



THE THREE CS OF ENTERPRISE MOBILITY: CONVENIENCE, CONTROL AND CO-EXISTENCE

Abstract

With the ever accelerating adoption of mobile devices and applications in both the consumer world and the workplace, there is an increasing challenge for organizations to find ways to secure those mobile devices for professional use all the while allowing employees to use those devices as they wish for personal use. This Executive Insight highlights some of the current challenges and opportunities for finding the right balance between the need for corporate control and personal convenience of mobile devices.

It is difficult to deny the fact that society is in the middle of a new computing revolution driven by the adoption of mobile devices such as smartphones and tablets. In just four short years, we have seen a massive proliferation and adoption of smartphones, driven by the consumerization of information technology.

This consumerization of information technology has been one of the most important factors in the creation of on demand information access for both individuals and businesses. In fact, market research firm Strategy Analytics predicts that by 2020, more than five billion consumers and businesses worldwide will be connected to the Internet and cloud via 20 billion wired and wireless devices. The Enterprise Mobility Foundation believes that as the world continues to ride the mobility adoption wave, we will collectively need to balance the desire for individual convenience, and the need for control of corporate information via a new mindset of co-existence that recognizes the increasingly blurred line between personal and professional needs/requirements.

CONVENIENCE

If there is one word to summarize the value proposition of using mobile devices, many would agree that it would be convenience. Mobile devices make it easier to not only stay connected with friends and colleagues, but additionally to quickly and easily – to conveniently – access information.

The explosion of mobile applications (with over 500,000 now available for the various mobile platforms) provides us a new paradigm for work and infotainment on the go. Today, we take for granted – and even expect – the ability to connect to the Internet to not only access (corporate) email, but also be able to consume and create information. Information obviously comes in different forms, whether it be news, updates from social networks, but also through applications that provide us other functionality to find and share information.

Although the explosion of mobile applications has provided individuals amazing opportunities for changing the way we (co)exist, the scale of change has created as many opportunities as challenges within the workplace.

CONTROL

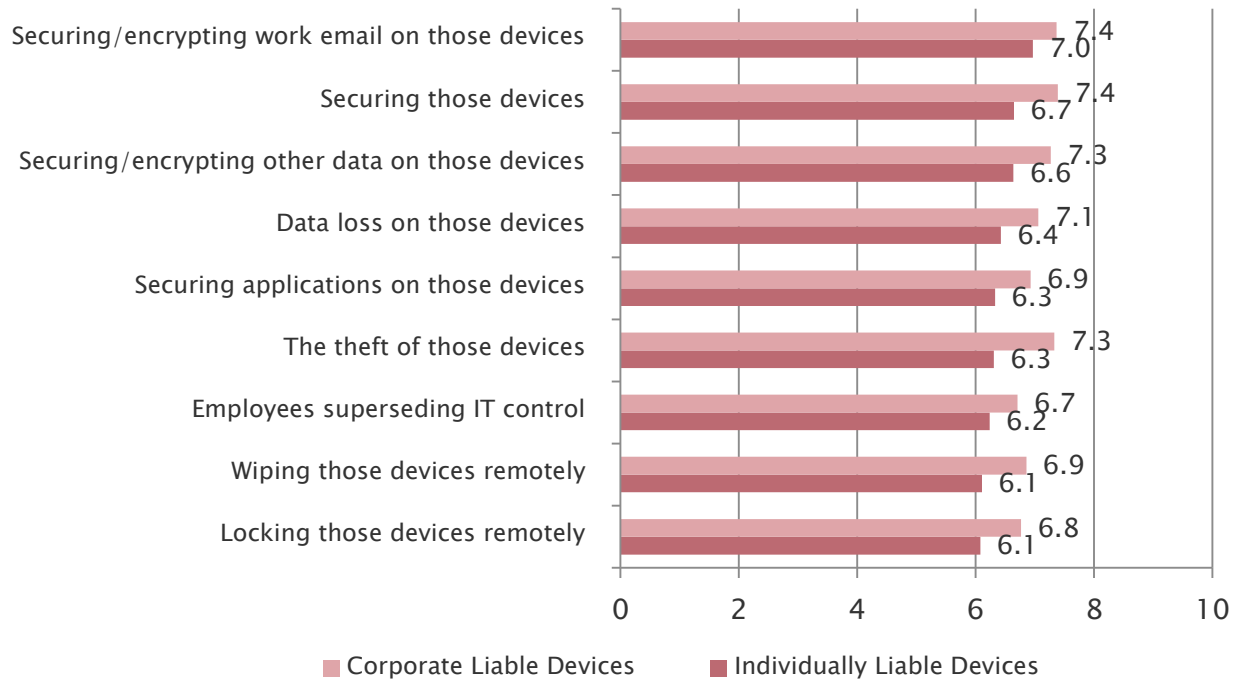
Historically, organizations – and particularly IT departments – have been used to having the ability to control every aspect of the IT infrastructure. When there was a major divide between the tech-savvy and the tech-phobic, it was relatively easy for the IT department to not only control, but dictate how technology was deployed and managed within the workplace.

As technology has become increasingly commoditized, it has permeated deeply into the home and hence created a new generation of technologically savvy individuals. From an enterprise mobility perspective, the consumerization of enterprise mobility over the past few years originated in part from the downturn in the economy. This downturn helped fuel the proliferation of individually liable mobile devices in the workplace. The combination of these two forces enabled a wave of individuals to purchase their own smartphones and connect them to their corporate email accounts and become “mobile.”

While there is no question that the consumerization of enterprise mobility has helped spark growth and innovation in the workplace, there is a growing concern and backlash regarding the potential negative repercussions of allowing so many individual – and hence uncontrolled – devices accessing sensitive corporate

information with unfettered access. This increased awareness regarding the repercussions of unfettered mobile access has been a key catalyst for the adoption of mobile device management (MDM) and security solutions.

FIGURE 1 : IT CONCERNS REGARDING MOBILE DEVICES IN THE WORKPLACE



Source: Strategy Analytics, Inc.

Data from market research firm Strategy Analytics shows however that there is an increasing level of concern on the part of IT departments in terms of how mobile devices – whether they be smartphones or tablets – are being secured in the workplace. The concern is both genuine and warranted as an increasing amount of corporate information is being accessed on both individually liable and corporate liable devices. The challenge however is two-fold. Firstly, organizations should not consider individually liable devices any differently than corporate liable devices (as evidenced in the above chart) because they will be accessing the same types of information regardless of ownership. Second, while it is relatively simple to completely lock down a device, that level of lock down would also make it highly inconvenient and frustrating for users to access and use the device, thus potentially reducing their use and the intended benefits of mobility in the workplace.

CO-EXISTENCE

To date, MDM and security solutions, while providing organizations deep capabilities for command and control, have also had their own limitations. For example, remote wiping a device would typically indiscriminately wipe the entire device, and hence remove personal applications and data that can and arguably should innocuously remain on the device (particularly in the scenario of when someone is simply changing jobs). This all or nothing approach to device wiping has created an employee pushback on device management, but also created opportunities for vendors to provide new solutions for managing this need for an equilibrium between managing personal & professional information.

Today, organizations can deploy mobile applications using “sandbox” solutions or can alternatively virtualize content on a mobile device, thus creating a clear line of demarcation between personal and professional information. The main challenge with these two approaches is that there is increasingly no clear line of demarcation separating how, where or when individuals are looking to access personal or professional information. The Enterprise Mobility Foundation believes that, for the most part, neither of these two approaches provides the most elegant solution possible for personal and professional information to co-exist on one mobile device because neither solution fully addresses the subtleties of how people are using their mobile devices on a daily basis for both personal and professional tasks. Hence, The Enterprise Mobility Foundation strongly believes that users would greatly benefit from a technology solution that can easily manage the personal and professional needs of individuals’ data in a seamless fashion.

CONCLUSION AND RECOMMENDATIONS

The Enterprise Mobility Foundation believes that organizations can no longer look at mobility solutions as either “consumer focused” or “enterprise focused.” Mobile solutions need to provide an uninhibited user experience that caters to all the needs of the user – whether it be for their personal or professional use.

Furthermore, the continuing transition towards individually liable devices provides organizations a unique opportunity. Specifically, organizations that have historically resisted allowing individually liable devices – primarily for security purposes – should instead consider this trend as an opportunity to

reinvest some of their mobile budget into mobility management solutions. These solutions are varied and offer broad sets of functionality. However, The Enterprise Mobility Foundation recommends that organizations look at mobility management solutions that have (among others) the following functionality:

- The solution provides not only basic mobile device management functionality, but also the ability to manage applications and provide real security features;
- The ability to delete your organization's data while leaving personal data intact via a management console;
- Administration and control through a web interface which allows it to be accessed wherever and whenever your IT administrators may need it;
- The ability to (if you choose) prevent a user from forwarding your organization's data to a personal email account;
- The ability to control which applications can access your organization's data (and through which means);
- The ability to support users and provide device updates over-the-air (OTA);
- The ability to access information or perform actions on the device even without a data connection;
- The ability to prevent a user from pasting your organization's data into personal applications (even if it's with genuine intentions).

These are just some high level recommendations, in terms of the kinds of device and application management functionality that will provide users and organizations the greatest flexibility as mobility evolves and proliferates within the workplace. Forward thinking organizations will deploy mobility management solutions that can elegantly address this need for seamless use of mobile devices such that personal and professional information can co-exist on a user's device of choice, while ensuring corporate data security and integrity.

ABOUT THE ENTERPRISE MOBILITY FOUNDATION

The Enterprise Mobility Foundation's mission is to be the global community builder and evangelist for showcasing the value of successfully deploying and managing mobility solutions within organizations in the public and private sector. The EMF is supported by organizations including its founding supporters: Tangoe and Zenprise. These and other friends of the Foundation respect our responsibility to independently pose questions, find and present answers and address issues as they are.

For more information on The Enterprise Mobility Foundation, please visit <http://www.theemf.org>.