Mobile devices
A security perspective

Stéphane Hurtaud
Partner
Governance Risk
& Compliance
Deloitte

Maxime Verac
Manager
Governance Risk
& Compliance
Deloitte

BYOD (Bring Your Own Device), COPE (Corporate Owned Personally Enabled) or CYOD (Choose Your Own Device) are often used as the names for projects ultimately aiming to put corporate data on mobile devices used by employees, even if those names only describe the provisioning approach of an often more complex mobile devices management project.

How to ensure that security threats will not jeopardise your mobile strategy

Recent mobile devices such as smartphones and tablets enable employees to work anytime and anywhere, and are powerful enough to handle most business activities and data, including email, documents, contacts and agendas. They are also used extensively for social media and access to cloud-stored data. This intermingling of access to business data and use of personal software applications in one device makes mobile devices a prime target for hackers and provides new entry points for attack, in addition to being easily lost or stolen.

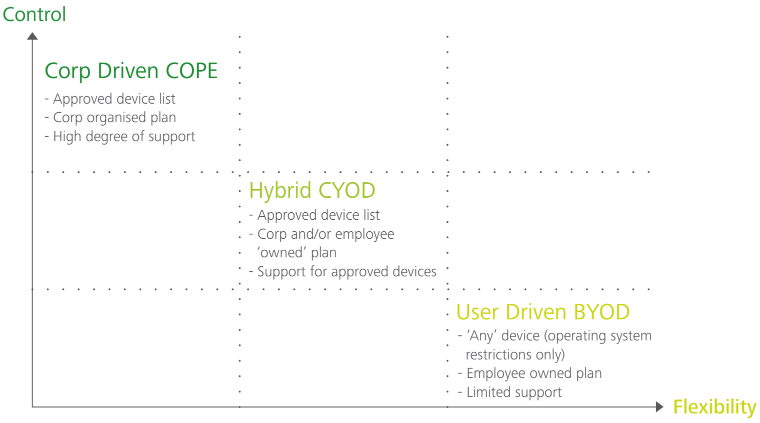
Mobile devices are a good example of the new information security paradigm resulting from the de-perimeterisation of IT, where IT assets, users and data are moved outside of the traditional Information System boundaries.

Many Luxembourg organisations across all industries are currently dealing with this type of project (either as a new service or as the migration of an obsolete system) and are facing the new security challenges presented by IT de-perimeterisation.

Understanding the threat landscape

According to the Norton Report 2013[1], 38% of smartphone users have experienced mobile cybercrime in a one-year timeframe, while 27% of adults have lost their mobile device or had it stolen.

Figure 1: 'Provisioning' approaches for mobiles devices: a trade-off between flexibility and control



It is not surprising that, for instance, TMT organisations now consider mobile devices to be their second biggest security risk, with 74% rating it as a 'high' or 'average' threat[2].

Considering that 57%[1] of users are not aware that security solutions exist for their mobile devices, it is easy to understand that security is an important topic when dealing with a BYOD project, especially when you examine the following threats[3], which are for the most part specific to mobile devices:

- **Lack of physical security controls:** mobile devices are not protected by the physical boundaries of the company's premises. Furthermore, because of their mobile nature, they are more likely to be lost or stolen than other devices

[1] Symantec, 2013 Norton Report: http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=norton-report-2013

[2] Deloitte, 2013 TMT Global Security Study: http://www2.deloitte.com/content/www/global/en/pages/technology-media-and-telecommunications/articles/2013-tmt-global-securitystudy.html

[3] NIST, Special Publication 800-124 Revision 1, Guidelines for Managing Security of Mobile Devices in the Entreprise: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r1.pdf

- **Use of untrusted mobile devices:** unless properly secured and continuously monitored, mobile devices should be considered as untrusted (jailbreaking, rooting, etc.).
- **Use of untrusted networks:** public Wi-Fi connections generally used by mobile devices are often a vector of choice for eavesdropping or man-in-the-middle type attacks. Organisations should therefore assume that the networks between the mobile device and the organisation cannot be trusted
- **Use of untrusted applications:** end-users can easily install applications – potentially with advanced rights – directly from various application stores containing malicious applications (by 2013, more than 42,000 apps in Google's store contained spyware and information-stealing trojan programs according to RiskIQ[4])
- **Interaction with other systems:** mobile devices are often connected to personal computers, which may be vulnerable and infect them. In addition, mobile devices are generally configured to automatically back-up their content on a cloud storage solution, which may lead to data leakage
- **Use of untrusted content:** Quick Response (QR) codes have been designed especially for mobile devices. Unfortunately, such QR codes are increasingly being used to direct mobile devices to malicious websites
- **Use of location services:** the GPS capabilities of smartphones can provide valuable information to attackers when planning a targeted attack. Uncontrolled use of location services may also lead to a privacy breach

The above threats and vulnerabilities have been grouped into four risk categories in the table below:

Figure 2: Overview of the main risks related to mobile devices

Operational risks	• End users (including corporate executives) are increasingly driving decisions concerning devices • Highly diverse mobile ecosystem due to multiple mobile OSs and carrier specific implementations • Lack of 'mobile-ready' support and operational processes, infrastructure • Lack of resources, skill sets and technical capabilities in-house
Legal & regulatory risks	• Potential privacy issues due to personnel activity, device use (location services), data exposure, etc. • Ethical and legal issues around monitoring, device wiping, securing devices and data upon employee termination, etc. • Regulatory requirements regarding e-discovery, monitoring and data archiving need to be considered
Technology & data protection risks	• Lack of native encryption on devices, memory cards and at OS level (for certain OSs) • Unauthorised and unapproved installation of applications by end users; control is challenging • Interaction with other systems (cloud storage, personal computer synchronisation, etc.) • Lack of mobile OS patching and update enforcement • Usage of untrusted devices: end-users modifying or bypassing device security controls (root or jailbreak)
Infrastructure & device risks	• Sophisticated and varying attack vectors targeting mobile users and devices (including untrusted network and untrusted content such as QR codes) • Diverse mobile ecosystem can result in an expanded attack surface or enterprise risk profile • Third party application vulnerabilities, applications with questionable motives • Lack of physical security controls (remote wipe is not a universal solution as attempts frequently fail for lost and stolen mobile devices)

3 RiskIQ report: http://www.riskiq.com/company/press-releases/riskiq-reports-malicious-mobile-apps-google-play-have-spiked-nearly-400

What are the key controls?

The first step to take in the early stages of every mobile device management project is a dedicated information security risk assessment. This assessment should take into account the specific threats targeting your business and context, and consider the resources to be accessed through the mobile devices.

In addition to the specific controls resulting from the risk analysis, the following controls should be considered on every occasion:

- **Use a centralised system to manage mobile devices:** there are generally two approaches to doing this, either by relying on messaging server management capabilities or by implementing a dedicated Enterprise Mobility Management solution (formerly known as Mobile Device Management solutions). The latter approach usually has more advanced features and is able to support devices from multiple vendors with different operating systems. Such a solution should be used to enforce the controls detailed in the mobile device security policy
- **Implement a dedicated mobile device security policy:** such a policy should define which of the organisation's resources may be accessed via mobile devices and the types of mobile devices allowed (and provisioning processes), as well as cover how the organisation's centralised mobile device management solution is administered

Moreover, the policy should detail the controls to be enforced to cover:

- User and device authentication (password policy, mobile lockout, etc.)
- Application security (applications permitted, etc.)
- Data and communication security (Wi-Fi and Bluetooth restrictions, data encryption, remote wipe capabilities, etc.)
- Device and operating system security (patch management, etc.)

Consider security for the whole lifecycle of mobile devices:

- Consider security during product selection (mobile device and management solutions)
- Fully secure each device before allowing a user to access it
- Regularly maintain mobile device security (security updates, applications updates, etc.)
- Fully wipe the device before any reallocation or decommissioning

Conclusion

As is the case for every sensitive IT project, security should be considered in the early stages of your mobile project. You should also ensure that the business has been involved in defining an approved mobile strategy in order to assess whether your security approach is in line with the organisation's long-term mobile roadmap.

One of the most pragmatic approaches to reducing the risk of allowing users to have both personal and professional data on a single mobile device is to rely on a dedicated security container. This container should be managed by an Enterprise Mobile Management solution.

Considering the provisioning option, a hybrid approach is the most suited to reducing operational risk by allowing the end-user to have a degree of freedom while limiting the number of supported devices.