databases/dem/

This report was prepared for the European Commission, Directorate-General Internal Market, Industry, Entrepreneurship and SMEs; Directorate F: Innovation and Advanced Manufacturing; Unit F/3 KETs, Digital Manufacturing and Interoperability by the consortium composed of PwC, CARSA, IDATE and ESN, under the contract Digital Entrepreneurship Monitor (EASME/COSME/2014/004)

Authors: Vincent Bonneau & Soichi Nakajima, IDATE; Laurent Probst, Bertrand Pedersen & Olivia-Kelly Lonkeu, PwC