Enterprise mobility in the French retail sector

Providing guidance to Microsoft France

Alessandro Bottarelli

Dissertation written under the supervision of
Dr. Pedro Celeste

Dissertation submitted in partial fulfilment of requirements for the International MSc in Management, at the Universidade Católica Portuguesa, 06/06/2016.

Abstract

The recent innovation in the world of IT has forever changed the way different players interact in the market. The questions around IT mobility in the work environment are today more relevant than ever. It is at the heart of most large IT companies to figure out answers to certain core questions for their customers and themselves above all. This study describes the different ways in which mobility comes to be in the work environment and the different issues a company might be facing when adopting a mobility strategy, and analyzing the factors that might be most influential to a large company in the retail sector that wishes to adopt such a mobility strategy. Through qualitative research, we attempt to provide recommendations to Microsoft France to better tackle this issue in such a "blank slate" sector. Our sample of 15 companies is based on what Microsoft France has classified as "large customer" in the "retail industry" on French soil. The results indicate that there is strong potential for Microsoft to penetrate this vertical (albeit not necessarily with phones, which remain the weakest link in the Windows range of devices), and that Microsoft has strong potential to achieve it. Even companies in a sectors that has been historically hard to reach, such as retail, Microsoft with its full stack of products has the opportunity and ability to convince companies to move forward towards a more mobile approach for their IT strategy on a unified platform that guarantees a secure environment.

Resumo

A recente inovação no mundo das TI mudou para sempre a forma como os diferentes intervenientes interagem no mercado. As questões em torno da mobilidade das TI no ambiente de trabalho são hoje mais relevantes do que nunca. Está no cerne da maioria destas grandes empresas encontrar respostas para certas questões nucleares para os consumidores e, acima de tudo, para elas mesmas. Este estudo descreve as diferentes formas como a mobilidade está presente no ambiente de trabalho e as diferentes situações que uma empresa pode enfrentar ao adoptar uma estratégia de mobilidade e analisando os factores que possam ser mais influentes para uma grande empresa do sector do retalho que deseje adoptar tal estratégia. Através de uma pesquisa qualitativa, pretendemos propor recomendações à Microsoft França de modo a melhor abordarem esta questão num sector ainda por explorar. A nossa amostra de 15 empresas é baseada no que a Microsoft França classificou como "grande cliente" na "indústria do retalho" em solo Francês. Os resultados indicam que há um forte potencial para a Microsoft penetrar este sector (embora não necessariamente com telefones, que permanecem o elo mais fraco no conjunto de dispositivos Windows), com um forte potencial de o atingir. Mesmo falando de empresas de um sector de difícil acesso como o retalho, a vasta selecção de produtos da Microsoft dá-lhe a oportunidade e a habilidade de convencer as empresas em progredir para uma abordagem mais móvel nas suas estratégias de TI através de uma plataforma unificada que garante um ambiente seguro.

Acknowledgements

Foremost, I express my infinite gratitude to my family who has supported me unconditionally throughout my life. Their invaluable patience and foresight led me to this point.

I am deeply thankful to my ESCP and UCP friends and colleagues for over three years of life-changing adventures, stimulating discussions and shared sleepless nights. We have truly gone through thick and thin.

I would like to gratefully and sincerely thank my research advisor, Dr. Pedro Celeste, for his patience and constructive feedback. I am very appreciative of his never-dwindling kindness. After months of no results, even the most accommodating academic would have given up on a slacker such as myself.

In addition, I would like to thank Microsoft France and all those who have helped me gather all the necessary information, upon which this entire study is based.

Finally, I would like to thank the Justice League of America, for the inspiration that its members have given me molding me into a better man today than I was yesterday. Especially you, Batman.

Table of Contents

1. Introduction

In a world where innovation is key, the IT Industry represents today one of the most competitive and fast-paced environments of the B2B scene, from Market Knowledge to Strategic Marketing.

Over the last decade, the industry has seen an incredible rise in the use of mobile devices in the workplace. Microsoft is one major provider of said devices and the support in security that comes with them. Recently, there has been a steep increase in visibility and attention paid to cases where security has been breached and companies handling said security have taken strong hits in image and credibility. These cases ranged from celebrity pictures leaking over the internet, to much more serious confidential information outflows (see Sony and JP Morgan Chase). Understandably, companies expecting variable levels of security are raising red flags on the reliability of both the hardware and (especially) the software they're provided with. Some companies expect low levels of security, while others can't settle for anything less than the very best.

In the specific case of the French market, Microsoft holds a relatively solid market share and enjoys a fairly strong image, particularly in terms of security, but some vertical segments are still very tough to even access. Microsoft aims not only to penetrate these segments, but to do it before its main competitors, and to gain a strong and sustainable hold from within.

In this paper we attempt to confirm that security is in fact a strong factor in the eyes of a number of enterprises within a subset of Microsoft France's client base, and get a grasp of their propensity to adopt mobile devices solutions; subsequently, we will try to find some way to strategically leverage Microsoft's value proposition to penetrate this "blank slate" vertical through mobile devices.

The paper is structured as follows: a literature review of existing academic articles on the topics at hand, most notably, on the subjects of technology in the retail sector, security

threats identification, and protection from security threats; then, some analyses of primary and secondary data to attempt to answer the various research questions.

The Problem Statement is defined by the need for Microsoft to gain insights on how to penetrate large enterprises in the French retail sector through mobile devices. Consequently, the main objective of the paper will be to provide some recommendations that can be applied by Microsoft to tackle its current issue.

To embark in this endeavor, the key Research Questions will inquire about the degree of maturity of the French retail sector regarding enterprise mobility, the drivers dictating adoption in favor of each of the two mainstream mobility strategies, and the actions that Microsoft France can take through its current offering.

In order to answer the research questions, we've devised a questionnaire for IT professionals within the fifteen large retail enterprises that Microsoft France, encompassing several topics, from current park of devices, to inclination towards a particular mobility strategy, to security software provision. The results were benchmarked against market research conducted on the entire French market by international Market Intelligence firms, most notably, Strategy Analytics.

Primary data will be collected and analyzed through "on the field" questionnaires, while secondary data will be collected through internal Microsoft sources and specialized sources (such as Strategy Analytics). We will develop a couple of sets of hypotheses building on the existing body of market research; we will then present the methodology for our study, and infer its findings: we discuss said findings and compare them to our initial sets of hypotheses.

We shall conclude by affirming the limitations of the study and set some grounds for future research.

2. Literature review

The following Literature review will be structured as follows: the first part of the review will provide a brief overview of the retail sector and the role that innovation plays in it; the different threats and security issues related to malware on mobile devices will be listed in the second part of this review, while the different ways for an enterprise to detect and take counter-measures against malware will be dealt with in the third part of this review.

Unfortunately, due to the relative modernity of the subject of enterprise mobility and the subsequent lack of academic papers, those cited will be limited in number, and the scope they shall mostly cover is that of supporting the review on the risks that mobility carries, along with ways to detect and insure a firm from falling prey to these risks; on the other hand, much more recent and relevant market studies by international Market Intelligence firms will be used to illustrate the current market state and the benefits of enterprise mobility adoption, and will be described in the "Case Study" section.

2.1. Technology in the retail sector

The most recent studies show that progresses in IT are one of the main drivers across industries for innovation; in fact, 5 categories seem to drive innovation adoption across industries:

- Market orientation: Market intelligence generation, distribution, and responsiveness; it is very customer-facing and inter-functional across departments (Boso et al., 2012; Fortuin and Omta, 2009; Hameed et al., 2012; Kohli and Jaworski, 1990; Lewrick et al., 2011; Rhee, Park, and Lee, 2010; Sandvik and Sandvik, 2003).
- Entrepreneurial innovation: The firm's own ability to innovate and adopt an innovation before the competition (Boso et al., 2012; Gunday et al., 2008; Marcati et al., 2008).

- Human capital: The openness and willingness of employees and General Management to be the first adopters of a particular idea or process improvement (Manley and McFallan, 2006; Marcati et al., 2008; Parrilli and Elola, 2012).
- Organizational characteristics: The firm's ability to understand and adapt to changes in the environment, through financial resources, infrastructure, and people (Ellonen et al., 2009; Gunday et al., 2008; Hameed et al., 2012; Rhee et al., 2010).
- Progresses in technology: Progress in science and technology provide many chances to improve and enhance specific organizational processes (Pantano and Viassone, 2014; Parrilli and Elola, 2012).

Information technology is increasingly considered as an enabler of business competitive advantage in addition to its contribution to satisfy consumers' demand of innovative and qualitative product and services (Chen & Tsou, 2012; Pantano & Viassone, 2014). Due to the large deal of research on advanced technologies and the subsequent speed of development of new systems for supporting retailers and consumers (Gunday, Ulusoy, Kilic, & Alpkan,2008; Pantano & Viassone, 2014), retail industry is frequently subject to a disruptive innovation process that makes available a large amount of novel information systems able to modify the traditional organizational process. Also, different retailers actually show a consistent heterogeneity in innovating strategies (Bennett & Savani, 2011; Fiorito, Gable,& Conseur, 2010; Pantano & Viassone, 2014; Walter, Battiston, Yildirim, & Schweitzer, 2012).

Pantano (2014) provides an interesting set of insights showing the diffusion of different innovations in the retail sector, listing the types of technologies adopted, the number of adopters and the amount of investment required. It seems that mobile apps are very widely adopted, perhaps due to its very low cost of implementation; even more noteworthy is the fact that differently from other innovations adopted in the retail sector, mobile apps seem to be adopted across the entire retail spectrum (luxury brands, low cost brands, small retailers and large retailers).

2.2. Threats to IT security

Cyber attackers may be moved by different motivations: the what and how has been

covered by quite a number of authors. According to Felt et al. (2011), to this day, mobile malware has as its primary motivations a desire to send premium-rate SMS messages and sell information; the former motivation can be defeated by making user confirmation mandatory for premium-rate SMS messages; however, the authors believe that more research is required for understanding how to best defend oneself against malware attacks that steal user data and credentials.

A more interesting mapping of malware characteristics is given by Suarez-Tangil et al. (2013). Characteristics are divided as follows: the three main characteristics to identify a piece of malware are "goals and behaviors", "distribution and infection", and its "privilege acquisition"; each of these characteristics are subdivided into more granular sections. Goals & behaviors include Sabotage, Fraud, Theft, SPAM, and Service Misuse. Distribution & infection include Market to Device (M2D), App to Device (A2D), Web to Device (W2D), SMS to Device (S2D), Network to Device (N2D), and USB to Device (U2D).
Privilege acquisition involve User manipulation, and Technical exploitation.

An overview of the major software threats is given by La Polla et al. (2013), by describing the following types of malware:

- A piece of code that can replicate itself is called a "virus". Different replica of the same virus can infect and affect different programs and files in different ways.
- A program that copies itself from one device to another is called a "worm"; it can use different kinds of transport mechanisms without any user intervention. Usually, it does not attach to other programs in the same infected device, but it may compromise its security or hinder (or even damage) its performance.
- A software that appears to provide some functionalities, but instead contains a type of malware is called a "Trojan".
- A type of malware that directly infects the OS is called a "rootkit": rootkits are especially sneaky and difficult to eradicate, since they hide in the OS itself; they achieve their malicious goals by installing Trojans, or disabling firewalls and anti-virus software.

- Finally, a set of devices that are infected by a virus is called a “botnet”. The virus gives the attacker the ability to remotely control the infected devices. Botnets pose a very severe security threat.

More specifically to botnets, Vural et al. (2010) states that a botnet is more dangerous than average malware, as upon infecting the device, the attacker gains access to the devices and can perform malicious activities by controlling apps on the device. A botnet is the network of such infected devices, thus, an attacker can access hundreds of infected devices as a single botnet.

Others authors have spoken of the dangers of botnets, but Pieterse & Olivier go even further and identify several categories of attacks by botnets, among which

- Repackaged Applications (following the principle behind Trojans)
- Receiving Commands
- Messaging
- Steal Information
- Third Party Application Markets (granting access to unauthorized parties)
- Additional Content Download

Knowing about these characteristics can help identify and prevent a botnet attack. Future research shall include the identification of these botnets by means of signature-based detection or behavior-based detection.

In a practical study conducted by Rastogi et al. (2014), anti-malware performance shows to have significantly improved over the last few years, as the authors point out in their wide comparison of popular commercial anti-malware applications; however, they remain stupefied by their findings, as none of the applications they've sampled seems to withstand some of the most common malware transformation techniques.

Building on the study by Rastogi et al. (2013), Maiorca et al. (2015) argue that an attacker can generate an obfuscated sample, by carefully understanding how signatures are designed to identify malware, and take that into account to evade detection. They also prove that it is not necessary to resort to extremely complex obfuscation strategies to obtain good

evasion performances. More robustness could be achieved by mixing static and dynamic analysis of the code.

As for where the future of malware motivation lies, Felt et al. (2011) explore a wide variety of potential future directions for malware development; in particular, they believe that credential theft, credit card theft via NFC, and advertising click fraud will be the most likely targets of malware in the future.

2.3. Malware detection and protection in the Enterprise

Before directly comparing the security of the main mobile operating systems, we shall look at some proposed practices of malware prevention concerning installed apps. In the pursuit of defense from malware for any device, previous authors have generally focused on two main stages of protection: the back-end (the developers) and the front-end (the users).

2.3.1. The back-end

The back-end of malware protection starts with the security mechanisms embedded in the ecosystem. Most authors propose a number of standard sandboxes, where any app submitted to any app store is made to run continuous tests in a controlled and isolated environment. Two prominent studies of this proposition come from Spreitzenbarth et al. (2013) and subsequently, Spreitzenbarth et al. (2015).

In the first study, dated 2013, the authors analyze the results of sandboxing a set of malicious software to test the reliability of the method. They find a number of flaws and they offer two possible solutions: the first is to run parallel sandboxes on the same software, so to pinpoint exactly what mistakes are made by the detection method; the second is to start implementing a detection method that no longer uses anti-viruses, and instead includes machine-learning techniques, so that the system would learn from its mistakes and evolve by teaching itself which software is malicious and which is benign, ideally at a faster pace than that at which malicious software adapts to detection methods.

In the second, and later study, they apply one of their previously proposed solution to three separate and subsequent tests: during the first test, they run a static analysis of the sandbox; during the second test, they run a dynamic analysis; while for the third test, they combine the results in the first two tests and analyze them with the help of machine-learning techniques. They conclude that the results are quite promising, albeit limited by the computing power of their utilized program.

Machine-learning seems to be the way of the future as it could not only improve performance in detecting malicious software that would normally pass unobserved under the radar, but also answer to problems such as that described by Maiorca et al. (2015) as deceiving the system through false positives: it is important that anti-malware engines not be easily deceived, with respect to false positives. In their study, results showed that the majority of the anti-malware engines classifies the benign samples they injected, as malware; hence, a clear flaw in most anti-malware detection capabilities. They conclude that anti-malware has greatly improved in the past few years; however, it is still very possible to evade detection or even have a piece of software be detected as malware by mistake. An additional fail-safe that could be implemented is proposed by Felt et al. (2011): in their analysis of the Apple AppStore, the market didn't approve of any of their proposed malicious software, which leads them to believe that prevention by human review is a feasible and effective, albeit not scalable, solution.

To enter more into the details of the main market players, Suarez-Tangil et al. (2013) have quite eloquently described the differences that exist between the security measures taken by each major marketplace. In a nutshell:

- Blackberry's security model is built in a way that applications have very limited access to the resources of the device they're installed on; in order to be granted access to some resources such as the user's professional information (a very limited set of resources nonetheless), the applications must be signed by the manufacturer, RIM. Also, applications must get authorization from the user to access external resources, such as the network. The downside might be that once the user has in fact granted access to an application to connect externally, the application can both

access the internet and send SMSs. Concerning the app development and marketplace, applications are not executed in a sandbox, but once installed they cannot interfere with each other (the apps are protected from one another).

- Android security model is much more anarchical than Blackberry's, as it lets users download apps from any market, regardless of if and how the apps have been tested for security. The system relies on a protection mechanism whereby applications declare the permissions they request at the point of installation, and it is up to the user to accept or refuse the conditions requested by the app. Many researchers are against this kind of up-to-the-user protection mechanism, as it increases risks of security breaches needlessly. Jeon et al. (2011) propose an extension of permissions enforcement, not to be requested just at installation, but also during runtime; Schreckling et al. (2012) propose that security policies be set for each individual resource and be valid for every app that requests permission to any one resource. Additionally, Android uses sandboxing to protect apps from malicious interference with other apps, though the apps can still communicate with each other using a rich functionality that is known to be a catalyst for malware infection, as described by Bugiel et al. (2011). Finally, Android requires that applications be signed with a certificate to identify the developer; however, these certificates can be self-signed, which means that no authority verifies the actual identity any one developer.
- iOS: Apple's App Store is a highly closed-off environment with a rigorous review process. iOS isolates each app that is developed by a third party, in a sandbox; however, once the app is approved and subsequently installed, it can access most of the device resources: detection of any misuse can only be carried out by the user after installation. Also, Apple's sandboxing is one of the weakest in the market, as it lets run all apps in the same standardized sandbox, whereas other players have a specific sandbox for each app. The certificate signing is fairly strong, as Apple does it in a systematic way: the certificates are issued by Apple to individuals or companies, and the signers must have verified Apple credentials. Nevertheless, iOS can be cracked (jailbroken), which is much harder to do on other OSs; and although this voids the warranty, Apple washes its hands with it.

- Windows: Microsoft's market protection model is based on the same principles Android's is. All apps on Windows 10 Mobile must be digitally signed and come from Windows Store or a trusted enterprise store. The Windows 10 Mobile security model uses app isolation to achieve the principle of least privilege: every app runs in its own isolated sandbox. The security policies that rule each sandbox defines the permissions each app has on accessing the rest of the OS (capabilities such as GPS or the camera). A set of default permissions are granted to each app, but additional permissions cannot be requested nor granted at runtime (as it would be normally for desktop applications).

2.3.2. The front-end

The front-end of malware protection is clearly what users make of the devices themselves. From an enterprise perspective, this translates into two separate and subsequent stages: what measures the IT department decides to implement at a company-wide level; and what personal measures the user decides (or is made to) implement on her own device.

The IT department is concerned mainly by two issues: what devices can access the enterprise network, and what each type of user has clearance to view, edit, share, etc. There exist several existing solutions that answer these needs: fall under the wide-encompassing umbrella of Enterprise Mobility Management. It is essentially the set of people processes and technology aimed at managing the mobile devices and services of any given company, as Kietzmann et al. (2013) explain. This seems rather straightforward, and it looks as if all a company has to do from a security perspective is to provide all its employees with devices secured by an Enterprise Mobility Suite and approved by its own IT department. The only issue would be the capital needed for the investment. Unfortunately, things get much trickier when some or all devices are not provided by the company (i.e. employees use their own devices in the professional environment); this phenomenon is called BYOD (Bring Your Own Device). Many authors have covered this subject in recent years, attempting to answer the question of its risks, or outlining its pros, or even trying to map out a formula that would answer the ultimate question for adoption. For instance, Scarfo, A. (2012) accepts the phenomenon as is, and presents several ways through which a company can

better adapt to the unavoidable paradigm change that BYOD brought to the enterprise scene. On the other hand, Miller et al. (2012), paint a much dimmer picture and present many of the privacy and security concerns that any enterprise might have to face, should it succumb to the temptation of BYOD's promised benefits. A much more unique approach is presented by Armando, et al. (2015), in which the authors introduce a fully theoretical framework, whereby they attempt to provide any given company with a unified formula to weigh out the pros and cons of BYOD adoption, based on any one company's data; supposedly, all the variables are accounted for. It seems to be a sort of "plug-and-play" scenario for any company wavering on BYOD. Though, they can't help but point out that any scrap of BYOD policy must abide to four basic principles: Transparency (user experience must not be impacted); Automatic verification (app compliance against the BYOD policy must be carried out in a fully automated way); Colluding apps (before installation, an app is validated only if it doesn't collude with other apps to work against the device configuration); Device configuration (changes to the configuration of a device must not lead to violations of the BYOD policy).

Onto the second issue, namely, the measures to be taken to secure a device at a more individual level, it is much easier to see by the naked eye what the devices can do to prevent security breaches through interaction with the user. Under this perspective, the most encompassing and clear evidence of factors for mobile device authentication is provided by Lowell Mooney et al. (2013) and Lowell Mooney et al. (2015). The two papers are nearly-identical, with the only difference being the year each was published. The authors attempt to give a clear and concise overview of some of the most common threats in the mobile devices environment, while at the same time provide ways for the end-user to protect herself through the security systems embedded in the device. They divide the user-based security systems into three main factors: Something the user knows (Knowledge-based, such as passwords, or visual cues); Something the user has (Ownership-based, such as device numbers, or smart cards); Something the user is (Inherent-based, such as fingerprints, or voice recognition). Each of these factors bluntly have various degrees of ease of use and cost for implementation associated to them. Jacobs, D. (2012) concentrates on these Inherent-based authentication methods, outlining three in particular, as they seem the most important for future development of security measures: Fingerprint recognition,

Voice recognition and Facial recognition. Finally, Lowell Mooney, et al. (2015), build on a study by Trend Micro to provide a ranking of the impact of what they believe to be the most important user-based features for security for each major mobile OS: Power on authentication, Inactivity time-out, SIM change, Password strength requirement, Protection from too many log-ins; Blackberry comes out largely on top scoring the highest, while iOS and Android score the lowest, with Windows is stuck in the middle.

3. Case Study

Large enterprises belonging to the French retail market account for over 300 thousand people, several hundred billions of Euros worth of revenue, and contribute strongly to the national economy. Within it, different activities are carried out by very different companies, from lux and fashion to building material distribution. This heterogeneity of activities may hint at the difficulty for IT companies to provide a proper and somewhat unified strategy to the vertical in terms of device provisioning.

To produce and maintain the large portfolio of equipment, appliances, clothing and what not, these large enterprises also employ quite a bit of technology themselves, as old school as it might be. Nonetheless, they understand the importance of efficiency and productivity: in the modern era, that translates into more connected, more secure, and more portable devices.

Through Windows 10, Microsoft provides several in-house built options (also available to the common consumer) to its enterprise customers, spanning from the Lumia family of smartphones, to the Surface family of tablets, both families positioned in a very similar fashion as Apple's iOS devices. However, Microsoft-branded devices aren't the only ones equipped with Windows 10; just like Google has done for mobile phones with its Android OS (by rendering it available to most smartphone manufacturers, such as Samsung and HTC), Microsoft doesn't limit the use of Windows 10 to its own in-house built devices, and many other device manufacturers can equip their respective tablet or laptop with it.

Through Windows 10, Microsoft can bring the concept of mobility to a whole new level for companies adopting the OS, thanks to the surrounding ecosystem of software offerings (spanning from cloud to productivity suites), as it is able to offer a much more connected experience to any company that may need a productivity suite, cloud solution, CRM, etc.; none of its current competitors can provide such added value through the whole stack of solutions.

However, penetration of the retail sector has been difficult so far for any enterprise mobility provider, perhaps because of some undetected BYOD adoption, perhaps because of a hidden massive adoption of a single competing solution, or perhaps for some other season. As this paper will attempt to answer questions regarding such difficulties, we shall first look at smartphones and tablets as physical devices, then describe the current state of the two main factors that constitute the concept of mobility: the operating systems and the mobility management suites. We will reference worldwide market trends, as depicted by IDC in years past, and data limited to France, should it be available.

3.1. Mobile devices

According to IDC, in its latest market trackers, while the smartphone market enjoys a slight, but solid growth in shipments year-over-year, the tablet market is suffering a steady decline since 2015 (and it is set to continue for the few coming years).

3.1.1. Tablets

Tablet life cycles have improved in length in the past few years, resembling more and more to those of PCs (likely to be somewhere between three and five years). Both small and large tablet manufacturers seem to be moving towards the detachable product lines, which has often resulted in increased product offerings and lower selling prices. PC manufacturers often consider detachable tablets to fall into the portable PC category, and have thus made an effort to address this new market as they would with traditional PCs; however, they're now finding themselves in competition with new manufacturers, who have created their market off of smartphones and slate tablets. This phenomenon brings about new marketing dynamics.

As Jean Philippe Bouchard, IDC research director, states "The detachable tablet segment is also considered by some manufacturers, like Apple, as a way to spur replacement cycles of the existing slate tablet installed base. One reason why the slate tablet market is experiencing a decline is because end-users don't have a good enough reason to replace them, and that's why productivity-centric devices like detachable tablets are considered

replacement devices for high-end larger slate tablets."

IDC still expects well over 100 million slates to ship annually through 2020. The lower cost associated with smaller screen slate devices seems to be the main driver: despite the small screen and typically lower configurations, for many this still provides a fairly decent computing experience, especially for people in emerging markets.

3.1.2. Smartphones

According to IDC's forecast, shipments are expected to only slightly grow (3.1%) in 2016; this is a remarkable decrease from the growth in 2015 (10.5%), and even more so from that of 2014 (27.8%). It seems that the continued slowdown in mature markets and China has strongly affected smartphone market shipments. While large markets like the United States, Western Europe, and China are expected to see low single digit growth rates in 2016, economies like Canada and Japan are expected to show negative growth, due mostly to recently-changing buying behaviors (most notably, new contracts proposed by mobile operators, and the rise of online marketplaces).

Ryan Reith, IDC program vice president, states "Consumers everywhere are getting savvy about how and where they buy their smartphones, and this is opening up new doors for OEMs and causing some traditional channels to lose some control of the hardware flow. Smartphones sold into eTailer channels grew 65% in 2015 and are expected to account for roughly 12% of smartphone shipments in 2016, up from just 4% in 2013. Consumers are having more say over which brands they want and at the same time able to bargain shop."

Other than the few remaining markets with low smartphone penetration, companies are shifting the focus towards ensuring that life cycles aren't extended any further, and keeping them around the two-year mark: Apple, for instance, is proposing early trade-in programs, while other manufacturers are providing a broader range of cheap unlocked devices.

3.2. Mobile OS

According to Microsoft, the French addressable market replaces about 4.5Mil. tablets and 5.5Mil. smartphones every quarter (three months). The latest data (January 2016) shows that while Windows holds a relatively solid (at least for a newcomer) position in the tablet market, it isn't faring so well with its phones, with 10% and 4% respective market shares. On the other hand, the iPad owns 22% of tablets market share and the iPhone 14% of smartphones', while Google's Android maintains a solid dominance in both the tablet and smartphone markets, with 69% and 82% market shares respectively. According to IDC, these figures are confirmed; however, it can be clearly seen from the latest Phone and Tablet Trackers (Q1 2016) in the Appendix that Android has started skyrocketing in both phone and tablet markets since around 2012, that Windows Phone is fighting a losing battle against an ever-increasing Android platform, and that Windows tablets are actually making the iPad having a run for its money.

Looking beyond mere numbers, here's what the three main OSs offer in terms of security.

3.2.1. Windows 10

Identity protection: Windows 10 replaces passwords with more secure biometric and hardware-based multi-factor authentication. Windows Hello enables secure fingerprint- and facial recognition–based authentication to revalidate user presence. Microsoft Passport enables PIN- and biometrics-based authentication through Windows Hello to securely identify users.

Data protection: Windows 10 ensures that only trusted software will run. BitLocker provides data protection that guards information at rest, in use, and in transit. In addition to BitLocker and BitLocker to Go for protecting data at rest, Windows 10 includes file-level encryption with Enterprise Data Protection that performs data separation and containment. When combined with Rights Management services, Windows 10 can keep data encrypted when it leaves the corporate network.

Threat protection: Windows 10 protects corporate identities with isolated credentials.

Device Guard is a feature set on Enterprise CBB that consists of both hardware and software system integrity hardening features. These features take advantage of new VBS options to protect the system core, the processes and drivers running in kernel mode. This is a 'trust-nothing' model seen in mobile device operating systems. A key feature is configurable code integrity, which allows IT to choose exactly which trusted software is allowed to execute code on devices.

Device security: Windows 10 protects sensitive corporate data with automatic encryption and persistent protection. UEFI Secure Boot protects users from bootkits by validating the integrity of the devices, firmware, and bootloader. Windows Trusted Boot feature protects the rest of the startup process by verifying that all Windows startup components are trustworthy (e.g., signed by a trusted source). TPM is a tamper-resistant cryptographic module that protects the encryption keys for BitLocker volumes, virtual smart cards & certificates – it includes cryptographic key management, safeguarding and reporting integrity measurements. (Source: *Microsoft: Windows 10 Security Value Proposition*)

3.2.2. iOS 9

Identity protection: Touch ID is Apple's equivalent of Windows Hello – it is a fingerprint sensing system for secure device access that makes using a longer, more complex passcode far more practical - because users won't have to enter it as frequently.

Data protection: File Data Protection is provided for iOS devices. All files in an iOS device's file system are encrypted with a random key that was created when the operating system was first installed, or the last time the device was wiped by a user. This key is stored in Effaceable Storage. The file system key is not used for confidentiality of data, but to be erased on demand directly by the user or remotely by the administrator issuing a remote erasure command from a Mobile Device Management Server, Exchange ActiveSync, or iCloud.

Threat protection: Application sandboxing: For application security, iOS provides layers of protection to ensure that apps are signed and verified, and are sandboxed to protect user data.

Device security: System security in iOS includes the boot-up process (secure boot chain), software updates and Secure Enclave. Secure boot chain helps ensure that the lowest levels of software are not tampered with and allows iOS to run only on validated Apple devices. Secure Enclave. Apple has customized a highly optimized version of TrustZone and created what is now known Secure Enclave. The Secure Enclave is a co-processor fabricated in the Apple A7 or later A-series processor. The Secure Enclave is responsible for processing fingerprint data from the Touch ID sensor, determining if there is a match against registered fingerprints, and then enabling access or purchases on behalf of the user. (Source: *iOS 9 Security Guide*)

3.2.3. Android

Identity protection: The latest Android 6.0 "Marshmallow" includes support for fingerprint sensors (only) for biometric authentication. Samsung Knox Workspace enables two-factor authentication. Configure the Workspace to accept a fingerprint as the primary authentication factor for the Knox container and a PIN, password or pattern as a second factor. Furthermore, Knox Workspace enables Single Sign-On which shares centralized authentication servers that all other applications and systems use for authentication.

Data protection: Cryptography and data protection are used in Android to provide confidentiality and data integrity (ex. Device encryption, Application signing, Network connectivity and encryption, including SSL, Wi-Fi, and VPN). Data encryption is only enabled by default in Android 6.0, and only if the device is fast enough.

Threat protection: Android apps run in an application sandbox which uses Security Enhanced Linux (SE Linux) to enforce Mandatory Access Control (MAC) over all processes. Android uses certificates to identify authors & the app developer holds the certificate's private key. Samsung KNOX addresses the security needs of individual applications with further security measures and sandboxing via KNOX Workspace (work container).

Device security: Some Android devices provide a secondary, isolated environment to run privileged or security sensitive operations. This environment is sometimes referred to as

Secure OS. These capabilities can be implemented on a separate processor (such as a standalone Secure Element or Trusted Platform Module), or can be isolated beneath the kernel on a shared processor (such as ARM TrustZone technology). Samsung KNOX provides device security including Hardware root of Trust, Secure Boot, Trusted Boot, ARM TrustZone-based Integrity Measurement Architecture (TIMA), Security Enhancements for Android (SE for Android), and TrustZone-based Security Services. (Sources: *Samsung Knox User Guide; Android for Work Security Whitepaper)*

3.3. EMM

According to IDC, the EMM market is defined as the following: "Enterprise mobility management is a competitive software market that pulls revenue from various enterprise systems management, security, and content management markets. EMM offerings include capabilities that enable the secure management of devices, applications, and content within a mobile computing context."

As of June 2015, according to Gartner, Microsoft enjoys a relatively solid position among other vendors in the EMM sphere, as it has often been placed as a "Visionary" or a "Leader" in Gartner's famous Magic Quadrants.

According to Microsoft, in 2014, two thirds of the Worldwide EMM market were divided amongst major vendors, while the remaining third was occupied by Open Source and other minor vendors' solutions. The total market amounts to roughly $1.5B, with Microsoft occupying just over 3% of it, and other major competitors such as Blackberry, AirWatch by VMWare, and MobileIron taking almost 40% of it all (19%, 11%, and 9% respectively). However, Blackberry plays very little part in the French market, while a smaller, albeit raising competitor is taking ground, Okta. The Competitive Landscape of the French market is outlined in the Appendix.

Cleary, due to its fickle and ever-changing nature, the technological landscape is bound to be (perhaps radically) different a few months from now. Further research will be needed.

4. Market Research

4.1. Research Questions

The rise in enterprise mobility and the unsubstantial research on the topic builds up the need to investigate whether the current assumptions held at worldwide level and at cross-segment level are in fact true, or if there exists a particular exception or oversight that applies to either the French geography or the retail sector. As the retail sector in France is still a "blank slate" for mobile devices, the applicability of the market intelligence at hand is questionable.

The paper aims to assess the validity of certain assumptions held true cross-country and cross-segment, while attempting to find hidden or previously overlooked factors that can explain the reasons for this segment to be so difficult to penetrate. In this regard, we build on the existing body of market intelligence available to us for France and analyze the aggregate factors that drive/hinder adoption of enterprise mobility. The above literature review provides us with an overview of the main reasons for companies to be so keen in adopting a mobility strategy, while not forgetting about the importance of security, due to the risks associated with such a strategy. We shall closer examine some determinants associated with positive attitude towards enterprise mobility that were identified in the literature review. In addition, we propose an "on field" analysis to better understand factors that may have been overlooked or whose importance may have been under/overestimated for the specific sector of retail.

We attempt to answer the following questions:

1. What is the degree of enterprise mobility of companies in the French retail sector?
    - Does it differ greatly from the rest of the market?
2. What drives adoption of company-liable devices vs BYOD strategies in the French retail sector?
    - Does it differ greatly from the rest of the market?

3. What actions can be put in place by Microsoft France to better push adoption to reticent firms in the retail sector?

The main objective of our study is to assess how an IT vendor, such as Microsoft can access a "blank slate" segment, such as retail, on the relevance of specific factors that may or may not play a role (and to which degree) in the adoption of mobile devices by a retail firm.

4.2. Hypotheses Development

Hypothesis 1: Albeit possible exception, the retail sector is not very mobile as a whole, and should thus not show higher signs of mobility than the market.

According to Microsoft France, they've so far had quite a hard time penetrating this segment (among few others); the main reason being not a shared common preference for different platforms than Windows or different manufacturers than Microsoft, but a low (if not negative) appeal that any mobility scenario brings to the business.

There might be exceptions within the particular segment, but the expectation is that they do not influence the overall mobility tendency of the segment.

Hypothesis 2: Adoption of corporate liable devices is driven mainly by the security level of the corresponding platform. This should hold true for the retail sector.

According to Microsoft France's CPE department (Customer and Partnership Experience), one of the main issues for large enterprises renewing their IT parks is the security linked to the solutions they're purchasing. While Microsoft constantly performs better than its two main competitors over this particular category, in the market overall (see Appendix), the expectation is for security to be even stronger an argument for companies in the retail sector, whose IT maturity is not as developed as the rest of the market.

Hypothesis 3: Adoption of a BYOD strategy is driven mainly by the perceived lower cost of implementation. The retail sector should not appear to be less susceptible to lower costs than the market as a whole.

The expectation is that companies in the retail sector are just as likely than those in the whole market to be enticed by the promise of lower costs. If this is the case, the expectation is that the platform of choice is dictated by consumer preferences, and the results should therefore not show a lower score than the market.

4.3. Research methodology

In order to address the research questions and analyze the drivers for mobility in the French retail sector, three different clusters of data sources were adopted:

- Quantitative secondary data: market research from international Market Intelligence firms; most notably, Strategy Analytics
- Qualitative secondary data: Microsoft internal data, from the following divisions: Market Intelligence, Competition, Windows, CPE.
- Primary data: interviews of selected IT profiles belonging to the sample of large French retail companies (e.g., CTO, IT Manager, Infrastructure Director, etc.).

The secondary data from Strategy Analytics was used to assess the readiness and inclination of the French market as a whole towards mobility. The study is divided in 6 sections: Budget, Cloud, Mobility use and devices, Mobility management and security, Mobility applications development, and Unified communication.

The secondary data coming from Microsoft internal sources has the sole objective of acting as supporting evidence to our conclusions. The tables shown are mere extracts and snippets of much larger studies and presentations carried out most recently (the farthest back that any of the data proposed was collected is twelve months ago).

Primary data was collected through a questionnaire; as reported in the Appendix, the questionnaire has been designed to tackle the two first questions separately, and provide grounds to answer the third as a whole: the first part aims at answering the first research question by focusing on the general mobility of employees and their use of the most commonly used mobile technologies; the second part aims at answering the second research question by focusing on the company's approach to mobility, through company expectations, devices adopted and IT support; the third part (plus possibly relevant findings from the previous two parts) aims at the very least to lay ground for recommendations to Microsoft France, hence also answering the third research question.

Finding the right metrics for measuring adoption and propensity to mobility was no easy task. However, Strategy Analytics had recently conducted a survey (2015) on the current state of mobility in the enterprise over the entire French territory. The study, "The State of Enterprise Mobility in France", provides good grounds on which to build a study limited to devices in the retail sector. In the two sections "Mobility use and devices" and "Mobility management and security", Strategy Analytics not only suggests valid metrics, but it also provides the whole market data needed for a sector-to-market comparison.

As already mentioned, the two sections from Strategy Analytics that are of interest to us are:

- *Mobility use and devices*: it provides an overview of the degree of workforce mobility, the most commonly used devices in the enterprise, the provisioning of said devices, and the reasons for choosing a particular mobile platform
- *Mobility management and security*: the different types of mobility management strategies are discussed, along with mobile security features, types of IT policies for mobile devices, and the importance of proper mobility management practices.

Through the help of the framework provided at large scale by Strategy Analytics, we were able to draw up a questionnaire to submit to the various IT Decision Makers of each large enterprise in the retail sector.

The purpose of the questionnaire was, once again, to challenge the hypotheses held true by Microsoft France over the retail sector, either by confirming their veracity or possibly by discovering anomalies in comparison to both the market and the common conviction, so to provide some guidance for better propositions over mobility strategies.

More on the questionnaire, the first few questions aim at tackling the first hypothesis; therefore, we've firstly asked the respondents what proportion of their workforce is mobile. As "mobile" can be interpreted very broadly, we've adopted the definition set by Strategy Analytics: "a mobile worker is a worker who spends at least 20% of its time traveling for business". 20% of time traveling for business seems reasonable enough for labeling a worker as "mobile" (even more so, if logistics isn't the revenue center of the business, but merely a cost center). Then, we've asked the respondents to provide us with a rough split of the use for some of the most common mobile devices and apps by their workforce. Finally, we've asked them about the company's provisioning strategy, whether the company has any BYOD strategies in place.

Moving on to the second set of questions, we've attempted to tackle the second and third hypotheses firstly by having the respondents tell us about their expectations over the coming months on whether full company provisioning was to increase or decrease, or if BYOD was to increase or decrease, and the reasons for said expectations. This would allow us to determine whether or not Microsoft has to concentrate on either selling to enterprises directly (B2B), or appealing to the consumer market (B2B2C) in order to penetrate the retail sector; subsequently, the reasons behind the expectations would tell us on which aspects or features Microsoft France should focus their marketing endeavors. We then asked the respondents to tell us about the split of OSs in their company among corporate-liable devices and personal devices; subsequently, we've also asked them about their intentions over supporting the different OSs over the coming months, and the main reason why. Thanks to these latter inquiries, we should be able to confirm or refute the third hypothesis.

Finally, we've saved the best for last. Hopefully, the answers to the third set of questions and the data collected through the first two sets of questions should give us the ability to

conclude whether or not security plays (or should play) a role of varying importance in the business environment, and if any particularly in the retail sector. We've asked the respondents about the various most commonly employed measures of security deployed within their own organizations, both for corporate-liable devices and for personal devices used by employees as part of a BYOD program.

4.4. Sample analysis

The questionnaire was conducted over the phone during approximately a two-months timespan (between December, 2015 and February, 2016). The sample of companies was provided by Microsoft France from the list of the companies that Microsoft France classifies as "large enterprises" in the retail sector. Contacts were primarily provided by the Microsoft France Account teams in charge of each customer; however, some contacts either were not inclined to take part to the study or did not feel qualified to answer all the questions; in the latter case, suggesting an (at least) equally qualified colleague as an additional source of information: the profiles selected belong to the ITDM (Information Technology Decision Marker) and IT Professional populations, each at the peak of their respective corporate ladder in their field. A full list of the companies participating to the study, along with the various job titles and the list of the people who gave consent to have their name cited, can be found in the Appendix.

As shown in Appendix, the survey is to be treated as purely qualitative research, as though the answers are collected in a quantitative manner (mostly percentages), the survey has no ambition to be of any solid statistical relevance, as the number of respondents is only thirty.

4.5. Results

Before setting out to begin the questionnaire, we've collected information on the activity carried out by each business (retail seems a little generic) and we've found at least a few clear and distinctive features that differentiate our fifteen companies over their respective

business lines: for instance, LVMH distributes (and even produces) fashion and luxury goods, while Accor is a hotel chain, and Pernod Ricard produces distilled beverages; differences of approach to any major strategy (in our case, mobility) is to be expected. Furthermore, we've collected information over their workforce, and it appears that one employee roughly equals one computer base; however, the distribution of portable devices employed for professional use is fickle across companies, therefore the proportion is not at all the same from one company to the next. The approximate numbers can be found in the Appendix.

Hypothesis 1

The first couple of questions of the survey should give us a decent idea of the degree of mobility of the retail sector, and what use is made of some of the most commonly adopted mobile devices and apps.

Keeping in mind that we've defined a mobile worker as "a worker who spends at least 20% of its time traveling for business", we've then distinguished companies with few mobile workers (>20%) from companies with some mobile workers (between 20% and 50%) and companies with many mobile workers (>50%). However, while the market shows this distinction to be somewhat important, we haven't found any company that comes even close to scoring 50% (and therefore being considered "highly mobile"), while the majority is "less mobile" with 5% to 15% of their workers being mobile, only four companies score slightly higher than 20% and classify for the label "fairly mobile". Compared to the French market, whereby the distribution for "less mobile", "fairly mobile" and "highly mobile" shows a Gaussian-like curve that is slightly skewed to the left, in favor of the "less mobile" (with 34%, 42%, and 24% respectively), the results from our sample suggest that in fact our hypothesis is correct, and the retail segment is factually less mobile than the market.

However, we shall take a look at the use that these companies make of some common mobile devices and apps. The proportions in the French market is as follows: for professional use, 36% of employees use a smartphone in the workplace, 55% use a tablet, 39% read mobile email, 47% use mobile apps for business (such as CRM), and 48% use mobile apps specific to the line of business (the so-called LOB apps). Our retail companies

yielded quite different proportions than those shown by the market: for professional use in the workplace, 52% of employees use a smartphone (vs. 36% in the market), 31% use a tablet (vs. 55% in the market), 29% read mobile email (vs.39% in the market), 23% use mobile apps for business, such as CRM (vs. 47% in the market), and 43% use mobile apps specific to the Line of Business, the so-called LOB apps (vs. 48% in the market). These results appear as mildly unexpected: while we would expect tablet, mobile email, and CRM use to be lower than market average (and LOB apps use to be not too far off from it), we are surprised to see professional use of smartphones firstly, so significant overall, and secondly, so significantly higher than market average. If we take a look at the split between the companies that we've defined as "less mobile" and those "fairly mobile", we can see that those who are "less mobile" have roughly the same proportion of professional use for smartphones that the market has, and it's driven mostly by three companies: L'Oréal, LVMH, and Mulliez; on the other hand, "fairly mobile" companies are overall the main driver for professional smartphone use in the retail sector, as more than 50% of their workers use a smartphone in the workplace: two companies in particular, Fnac and Rexel, are strongly driving this percentage upwards.

The fact that, as a whole, the retail sector is surpassing the French market at professional use of smartphones doesn't really refute our hypothesis; in fact, all other factors to determine the mobility of a sector, tell us otherwise. However, it would be interesting to see whether the companies that drive the numbers up for smartphones do so because of BYOD policies or because of company-specific reasons.

Hypothesis 2

Testing for Hypothesis 2 was a little trickier than for Hypothesis 1. Firstly, if successful, it only answers half of the second Research Question at best (as Hypothesis 3 represents the other half); secondly, though fairly intuitive, the hypothesis that adoption of corporate-liable devices in the market is driven by the corresponding OS's level of security is only confirmed by verbatims of Microsoft France's account managers. However, we attempt to confirm that hypothesis in the retail sector specifically.

The first thing to check is how companies manage mobile provisioning to their employees. Five companies allow employees to use their own personal devices in the workplace, namely, Danone, Kering, L'Oréal, LVMH, and Mulliez, while the others provide all corporate-liable devices. This does not denote a higher BYOD adoption than the market; if anything, not a single company lets employees provide all mobile devices, whereas other companies in the market do. From this point on, for the sake of convenience, we will label those five companies as "BYOD companies", though clearly, they haven't adopted a full BYOD strategy.

Digging a little deeper into companies' ambitions, respondents were asked if they expect the proportion of company-liable devices (and subsequently, of personal devices) to increase, decrease, or remain the same; and in case of increase or decrease, they were asked the main reason for said expectation. Results are much more one-sided than we had expected: not a single company expects the proportion of corporate-liable devices to decrease, about half expects it to stay the same, and the remaining half expects it to increase; it is striking to see that four out of the five BYOD companies are part of the latter half. The prevailing reason for the expected increase among BYOD companies is plans to downscale BYOD programs. As for expectations on personal devices, we've asked the same questions to our respondents and all of the companies but three expect the proportion of personal devices to stay the same. Unsurprisingly, the same three companies that told us they plan to scale down on BYOD programs are the ones who expect the proportion of personal devices to decrease (Kering, L'Oréal, and Mulliez). The reason for this carries the label "security concerns".

After looking at the results, we cannot say for sure that we've confirmed our hypothesis. Though it is most often the case (it just happens to be in the retail sector), BYOD vs Corporate-liable provisioning is not always a dichotomy. We can extrapolate a likely confirmation to our hypothesis from the fact that three of the BYOD companies that plan on scaling down on BYOD programs will do so, due to security concerns, while the other two are fairly agnostic on the matter.

Hypothesis 3

Without losing track of what transpired in the previous Hypothesis' testing, we've suggested what drives retail companies away from BYOD, while confirming the likelihood that security is an important feature within the mobility sphere; however, we still have to answer to what drives adoption of BYOD strategies. To do so, we will look at the reasons the respondents declared for supporting the different OSs. While fourteen out of fifteen companies are planning to support Apple's iOS in the coming months, twelve plan to support Windows, and only nine plan to support Android. The reasons behind the support of each platform are both different on a platform to platform basis (no surprise here), and on a segment to market basis: the latter difference is most interesting, but first, let's look at the reasons on a platform to platform basis. On Windows, respondents seemed to amplify what the market picked as most and least important, choosing in-house developer experience and employee preference as the top and least cited reasons respectively, giving ample higher and lower margins compared to the market. On iOS, respondents seemed to go against the market and choose the least cited reason (app ecosystem) by the market as the top reason for supporting this platform; however, not a single firm picked price as a reason to support iOS. On Android, respondents seemed to largely confirm what the market picked as the first reason for supporting the platform (price), by almost doubling the rate of responses, while paying no attention to the app and the developer aspects of the OS.

Unfortunately, this does not fully confirm or refute our third hypothesis, as there is only one company (LVMH) that has both a BYOD policy with Android devices in place and expects its proportion not to change in the coming months. To LVMH the most important reason to keep supporting Android is indeed price.

5. Guidance and recommendations

As we've stated earlier, the three hypotheses we've covered in the previous section would help us answer the first two research questions.

The first research question was concerned with the state of mobility of the French retail sector: we've compared our results to those of the market and found more than sufficient evidence to determine that the hypothesis is verified; however, we've also discovered some details that might help us provide some guidance to Microsoft France; we shall discuss them in this section.

The second research question was much harder to tackle, as what we have really been investigating are two different trends. We believe to have found sufficient evidence to support the hypothesis that security is in fact one of the main drivers for adoption of company-liable devices. However, we have found little evidence to support the hypothesis that price is one of the main drivers for BYOD policy adoption: the reason for this is that there is too little BYOD adoption (or intent for future adoption) in the French retail sector to deduce any conclusion from our questionnaire. Intuitively, the answer would be the same as for the market, but more research is needed to confirm this hypothesis. In any case, we've at least discovered that security is an important factor for companies in the retail sector on corporate-liable device adoption: as Microsoft France sells its devices almost exclusively on a B2B model, this is good news; should the retail sector have strong BYOD support, much more consumer-focused research would be needed.

The third and final research question is most likely the trickiest to answer and the most open for debate. As we've stated, our questionnaire wasn't limited to device use and adoption, but it covered a bit of security measures in a third part. We shall use the findings of the entire questionnaire to attempt to accurately answer the final research question. Let's take a look at the most striking results of the questionnaire:

- The companies that are most mobile

- The companies that are less mobile but still show advanced signs of mobility
- The split of OSs for corporate-liable devices
- The reasons for supporting Windows in the upcoming months
- The security management policies for corporate-liable and personal devices

The companies that are most mobile

Compared to the market, the most mobile companies in the retail sector are just barely over the level to be classified as "fairly mobile"; however, two companies in particular, Fnac and Rexel, show an overwhelmingly higher percentage of employees using mobile devices and apps than the rest of the segment (and the market, for that matter). More research is needed to determine whether this is a replicable effect, or if it's just a company-specific behavior (intuitively, it is reasonable to presume that as technology is part of their business, they equip more employees with devices).

The companies that are less mobile but still show advanced signs of mobility
Among the eleven "less mobile" companies, we find three (that just also happen to be three of the five BYOD companies) that behave very differently from the rest of the "less mobile" pack, and are in fact driving the mobility numbers upwards. L'Oréal, LVMH and Mulliez, all appear to be much more mobile than the percentage of their mobility workers would suggest. We see very high percentages of utilization of smartphones, tablets, mobile email, business apps and LOB apps, very much comparable to the numbers from Fnac and Rexel. The same reasoning applies here: more research is needed to know whether or not this effect is replicable (even more so, for companies whose workers aren't very mobile); however, we can't seem to find an intuitive way to explain this other than either company culture (not replicable) or an unexpected use employees make of the technologies (higher percentages than the market are shown for use of LOB apps, for instance).

The split of OSs for corporate-liable devices

The split of Operating Systems among corporate-liable devices painted quite a pretty picture in favor of Apple and a much dimmer one for Google; while iOS is already present in many companies, and in some, it even has a very strong hold on the current park of

devices, Android is barely making it into the sector, with only one company (Pernod Ricard) providing 40% of Android devices, and three others providing 10% each. As expected, although a little better than Android, Windows is not faring too well, penetrating only five companies (Kering, LVMH, Mulliez, Carrefour and Fnac). Nevertheless, the most interesting and promising figures come from the bottom row of the list of OSs. It seems that the strongest hold any OS has on this sector is the category "other", which can only mean one brand of handsets: Blackberry. This being the case, there is remarkable potential for Microsoft to propose value in the coming months to these companies; even before approaching the topic of equipping more employees with mobile devices, there could be a discussion over the antiquity of the Blackberry devices currently employed, which amount to almost one third of corporate-liable devices for the retail sector. This is an opportunity for the other three IT vendors that Microsoft France should attempt to be the first one to exploit.

The reasons for supporting Windows in the upcoming months

The fact that price is the main reason to support Android shouldn't come as a surprise; and neither should the fact that the main reason to supporting Apple is their app ecosystem. We weren't sure what respondents would say to why they plan to support Windows. Given that half reported "in-house developer experience" as the number one reason, we believe Microsoft could use this as a strong selling point to (any audience, but particularly) the retail sector. What in-house developer experience translates to in business terms is the creation and implementation of LOB apps: we've seen from previous results that mobile LOB apps are being used by every company in the sector, and used intensively by many of them. This means that the willingness to develop on the Windows platform is not only stronger than it is for other platforms, but also much more effective once it produces its results. In turn (and perhaps at a later stage), this could even be an opportunity to increase the percentages of Windows tablets sold in the sector.

The security management policies employed for corporate-liable and personal devices

The last two questions asked the respondents to indicate which security management policies are in place respectively for corporate-liable devices personal. Results are

staggering to say the least; as French retail companies seem to be lagging much too far behind what we had expected. On corporate-liable devices, no other company than Fnac has implemented all of the most common security management policies; Rexel, L'Oréal, LVMH and Mulliez have implemented most of them, while companies like Pernod Ricard and Saint Gobain have implemented none at all. Results are even more worrisome when we asked the BYOD companies about their security management policies for personal devices; we would expect even more restrictions and impositions on personal devices; what we found was quite the opposite, as L'Oréal, LVMH and Mulliez have implemented only a couple of measures, while Danone and Kering have implemented none

As dangerous as this is in absolute terms, this is yet another selling point that Microsoft could leverage for its devices, as not only Windows 10 supposedly is a more secure environment for the end-user than other platforms, but Microsoft has at its disposal a suite of mobile management solutions (EMS) that can manage the entire park of devices securely. This scenario offers Microsoft the possibility to leverage some of its complete stack of products, something each of its competitors cannot do by itself.

6. Study limitations and further research

The limitations of our study are rather self-explanatory. The study was conducted over a sample of 15 companies, gathering answers from the ITDMs from each company.

The main limitation is obviously the limited number of respondents, which make the study statistically insignificant: although statistical significance is not at the core of our purely qualitative study, some might wonder why we would compare our results to the purely qualitative study by Strategy Analytics; merely as a frame of reference to the French market as a whole. Perhaps, going one step further, one bias of having so few respondents is the possibility of some ITDMs not being entirely sincere about the information shared with us, due to the confidential nature of the subject.

Another enormous bias we've encountered is embedded in the definition of retail sector by Microsoft standards: unfortunately, we believe to be unable to explain certain anomalies in the responses, precisely due to the fact that the very different nature of the businesses encompassed by the large umbrella of "retail".

Furthermore, while the structure of the questionnaire had been validated by Microsoft France, some of the questions we've drafted appeared to require more inquiry from the very beginning; however, the stakeholders of this survey were too many and with different agendas for a thorough drilldown of customers' internal information; thus some questions shall remain incomplete.

Finally, due to the many aforementioned biases, further and more targeted research is needed to better understand the best ways to address certain historically reticent sectors through devices and mobility. More research could be done in countless ways, however, a few axes of work come to mind:

- Enlarging the scope; perhaps by integrating smaller, yet still large businesses, or aggregating more data from secondary sources

- Refining the scope: better define segment what one defines as “retail” and add more sector-specific questions, such as the specific mobile LOB apps used
- Comparing to other sectors: approaching the corporate-liable vs BYOD question with a deep-dive on its drivers within other sector; measuring perception vs reality of BYOD policies vs corporate-liable devices provision (ROI, NSAT, etc.)

There are many ways in which future research can address the issues of penetrating “blank slate” segments; however, one should be aware of the difficulties related to accessing the information desired.

7. Conclusion

The aim of our research is to provide Microsoft France with some ground to better understand what can be done to penetrate one of the "blank slate" verticals they've been having a hard time reaching. For this purpose, we have taken a look at what other market intelligence firms have done in the recent past and drafted a questionnaire to submit to ITDMs, each at the top of their respective field within the selected companies. Our sample included fifteen large enterprises in the French retail sector.

Our results indicate that there is strong promise for Microsoft to provide this segment with valid talking points on mobility in general, and particularly on security and apps. We conclude that there is strong potential in this sector due to a variety of reasons: some evidence suggests potential for replacement of old devices; some suggests it due to the LOB apps that can be developed; some suggests it due to the low level of development over security management policies.

To answer our first Research Question, we've developed a Hypothesis to test against the market that, if confirmed, it would have meant that the road ahead would be tough. Though the hypothesis was confirmed, a few exceptions came to surface.

To answer our second Research Question, we've developed two Hypotheses to test against the market, one on corporate-liable devices, and the other on BYOD policies. Should the former be confirmed, Microsoft would be at an advantage in front of the competition; should the latter be confirmed, Microsoft would have to focus more resources on gaining consumer share.

To answer our third and final Research Question, we've analyzed the entire questionnaire and compared it to the current product resources at Microsoft disposal. From the bases of the first two Research Questions, we've been able to elaborate some recommendations to provide to Microsoft France to better address the retail sector.

8. Teaching Notes

Synopsis

The case revolves around finding ways for Microsoft France to address the historically hard to access retail sector through mobile devices. The context in which the case is set is clearly that of a modern era, where companies are finding different factors of hindrance to change from a sector to the next.

Target and objectives

The target learning group for this study are the Windows BG (responsible for the Marketing of Windows and Surface) and the Account teams at Microsoft France. The objective is to provide some insights on factors that might be worth leveraging to access the retail sector with mobile devices.

Relevance of Study

Very few academic studies have been conducted on the subjects of mobile devices adoption, enterprise mobility perception and related use cases; and while much market research has been carried out on those same subjects by large Market Intelligence corporations over the last few years, none has covered in specific the aspects that might differentiate a particular segment from another; much less, focusing on a particular geography, such as France; and even less, doing so from the point of view of a specific IT vendor, such as Microsoft. Geographically speaking, the collected evidence is either specific to a particular geography that doesn't concern us (i.e., within the United States), or not specific enough (i.e., worldwide studies). Industry-wise, the studies that have been carried out have in fact been heterogeneous across different sectors, but the results proposed are shown as aggregate figures, with no deep dive into one particular segment.

Bibliography

"Android for Work Security White Paper." Web. 2 June 2016.

Armando, Alessandro et al. "Formal Modeling and Automatic Enforcement of Bring Your Own Device Policies." *International Journal of Information Security* 14.2 (2014): 123–140. *link.springer.com*. Web.

Boso, Nathaniel, John W. Cadogan, and Vicky M. Story. "Entrepreneurial Orientation and Market Orientation as Drivers of Product Innovation Success: A Study of Exporters from a Developing Economy." *International Small Business Journal* (2012): 266242611400469. *isb.sagepub.com*. Web.

Bugiel, Sven et al. "Practical and Lightweight Domain Isolation on Android." *Proceedings of the 1st ACM Workshop on Security and Privacy in Smartphones and Mobile Devices*. New York, NY, USA: ACM, 2011. 51–62. *ACM Digital Library*. Web. 2 June 2016. SPSM '11.

CPE Harmoni Rapport Bi-Annuel FY16H2. Microsoft France - CPE. Print.

Ellonen, Hanna-Kaisa, Patrik Wikström, and Ari Jantunen. "Linking Dynamic-Capability Portfolios and Innovation Outcomes." *Technovation* 29.11 (2009): 753–762. *ScienceDirect*. Web.

Feizollah, Ali et al. "A Review on Feature Selection in Mobile Malware Detection." *Digital Investigation* 13 (2015): 22–37. *ScienceDirect*. Web.

Felt, Adrienne Porter et al. "A Survey of Mobile Malware in the Wild." *Proceedings of the 1st ACM Workshop on Security and Privacy in Smartphones and Mobile Devices*. New York, NY, USA: ACM, 2011. 3–14. *ACM Digital Library*. Web. 2

June 2016. SPSM '11.

Frances T.J.M. Fortuin, and S.W.F. (Onno) Omta. "Innovation Drivers and Barriers in Food Processing." *British Food Journal* 111.8 (2009): 839–851. *emeraldinsight.com (Atypon)*. Web.

Gunday, G. et al. "Modeling Innovation: Determinants of Innovativeness and the Impact of Innovation on Firm Performance." *4th IEEE International Conference on Management of Innovation and Technology, 2008. ICMIT 2008*. N.p., 2008. 766–771. *IEEE Xplore*. Web.

Hameed, Mumtaz Abdul, Steve Counsell, and Stephen Swift. "A Conceptual Model for the Process of IT Innovation Adoption in Organizations." *Journal of Engineering and Technology Management* 29.3 (2012): 358–390. *ScienceDirect*. Web.

Holzer, Adrian, and Jan Ondrus. "Trends in Mobile Application Development." *Mobile Wireless Middleware, Operating Systems, and Applications - Workshops*. Ed. Cristian Hesselman and Carlo Giannelli. Springer Berlin Heidelberg, 2009. 55–64. *link.springer.com*. Web. 2 June 2016. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 12.

IDC French Client Computing Device Overview. IDC. Print.

IDC WW Quarterly Mobile Phone Tracker - 2016Q1. IDC. Print.

IDC WW Quarterly Tablet Tracker - 2016Q1. IDC. Print.

"iOS Security Guide." Web. 2 June 2016.

Jeon, Jinseong et al. "Dr. Android and Mr. Hide: Fine-Grained Security Policies on Unmodified Android." (2011): n. pag. *drum.lib.umd.edu*. Web. 2 June 2016.

Kietzmann, Jan et al. "Mobility at Work: A Typology of Mobile Communities of Practice

and Contextual Ambidexterity." *The Journal of Strategic Information Systems* 22.4 (2013): 282–297. *ScienceDirect*. Web.

Kohli, Ajay K., and Bernard J. Jaworski. "Market Orientation: The Construct, Research Propositions, and Managerial Implications." *Journal of Marketing* 54.2 (1990): 1–18. *JSTOR*. Web.

Lewrick, Michael, Maktoba Omar, and Jr Williams. "Market Orientation and Innovators' Success: An Exploration of the Influence of Customer and Competitor Orientation." *Journal of technology management & innovation* 6.3 (2011): 48–62. *SciELO*. Web.

"Magic Quadrants & Critical Capabilities | Gartner Inc." N.p., n.d. Web. 2 June 2016.

Maiorca, Davide et al. "Stealth Attacks: An Extended Insight into the Obfuscation Effects on Android Malware." *Computers & Security* 51 (2015): 16–31. *ScienceDirect*. Web.

Manley, Karen, and Steve Mcfallan. "Exploring the Drivers of Firm-level Innovation in the Construction Industry." *Construction Management and Economics* 24.9 (2006): 911–920. *Taylor and Francis+NEJM*. Web.

Marcati, Alberto, Gianluigi Guido, and Alessandro M. Peluso. "The Role of SME Entrepreneurs' Innovativeness and Personality in the Adoption of Innovations." *Research Policy* 37.9 (2008): 1579–1590. *ScienceDirect*. Web.

Miller, Keith W., Jeffrey Voas, and George F. Hurlburt. "BYOD: Security and Privacy Considerations." *IT Professional* 2012: 53–55. Print.

Mooney, J. Lowell, Abbie Gail Parham, and Timothy D. Cairney. "Your Guide to Authenticating Mobile Devices." *Journal of Corporate Accounting & Finance*

24.5 (2013): 51–68. *Wiley Online Library*. Web.

---. "Your Guide to Authenticating Mobile Devices." *Journal of Corporate Accounting & Finance* 26.4 (2015): 65–82. *Wiley Online Library*. Web.

Pantano, Eleonora. "Innovation Drivers in Retail Industry." *International Journal of Information Management* 34.3 (2014): 344–350. *ScienceDirect*. Web.

Pantano, Eleonora, and Milena Viassone. "Demand Pull and Technology Push Perspective in Technology-Based Innovations for the Points of Sale: The Retailers Evaluation." *Journal of Retailing and Consumer Services* 21.1 (2014): 43–47. *ScienceDirect*. Web.

Parrilli, Mario Davide, and Aitziber Elola. "The Strength of Science and Technology Drivers for SME Innovation." *Small Business Economics* 39.4 (2011): 897–907. *link.springer.com*. Web.

Pieterse, H., and M. S. Olivier. "Android Botnets on the Rise: Trends and Characteristics." *2012 Information Security for South Africa*. N.p., 2012. 1–5. *IEEE Xplore*. Web.

Rhee, Jaehoon, Taekyung Park, and Do Hyung Lee. "Drivers of Innovativeness and Performance for Innovative SMEs in South Korea: Mediation of Learning Orientation." *Technovation* 30.1 (2010): 65–75. *ScienceDirect*. Web.

"Rpt_enterprise_readiness_consumerization_mobile_platforms.pdf." Web. 2 June 2016.

"Samsung KNOX User Guide Enterprise Edition 2014." Web. 2 June 2016.

Sandvik, Izabela Leskiewicz, and Kåre Sandvik. "The Impact of Market Orientation on Product Innovativeness and Business Performance." *International Journal of Research in Marketing* 20.4 (2003): 355–376. *ScienceDirect*. Web.

Scarfo, A. “New Security Perspectives around BYOD.” *2012 Seventh International Conference on Broadband, Wireless Computing, Communication and Applications (BWCCA)*. N.p., 2012. 446–451. *IEEE Xplore*. Web.

Schreckling, Daniel, Joachim Posegga, and Daniel Hausknecht. “Constroid: Data-Centric Access Control for Android.” *Proceedings of the 27th Annual ACM Symposium on Applied Computing*. New York, NY, USA: ACM, 2012. 1478–1485. *ACM Digital Library*. Web. 2 June 2016. SAC ’12.

“Tablets Set to Return to Growth in 2018 Driven by Emergence of Detachables and Ongoing Need for Slates, According to IDC.” *www.idc.com*. N.p., n.d. Web. 2 June 2016.

The State of Enterprise Mobility in France - June 2015. StrategyAnalytics, 2015. Print.

Vural, Ickin, and Hein Venter. “Mobile Botnet Detection Using Network Forensics.” *Future Internet - FIS 2010*. Ed. Arne J. Berre et al. Springer Berlin Heidelberg, 2010. 57–67. *link.springer.com*. Web. 2 June 2016. Lecture Notes in Computer Science 6369.

“Windows 10 Differentiated Value Proposition.” N.p., n.d. Web. 2 June 2016.

“Worldwide Enterprise Mobility Management Software Market Shares, 2014: Fragmentation Continues, But the Dust Is Starting to Settle.” *www.idc.com*. N.p., n.d. Web. 2 June 2016.

“Worldwide Smartphone Growth Forecast to Slow to 3.1% in 2016 as Focus Shifts to Device Lifecycles, According to IDC.” *www.idc.com*. N.p., n.d. Web. 2 June 2016.

Appendix

Figure 1: IDC WW Quarterly Tablet Tracker – 2016Q1

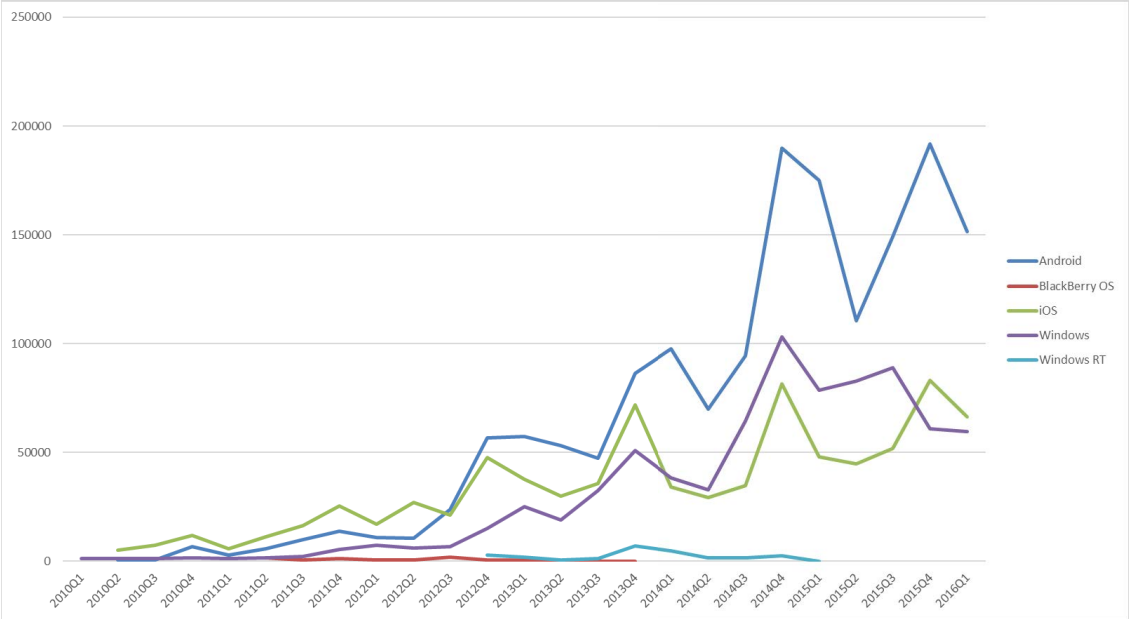


Figure 2: IDC WW Quarterly Mobile Phone Tracker - 2016Q1

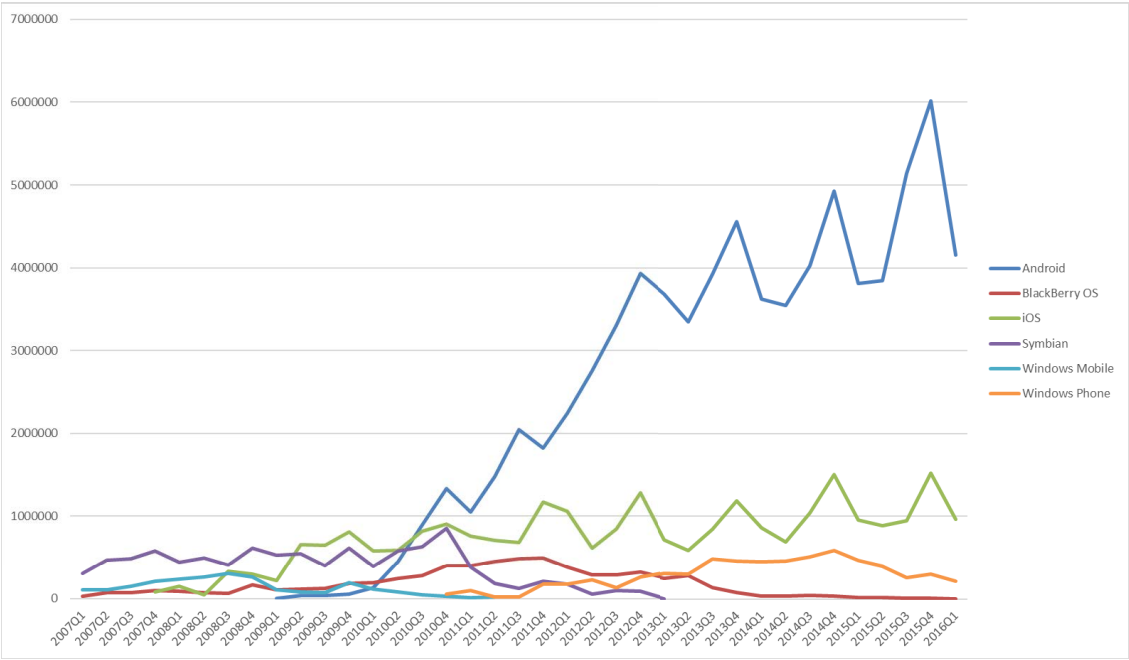


Figure 3: EMS Gartner's Magic Quadrants, 2015

Figure 4: IDC Worldwide Enterprise Mobility Management Software Market Shares, 2014

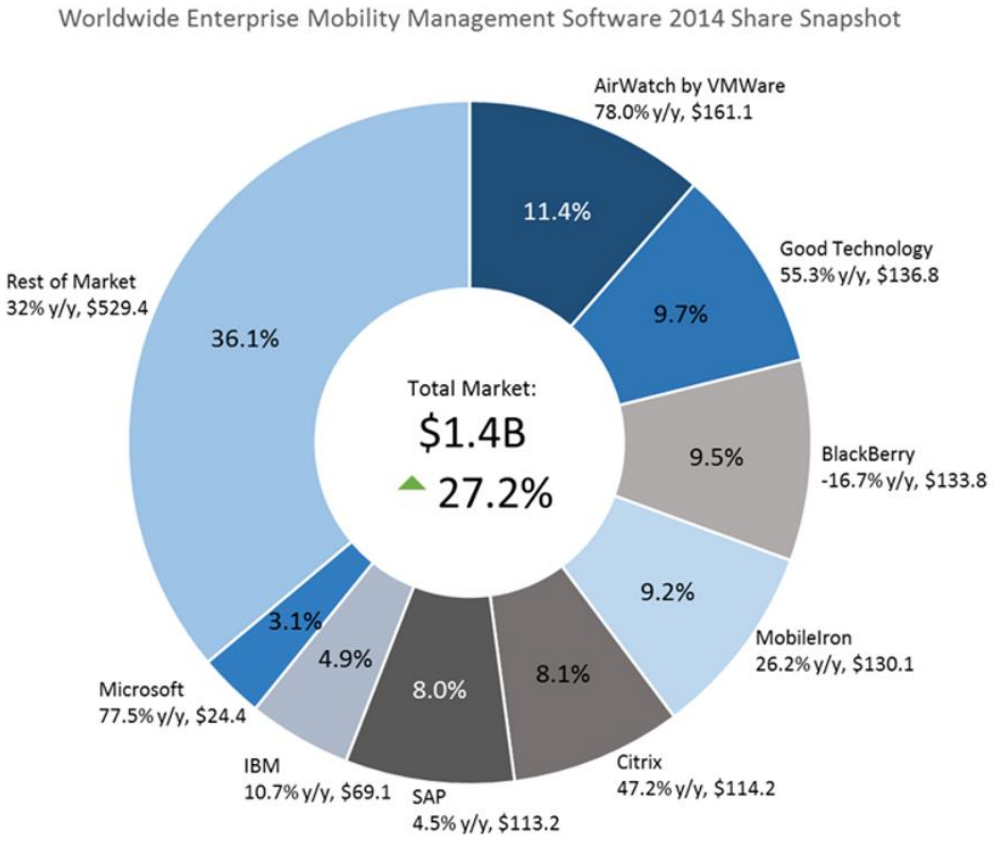
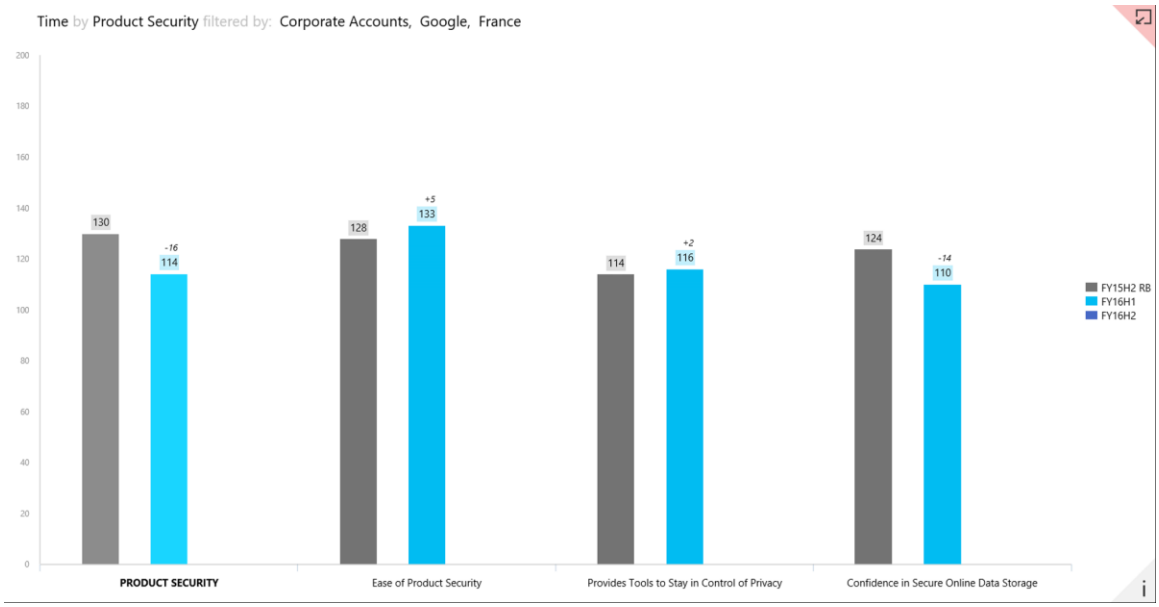
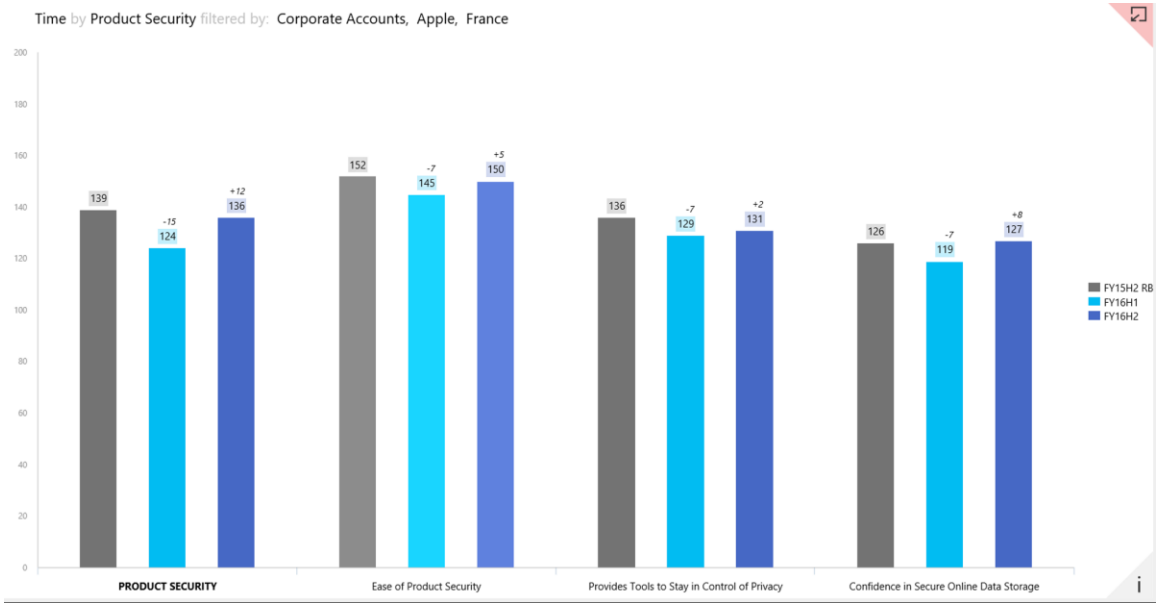


Figure 5: CPE Harmoni Rapport Bi-Annuel FY16H2





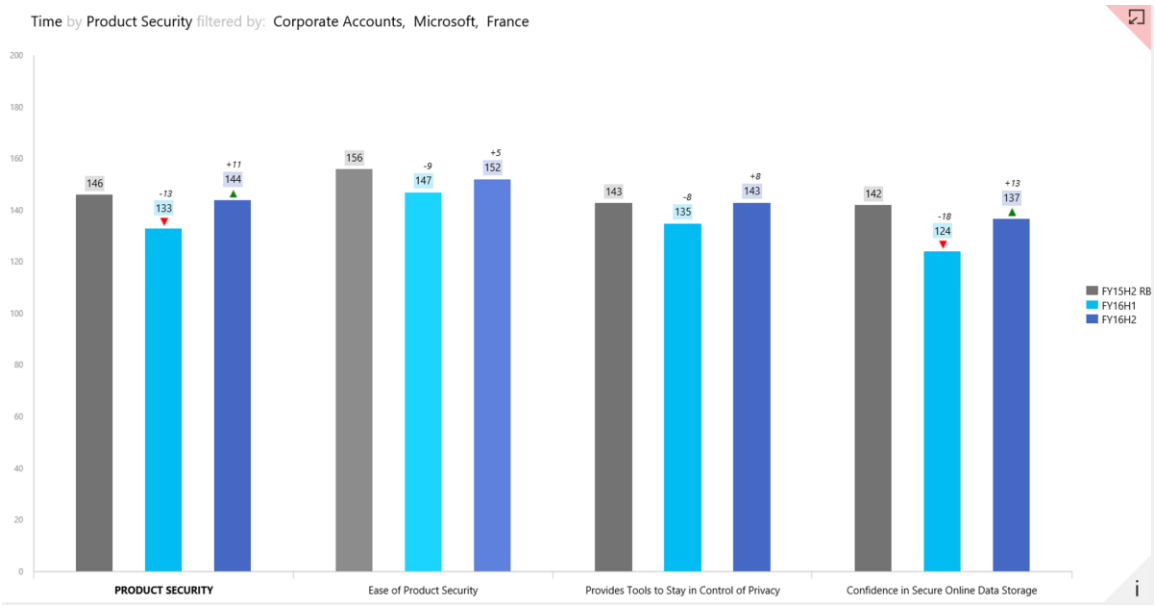


Table 1: French market Competitive Landscape

Competitor Type	Current Status	Future Outlook
Point MDM/EMM, Platform company – VMWare AirWatch Similar to: Citrix XenMobile, IBM Maas360 2014 EMM revenue, market share: Threat Level: High	• **Entrenched MDM incumbent**, perceived as leader in features (Garter EMM MQ leader) • VMWare seeing **stagnation of overall desktop virtualization market**, but will continue to take share from Citrix and have moderate growth • Recent announcement of **VMWare Identity Manager** based on 5 year old acquisition of Tricipher • Best Android feature set including email profiles	• Will continue to **refine Identity Manager** • Will **push Airwatch with heavy discounting as part of Horizon Workspace Suite** • Attempt to **defend feature leadership** with new capabilities in Mobile Content Management and Location led features like geo-fencing
Point MDM/EMM, independent – Mobile Iron Similar to: Good Technology (now part of BB) 2014 EMM revenue, market share: Threat Level: Low	• **Entrenched MDM incumbent**, perceived as leader in iOS experience (Garter EMM MQ leader) • Dominance has peaked; **has faced low growth over 2014**, and various org challenges including exec. Attrition and SEC investigations • Still **point MDM/EMM** with no visible plans to enter Identity+Access Management	• Will continue to be relevant in Small+Medium businesses not requiring comprehensive mobility solutions • Will see **stagnating and potentially negative growth** owing to heightened fragmentation of market and increasing competition from "lightweight" MDM/MAM players like Kaseya, App47
Point IdaaS solutions – Okta Similar to: Ping, Centrify 2014 IdaaS revenue, market share: Threat Level: High	• **Early innovator in cloud based Identity+Access Management** (Garter IdaaS MQ leader) • Early mover's advantage, strong in SMB; "easy to set up" positioning with high quality UI • Launched EMM solution **"Okta Mobility Management" in Nov 2014, not seeing much traction** • Integration with 4K+ SaaS apps	• Will continue exaggerated claims about having "partnership" with Microsoft and Office 365 • Continued investment in OMM, although no major capabilities will be built in device management • Continued push to have best in class UI.

Table 2: Company profiles

Accor

AccorHotels formerly known as Accor S.A. is a French hotel group, part of the CAC 40 index, which operates in 94 countries. Headquartered in Paris, France, the group owns, operates and franchises 3,700 hotels on 5 continents representing several diverse brands, from budget and economy lodgings to luxurious accommodations in exotic locales.

Carrefour

Carrefour S.A. is a French multinational retailer headquartered in Boulogne Billancourt, France, in the Hauts-de-Seine Department near Paris. It is one of the largest hypermarket chains in the world.

Casino

Groupe Casino is a French mass retailer with operations around the world. The company is listed on the NYSE Euronext Paris stock exchange and its majority shareholder is Rallye SA. The company's head office is in Saint-Étienne

Danone

Danone is a French multinational food-products corporation based in Paris. It has four business lines: Fresh Dairy products, Waters, Early Life Nutrition and Medical Nutrition. The company is a component of the Euro Stoxx 50 stock market index.

Fnac

Fnac is a large French retail chain selling cultural and electronic products, founded in 1954. Its head office is in Le Flavia in Ivry-sur-Seine, near Paris. Fnac is an abbreviation of Fédération Nationale d'Achats des Cadres ("National Shopping Federation for Executives").

Intermarché

Intermarché is the brand of a general commercial French supermarket, founded in 1969 by Jean-Pierre Le Roch. The orignal "EX Offices" was renamed Intermarché in 1972.

Kering

Kering (previously PPR) is the French luxury goods holding company owner of Alexander McQueen, Balenciaga, Brioni, Gucci, Puma, Volcom, Saint Laurent Paris, and other luxury, sport & lifestyle brands distributed in 120 countries. The company was founded in 1963 by businessman François Pinault and is now run by his son François-Henri Pinault. It is quoted on Euronext Paris and is a constituent of the CAC 40 index.

Leclerc

E.Leclerc (informally simply Leclerc) is a French cooperative society and hypermarket chain, headquartered in Ivry-sur-Seine. E.Leclerc was established on 1 January 1948 and currently has more than 500 locations in France and 114 stores outside of the country, as of 2012. The chain enables semi-independent stores to operate under the Leclerc brand.

L'Oréal

L'Oréal S.A. is a French cosmetics company headquartered in Clichy, Hauts-de-Seine with a registered office in Paris. It is the world's largest cosmetics company and has developed activities in the field of cosmetics, concentrating on hair color, skin care, sun protection, make-up, perfumes and hair care, the company is active in the dermatology, toxicology, tissue engineering, and biopharmaceutical research fields and is the top nanotechnology patent-holder in the United States. The company is a component of the Euro Stoxx 50 stock market index.

LVMH

LVMH Moët Hennessy Louis Vuitton SE, better known as LVMH, is a French multinational luxury goods conglomerate, headquartered in Paris, France. The company was formed by the 1987 merger of fashion house Louis Vuitton with Moët Hennessy. It controls around 60 subsidiaries that each manage a small number of prestigious brands. The oldest of the LVMH brands is wine producer Château d'Yquem, which dates its origins back to 1593.

Mulliez

Mulliez is a family-owned conglomerate with interests in a large number of companies, among which, Decathlon, Norauto, Groupe Adeo, Boulanger, Phildar, Accord Bank, Kiabi, Cultura, and Pimkie. It is owned by one of the wealthiest families in France and in Europe.

Pernod Ricard

Pernod Ricard is a French company that produces distilled beverages. The company's eponymous products, Pernod Anise and Ricard Pastis, are both anise-flavored liqueurs and are often referred to simply as Pernod or Ricard. The company also produces several other types of pastis.

Rexel

Rexel is a French group founded in 1967, which specializes in the distribution of electrical supplies to professional users. It distributes products and services in the areas of automation, technical supply and energy management. The company offers a wide range of products and services, including products in the lighting, security, automation, climate control, communication, building automation and renewable energies sectors.

Saint Gobain

Saint-Gobain S.A. is a French multinational corporation, founded in 1665 in Paris and headquartered on the outskirts of Paris, at La Défense and in Courbevoie. Originally a mirror manufacturer, it now also produces a variety of construction and high-performance materials. The company is a component of the Euro Stoxx 50 stock market index.

Système U

Système U is a French retailers' cooperative, comprising about eight hundred independent hypermarkets and supermarkets, headquartered in the Parc Tertiaire SILIC in Rungis, France.

Table 3: Consenting contacts for citation

Accor – José Llorens, Responsable Support Informatique
Accor – Yves Djedje, Directeur Adjoint des Solutions Informatiques
Kering – Eric Bohec, End User Solution Manager
L'Oréal - Pierre Clapier, Infrastructure Project Director
L'Oréal - Franck Bugnot, Directeur de l'organisation et des méthodes
LVMH - Philippe Zitoune, CTO
Mulliez - Jacques Honoré, CIO
Mulliez – Jean-Claude Cosson, CTO
Pernod Ricard – Stéphane Dauphin, IT Support Manager

Table 4: Questionnaire

Company
Installed base
Mobile devices - Corporate-liable
Mobile devices - Personal
What percentage of your total workforce is mobile? (mobile worker = travels for business at least 20% of the time)
Less mobile (<20%)
Fairly mobile (20-50%)
Highly mobile (>50%)
What percentage of your organization's workforce employs the following devices and apps for professional use?
Smartphones
Tablets
Mobile email
Mobile apps for business other than email (e.g., CRM)
Mobile apps specific to Line of Business (e.g., Workflow Management, Knowledge and Document Management Systems, Tracking Systems, etc.)
How does your company manage mobile provisioning?
Company provides all mobile devices
Company provides some devices and offers an approved list of devices for employees to use/purchase on their own
Company provides some devices and allows employees to bring any device on their own
Employees provide all mobile devices
Do you expect the proportion of company-liable devices to increase, decrease, or stay the same over the next few months?
Increase
Stay the same
Decrease
What is the main reason for you to expect an increase in company-liable devices?
Growing mobile workforce

Replacing personal devices for key personnel

Scaling down on BYOD programs

Do you expect the proportion of personal devices to increase, decrease, or stay the same over the next few months?

Increase

Stay the same

Decrease

What is the main reason for you to expect a decrease in personal devices?

Security concerns

Support commitments making it prohibitive

Not cost effective

Too difficult to manage

What is the mobile OS split among your organization's corporate-liable devices?

Windows

iOS

Android

Other

What is the mobile OS split among your organization's BYOD devices?

Windows

iOS

Android

Other

If you plan to support Windows in the coming months, what is the main reason?

In-house developer experience

Price

Employee preference

App ecosystem

If you plan to support iOS in the coming months, what is the main reason?

In-house developer experience

Price

Employee preference

App ecosystem

If you plan to support Android in the coming months, what is the main reason?

- In-house developer experience
- Price
- Employee preference
- App ecosystem

Which security management policies does your organization implement for corporate-liable devices?

- Password enforcement
- Wipe for lost or stolen devices
- Lock for lost or stolen devices
- Internet domain restrictions
- Applications restrictions
- Data encryption

Which security management policies does your organization implement for personal liable devices?

- Password enforcement
- Wipe for lost or stolen devices
- Lock for lost or stolen devices
- Internet domain restrictions
- Applications restrictions
- Data encryption

Table 5: Questionnaire results

			Less Mobile											Fairly Mobile					
Company			**Accor**	**Casino**	**Danone**	**Intermarché**	**Kering**	**Leclerc**	**L'Oréal**	**LVMH**	**Mulliez**	**Pernod Ricard**	**Saint Gobain**	**Carrefour**	**Fnac**	**Rexel**	**Système U**	**Less Mobile**	**Fairly Mobile**
Installed base			15000	32000	6500	10000	9000	12000	23000	15000	120000	6000	18000	30000	7000	5000	5000		
Mobile devices - Corporate-liable			3000	5000	2000	1000	2000	2000	15000	10000	60000	2000	5000	20000	7000	4000	3000		
Mobile devices - Personal					1000		2000		5000	5000	15000								
	French market	**Retail**																	
What percentage of your total workforce is mobile? (mobile worker = travels for business at least 20% of the time)																			
Less mobile (<20%)	34%	73%	10%	15%	5%	10%	5%	15%	10%	5%	10%	10%	10%					10%	
Fairly mobile (20-50%)	42%	27%												20%	25%	20%	20%		21%
Highly mobile (>50%)	24%	0%																	
What percentage of your organization's workforce employs the following devices and apps for professional use?																			
Smartphones	36%	57%	20%	20%	40%	10%	30%	20%	60%	60%	60%	30%	30%	40%	70%	60%	40%	35%	53%
Tablets	55%	38%		20%	20%		20%	10%	50%	60%	30%			20%	60%	40%	20%	30%	35%
Mobile email	39%	29%	20%	20%	40%	20%	10%	20%	50%	50%	40%	30%	20%	20%	40%	40%	20%	29%	30%
Mobile apps for business other than email (e.g., CRM)	47%	23%	10%	10%	10%	10%	10%	10%	40%	40%	40%	20%	20%	20%	30%	40%	30%	20%	30%
Mobile apps specific to Line of Business (e.g., Workflow Management, Knowledge and Document Management Systems, Tracking Systems, etc.)	48%	43%	20%	40%	50%	10%	20%	20%	70%	70%	60%	30%	30%	40%	60%	70%	50%	38%	55%
How does your company manage mobile provisioning?																			
Company provides all mobile devices	58%	67%	x	x		x		x				x	x	x	x	x	x	55%	100%
Company provides some devices and offers an approved list of devices for employees to use/purchase on	2%	0%																0%	0%
Company provides some devices and allows employees to bring any device on their own	24%	33%			x		x		x	x	x							45%	0%
Employees provide all mobile devices	16%	0%																0%	0%
Do you expect the proportion of company-liable devices to increase, decrease, or stay the same over the next few months?																			
Increase	11%	47%		x		x	x	x	x	x	x								
Stay the same	79%	53%	x		x							x	x	x	x	x	x		
Decrease	10%	0%																	
What is the main reason for you to expect an increase in company-liable devices?																			
Growing mobile workforce	60%	43%		x		x		x											
Replacing personal devices for key personnel	29%	14%								x									
Scaling down on BYOD programs	11%	43%					x		x		x								
Do you expect the proportion of personal devices to increase, decrease, or stay the same over the next few months?																			
Increase	19%	0%																	
Stay the same	52%	80%	x	x	x	x		x		x		x	x	x	x	x	x		
Decrease	29%	20%					x		x		x								
What is the main reason for you to expect a decrease in personal devices?																			
Security concerns	30%	100%					x		x		x								
Support commitments making it prohibitive	35%	0%																	
Not cost effective	19%	0%																	
Too difficult to manage	16%	0%																	
What is the mobile OS split among your organization's corporate-liable devices?																			
Windows	19%	21%					50%			40%	20%			20%	20%				
iOS	39%	52%	20%	40%	50%			40%	80%	50%	50%		10%	30%	80%	100%	90%		
Android	18%	7%		10%					10%		10%	40%							
Other	24%	20%	80%	50%	50%	100%	50%	60%	10%	10%	20%	60%	90%	50%			10%		
What is the mobile OS split among your organization's BYOD devices?																			
Windows	8%	7%							10%		10%								
iOS	22%	32%			20%		40%		50%	50%	20%								
Android	68%	55%			80%		50%		40%	50%	60%								
Other	2%	6%					10%				10%								
If you plan to support Windows in the coming months, what is the main reason?																			
In-house developer experience	35%	100%			x	x			x		x	x	x						
Price	25%	33%					x								x				
Employee preference	17%	17%												x					
App ecosystem	23%	50%		x				x		x									
If you plan to support iOS in the coming months, what is the main reason?																			
In-house developer experience	37%	56%		x	x				x					x			x		
Price	25%	0%																	
Employee preference	24%	33%						x		x					x				
App ecosystem	14%	67%	x			x	x				x		x			x			
If you plan to support Android in the coming months, what is the main reason?																			
In-house developer experience	21%	0%																	
Price	46%	89%	x	x	x				x	x	x			x	x				
Employee preference	14%	11%										x							
App ecosystem	19%	0%																	
Which security management policies does your organization implement for corporate-liable devices?																			
Password enforcement	69%	60%		x	x		x		x	x	x			x	x	x			
Wipe for lost or stolen devices	57%	40%			x		x		x		x				x	x			
Lock for lost or stolen devices	60%	60%			x		x		x	x	x			x	x	x	x		
Internet domain restrictions	57%	20%									x				x	x			
Applications restrictions	55%	20%							x	x					x				
Data encryption	56%	47%	x	x		x			x	x					x	x			
Which security management policies does your organization implement for personal liable devices?																			
Password enforcement	33%	20%									x								
Wipe for lost or stolen devices	44%	40%							x		x								
Lock for lost or stolen devices	41%	40%							x	x									
Internet domain restrictions	36%	0%																	
Applications restrictions	33%	20%								x									
Data encryption	27%	0%																	