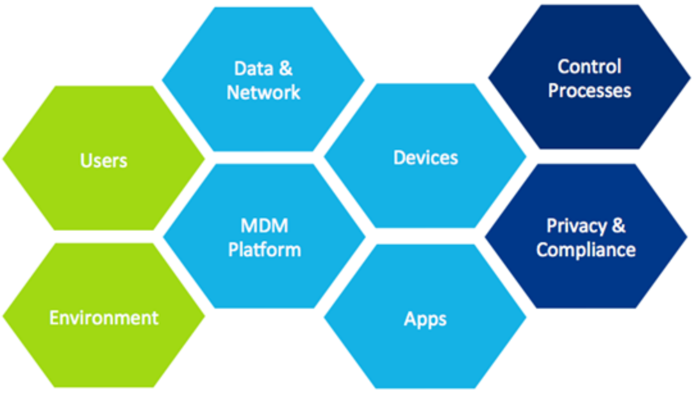
M-RAM: a Mobile Risk Assessment Method for Enterprise Mobile Security



NB: This manuscript was originally submitted in April 2014 to the Journal of Research and Practice in Information Technology, but was not assigned a decision before 2017 when the journal apparently ceased to exist...

Joey Janssen
Marco Spruit

Technical Report UU-CS-2019-009
December 2019

Department of Information and Computing Sciences
Utrecht University, Utrecht, The Netherlands
www.cs.uu.nl

ISSN: 0924-3275

Department of Information and Computing Sciences
Utrecht University
P.O. Box 80.089
3508 TB Utrecht
The Netherlands

M-RAM: a Mobile Risk Assessment Method for Enterprise Mobile Security

Joey Janssen[1] and Marco Spruit[1]

[1] Utrecht University, Department of Information and Computing Sciences, Princetonplein 5, 3584CC Utrecht, the Netherlands
J.Janssen@uu.nl, M.R.Spruit@uu.nl

Abstract. Mobile solutions seem to outrun the control and governance within enterprise organizations. The acceptance of smartphones and tablets in business has gone at such a high pace that organizations are no longer able to oversee the risks of their mobile usage. Traditional risk assessment methods do not consider usage of mobile devices— mobility—despite the fact that enterprise organizations struggle with managing mobile risks. We aim to fill this gap by introducing a Mobile Risk Assessment Method (M-RAM). The method is based on an evaluation of industry standard risk methods and 22 interviews with mobile security experts. Three components compose the method: (1) a risk assessment process that is customized for mobility, (2) involved entities that oppose risks, and (3) attention areas that can contain vulnerabilities as well as controls. Moreover, the study provides a practical work program to conduct the M-RAM and validates the approach by conducting a case study.

Classification: K.6.5 (Security and Protection): Management of Computing and Information Systems

Keywords: mobile risks, enterprise mobility, mobile devices, risk management, mobile security, risk assessment.

1 The Need for Mobile Risk Management

The use of mobile solutions within enterprise environments is growing rapidly. “Mobility means more devices, more locations, and more apps”. Information workers in the US who are using more than two devices in their daily work have risen from 15% in 2011 to 29% in 2012 (Forrester, 2013). The possibilities of mobile devices seem to be endless and replace a lot of conventional desktop solutions. Besides the great advantages of these mobile solutions, there are serious risks that need to be considered, while users are only worried about preserving the convenience on their mobile device (Air-Watch, 2013). 92% of the top 100 paid iOS apps have been hacked compared to 100% of the top 100 paid Android apps (Cisco, 2012). Identifying and controlling these risks is an immature area and a concern for CIOs around the world (TechTarget, 2013).

Information security management is the main focus as mobile solutions are more and more dealing with corporate information using email, mobile ERP applications and corporate portals (Spruit & Roeling, 2014). The main problem is that organizations don't have the means and knowledge to control and govern their mobility usage. Therefore, the demand for a solid approach to identify and control mobile risks within organizations is growing rapidly. The consequences of not dealing with the risks that originate from enterprise mobility can be devastating. Leaking sensitive information, violating personnel privacy, violating corporate image, providing access to corporate resources and getting financially robbed through malware exploits are just examples of possible consequences.

In this research we aim to answer the question *"How can a rigorous and relevant method be developed to assess the risks that originate from the usage of enterprise mobility within enterprise organizations?"*. We answer this question by providing a method including a practical work program to assess the risks of mobile usage within enterprise organizations. This approach should allow managers to identify how their organization is threatened by the usage of mobile devices, what the organization already does to mitigate these threats and what the residual risks are regarding mobility. In order to prevent confusion, the following definitions are elaborated:

- *Mobile Device* - "Device with limited (power) resources, that is portable and not using a full blown operation system" (e.g. Smartphone, tablet. NOT laptops)
- *Enterprise Mobile Security* - "Securing mobile usage within enterprise organizations" (e.g. MDM, policies, encryption. NOT security for mobile apps or using mobile for security)
- *MDM (Mobile Device Management)* -"Tooling that enables organizations to manage and govern mobile devices"
- *BYOD (Bring Your Own Device)* - "Situation where employees bring their personally owned device to work for business purposes"

In the following, we first will explain the analysis phase including an evaluation of industry accepted risk assessment standards and 22 mobile risk and security expert interviews. Then, we introduce the components of the method we dub the Mobile Risk Assessment Method (M-RAM), the actual artifact including a work program to execute the introduced approach, and finally, we present our case study validation.

2 Assessing Enterprise Mobility Risks

In order to design a rigorous and relevant method an elaborate analysis is performed by evaluating industry standard IT risk assessment methods and interviewing experts on mobile technology and security from different professional fields. A total of 12 mobile security experts were interviewed from leading security consultancy firms and 10 mobile security managers that are responsible for the security and risks of mobile device usage in large enterprise organizations. The outcome of the evaluation of the industry standard IT risk assessment methods is further discussed in section 3: The Three M-RAM Components.

Empirical findings

Both Mobile Security Experts (MSEs) and Mobile Security Managers (MSMs) were interviewed to understand why and how mobile devices are used within enterprise organizations, how organizations manage mobility and how organizations deal with trends such as BYOD and MDM. The most interesting empirical findings are discussed here. Figure 1 provides an overview of what our 22 MSEs and MSMs consider as the most important threats of mobile device usage. Noticeable is that the concerns about corporate reputation damage and leaking client's data are important to MSMs, but were not mentioned by MSEs. Furthermore, it can be concluded that the leakage of corporate data is the threat both MSEs and MSMs are most concerned about. Figure 1 also explains how organizations assess these risks, according to the MSEs and MSMs. Noteworthy is that most organizations use standard IT risk assessment methods or an own interpretation of a likelihood times impact assessment. Moreover, 25% of the MSEs state that organizations are not assessing risks at all.

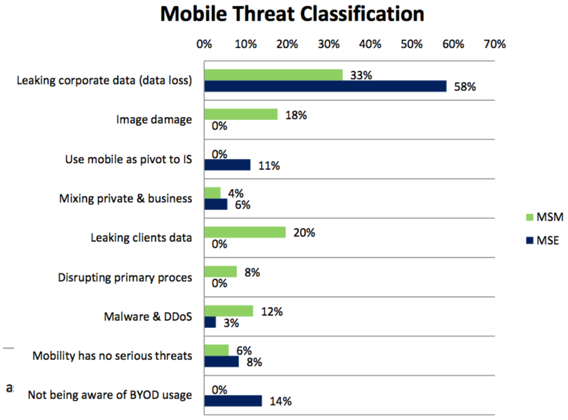


Figure 1: Mobile Threat Classification & Risk Assessment Approach

Furthermore, the MSEs were confronted with a high-level concept of the envisioned M-RAM artifact. They were asked what they consider to be the most important attention areas that can contain mobile vulnerabilities as well as mobile controls. Figure 2 provides an overview of the opinion of MSEs on the attention areas. Also, each MSE is asked to name and group the different entities that are involved in the usage of mobile devices in enterprises. Figure 2 shows that the MSEs mostly agree on the involved entities, as there are very little differences in the results. The X-axis represents the different areas and entities and the Y-axis represents how often an area or entity is named as important.

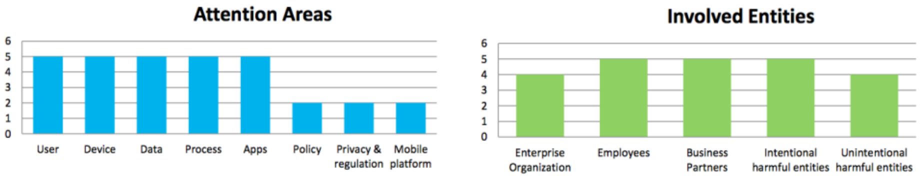


Figure 2: Attention Areas & Involved Entities

3 The Mobile Risk Assessment Method: M-RAM

The three components of the M-RAM

From the analysis presented we determined and developed the Mobile Risk Assessment Method (M-RAM) that consists of three components. The first component is the risk assessment process that is the core of the M-RAM approach. Second are the entities involved in order to understand where threats are initiated. The third component denotes the attention areas that guide the assessor to find specific vulnerabilities and controls related to the field of mobile device usage and mobile security. Below we elaborate on each component to explain how the M-RAM materialized.

Component 1: Risk Assessment Process

Risk assessments on IT systems are usually executed using industry-accepted standards from organizations such as ISO, NIST, COSO, ISACA, ISF and CERT (Ramirez, 2008). In order to determine a solid mobile risk assessment process we evaluated each step of the industry-accepted standards on the applicability for a mobile risk assessment. Then, based on the evaluated industry standards we determined a reference method (Levantakis et. al, 2008) and adapted each step of the reference method to the context of enterprise mobility. Figure 3 provides an overview of the adapted Mobile Risk Assessment Process. The process starts with a preliminary step that is needed to define the 'mobile profile' of the assessed organization. This 'mobile profile' contains the organization's mobile demand, usage, policy and vision. The first step of the actual assessment aims to identify and classify each device asset and information asset that is on a device or can be accessed by a device. The second step determines the mobile threats to the assessed organization and determines the vulnerabilities that expose these threats. Step 3 is the quantification of the initial risks (without considering installed controls) that are exposed to the organization. The risk quantification is done by determining the product of the likelihood that a threat occurs and the impact that a threat can have to the organization. In the fourth step, we determine which controls are already installed to mitigate the determined risks. Then in the fifth step, the residual risk is defined by determining how the identified controls mitigate the likelihood and impact of the identified threats. Moreover, each control is evaluated on its impact on mobile usability and innovation possibilities. The follow-up step 'Define action plan' is not part of the actual assessment, but is added to guide organizations in how the outcome of the assessment should be addressed.

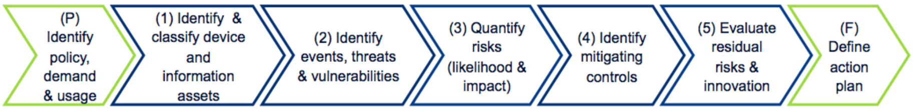

(P) Identify policy, demand & usage
(1) Identify & classify device and information assets
(2) Identify events, threats & vulnerabilities
(3) Quantify risks (likelihood & impact)
(4) Identify mitigating controls
(5) Evaluate residual risks & innovation
(F) Define action plan

Figure 3: Mobile Risk Assessment Process

Component 2: Involved Entities

One of the main differences of the M-RAM approach compared to existing IT risk assessments is its specific context (i.e. the usage of mobile technology in enterprises). Contrary to general IT systems, mobile devices are constantly leaving the enterprise and are much more accessible to various different entities other than the end user. In order to determine and assess the threats of mobile usage, one should understand the different entities that threaten the organization. To provide this understanding a second component explaining the different involved entities with mobile usage is added to the M-RAM approach. The involved entities component consists of four entities, two internal and two external:

1. *Enterprise Organization (internal)*
2. *Employees (internal)*
3. *Business Partners (external)*
4. *Potential Harm-doers (external)*

The first internal entity 'Enterprise Organization' represents the assessed organization and contains only entities that have a role in providing or managing mobile technology in the broadest sense. 'Employees', the second internal entity is the center as the employees are using the mobile devices. The entity exists of all employees that are using one or more, company or personally owned mobile devices to execute work-related tasks. The external 'Business Partners' entity exists of all entities that work with or for the assessed organization and make use of their enterprise mobile solutions. The most complex and extensive entity is the 'Potential Harm-doers', representing all entities that intentionally or unintentionally harm the assessed organization. Hackers and malicious parties are common examples of intentional harm-doers, whereas children and relatives are often forgotten examples of unintentional harm-doers.

Component 3: Attention Areas

The identification of vulnerabilities that expose threats, and controls that mitigate these threats, are part of the core steps of the risk assessment process. In order to successfully identify these vulnerabilities and controls, a thorough understanding of the different attention areas of mobile device usage is needed. This is the third component, 'Attention Areas', that is added to the mobile risk assessment method. As shown before (Figure 2), we determined specific attention areas based on the gained insights from the 22 interviewed mobile risk & security experts, and the special publications from NIST (2013), the ISF (Davis et. al, 2011) and the NCSC (2012). Figure 4 provides a classification and overview of the eight determined attention areas, each help to understand which vulnerabilities and controls can be determined from the attention areas.

The colors represent a mapping to the people-process-technology model (Chen, Popovich, 2003): green represents People, light blue denotes Technology, and dark blue signifies Processes.

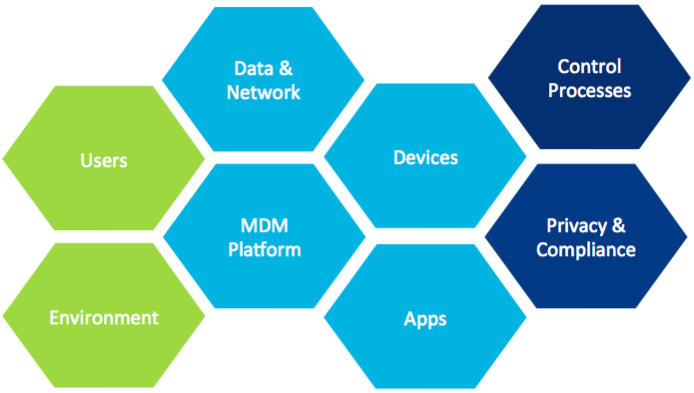


Figure 4: Mobile Attention Areas

'Users' - Contains vulnerabilities that are initiated by the end users of the mobile devices. Furthermore, all mitigating controls that are appointed to positively influence the user on their mobile usage are part of this attention area.

'Environment' – Contains all vulnerabilities and controls that exist as a result of the 'on the go' property of mobile devices. Devices can be everywhere and cannot be physically controlled.

'Devices' - Contains all vulnerabilities and controls that can be identified on the physical hardware and operating system of the mobile devices.

'MDM Platform' **-** Contains all vulnerabilities and controls related to the Mobile Device Management (MDM) system that is used and systems that enable services that are used on mobile devices.

'Apps' **-** Contains all vulnerabilities that can be found in any app (self-developed or third party) that is running on a mobile device within the assessed organization. Controls that are installed to mitigate these vulnerabilities, i.e. black/white list apps or manage the rights of apps are also part of this attention area.

'Data & Network' - Contains all vulnerabilities that are directly related to the exposure or loss of enterprise data (via any mobile network connection). Controls that are installed in order to mitigate the possibility of exposing or losing enterprise data are also part of this attention area.

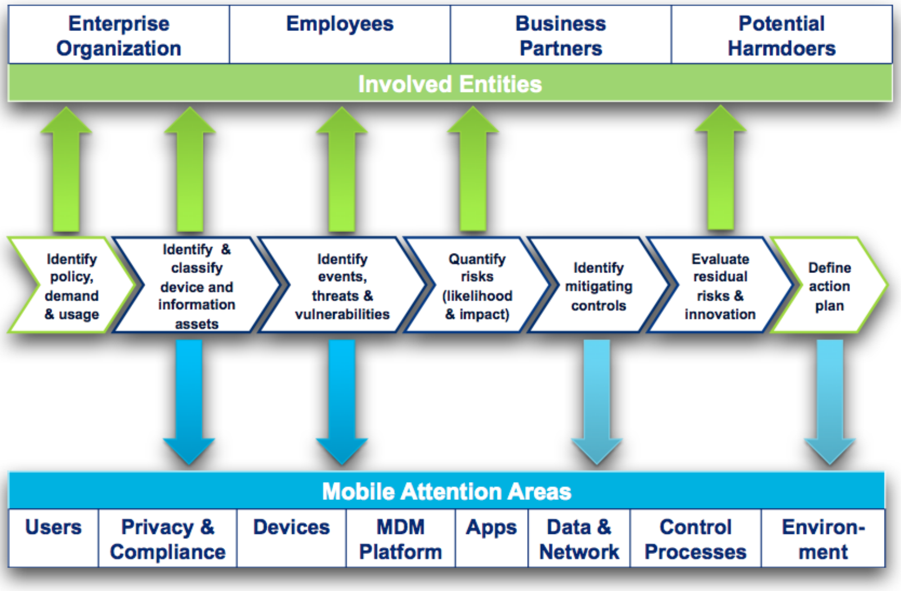
‘Control Processes’ **-** Contains all vulnerabilities that are posed by organizational processes that are not, or not efficient arranged to manage the use of mobile devices. Introduced or optimized processes that are installed to mitigate these vulnerabilities are also part of this attention area.

‘Privacy & Compliance’ **-** Contains vulnerabilities that can violate the privacy of employees in one way or another, as well as vulnerabilities that can lead to consequences to the organizations for not being compliant with (inter)national legislation on privacy, encryption or other mobile-related laws. Controls that prevent the violation of privacy or legislation are also part of this attention area.

The M-RAM approach

The final M-RAM artifact enables a high-level approach based on combining the three components and translates it into a practical method (a ‘work program’) that enables managers and consultants to use the M-RAM approach to assess organizations.

Figure 5 depicts the M-RAM and its approach. It shows how the three discussed components are related to each other. The mobile risk assessment process is the core of the method and is positioned in the middle. The components ‘Involved Entities’ and ‘Attention Areas’ are depicted above and below the process, respectively. The arrows between the process layer, and the other two components/layers above and below it, indicate when the involved entities on the one hand and the attention areas on the other should be used in the different process steps.



Enterprise Organization
Employees
Business Partners
Potential Harmdoers
Involved Entities
Identify policy, demand & usage
Identify & classify device and information assets
Identify events, threats & vulnerabilities
Quantify risks (likelihood & impact)
Identify mitigating controls
Evaluate residual risks & innovation
Define action plan
Mobile Attention Areas
Users
Privacy & Compliance
Devices
MDM Platform
Apps
Data & Network
Control Processes
Environ-ment

Figure 5: M-RAM Approach

The M-RAM Work Program

In order to execute the M-RAM, we introduce a practical work program interpretation of the high-level approach as shown in Figure 5. The practical work program defines detailed activities for the preliminary step, each of the five mobile risk assessment steps and the follow-up step. The work program contains interview, workshop, technical as sessment, field test, analyses and report activities. Moreover, the work program defines which stakeholder representatives (User, Business, IT, Security and R&D) should be involved in which activities. Figure 6 provides an overview of the practical M-RAM work program containing all activities, involved stakeholders and signing points for the organization under assessment. The preliminary and follow-up steps are not included in Figure 6. The details and output of the work program are further illustrated in the next section by means of a case study.

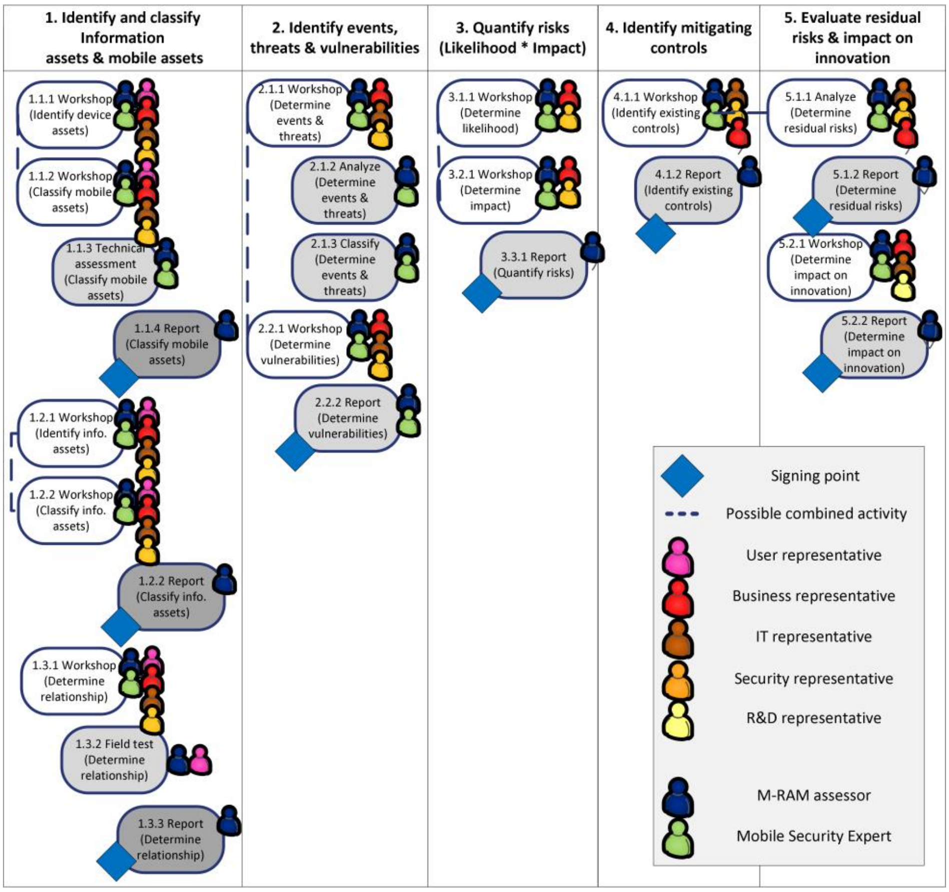

1. Identify and classify Information assets & mobile assets
2. Identify events, threats & vulnerabilities
3. Quantify risks (Likelihood * Impact)
4. Identify mitigating controls
5. Evaluate residual risks & impact on innovation
1.1.1 Workshop (Identify device assets)
1.1.2 Workshop (Classify mobile assets)
1.1.3 Technical assessment (Classify mobile assets)
1.1.4 Report (Classify mobile assets)
1.2.1 Workshop (Identify info. assets)
1.2.2 Workshop (Classify info. assets)
1.2.2 Report (Classify info. assets)
1.3.1 Workshop (Determine relationship)
1.3.2 Field test (Determine relationship)
1.3.3 Report (Determine relationship)
2.1.1 Workshop (Determine events & threats)
2.1.2 Analyze (Determine events & threats)
2.1.3 Classify (Determine events & threats)
2.2.1 Workshop (Determine vulnerabilities)
2.2.2 Report (Determine vulnerabilities)
3.1.1 Workshop (Determine likelihood)
3.2.1 Workshop (Determine impact)
3.3.1 Report (Quantify risks)
4.1.1 Workshop (Identify existing controls)
4.1.2 Report (Identify existing controls)
5.1.1 Analyze (Determine residual risks)
5.1.2 Report (Determine residual risks)
5.2.1 Workshop (Determine impact on innovation)
5.2.2 Report (Determine impact on innovation)
Signing point
Possible combined activity
User representative
Business representative
IT representative
Security representative
R&D representative
M-RAM assessor
Mobile Security Expert

Figure 6: M-RAM Work Program

5 M-RAM in public: a case Study

In order to evaluate the M-RAM approach, we conducted a case study in the practical work program actually executed. The assessed organization is active in the public sector within the Netherlands, employs more than 10,000 employees and manages over 5.000 corporate-owned mobile devices. An experienced IT risk management consultant assisted in the case study and fulfilled the role of mobile security expert. The case study was conducted in a time span of six weeks.

The results from the case study are anonymized and represent indicative samples to maintain confidentiality of the assessed organization. The five defined process steps of the M-RAM structure the work program activities as well as the outcome of the case study.

1. Identify & classify device and information assets – The main activities of the first step were three workshops. The first workshop helped participants to identify all mobile devices with their related security properties and classify all mobile devices on a trust level. The second workshop aimed to identify information assets that can be accessed by a mobile device or can be stored on a mobile device and classify information assets on their confidentiality levels. Both the outcome of workshop 1 and 2 were validated with a field/technical test that validated the devices as well as the identified information assets. The third and last workshop of this step was included to define the relation between device and information asset classes, in order to understand which level of information confidentiality is allowed on each level of device trustworthiness.

2. Identify event, threats & vulnerabilities – The second step appeared to be the most challenging and complex step as (partly) unknown events, threats and vulnerabilities have to be determined. The first activity was a workshop where the participants needed to determine all possible threats that can be posed to the organization, based on possible events (i.e. the report from step 1 and knowledge about common mobile threats). In the next (workshop) activity, for each threat, the participants determined the vulnerabilities that can expose the threat. Each of the eight M-RAM attention areas were considered for possible vulnerabilities. Furthermore, a list of general known vulnerabilities based on (Davis et al, 2011), (NIST, 2013) and (NCSC, 2013) was used to complete the list of identified vulnerabilities. Table 1 provides a sample of identified threats and related vulnerabilities addressed in this part of the case study.

No	Threats	No	Vulnerability	Attention Area
1	Theft & Loss	1	Lack of physical security	Environment
		2	Popular good	Environment
		3	Location (device is everywhere)	Environment
		4	Carelessness of employees	Users
		5	Lacking user awareness	Users
2	Eavesdropping	6	Unconscious of possibility	Users
		7	Usage in public locations	Environment
3		8	24/7 possibility of leaking data	Environment

	Data leakage (conscious)	9	Easy to link data to private environment	Data & Network
		10	Data is stored on device	Data & Network
4	Data leakage (unconscious)	11	Human error	Users
		12	Access to relatives	Environment
		13	Access to app/cloud suppliers	Apps
		5	Lacking user awareness	Users

Table 1: Threats & vulnerabilities sample

*3. Quantify risks (likelihood * impact)* – This step aimed to value the determined threats by quantifying risks based on the likelihood and impact of a threat. As for this workshop the output quality depended on the expertise of the workshop participants, they were selected carefully. Besides the M-RAM assessor and a mobile security expert, a business and security representative sat together to value the likelihood and impact of a threat. The values represent the initial likelihood (I-L) and initial impact (I-I) without taking any existing mitigating controls in mind. The product of I-L and I-I represents the initial risk (I-R) that is opposed to the organization when no controls are in place. Table 2 provides a sample of threats that were valued on I-L, I-I and I-R.

No	Threat	I-L	I-I	I-R		R-L	R-I	R-R
1	Theft & Loss	4	5	**20**		4	1	**4**
2	Eavesdropping	3	3	**9**		3	3	**9**
3	Data leakage (conscious)	3	5	**15**		2	5	**10**
4	Data leakage (unconscious)	4	5	**20**		3	5	**15**

Table 2: Initial & Residual risk sample

4. Identify mitigating controls – In the forth step the existing controls of the assessed organization were identified. Inputs for this step are the eight mobile attention areas that need to be considered, the identified vulnerabilities of step 2 and a list of general mobile controls based on (Davis et al, 2011), (NIST, 2013) and (NCSC, 2013). The main activity in step four was a workshop with representatives from Business, IT and Security that are responsible for mobile policies and controls within the organization. Based on the discussed input of this step, the workshop participants identified all existing controls and linked them to the threats and vulnerabilities that they mitigate. Depending on the allocated time for this step, different control aggregation levels were used (E.g. 'Technical control', 'Device encryption' or 'Encryption of application X').

5. Evaluate residual risk and impact on usability & innovation – Step five provided the output of the complete M-RAM, by determining the residual mobile risks and the impact of installed controls on mobile usability & innovation. The main activities of this step were two workshops. In the first workshop, the residual likelihood (R-L), residual impact (R-I) and the residual risk (R-R) were determined. Based on the output of step 4 (controls), each I-L and I-I from step three was evaluated and provided with a (residual) value that was left after the installed mitigating controls. Table 2 provides a sample of the R-L, R-I and R-R values of the threats that were identified in the case study. The second workshop determined how the installed controls affect and impact the usability and innovation possibilities of mobility. Each control that impacted the usability or possibility of mobile innovation is valued on an impact scale from 1 to 5.

6 Concluding Remarks

The M-RAM presented in this paper aims to be a rigorous and relevant approach to assess enterprise organizations. The core of the approach is the risk assessment process that is complemented with knowledge about involved entities and attention areas with regard to mobile device usage in enterprises. The case study shows how the practical M-RAM program translates the M-RAM approach.

We believe the M-RAM assessment described and explained in this paper is fulfilling a strong need of managers and consultants, but it should be recognized that so far it has only been validated through an extensive but single case study. Further validation is, therefore, needed in different types of organizations. In addition, it is to be expected that the maturity of enterprise mobility in the Netherlands is quite different compared to other countries like the United States (Cisco, 2013). As almost all expert interviewees were active in the Netherlands, the results of this research may not yet be generalized. Nevertheless, we firmly believe that the M-RAM approach will prove valuable throughout the globe as-is, and we will further our empirical research efforts to demonstrate so.

References

1. AIR-WATCH (2013). Enabling Bring Your Own Device (BYOD) In the Enterprise. Retrieved August 2013. From http://www.airwatch.com/resources/
2. ARXAN (2012) State of Security in the App Economy: “Mobile Apps Under Attack”. Retrieved August 2013. From http://www.arxan.com/resources/state-of-security-in-the-app-economy/
3. CISCO (2012) BYOD: A Global Perspective. Retrieved August 2013. From http://www.cisco.com/web/about/ac79/docs/re/BYOD_Horizons-Global_Top10-Insights.pdf
4. Chen, I. J., & Popovich, K. (2003). Understanding customer relationship management (CRM): People, process and technology. Business Process Management Journal, 9(5), 672-688.
5. Davis, A., Nowak, G., & Vrhovec, G. (2011). Securing consumer devices. Information Security Forum.
6. FORRESTER (2013). Benchmarking Mobile Engagement: Consumers And Employees Outpace CIOs’ Readiness. Retrieved, August 2013. From http://www.forrester.com/Benchmarking+Mobile+Engagement+Consumers+And+Employees+Outpace+CIOs+Readiness/fulltext/-/E-RES95601
7. Levantakis, T., Helms, R., & Spruit, M. (2008). Developing a reference method for knowledge auditing. In Practical Aspects of Knowledge Management (pp. 147-159). Springer Berlin Heidelberg.
8. NIST (2013). National Institute of Standards and Technology. Retrieved August 2013, from http://www.nist.gov/index.html
9. National Cyber Security Centrum. (2012) Beveiligingsrichtlijnen voor mobiele apparaten.

Retrieved July 2013, from https://www.ncsc.nl/dienstverlening/expertiseadvies/kennisdeling/whitepapers/beveiligingsrichtlijnen-voor-mobiele-apparaten.html

10. Ramirez, D. (2008). Risk management standards: The bigger picture. Information Systems Controls Journal, 4.
11. Spruit, M., & Roeling, M. (2014). ISFAM: the Information Security Focus Area Maturity model. *22nd European Conference on Information Systems*. Tel Aviv, Israel.
12. TECHTARGET (2013). IT Security Trends 2013: Mobile security concerns tops the list. Retrieved August 2013, from http://searchsecurity.techtarget.com/feature/IT-Security-Trends-2013-Mobile-security-concerns-tops-the-list
13. FORRESTER (2013). 2013 mobile workforce adoption trends. By Ted Schadler with Simon Yates, Nancy Wang. Retrieved March 2014. From https://www.vmware.com/files/pdf/ Forrester_2013_Mobile_Workforce_Adoption_Trends_Feb2013.pdf