***IBIMA Publishing***
*Journal of Mobile Technologies, Knowledge and Society*
*http://www.ibimapublishing.com/journals/JMTKS/jmtks.html*
*Vol. 2017, Article ID 593035, 9 pages*
*DOI:10.5171/2017.593035*

*Research Article*

# Mobile Device Strategy: From a Management Point of View

**Martin Brodin**

University of Skövde and Actea Consulting AB, Skövde, Sweden

martin.brodin@his.se

Received date: 2 March 2016; Accepted date: 13 June 2016; Published date: 26 January 2017

Academic Editor: Lasse Berntzen



**Abstract**

In recent years, mobile devices have become an indispensable part of working life. However, in many cases the same device is also used privately, which has blurred the line between personal and company data. This situation needs to be analysed, and a long-term strategy implemented for organisations not to lose control of their data. This article is based on interviews with executives and a theoretical framework for managing mobile devices. Empirical input from practice is used to update the framework to help organisations to better respond to emerging trends for mobile devices.

**Keywords:** Information Management, Mobile Device Strategy, BYOD, CYOD.

## Introduction

Since smartphones entered the market, the need for them has exploded; today 85 % believe that their mobile is a central part of their life (Salesforce 2014). Despite the major focus on mobile devices and increased budgets, there are still many organisations missing a strategy for mobile devices. These devices may cause organisational problems including unwanted disclosure of data and a new attack surface. A strategy may include policies and guidelines, but more important is that it aligns with company strategy and the organisational culture. Nevertheless, a recent survey revealed that only 42 % of the responding decision makers have a clear enterprise mobility strategy in place (Matrix42 2015). Even if they have a strategy this does not imply that it is implemented, the research literature shows a major gap when it comes to the implementation of mobile device strategies (Brodin et al. 2015).

The use of mobile devices is certain to increase because of social trends. The ability to access information whenever and wherever you want has become very important for most people today (Salesforce 2014). If the organisation does not allow the user to access information outside the office, the employees will probably try to find ways to do it anyway, which leads to security issues (Györy et al.

**Cite this Article as:** Martin Brodin (2017)," Mobile Device Strategy: From a Management Point of View",

2013; Walters 2013; Silic & Back 2014; Simkin 2013). Employees that are allowed to use mobile devices for both work and private purpose are more productive since they can manage small tasks during private time. There are reports that talk about savings for the organisation with up to 240 hours per year and employee (iPass 2011; Miller & Varga 2011). This gives the employer much to gain from allowing mobile devices in a controlled way.

The absence of implemented strategies in practice is a major problem for public and private enterprises, large and small, since the greatest threat is security and keeping control of company data. This is something that is also lacking in the literature.

The objective of this paper is to investigate how strategies for mobile devices are implemented in practice through interviews with executive managers. Further an updated version of a mobile device management framework will be presented.

The research questions are therefore:

- What are the most important steps to take when implementing a mobile device strategy?
- How are mobile device strategies implemented in practice?

The study is a pre-structured qualitative investigation combined with a literature review. 13 interviews were conducted with executives in small, medium and large companies and municipalities in Sweden.

The paper is structured as follows. Section two explains how literature looks at mobile device strategy, in section three the research method and analysis model are explained, section four presents the findings from the empirical study and section five introduces an improved version of the framework. Finally, section six gives the conclusions of the analysis, and offers directions for future research.

**Mobile Device Strategy**

Brodin (2015) has developed a framework (figure 1) for managing strategies for mobile devices from initial analysis to fully implemented. The framework is adapted from Johnson and Scholes' (Johnson & Scholes 1993) seminal work on strategic management, and the international standards ISO/IEC 27001 (ISO/IEC 2013a) and ISO/IEC 27002 (ISO/IEC 2013b). It divides the tasks into three categories:

- *Analysis – of* organisation before a strategy is in place, mostly about risks and opportunities.
- *Design* - dealing directly with strategies, different options and development.
- *Action* - about the implementation of strategies.

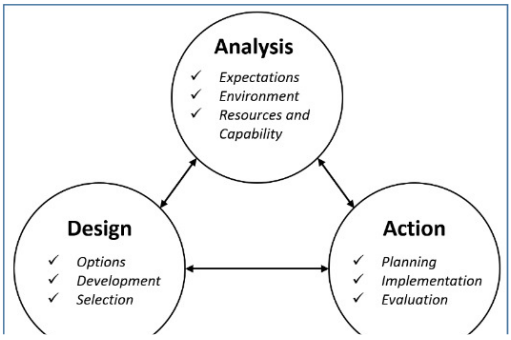


**Fig. 1: A framework for implementing a mobile device strategy, adopted from Brodin (2015)**

### *Analysis*

People who do research in this category mostly focus on opportunities and threats. When it comes to possible benefits that come with the mobile devices, the most common ones are increased personal productivity (Miller & Varga 2011; Dhumal et al. 2012; iPass 2011; Barbier et al. 2012), time/space flexibility (Singh 2012; Harris et al. 2012; iPass 2011; Green 2002; UNICEF 2014) and increased user satisfaction (Miller & Varga 2011; Disterer & Kleiner 2013; Harris et al. 2012).

Threats associated with mobile devices include fear of losing control over information (Pettey & Van Der Meulen 2012; Camp 2012; Walters 2013; Kehoe 2013) and the ability to protect all devices (Disterer & Kleiner 2013; Camp 2012; Walters 2013; Tokuyoshi 2013; Morrow 2012; Skype et al. 2012; Wilson 2012). Another thing that is feared to have a negative effect on the organisation is cost for support (Walters 2013; Harris et al. 2012; Intel 2012) although some argue that there will be no impact (Miller & Varga 2011; Brooks 2013).

### *Design*

Design is about how organisations handle or may handle mobile devices (Mourmant et al. 2013; Harris et al. 2012; Yang et al. 2013; Zahadat et al. 2015; Brodin 2015) and how to design a strategy and selection of strategy. Most articles about designing strategy for mobile devices focus on policies; developing one and keeping it up to date (Oliver 2012; Harris et al. 2012; Gatewood 2012; Montaña 2005; Yang et al. 2013). When it comes to setting the mobile device strategy, it is up to senior management (Ring 2013; Borrett 2013; Mooney et al. 2014) and it is important to have full support from all stakeholders (Silic & Back 2013).

### *Action*

The action part of the framework is the steps to take after selecting a strategy and deals with planning (allocating resources and conducting risk assessment for implementation), implementation (managing change) and evaluation. Some researchers emphasise training (Gatewood 2012; Walters 2013; Markelj & Bernik 2012); we only found two articles dealing with the complete implementation (Brodin 2015; Zahadat et al. 2015). Zahadat et al. (2015) focus on risk management and propose a way to address the security concerns connected to the introduction of mobile devices.

In our literature review, we found a major gap when it comes to the implementation of a mobile device strategy and as a result of that we conducted an empirical study to adjust the action part to practice.

## Method

The empirical work is a pre-structured qualitative investigation (Jansen 2010) where the objective is 'to gather data on attitudes, opinions, impressions and beliefs of human subjects' (Jenkins 1985). Data analysis was conducted using thematic analysis (Braun & Clarke 2006).

13 semi-structured interviews were conducted with executive managers responsible for mobile device strategy, usually CIO but in some organisations CSO, CFO, CSIO or head of IT. The respondents are from different sectors; food industry, manufacturing industry, defence industry, health care, municipality and consulting firms from various sectors (security, IT, management and logistics). The size of their organisations is from 50 to 15 000 employees. Interviews lasted approximately 45 minutes and were recorded and transcribed. The information provided by participants is kept strictly confidential. The coding was conducted with qualitative data analysis software using codes from the framework in section 2. These codes were complemented with additional codes derived from trends detected in the qualitative material.

## Mobile device strategy implementation in practice

The framework shown in section two suggested planning, implementation and evaluation in the action part, which is derived from the strategic management and ISO/IEC 27 000-series. We have looked at literature about mobile device implementation without finding much support for these sub-categories. While analysing the interviews, we instead found three new categories; communication, training and adjustment.

### *Not planning, but communication*

Although our theoretical model required planning, we found that communication is a more central part of implementation. A well communicated strategy is very important since the users have to understand the purpose and benefits of the strategy. One of the respondents talked a lot of the importance of making sure that all employees understand the risks and ended the interview stating that technology will not help you:

*"My main message is that it is not about technology but people. You cannot solve methodological problems with technology, you have to solve the method and it must be easy to do right. If you have a very complicated method where you have to start with two backward somersaults, then it would not be used. This is where it often goes wrong, it gets too complicated with too many things you must do. You cannot solve this with technology; it must be solved with methods."*

Another respondent testified that a policy which is not anchored in staff practice is useless. "*When we looked at how many were actually using mobile email we found 5-600 tablets connected to our network - even though our policy says no to tablets. So it has been just a paper policy, nothing else."*

How changes in policies are communicated differs a lot from organisation to organisation, but current policies can normally be found on the intranet. New or revised policies are communicated mostly by middle managers or as news on the intranet.

Out of the empirical work we found that communication is a key to success, not so much detailed planning for special activities as the model in section 2 indicates.

### *Not implementation, but training*

Communication of a new strategy or policy is important, but effective implementation takes place through training; employees need to understand the core values in the policy and how they are expected to use their device to gain the most benefit and minimize risk. One organisation with many employees with low IT skills chose to hand out all devices just before the summer, so that everyone could learn how to use their device during the summer. When everyone was back from holiday, the organisation officially introduced the device and taught how the device was supposed to be used to facilitate work. Another organisation introduced tablets to their sales' unit together with education in both security and the device itself. "*When we introduced iPad we had people from my department there to educate."* The same tactic was used by another respondent's organisation during implementation of mobile devices; the user received their device and received training on the same day with follow-up sessions to make sure that even persons with low IT skills know how to benefit from their new device.

What type of training users get differs between organisations; five of the respondents said that their organisation provides training in both the device and security, two in only the device, four in only security and two introduced mobile devices without any training program at all. One respondent pointed out that you cannot provide some training and imagine everyone behave as instructed. The users must gain something to embrace the new device in a way that is expected from the organisation. *"…because it's not just education. Here is a tool, and this is an education. They do not care at all, there must also be "what's in it for me". Then all of*

*a sudden we are talking about a change in approach."*

In some cases, the training is done on a regular basis, mostly with a focus on security. Usually the reasons behind it are the demands of customers or certification organisations. "*We are certified to ISO 27001, not the whole company, but some parts, and it is my responsibility to ensure that we really can this and comply with it. And then we implement programs that everyone should have undergone so that you know what is expected of you. But that does not happen every year, the idea is to do it every five years and in between we got introduction with new employees. We are trying to find ways on how to measure and control this so that you can find deviations."* Only two organisations did not arrange any kind of training connected to the mobile devices.

Though the model in section 2 referred to implementation, the organisations in the interview survey were more focused on the most successful means of implementation: training. Training is an important task that needs to be highlighted and performed well.

***Not Evaluation, But Adjustment***

Our theoretical model highlights the importance of evaluation, but in our empirical study only four organisations did an evaluation after the implementation. Some made a proof of concept before the implementation, which was evaluated. Even where there is no formal evaluation some of the respondents felt like they evaluated it by discussions in different forums. "*Yes, maybe we have done this to my unit, we have planning meetings every week and often we have discussions and evaluations of how they use mobile devices - both the security perspective, practical perspective and support perspective. So I would say that we check-up frequently."* A problem with evaluation is in some cases how to conduct the evaluation.

*"But just how to evaluate how employees follows a policy? I do not know exactly how to put in such a control mechanism. What I can control is when we have done an education, and have it online on the web, I can control how many completed the course and you can put controls on how well people understand these questions."* Since it is so hard to evaluate, it is more common to use follow-ups, informal discussions and agenda items at management meetings than a full evaluation and analysis after the strategy is implemented. As one respondent expressed it: "*We have a strategy in place and I think it works quite well. We have not done any proper evaluation, but we discuss the topic from time to time and make adjustments to strategy or people."*

Evaluation is important, but it is not something that is generally done. More common are small, frequent, informal evaluations that lead to some adjustment, which is then communicated to all employees.

***The process***

The original Johnson and Scholes' model (Johnson & Scholes 1993; Johnson et al. 2008) presents a model which is iterative to the extent that you are intended to go back and forth between the phases. Most of the security literature implies a more linear process - create a policy and then implement it. Our empirical studies of practice usually reveal processes best described as punctuated equilibrium: an infrequent major strategy/policy development with additional smaller adjustments when needed, with regular training and communication.

*"... but where we notice that there is a problem, many make a mistake or in a way that is not good or if many are beginning to get to me with issues, several questions about the same thing. We see that there is a need to structure the details and make a statement to clarify things."*

**Improved Framework**

The framework in section two is based on standards and well-known literature. There is a gap in the literature when it comes to the implementation of mobile

device strategies - in this study we have looked at implementation in practice to reduce that gap. With the new insight, we are able to improve the framework.

Our empirical study showed that the steps that organisations take are:

- Training – to increase security awareness, and to gain more benefits from the use of the device itself.
- Communication – to ensure that everyone in the organisation is aware of what the new strategy entails.
- Adjustment – when ambiguities or deficiencies appear in the strategy, adjustments are made.

This gives us the framework in figure 2, where Analysis and Design remain the same as in the original framework. After the initial work with analysis and design, the work moves into an iterative process where the strategy is communicated and training is arranged. When problems, uncertainties or need for improvement arises, adjustments to the strategy are made and communicated. When major changes occur, for instance new mobile devices that do not fit in the current strategy or a change in the organisations overall strategy, the process goes back to analysis again.

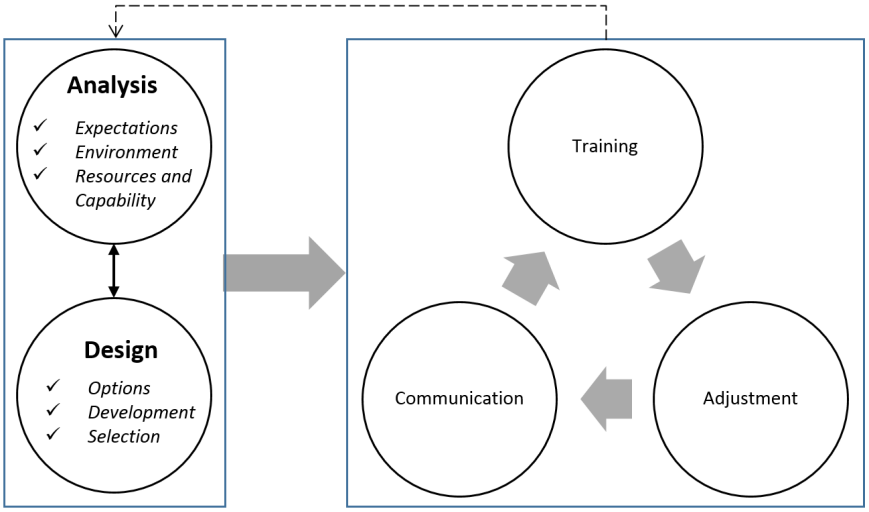


**Fig. 2: The improved framework**

## Discussion and conclusions

Literature tends to focus on policies and the importance of creating them and keeping them up to date. However, many of the respondents in this study do not have a policy for mobile devices, although they do have a successful strategy. In many cases it seems to be more important to work with organisational culture and to educate and communicate. Of course there are policies in the organisation, but they are often short and rather general. It is well known from the literature that employees seldom read, understand or follow policies and with that in mind it seems to be a good plan to focus on the people instead of writing a document if you really want to encourage change.

In our empirical study, we found that the most important steps to take when implementing a mobile device strategy are communication and training. You need to communicate your strategy to all employees and make sure that they understand. However, people understand in different ways and at different speeds, and they tend to forget. That is why

communication needs to be supported with training and cannot be a one-time happening.

There are some limitations in our study; all interviews were conducted within organisations in Sweden, although some of the respondents are responsible for their organisation throughout Europe. Further, we only conducted 13 interviews and can see a trend, but cannot make fully generalizable conclusions. Future work should investigate if this trend can be applied in other countries and more organisations. This updated framework may help researchers and practitioners to understand the important steps to take when implementing a strategy for mobile devices.

**References**

1. Barbier, J., Bradley J., Maculay J., Medcalf R. and Reberger C. (2012). 'BYOD and virtualization - top 10 insights from Cisco IBGS Horizons study,' *Cisco IBSG Horizons Study* , 1-5.

2. Borrett, M. (2013), 'Compliance: keeping security interest alive,' *Computer Fraud & Security*, 2013(2), 5–6.

3. Braun, V. and Clarke, V. (2006), 'Using thematic analysis in psychology,' *Qualitative Research in Psychology*, 3(May 2015), 77–101.

4. Brodin, M. (2015), 'Combining ISMS with strategic management: the case of BYOD,' Proceedings of the 8th IADIS International Conference on Information Systems 2015, ISBN: 978-989-8533-33-3, 14-16 March, Madeira, Portugal, 161–168.

5. Brodin, M., Rose, J. and Åhlfeldt, R.-M. (2015), 'Management issues for Bring Your Own Device,' Proceedings of the 12th European, Mediterranean & Middle Eastern Conference on Information Systems (EMCIS), ISBN: 978-960-6897-08-5, 1-2 June, Athens, Greece, 586-597.

6. Brooks, T. (2013), 'Classic enterprise IT: the castle approach,' *Network Security*, 2013(6), 14–16.

7. Camp, C., (2012), 'The BYOD security challenge - How scary is the iPad, tablet, smartphone surge,' [Retrieved July 15, 2013], http://blog.eset.com/2012/02/28/sizing-up-the-byod-security-challenge.

8. Dhumal, A., Faley, C. and Rodgers, C. (2012), 'Exploring a Bring-Your-Own PC employee stipend at Intel,' *IT@Intel Brief,* November 2012, 1-4.

9. Disterer, G. and Kleiner, C. (2013), 'BYOD Bring Your Own Device,' *Procedia Technology*, 9(2013), 43–53.

10.Gatewood, B. (2012), 'The nuts and bolts of making BYOD work,' *Information management*, (November/December), 26–30.

11.Green, N. (2002), 'On the move: technology, mobility, and the mediation of social time and space,' *The Information Society*, 18(4), 281–292.

12.Harris, J., Ives, B. and Junglas, I. (2012), 'IT consumerization: when gadgets turn into enterprise it tools,' *MIS Quarterly*, 2012(September), 99–112.

13.Intel, (2012). 'Insights on the current state of BYOD in the enterprise – Intel's IT manager survey,' *Peer Research Report,* October 2012, 1-25.

14.iPass, I. (2011), 'Mobilemania sweeps the enterprise,' *The iPass global mobile Workforce report*, November 16(2011), 1–27.

15.ISO/IEC. (2013a), 'ISO/IEC 27001:2013 – information technology – information security management systems – requirements,'ISO/IEC. (2013b), 'ISO/IEC 27002:2013 – information technology – security techniques – code of practice for information security controls,'

16.Jansen, H. (2010), 'The logic of qualitative survey research and its position in the field of social research methods,' *Forum Qualitative Sozialforschung/Forum: Qualitative Social Research*, 11(2).

17.Jenkins, A.M. (1985), Research methodologies and MIS research, research methods in information systems, Mumford E., Hirschheim R., Fitzgerald G., and Wood-Harper A. T. (Eds.), Elsevier Science Publishers B.V., Amsterdam, Holland.

18.Johnson, G. and Scholes, K. (1993), Exploring corporate strategy, Prentice Hall, Hemel Hempstead, United Kingdom.

19.Johnson, G., Scholes, K. and Whittington, R. (2008), Exploring corporate strategy, text cases, Pearson Education, Harlow, United Kingdom.

20.Kehoe, B. (2013), 'BYOD - proceed with caution,' *Hospitals and Health Networks*, 87(6), 17.

21.Markelj, B. and Bernik, I. (2012), 'Mobile devices and corporate data security,' *International Journal of Education and Information Technologies*, 6(1), 97–104.

22.Matrix42 (2015), 'Mobility survey,' *Matrix42*. [Online], [Retrieved November 3, 2015], https://www.matrix42.com/en/white-paper/mobility-survey-2015/

23.Miller, R.E. and Varga, J. (2011), 'Benefits of enabling personal handheld devices in the enterprise - Intel,' IT@Intel White Paper.

24.Montaña, J.C. (2005), 'Who owns business data on personally owned computers?,' *Information Management Journal*, 39(3), 36.

25.Mooney, J.L., Parham, A.G. and Cairney, T.D. (2014), 'Mobile risks demand C-suite action!,' *The Journal of Corporate Accounting & Finance*, 25, 13–24.

26.Morrow, B. (2012), 'BYOD security challenges: control and protect your most sensitive data,' *Network Security*, 2012(12), 5–8.

27.Mourmant, G., Niederman, F. and Kalika, M. (2013), 'Spaces of IT intrapreneurial freedom: a classic grounded theory,' Proceedings of the 2013 annual conference on computers and people research. 30 May - 1 June 2013, ISBN: 978-1-4503-1975-1, Cincinnati, OH, USA, 33–43.

28.György, A., Cleven, A., Uebernickel, F. and Brenner W. (2012), 'Exploring the shadows: IT governance approaches to user-driven innovation,' Proceedings of the 20th European Conference on Information Systems, ISBN: 978-84-88971-54-8, Barcelona, Spain, 1–12.

29.Oliver, R. (2012), 'Why the BYOD boom is changing how we think about business it,' *Engineering and technology*, 7(10), 28.

30.Pettey, C. and Van Der Meulen, R. (2012), 'Gartner identifies three security hurdles to overcome when shifting from enterprise-owned devices to BYOD,' *Gartner Inc.* [Online], [Retrieved July 20, 2013], http://www.gartner.com/newsroom/id/2263115.

31.Ring, T. (2013), 'IT's megatrends: the security impact,' *Network Security*, 2013(7), 5–8.

32.Salesforce (2014), '2014 mobile behavior report,' *Marketing cloud*, [Online], [Retrieved Febuary 25, 2014], https://www.marketingcloud.com/sites/exacttarget/files/deliverables/etmc-2014mobilebehaviorreport.pdf

33.Silic, M. and Back, A. (2013), 'Factors impacting information governance in the mobile device dual-use context,' *Records Management Journal*, 23(2), 73–89.

34.Silic, M. and Back, A. (2014), 'Shadow IT - A view from behind the curtain,' *Computers and Security*, 45, 274–283.

35.Simkin, S. (2013), 'Cisco security intelligence - annual security report & cisco connected world technology report,', 1-17.

36.Singh, M.N. (2012), 'B . Y . O . D . genie is out of the bottle – " devil or angel" ,' *Journal of Business Management & Social Sciences Research (JBM&SSR)*, 1(3), pp.1–12.

37.Skype, Norton and TomTom (2012), 'Survey finds nearly half of consumers fail to upgrade software regularly and one

quarter of consumers do not know why to update software,' [Online], [Retrieved October 19, 2015], http://about.skype.com/press/2012/07/survey_finds_nearly_half_fail_to_upgrade.html

38.Tokuyoshi, B. (2013), 'The security implications of BYOD,' *Network Security*, 2013(4), 12–13.

39.UNICEF (2014), 'Om föräldrars tillgänglighet i mobilen efter arbetstid,' [Online], [Retrieved May 1, 2014], http://blog.unicef.se/wp-content/uploads/2014/05/UNICEF_Faktablad_barnrättsprinciperna.pdf

40.Walters, R. (2013), 'Bringing IT out of the shadows,' *Network Security*, 2013(4), 5–11.

41.Wilson, J. (2012), 'Enterprises rate mobile device security vendors, reveal BYOD concernsle,' *Infonetics*. [Online], [Retrieved July 13, 2013], http://www.infonetics.com/pr/2012/Enterprise-Mobile-Security-Strategies-Survey-Highlights.asp.

42.Yang, T.A., Vlas, R., Yang, A. and Vlas, C. (2013), 'Risk management in the era of BYOD the quintet of technology adoption, controls, liabilities, user perception, and user behavior,' Proceedings of SocialCom/PASSAT/BigData/EconCom/BioMedCom 2013, ISBN: 978-0-7695-5137-1, 8-14 September, 2013, Washington D.C., USA, 411–416.

43.Zahadat, N., Blessner, P., Blackburn, T. and Olson B. (2015), 'BYOD security engineering: a framework & its analysis,' *Computers & Security*, 55(2015), 81–99.