MOBILE DEVICE STRATEGY
A management framework for securing company information

MARTIN BRODIN
Informatics
MOBILE DEVICE STRATEGY

A management framework for securing company information assets on mobile devices
LICENTIATE DISSERTATION

MOBILE DEVICE STRATEGY

A management framework for securing company information assets on mobile devices

MARTIN BRODIN
Informatics

UNIVERSITY OF SKÖVDE
Martin Brodin, 2016

Title: Mobile Device Strategy
A management framework for securing company information assets on mobile devices

University of Skövde 2016, Sweden
www.his.se

Printer: Runit AB, Skövde

Dissertation Series, No. 15 (2016)
ABSTRACT

The problem addressed by this research is a demand for increased flexibility in access to organisational information, driven by the increasing popularity of mobile devices. Employees increasingly bring private devices to work (Bring Your Own Device, BYOD) or use work devices for private purposes (Choose Your Own Device, CYOD). This puts managers in a difficult position, since they want the benefits of mobility, without exposing organisational data to further risk. The research focuses on management (particularly information security management) issues in the design and implementation of strategies for mobile devices. There are two objectives. The first is to identify existing information security management strategies for mobile and dual-use devices. The second is to develop a framework for analysing, evaluating and implementing a mobile device strategy.

The overall research strategy is inspired by Design Science; where the mission is to develop an artefact, in this case a framework, which will help to solve a practical problem. Methods include literature review, theoretical development, and the collection and analysis of qualitative data through interviews with executives. The main result of this work is the framework, which deals with the complete process, including analysis, design and implementation of a mobile device management strategy. It helps researchers to understand necessary steps in analysing phenomenon like BYOD and gives practitioners guidance in which analyses to conduct when working on strategies for mobile devices. The framework was developed primarily through theoretical work (with inspiration from the mobile security and strategic management literature, and the ISO/IEC 27000 standard), and evaluated and refined through the empirical studies. The results include twelve management issues, a research agenda, argumentation for CYOD and, guidance for researchers and practitioners.
SAMMANFATTNING

Under de senaste åren har fler och fler organisationer fått problem med att de tappar kontrollen över sin information på grund av förändrad användandet av mobila enheter. Organisationerna har helt enkelt inte hängt med i utvecklingen och kunnat möta upp de anställdas krav på ökad flexibilitet. Detta i kombination med bristande uppdatering av policies och implementering av ledningssystem gör att organisationen inte klarar av att möta de nya kraven, vilket innebär ökad behov av ett nytt angreppssätt för att återfå kontrollen över informationen. Inom aktuell forskning finns det brister i området och denna avhandling är ett bidrag till att öka kunskapen samt ge organisationer stöd i arbetet med mobila enheter.

ACKNOWLEDGEMENTS

First of all, I would like to express my gratitude towards my supervisors; Professor Anne Person, who started this journey and convinced me that this is what I shall do the coming years, Dr. Rose-Mharie Åhlfeldt, for discussions around security issues, orientation among all standards, and Professor Jeremy Rose for invaluable support in finding a way in the world of research and academic writing in English. In addition, a thank you to my mother, Barbro Brodin, for the introduction to strategic management.

Furthermore, I send a lot of thanks to past and present colleagues at Actea Consulting AB for support and good comments on my work. A special thanks to Lena Ask, Fredrik Rehnström, Fredrik Pettersson and Stefan Gerner who all in some point played the role as my company mentor and to Lars Andreasson for all help with finding respondents to my empirical study. I also would like to send a special thanks to Anders Larsson, who made this possible and also came up with the title to this thesis.

Without the financial support from Actea Consulting AB, KK-foundation and University of Skövde, this would not have been possible.

It can be boring to sit alone in an office and try to conduct some research, luckily I did not get my own office at the university. Thank you Kristens Guddfinsson and Hanife Rexhepi for this time, lets finish our PhD like we started!

I cannot describe in words how important my family has been in this process. Thank you Anna-Karin Brodin, for everything, and our children, Julia and Oscar, for (almost) always make me happy and proud!
PUBLICATIONS

PUBLICATIONS WITH HIGH RELEVANCE

PUBLICATIONS WITH LOWER RELEVANCE
# CONTENTS

1. INTRODUCTION .................................................................................................... 1
   1.1 Problem description ......................................................................................... 2
   1.2 Aims and objectives ......................................................................................... 2
   1.3 Research delimitations .................................................................................... 3
   1.4 Definitions ........................................................................................................ 3

2. THEORETICAL BACKGROUND ............................................................................ 5
   2.1 Strategic management..................................................................................... 5
   2.2 Information Security Management system ...................................................... 7
   2.3 Mobile devices in organisations ....................................................................... 8

3. RESEARCH METHOD ......................................................................................... 11
   3.1 Approaches to research ................................................................................. 11
   3.2 Research strategy .......................................................................................... 12
       3.2.1 Awareness of problem Step - Literature review .................................. 13
       3.2.2 Suggestion step .................................................................................. 14
       3.2.3 development and Evaluation steps - Data collection and analysis .... 14
       3.2.4 Communication step ........................................................................... 16
   3.3 The trustworthiness of the research .............................................................. 16
       3.3.1 Credibility ............................................................................................ 16
       3.3.2 Dependability ...................................................................................... 17
       3.3.3 Transferability ...................................................................................... 17
       3.3.4 Conformability ..................................................................................... 17

4. RESULTS ............................................................................................................. 19
   4.1 Management issues for Bring Your Own Device ........................................... 19
   4.2 Combining ISMS with strategic management: The case of BYOD .......... 20
   4.3 BYOD vs. CYOD – What is the difference? .................................................. 21
   4.4 Management of mobile devices – How to implement a new strategy ....... 22
   4.5 Synthesized results........................................................................................ 23
       4.5.1 The framework .................................................................................... 23

5. CONCLUDING REMARKS AND FUTURE WORK .............................................. 25
   5.1 Method ........................................................................................................... 25
   5.2 From aim to result ........................................................................................ 26
       5.2.1 Objective 1 - Identify existing information security management strategies for mobile and dual-use devices................................. 26
5.2.2 Objective 2 - Develop a framework (artefact) for analysing, evaluating and implementing a mobile device strategy ........................................ 26
5.3 Contributions.................................................................................................. 26
5.4 Future work.................................................................................................... 27

6. REFERENCES ..................................................................................................... 31

7. THE PAPERS........................................................................................................... 37
CHAPTER 1
INTRODUCTION

In society today the boundaries between information categories overlap since the same media and equipment (e.g. smartphones, social media and cloud services) are increasingly used for both private and business purposes. Many organisations allow their employees to use the same devices for both private and work purposes. One reason for this is the promise of increased personal productivity, which is reported to save $300 to $1300 per employee each year for the organisation (Barbier, Bradley, Macaulay, Medcalf, & Reberger, 2012).

A popular version of this phenomenon is Bring Your Own Device (BYOD), where employees use their private devices for work tasks. Independent surveys show that more organisations are changing their device strategies towards a more open device environment (Barbier et al., 2012; Camp, 2012). In 2013 Gartner predicted that BYOD would be mandatory in four years (Van Der Meulen & Rivera, 2013). At that point it looked like almost all organisations would have introduced BYOD by 2017, but today we know that is not the case. The trend has turned and the popularity of BYOD is decreasing (Kane, Koetzle, Voce, & Caputo, 2014). Even though BYOD is losing ground, the question of how mobile devices should be handled, regardless of owner, is still relevant. Even if the mobile device is owned by the company, it can be assumed that the user may choose to use it for private purposes also, so it becomes a dual-use device. A trend that is gaining a lot of popularity is Choose Your Own Device (CYOD), where the employer pays for the device and is the formal owner, but the user is also allowed to use it as a private device (Kane et al., 2014).

These new and complex technical and organisational environments require higher awareness from both employees and the organisation about information security implications. They also set higher demands for the organisation’s information security functions and information architecture. When information gets easier to access for the rightful owner, it also increases the risk that it may fall into the wrong hands. Users want the freedom to work anywhere, anyhow, and anytime they want, and if the business does not meet this demand some users will ignore policies for their own convenience (Harris, Ives, & Junglas, 2012; Simkin, 2013). That is why organisations need to understand the benefits and risks of mobile devices and devise a strategy to meet these demands.

Popular information management approaches strive for standardization, consolidation and reduction of complexity, which in many aspects contradict the idea of mobile devices (Disterer & Kleiner, 2013). One survey reveals that 86% of the costs are non-hardware, which leads the authors to the conclusion that it is very important to choose the right model for governance and support (Barbier et al., 2012). As a result, adoption of mobile devices requires new strategic decisions.
1.1 PROBLEM DESCRIPTION

The problem addressed by this research is a demand for increased flexibility when it comes to access to organisational information, driven by increasing popularity of mobile devices. This puts managers in a difficult position, since they want the benefits of mobility and to satisfy employees, without exposing organisational data to further risk.

With dual-use devices, which are used for both private and professional purposes, there is a risk that organisational data gets mixed with the user’s personal data. Even if a device is owned by the organisation, users will eventually see it as their own. This may lead to uncertainty about how the organisation’s rules should be applied and what impact they will have on the user’s privacy. Managers must also be aware that information on private devices easily falls outside the organisation’s control. Currently there is no standard or known method that properly addresses this problem (Brodin, 2016b; Disterer & Kleiner, 2013).

The problem has two dimensions, one technical and one managerial (Åhlfeldt, Spagnoletti, & Sindre, 2007). The main scope of this research falls under the managerial part - particularly information security management, and how to design and implement a strategy for mobile devices. The research is technology independent.

1.2 AIMS AND OBJECTIVES

The aim of this research is to develop an artefact that can support managerial strategy development for the introduction of mobile devices based on an information security perspective. In order to address this aim, a set of objectives has been specified. The first objective is to identify existing strategies to find gaps in knowledge and improve understanding of the target area. The second is the design of an artefact to support managerial strategy development.

O1. Identify existing information security management strategies for mobile devices.

O2. Develop a framework for analysing, evaluating and implementing a mobile device strategy.

Figure 1.1: Papers related to objectives.
1.3 RESEARCH DELIMITATIONS

When looking at information security there are mainly two approaches regarding the information security area; technical security and administrative security (Åhlfeldt et al., 2007). This work has chosen the administrative approach and does not examine technical solutions since support managerial strategy development is on the administrative part. The focus is on people, policies and strategies, and how to help managers responsible for organisational information. Since the focus is on supporting managers, interviews were conducted with executives to develop a picture of their reality, and to help develop a framework that can support them in their work. When the framework is developed and evaluated, it may be interesting to interview employees to get input from them to further expand the framework. An approach with more empirical material from employees might have moved the study’s focus towards aspects such as privacy and working hours.

Even though the literature base is international, all the empirical material is from a Swedish context and qualitative in nature.

1.4 DEFINITIONS

There are expressions and definitions in this thesis that not everyone may be familiar with and that may have different meaning to different people. This section gives a short description of some key concepts used in this thesis.

**Framework** is a system of rules, ideas, or beliefs that is used to plan or decide something (Cambridge University Press, 2016).

**Information management** is the process of collecting, organising, storing, and providing information within a company or organisation (Cambridge University Press, 2016).

**Information security management** is processes and procedures for putting information security into practice.

**Information security management system (ISMS)** is a systematic approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an organization’s information security to achieve business objectives (ISO/IEC 27000, 2016, s. 14).

**Mobile device** is a device that can be carried around, while being used to access organisational data.

**Bring Your Own Device (BYOD)** refers to a device that is used and owned by the employee.

**Choose Your Own Device (CYOD)** refers to a device which is chosen and used by the employee, both private and professional, and is owned by the employer.

**Use What You are Told (UWYT)** is the traditional way to manage mobile devices, the employer choose and own the device that is used by the employee.

**Strategic management** is the way that a company’s executives decide what they want to achieve and plan actions and use of resources over time in order to do this (Cambridge University Press, 2016).
CHAPTER 2
THEORETICAL BACKGROUND

The central theme of this thesis is how to manage mobile devices on a strategic level in an organisation where the employees challenge existing policies and environments. In this chapter some of the main concepts and theories will be explained.

2.1 STRATEGIC MANAGEMENT

Strategy is about what direction an organisation should take in the long run (Johnson, Scholes, & Whittington, 2012) and strategic management is about developing and implementing strategy. Since this research concerns a framework for mobile device strategies, it is important to understand the basics of strategic management for the framework development process. It is a large area and to give a brief introduction this section will present a short overview by summarizing the best available literature review of the field: Mintzberg et al (1998). Furthermore, this research adapts a framework for strategic management that is also explained in this section. The search process to find a suitable framework was to consider well-known candidates and stop when one appears that fits for purpose. In this case it is an explorative strategy framework (Johnson, Whittington, Scholes, Angwin, & Regnér, 2015).

According to Mintzberg et al (1998) the field of strategic management can be summarised in ten schools of thoughts. The first three schools are concerned with how strategies should be formulated rather than how they are formed in practice; the next six schools focus on specific aspects of strategy formation and how they are made. The last school synthesizes the previous nine.

1. The Design School – The internal situation is used to match the external environment. Clear and unique strategies are formulated.
2. The Planning School – A rigorous set of steps are taken, from analysis to implementation.
3. The Positioning School – Focus on how the organisation can improve its strategic position within their industry sector.
4. The Entrepreneurial School – The founder or leader makes visionary strategies relying on their intuition and experience.
5. The Cognitive School – The strategic development process takes place in human brains and is about how management process information and make choices based on different options.
6. The Learning School – Strategies develops from “lessons learned” as the management pays close attention to what works and learn from experiences.
7. The Power School – Strategies are built after negotiation between strong forces within the organisation or between the organisation and external stakeholders.

8. The Cultural School – Strategies are formed collectively involving several departments and reflect the organisation’s culture.

9. The Environmental School – Strategy is a response to challenges from the external environment.

10. The Configuration School – The process of forming a strategy comes from a change from one decision-making structure to another.

Strategies can be developed in two ways; rational-analytic (through a rational and analytical process), or emergent (strategies emerge in the organisation over time from the bottom-up (Johnson et al., 2015). The phenomenon of employees bringing their private devices to work (or using their work devices in ways that violate current policies) is a good example of emergent strategy.

Johnson et al. (2015) created an explorative strategy framework that summarises strategic management in three main steps; strategic position, strategic choices and strategy in action with sub-tasks and focus areas.

![Figure 2.1. The Exploring Strategy Framework, adapted from Johnson et al. (2015)](image)

Strategic Position is concerned with the impact on external environment, the organisation’s purpose, organisational culture and capability when it comes to resources and competences. Strategic Choices involve options for strategy in terms of directions and methods. Strategy in Action is the final part and were the strategy is implemented.

The Exploring Strategy Framework (Johnson et al., 2015) has many connections with Mintzberg et al (1998) and is sometimes used as an example of the cultural school (White, 2004). Besides culture, the schools of positioning, entrepreneurship and environment are also represented in the first part of Johnson and Scholes framework. When it comes to strategic choices, we find the schools of design and cognition incorporated. Finally, the planning school pervades the entire framework.

How The Exploring Strategy Framework is used in this research is presented in paper 2.
2.2 INFORMATION SECURITY MANAGEMENT SYSTEM

To fully understand information security management system (ISMS), it is important to get the picture of how it relates to information management (IM) and information security management (ISM). Information management is the process of collecting, organising, storing, and providing information within a company or organisation (Cambridge University Press, 2016). Information security management concerns managing the security of information in a proactive way, to ensure that it is not compromised (Kritzinger & Smith, 2008). An information security management system (ISMS) is a systematic way to work with IM, ISM and governance.

The most commonly used and known ISMS is the ISO/IEC 27000-family, which consists of several standards. The established standards in the 27000-family that are of interest when working with a strategy for mobile devices are shown in table 2.1. ISO/IEC 27000 defines information security management system:

> An Information Security Management System (ISMS) consists of the policies, procedures, guidelines, and associated resources and activities, collectively managed by an organisation, in the pursuit of protecting its information assets. An ISMS is a systematic approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an organization’s information security to achieve business objectives. (ISO/IEC 27000, 2016, s. 14)

<table>
<thead>
<tr>
<th>Standard</th>
<th>About</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO/IEC 27000</td>
<td>Information security management systems -- Overview and vocabulary</td>
</tr>
<tr>
<td>ISO/IEC 27001</td>
<td>Information security management systems -- Requirements</td>
</tr>
<tr>
<td>ISO/IEC 27002</td>
<td>Code of practice for information security controls</td>
</tr>
<tr>
<td>ISO/IEC 27003</td>
<td>Information security management system implementation guidance</td>
</tr>
<tr>
<td>ISO/IEC 27005</td>
<td>Information security risk management</td>
</tr>
</tbody>
</table>

Table 2.1: ISO/IEC standards of primary interest when adopting to dual-use devices.

ISO/IEC 27000 defines terms that are used in the series and provides an overview of information security management systems. ISO/IEC 27001 specifies requirements for the establishment, implementation, maintenance and continuous improvement of an information security management system. ISO/IEC 27001 also includes requirements for the assessment and processing of information security risks. ISO/IEC 27002 provides best practice recommendations for information security controls, ISO/IEC 27003 give some guidance for an ISMS implementation and ISO/IEC 27005 is about risk management.

The ISO/IEC 27000-family focus on what to do when it comes to ISM. The step from knowing what to do to understanding how to do it has proved to be overly complex and costly for many organisations (Gillies, 2011). The ISO/IEC 27000-family is intended to assist organizations of all types and sizes with implementation and operation. Through the use of the standards, organizations can develop and implement a framework for managing the security of their information assets, and it can also be used to prepare for an independent assessment (ISO/IEC, 2016).
2.3 MOBILE DEVICES IN ORGANISATIONS

In this thesis, a mobile device is a device that can be carried around, while being used to access organisational data. In recent years, the evolution of mobile devices has been rapid, and they more and more resemble general purpose computers. Organisations are having a hard time keeping up with this pace; at the same time the demand from users for the newest devices to make their jobs easier, is increasing. When organisations fail to adopt the latest technology, more users start to bring their personal devices and use them in the work. This trend is in many ways the opposite of popular information management approaches, which strive for standardization, consolidation and reduction of complexity (Disterer & Kleiner, 2013). At the same time, it is important to find the right model for governance since 86% of the costs connected with Bring Your Own Device (BYOD) adoption are non-hardware (Barbier et al., 2012). This is not an information security specialist’s nor a technician’s decision, it is something that has to be decided by senior management (Borrett, 2013; Mooney, Parham, & D, 2014; Ring, 2013).

Five years ago, it was commonly understood that Bring Your Own Device (BYOD), where employees bring their private devices to work instead of receiving devices from their employer, would conquer the world and be more or less mandatory by 2017 (Van Der Meulen & Rivera, 2013). Lately its popularity in the USA is decreasing and in Europe, it has never really taken hold (Kane et al., 2014). An alternative that has become popular in Europe and gaining in popularity on the US is Choose Your Own Device (CYOD) (Kane et al., 2014), where the employee may choose a device, use it both for private and work purposes, but the organisation owns and controls the device. It may be seen as a hybrid of BYOD and the traditional way to deal with devices where they are strictly for business use and the organisation owns and control everything. The traditional way is sometimes referred as Use What You are Told (UWYT) (Brodin, 2016a). What differs most between these ways to manage mobile devices are the amount of control from the organisation, freedom of choice and ownership. Figure 2.1 shows some examples of strategies for handling devices.

A popular way to solve the issues with mobile devices in literature is to create a policy that states what users are allowed to do (Gatewood, 2012; Harris et al., 2012; Montaña, 2005; Oliver, 2012; Simkin, 2013; Yang, Vlas, Yang, & Vlas, 2013). A policy is an organisation’s
overall intention and direction, as formally expressed by management (Isaca, 2013; ISO/IEC, 2016). An organisation normally has many policies and guidelines. A mobile device policy is the one that deals with directions for mobile devices and is a good start, but creating a policy does not solve the whole problem; since policies are seldom followed by all, and the understanding of them is poor - if the user is aware of them at all (Oliver, 2012; Simkin, 2013).
CHAPTER 3
RESEARCH METHOD

“Research is a systematic investigation to find answers to a problem” (Burns, 1990, p. 1). This chapter presents the methodological approach used for the research presented in this thesis.

3.1 APPROACHES TO RESEARCH

Research can be classified in different ways, for instance basic or applied, inductive or deductive, or qualitative or quantitative. A research approach may therefore be applied, inductive and qualitative.

Basic research is theoretical, strives to deliver new knowledge and does not necessarily address a practical problem. This kind of research tends to focus on theory building and testing of hypotheses. Applied research on the other hand is concerned with solving a real life problem (Williamson et al., 2002).

Inductive research begins with investigations of a specific phenomenon or instance and ends with a general theory; deductive research is the other way around, it starts with a general theory and tests specific instances of it (Robson, 2011; Williamson et al., 2002).

When data are collected, they must be analysed - data analysis can either be qualitative or quantitative. Qualitative analysis is used when data is non-numerical, usually words, and is not for statistical presentation. A focus is on meaning and context is important, in order to understand a phenomenon in its natural environment or setting. When a research process is based on qualitative research, the approach is commonly inductive and design is flexible and may be changed throughout the process (Robson, 2011). When dealing with numbers, quantitative analysis is the natural choice and some kind of statistical result is expected. A quantitative research approach is planned in detail from the beginning, so it will be easy to repeat, the logic is usually deductive (Robson, 2011).


- **Survey** – Focus is to get data from a large group of people, then look for patterns and make generalizations to a larger group.
- **Design and creation** – Focus is on developing an artefact, for instance a new construction, framework or method to solve a business problem.
• **Experiment** – Focuses on investigating cause and effect of relationships, testing hypotheses and trying to prove or disprove links between factors and observed outcomes.

• **Case study** – Focuses on one part of the problem that will be investigated and aims to obtain rich and detailed insight into that part.

• **Action research** – Focuses on getting something done in real life. Researchers plan, do and reflect on the result.

• **Ethnography** – Focuses on understanding the culture of a particular group of people.

This research involves designing a framework to help managers with a strategy for mobile devices. Survey and experiment by itself would not result in a framework, although surveys could be used to gain information about existing strategies and thoughts about the area. Case studies are not appropriate because they are for finding out about particular problems in organisations, not solving them by constructing artefacts. Action research is not appropriate because it focuses on improvement in a particular organisation setting, whereas this work is focused on developing an artefact. Ethnography would not help either since it is about understanding culture in a specific group over time. The most appropriate strategy of the six above is therefore design and creation, also known as design science, since it is about designing something that addresses a business problem. It also gives the opportunities to collect and test data from, and in different organisations.

### 3.2 RESEARCH STRATEGY

This is applied research inspired by Design Science, where the mission is to develop an artefact, in this case a framework, which is relevant to an unsolved business problem. There are several approaches to Design Science in the field of Information Systems (IS). Most of them starts with some kind of problem identification (A. Hevner & Chatterjee, 2010; Nunamaker, Chen, & Purdin, 1991; Peffers, Tuunanen, Rothenberger, & Chatterjee, 2007; Rossi & Sein, 2003; Vaishnavi & Kuechler, 2007; Walls, Widmeyer, & El Sawy, 1992).

Before designing the solution some argue that a proposal or objective for the solution should be presented (Gregor & Jones, 2007; A. Hevner & Chatterjee, 2010; Peffers et al., 2007; Vaishnavi & Kuechler, 2007; Walls et al., 1992). As the name design science implies, design is the central part of the research process, this is where development of the artefact take place (Gregor & Jones, 2007; A. Hevner & Chatterjee, 2010; Nunamaker et al., 1991; Peffers et al., 2007; Rossi & Sein, 2003; Vaishnavi & Kuechler, 2007; Walls et al., 1992). Hevner et al. (2010) point out that development is an iterative search process.

When the artefact is designed it must be evaluated (A. Hevner & Chatterjee, 2010; Nunamaker et al., 1991; Peffers et al., 2007; Rossi & Sein, 2003; Vaishnavi & Kuechler, 2007; Walls et al., 1992) and communicated (A. Hevner & Chatterjee, 2010; Peffers et al., 2007). Some design science approaches argue for demonstration or making some proof-of-concept of the solution (Nunamaker et al., 1991; Peffers et al., 2007).

This work combines common aspects from these different approaches in a process (figure 3.1) with the stages: awareness of problem, suggestion, development, evaluation and communication. The work is evaluated during and after development as an iterative process and the result is communicated in several scientific and public fora.
3.2.1 AWARENESS OF PROBLEM STEP – LITERATURE REVIEW

Previous studies are a good way to start any academic work, to find gaps in existing knowledge and improve understanding of the problem. Since the initial problem of this research is identified in industry by practitioners, it is natural to start with a literature review to find out how the problem is addressed by researchers. Webster and Watson (2002) make this clear: “A review of prior, relevant literature is an essential feature of any academic project. An effective review creates a firm foundation for advancing knowledge. It facilitates theory development, closes areas where a plethora of research exists, and uncovers areas where research is needed.” The search for relevant literature in this research is derived from Webster and Watson’s structured approach, with the principal steps:

1. An extensive literature search.
3. Backward chaining by reviewing the citations in the articles identified as relevant in step 2.

The search was considered complete when the complementary searches revealed few new articles of relevance. Webster and Watson (2002) also require a literature review to be concept-centric, where the concepts determine the ‘organizing framework’ of the review. Concepts may derive from the analysis, but a common practice is to adopt a suitable conceptual framework from the literature, which is the case here.

The search for interesting papers started with pre-defined keywords in major databases. When interesting articles were found, relevant keywords were included in further searches. The articles were screened first by reading the abstracts to remove irrelevant papers; after the first screening the remaining articles were downloaded and read in full text and screened again. Then the reference list of all relevant articles was inspected to find new articles. Finally, a new search round was conducted in new databases and search engines.

The literature review started broad in the area of information management, to be later narrowed down to mobile devices and BYOD. For more details about the literature review and keywords, see paper 1.
3.2.2 SUGGESTION STEP
With support from strategic management literature, ISO/IEC 27000 series and the literature review, a suggestion for a framework was developed. The first version of the framework is presented in paper 2.

3.2.3 DEVELOPMENT AND EVALUATION STEPS - DATA COLLECTION AND ANALYSIS
The suggested framework from the literature review were evaluated together with experience executives and further developed with empirical studies. 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). This is achieved by semi-structured interviews with a standard list of questions which allows the interviewer to follow up leads and add follow-up questions (Williamson et al., 2002). An alternative to interviews are questionnaires, which take less time to administrate. However interviews have the following advantages (Williamson et al., 2002):

- Complex and complete responses due to the opportunity for probing, explanation and clarification during interview.
- Possibility of discussion before and after interview to get extra input to respondents’ opinions.
- Face-to-face help to motivate respondent to answer all questions.
- Interviewer can control the context and make sure that respondent concentrates on right issues.
- Gives much richer data.

Thirteen semi-structured interviews were conducted for paper 4 and twelve for paper 3 in twelve organisations (food industry, manufacturing industry, defence industry, health care, municipality and consulting firms from various sectors (information security, IT, management and logistics)). The organisations vary in size from 50 to 15 000 employees. All respondents are executives in the role of CIO, CSO, CFO, CSIO or head of IT. The respondents were selected from a wide range of areas and sizes, and from both private and public sectors. This was to find out if there are differences of approach in different organisation types. Interviews lasted approximately 45 minutes and were recorded and transcribed. In one organisation two interviews were conducted; first with a branch CSIO and then a complementary interview with the global CSIO. The goals of the empirical study were to find existing strategies and to get input to development of the framework. The information provided by participants is kept strictly confidential; names of individuals or organisations are not revealed.

Qualitative data analysis is a way of making sense of the data collected, so that a result can be communicated (Williamson et al., 2002). There are many approaches to qualitative analysis - some of the better known (Robson, 2011) are:

- Quasi-statistical approach – Uses word or phrase frequencies to determine importance of terms and concepts.
- Thematic coding approach – Identifying patterned meaning across a dataset.
- Grounded theory approach – A version of thematic coding where codes are based on the researcher’s interpretation of the meanings or patterns in the text.

In this work data analysis was conducted using a thematic analysis six-phase process as shown in table 3.3.
**Phase** (Braun & Clarke, 2006) | **Action**
--- | ---
Familiarisation with the data | Transcribing data and reading it through to get initial ideas.
Coding | Coding the data with codes from a well-known framework and previous literature study. This was done in a spreadsheet.
Searching for themes | Collating codes into potential themes.
Reviewing themes | Checking whether the themes tell a convincing story of the data that answers the research question. Adding new codes to make a better story.
Defining and naming themes | Detailed analysis of each theme and giving informative names in a qualitative data analysis software.
Producing the report | Writing articles and this thesis.

Table 3.3: Thematic analysis six-phase process in this work.

Thematic analysis may be approached in the following ways (Braun & Clarke, 2006):

- Inductive – codes and themes are developed from the content of the data.
- Deductive – codes and themes are developed from existing concepts or ideas.
- Semantic – codes and themes reflect the explicit content of the data.
- Latent – codes and themes report concepts and assumptions underpinning the data.
- Realist or essentialist – focuses on reporting an assumed reality evident in the data.
- Constructionist – focuses on looking at how a certain reality is created by the data.

This research used a combination of deductive and inductive analysis strategies. The analysis started deductively, using codes from an existing theoretical framework. After the first analysis round, it turned out that the theoretical framework did not match reality perfectly, at least according to the interviews. New codes were developed inductively from the data and a new analysis conducted.

Each version of the framework was evaluated for its relevance to practice by interviews with executives, first round the thirteen in paper 4 and the updated framework was evaluated with five new interviews from other organisations.
3.2.4 COMMUNICATION STEP
To be able to communicate a result in research there must be some kind of contribution to research community and industry. A way to visualise different types of contribution in design science is the DSR Knowledge Contribution Framework (Gregor & Hevner, 2013).

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>Routine design: Apply known solutions to known problems. No major knowledge contribution</td>
<td>Exaptation: Extend known solutions to new problems (e.g., Adopt solutions from other fields) Research opportunity and Knowledge contribution</td>
</tr>
<tr>
<td>Low</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Application Domain Maturity

Figure 3.2: DSR Knowledge Contribution Framework, adopted from Gregor & Hevner (2013).

In this case the solution maturity is low, because there is no existing well documented solution. The application domain maturity is high, since the problem is known in practice and discussed in existing research. This gives us the contribution Improvement - a new solution for a known problem, described in chapter 1.1.

Clarifying the type of contribution (see chapter 6.2 for contributions in this work) makes it easier to communicate to the right audience. Contributions to research were communicated through articles in conferences (see list at the beginning of this thesis) presentations in various meetings, for instance SWITS, COINS and at University of Skövde. The results are communicated to industry through actea.se, LinkedIn, twitter and meetings with invited organisations.

3.3 THE TRUSTWORTHINESS OF THE RESEARCH
The conventional positivist research paradigm often uses validity, reliability, and objectivity as criteria for evaluating the quality of research. Qualitative analysis differs from the positivist tradition in its fundamental assumptions, research purposes, and inference processes, thus making the conventional criteria unsuitable for judging its research results (Bradley, 1993). Instead of using those three criteria to evaluate the quality of this work we use Lincoln and Guba’s (1985) four criteria for evaluating interpretive research work: credibility, transferability, dependability, and confirmability.

3.3.1 CREDIBILITY
Credibility is about whether the result is credible or believable. In this work the credibility is iteratively improved through complementary theoretical and empirical investigations, which gives input to the final result. The result has also been evaluated both in practice, (though interviews), and academia (through peer-review and during presentations), where experts have given input and confirmed the relevance of the framework.
3.3.2 DEPENDABILITY
Dependability is equivalent to reliability in quantitative research, indicating the stability of the result over time (Lincoln & Guba, 1985). To improve dependability and to make sure that the analysis was made on original data all interviews were recorded and then transcribed in the original language. Another way to work with dependability is by an inquiry auditor, where an expert examines the work. In this case this has been done in two ways, both the result and the process. All articles have been submitted to blind peer-reviewed conferences where experts have looked at the results. The whole research process has been monitored by both industry experts and academia; with meetings between university and industry to ensure that the project lives up to established standards, and in order to assure the quality of the work.

3.3.3 TRANSFERABILITY
Transferability is about how well the results can be applied in another context. It is not up to the researcher to judge, but the researcher has to deliver good descriptions so that other researchers may assess whether it is transferable to their context. In this work the method is clearly specified, and the interviewed executives saw several practical ways to use this research. There is also a solid transferability from research to practice.

3.3.4 CONFORMABILITY
Two of the best ways to ensure conformability are recordings and field notes (Lincoln & Guba, 1985). Both of these strategies are used in this work, which makes it possible for anyone to check the empirical base for the conclusions.
CHAPTER 4
RESULTS

This chapter presents a brief summary of the papers included in this thesis, the development of the framework, and ends with synthesized results.

4.1 MANAGEMENT ISSUES FOR BRING YOUR OWN DEVICE

Paper 1 explores management issues for Bring Your Own Device (BYOD) through an extensive literature review. It shows that there are many information security related problems concerning the use of BYOD, and it should therefore be considered an issue of strategic importance for senior managers. The analysis reveals early work in the analysis and design aspects of BYOD strategies, but a lack of research in operationalizing (planning, implementation and evaluating) strategy – the action phase. The resulting research agenda identifies twelve management issues for further research and four overall research directions that may stimulate future research as shown below in table 4.1.

<table>
<thead>
<tr>
<th>Framework category</th>
<th>BYOD management issues</th>
<th>BYOD research agenda</th>
</tr>
</thead>
</table>
| Analysis expectations | 1. increased personal productivity  
2. time/space flexibility  
3. increased user satisfaction | benefits and costs should be established empirically by independent researchers using methodologically sound techniques. |
| environment | 4. information control  
5. device protection | cataloguing of known mobile information security threats and responses for BYOD area, and identification of new threats and responses; protection of employee privacy. |
| resources and capability | 6. awareness  
7. support | investigation of distributed and user-led information security awareness and support; information classification. |
This article identified twelve BYOD core management issues addressed by the literature and provided a focused research agenda for each of these existing issues. We also analysed prominent gaps in the literature and identified four overall research directions that can help address those gaps. The twelve management issues, together with these four overall research directions provide a basis for a stimulating and useful programme of research. Other researchers have already used these findings.

This article also directly contributed to the progress of this work by giving twelve management issues when dealing with this problem. It gives a better awareness of the problem and the fact that the action part is under researched, gives an indication of where to focus on in the development of a framework when it comes to collecting empirical data.

### 4.2 COMBINING ISMS WITH STRATEGIC MANAGEMENT: THE CASE OF BYOD

Paper 2 presents a framework for managing mobile devices by combining a well-known strategic management framework, the exploring strategy (Johnson & Scholes, 1997; Johnson et al., 2012), with ISO/IEC 27000-series and input from paper 1. The framework consists three main parts with three subcategories each.

![Figure 4.1: The proposed framework for BYOD adoption.](attachment:image.png)
CHAPTER 4 RESULTS

Connected to each category are some actions to take, see table 4.2. The actions are derived from the ISO/IEC 27000 series (ISO/IEC, 2013a, 2013b, 2016) or from strategic management (Johnson & Scholes, 1997; Johnson et al., 2012).

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Source</th>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Analysis</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Environmental analysis</td>
<td>J&amp;S</td>
<td>Environment</td>
</tr>
<tr>
<td>Risk assessment</td>
<td>ISO</td>
<td>Environment</td>
</tr>
<tr>
<td>Business ethics</td>
<td>J&amp;S</td>
<td>Expectations</td>
</tr>
<tr>
<td>Stakeholder analysis</td>
<td>ISO and J&amp;S</td>
<td>Expectations</td>
</tr>
<tr>
<td>Cultural context analysis</td>
<td>J&amp;S</td>
<td>Expectations</td>
</tr>
<tr>
<td>Information classification</td>
<td>ISO</td>
<td>Resources &amp; Capability</td>
</tr>
<tr>
<td>Resource audit</td>
<td>J&amp;S</td>
<td>Resources &amp; Capability</td>
</tr>
<tr>
<td>Value chain analysis</td>
<td>J&amp;S</td>
<td>Resources &amp; Capability</td>
</tr>
<tr>
<td>GAP analysis</td>
<td>ISO and J&amp;S</td>
<td>Resources &amp; Capability</td>
</tr>
<tr>
<td><strong>Design</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cost/benefit analysis</td>
<td>J&amp;S</td>
<td>Option</td>
</tr>
<tr>
<td>Shareholder value analysis</td>
<td>J&amp;S</td>
<td>Option</td>
</tr>
<tr>
<td>Risk elimination</td>
<td>ISO</td>
<td>Development</td>
</tr>
<tr>
<td>Development of the strategy</td>
<td>J&amp;S</td>
<td>Development</td>
</tr>
<tr>
<td>Selection</td>
<td>J&amp;S</td>
<td>Selection</td>
</tr>
<tr>
<td><strong>Action</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Planning &amp; allocating resources</td>
<td>ISO and J&amp;S</td>
<td>Planning</td>
</tr>
<tr>
<td>Risk assessment for implementation</td>
<td>ISO</td>
<td>Planning</td>
</tr>
<tr>
<td>Managing change</td>
<td>J&amp;S</td>
<td>Implementation</td>
</tr>
<tr>
<td>Evaluation</td>
<td>ISO and J&amp;S</td>
<td>Evaluation</td>
</tr>
</tbody>
</table>

Table 4.2: Tasks in the proposed framework, italic text show main contributions from each source.

The result in this article helps researchers to understand the steps to deal with when analysing phenomenon like BYOD. It also gives practitioners guidance in which analysis to conduct when working on strategies for mobile devices.

In the design science research process, this provides a suggestion for a framework, the artefact, which is the foundation that is later developed by analysis of empirical data.

4.3 BYOD VS. CYOD – WHAT IS THE DIFFERENCE?

Paper 3 examines the two most popular strategies for mobile devices, Bring Your Own Device (BYOD) and Choose Your Own Device (CYOD), in organisations and looks for strengths and weaknesses in those. This is done through a systematic literature review and semi-structured interviews with executives, for instance CIO’s. The main findings are as shown in table 4.3.
CHAPTER 4 RESULTS

<table>
<thead>
<tr>
<th>Management issues</th>
<th>BYOD</th>
<th>CYOD</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. personal productivity</td>
<td>Increase since the employees can work from any place at any time and go a device that they are familiar with.</td>
<td>Increase since the employees can work from any place at any time and go a device that they are familiar with.</td>
</tr>
<tr>
<td>2. time/space flexibility</td>
<td>Very high</td>
<td>Very high</td>
</tr>
<tr>
<td>3. user satisfaction</td>
<td>High, since they use a device they know and like. Although lower if they used to CYOD.</td>
<td>High, since they choose device by them self and do not have to pay for it.</td>
</tr>
<tr>
<td>4. information control</td>
<td>Unsure, organisational data may remain on private devices.</td>
<td>Information may be stored outside the organisation.</td>
</tr>
<tr>
<td>5. device protection</td>
<td>Up to the user.</td>
<td>Organisation controls the device.</td>
</tr>
<tr>
<td>6. awareness</td>
<td>More important since private, uncontrolled devices are used.</td>
<td>Important</td>
</tr>
<tr>
<td>7. support</td>
<td>Problem mainly for the network. Complex with a lot of different devices with no control software.</td>
<td>Organisation configures and controls the device. Same pressure on service desk as before mobile devices.</td>
</tr>
</tbody>
</table>

Table 4.3: Comparison of management issues for BYOD and CYOD.

The article concludes that BYOD and CYOD come with similar strengths, but CYOD brings somewhat fewer information security risks.

In the last six years BYOD has dominated the literature for both researchers and practitioners, primarily as a contrast to traditional strict mobile use policy. This article combines findings from the literature with empirical data to reveal a credible alternative to BYOD. This helps both researchers and practitioners to develop insight into CYOD and to compare it with BYOD.

The contribution to this research is to connect issues found in the literature review on BYOD with the most common strategy in Sweden today - CYOD. This helps to link empirical and theoretical findings.

4.4 MANAGEMENT OF MOBILE DEVICES – HOW TO IMPLEMENT A NEW STRATEGY

Paper 4 is based on a pre-structured qualitative investigation, and extends the framework from paper 2 with a more substantial action phase, which (according to the literature review presented in paper 1) is the part that is under researched. The most important steps to take when implementing a mobile device strategy are communication and training. Managers need to communicate their strategy to all employees and to make sure that they understand it. However, people understand in different ways and at different speeds and tend to forget. That is why communication needs to be supported with training, and why training is not just a one-time event. Minor changes in the environment (for example a new information security threat) require small adjustments. Less frequently there are major changes in the environment, not accounted for in the strategy (for instance the emergence of smartphones in common use), which demand a bigger change in the current strategy. In those cases, adjustment is not sufficient; rather a complete remake of the strategy is required. That is why the updated version of the framework has a dashed line back to the analysis. The improved framework is shown in figure 4.2.
This updated framework may help researchers and practitioners to understand the important steps to take when implementing a new strategy for mobile devices. This is also the final version of the framework in this thesis.

4.5 SYNTHESIZED RESULTS

At the beginning of this project, BYOD was a hot topic in the practice world that created problems in many organisations, and also an emerging research area. Nevertheless, BYOD is not the primary focus of the eventual framework; more how phenomenon that emerge bottom-up and which do not fit into an existing ISMS should be handled. Initially, this was exemplified with the help of BYOD.

4.5.1 THE FRAMEWORK

The framework has its foundation in strategic management and ISO/IEC 27000-family and has been further developed with help from a literature review and interviews with executives, seventeen different respondents in total. It derived business ethics and analysis of environment, cultural context, stakeholders/shareholder, value chain and cost/benefit from strategic management theory. Though these sound like many separate analyses to make, they serve as a broad analysis to give support to the cost/benefit analysis, which is important for gaining support from top management. The ISO/IEC 27000 family, on the other hand, contribute with the information security aspects and above all risk assessment and information classification. The interviews supported the need for the analyses mentioned above, and highlighted the importance of communication and education after a new strategy is implemented. The literature review also contributed to the framework by revealing the need for it, and the lack of research into mobile device strategies.

The framework itself contains of three phases; analysis, design and action. The first has a focus on analysis necessary to facilitate the others. Most of this analysis serves to form a picture of the stakeholders and to get input to a cost-benefit analysis - essential for getting support from top management. It is easy to understand the importance of cost-benefit, but what is equally important, and often overlooked, is risk assessment. If risk assessment is properly undertaken it is easier to accommodate all risks during design, and easier to go-
ern and to manage in operation. All information needs to be classified before the risk assessment, in order to understand the value of the information for the organisation. Without information classification it is hard to retain control over information in a mobile world. The analysis phase consists of three parts; expectations, environment and, resources & capability. In the first part the organisational culture, business ethics and stakeholders are analysed. At this point it is mostly about identifying opportunities and people with interests in the project. When expectations are identified it is time to look into resources & capability; conducting resource audit, value chain analysis, GAP analysis and classifying information. Analysis phase ends with an environmental analysis and risk assessment.

When designing a strategy, it is important to get the support of top management, and it will be easier to get that by being able to specify benefits, costs and risks. Responsible managers must be well prepared - they may only get five minutes with top management. The strategy should synchronise with the organisation’s long-term overall strategy and culture to reduce the risk of it remaining a paper product. Just like the analysis phase, the design phases consist of three parts: options, development and selection. When looking at options it is important to do a cost/benefit analysis and shareholder analysis, to show that it is financially feasible. Next step is development of a new strategy with risk elimination. Finally, it is time for top management to select the strategy to be used in the organisation.

After a new strategy is adopted it is time for action - the enactment of the strategy on a daily basis - a cycle of communication, training and adjustment. When the strategy is decided (or when something needs to be clarified) it is important to communicate it through the right channels to all employees. Even if communication is clear and reaches everyone there will still be a need for training, and not just once. Training should not only cover policies and written strategies, but should focus on organisational culture and information security. Actively working with culture and information security awareness gives better effect in the long run. It is best to conduct training in several ways since people have different learning styles. Adjustment is more or less about managing variance, and following minor internal and external changes or lack of clarity in communication of the strategy. Sometimes there will be exchanges that demand a complete new strategy - for instance a major change in the market, organisational change or new technology platforms. When something like that occurs, iteration of this cycle is aborted, and the process goes back to the first phase again: analysis.
CHAPTER 5
CONCLUDING REMARKS AND FUTURE WORK

This chapter conclude the thesis by looking at method, how aim and objectives are met, contributions and future work.

5.1 METHOD

Industry practitioners identified the problem, and the results should benefit both research and industry. Therefore, the method for this research has to take industry into account. We looked at Action Research (Davison, Martinsons, & Kock, 2004; Mathiassen, 2002; Mckay & Marshall, 2001), Design Science (Gregor & Hevner, 2013; Gregor & Jones, 2007; A. R. Hevner, March, Park, & Ram, 2004; Peffers et al., 2006, 2007; Vaishnavi & Kuechler, 2007) and Action Design Research (Sein, Henfridsson, Rossi, & Lindgren, 2011).

Action Research focuses on practical issues and follows an iterative cycle of plan, act and reflect, where the research intends to plan change in the real world, enact it and then reflect over the result (Oates, 2006). In this case, we intend to solve a real world problem, but the implementation in an organisation is beyond our scope.

An alternative to Action Research is Action Design Research where the researcher acts both as a researcher at the institution, while designing an artefact, and as a practitioner when testing the artefact in practice. The process goes in cycles until a fully working artefact is built (Sein et al., 2011). The problem with this approach is that we have a general problem which is not identified in a specific organisation that needs our help. If that had been the case, Action Research would have been a good approach.

The chosen method, Design Science, is not completely unproblematic and it has been argued whether it is science or practice. Hevner and Chatterjee (2010) have defined the difference between design science and professional design as the identification of a contribution to the current knowledge base, methodologies and the communication of the contribution to the stakeholder communities. Zimmerman, Stolterman and Forlizzi (2010) point out that some problems with Design Science are created by researchers in the field who argue that an artefact should stand for itself, while a lot of the critique is that Design Science in general is poorly documented. To distinguish Design Science from Design Practice, and to meet this critique, both process and contribution must be documented. That is something that design professionals are not generally trained for, but scientists are good at (Swann, 2002). This work has been carefully documented both in terms of methodology and results.
5.2 FROM AIM TO RESULT

The aim of this work was to develop an artefact (a framework) that can support managerial strategy development for the introduction of mobile devices from an information security perspective. In order to address that aim, two objectives were specified. In this section, each of the objectives will be presented with an explanation of how the objective was reached.

5.2.1 OBJECTIVE 1 - IDENTIFY EXISTING INFORMATION SECURITY MANAGEMENT STRATEGIES FOR MOBILE AND DUAL-USE DEVICES

Paper 1, Management issues for Bring Your Own Device, and paper 3, BYOD vs. CYOD – What is the difference?, respond to this objective. Paper 1 is a systematic literature analysis using a BYOD strategic management framework to assess developing research trends. The analysis reveals early work in the analysis and design aspects of BYOD strategies, but a lack of research in operationalizing (planning, implementation and evaluating) strategy – the action phase. The resulting research agenda identifies twelve management issues for further research and four overall research directions that may stimulate future research. It also reveals that there is no existing framework that manages a mobile device strategy from first discussion to a fully implemented and evaluated strategy, but there is some literature that deals with some parts of the strategy work around mobile devices.

An interview study was conducted to see if the results of the literature study also apply in the world of organisation practice in Sweden, and to research gaps identified in the literature review. The interviews resulted in the identification of strategies that did not exist in the literature, and showed that the BYOD trend was not as strong in Sweden as the literature indicated. Some later studies tend to confirm this result. The main contribution of the interview study was a clear picture of existing and implemented strategies in Swedish organisations, and valuable input to the framework.

5.2.2 OBJECTIVE 2 - DEVELOP A FRAMEWORK (ARTEFACT) FOR ANALYSING, EVALUATING AND IMPLEMENTING A MOBILE DEVICE STRATEGY

In paper 2 (Combining ISMS with strategic management: The case of BYOD) a framework is proposed based on literature, and in paper 4 (Management of mobile devices – how to implement a new strategy) the framework is updated after interviews with executives. The first version of the framework, in paper 2, was derived from strategic management (Johnson & Scholes, 1993), together with ISO/IEC 27000 family (ISO/IEC, 2016), and is purely theoretical. To make sure the framework works in practice as well, an interview study was conducted with the framework from paper 2 as a basis. After the first analysis round, it emerged that the framework was incomplete since there were dimensions that it did not capture. After a second analysis round, with patterns from the interviews as codes, a new version of the framework was developed and presented in paper 4. The new version was improved in areas where existing literature gave no input, and with this version the second objective was fulfilled.

5.3 CONTRIBUTIONS

The main contribution is of the design science type improvement; it gives a new solution to a known problem. During the last 6-7 years a new way of using mobile devices has become
popular and attracted the interest of both researchers and practitioners. Despite the increased interest there is still a gap when it comes to frameworks that deal with the complete cycle. This work brings more knowledge to the area with a framework that works in all three parts of strategic management; analysis, design and implementation.

Further contributions are:

- Highlighting several gaps in current literature. Twelve management issues, together with four overall research directions have been identified. These findings have already been used by other researchers.
- Improving understanding of CYOD in the research community, a strategy which is well known in industry but not so evident in academic literature.
- Helping researchers to understand necessary steps in analysing phenomenon like BYOD.
- Giving practitioners guidance in which analyses to conduct when working on strategies for mobile devices.
- Giving practitioners a better understanding of what steps to take and analyses to make when dealing with strategies for mobile devices.
- Supporting the argument for CYOD instead of BYOD or the more traditional Use What You are Told (UWYT).

5.4 FUTURE WORK

In paper 1, twelve management issues were identified; most of them have not been addressed in this work and remain unexplored areas.

Most organisations today have an information management system and do not necessarily need further ways to manage information. Future work could build a proof-of-concept for how this framework can integrate into an existing information management system.

Furthermore, cybersecurity is something that gets a lot of attention in organisations at this time. Possible directions for further research could be either to test this framework in the context of cybersecurity, or to connect a cybersecurity maturity indicator to this framework to increase input to the design phase.

In the action part we have two areas that are not specific for mobile devices - rather a general problem in many organisations which is interesting to look deeper into. The first area is training and future work could be connected to information security awareness training. How can that kind of training be conducted to reach out to most of the employees and to get the desired effect? The second area that is of interest for further investigation is communication; how can policies and strategies be communicated in an effective way with today's information systems?
REFERENCES


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

Peffers, K., Tuunanen, T., Gengler, C. E., Rossi, M., Hui, W., Virtanen, V., & Bragge, J.


Van Der Meulen, R., & Rivera, J. (2013). Gartner Predicts by 2017, Half of Employers will Require Employees to Supply Their Own Device for Work Purposes.


THE PAPERS
MANAGEMENT ISSUES FOR BRING YOUR OWN DEVICE

Martin Brodin, University of Skövde, martin.brodin@his.se
Jeremy Rose, University of Skövde, jeremy.rose@his.se
Rose-Mharie Åhlfeldt, University of Skövde, rose-mhariahlfeldt@his.se

Abstract

Bring Your Own Device (BYOD) is an emerging research area focusing on the organisational adoption of (primarily mobile) devices used for both private and work purposes. There are many information security related problems concerning the use of BYOD and it should therefore be considered an issue of strategic importance for senior managers. This paper presents a systematic literature analysis using a BYOD strategic management framework to assess developing research trends. The analysis reveals early work in the analysis and design aspects of BYOD strategies, but a lack of research in operationalizing (planning, implementation and evaluating) strategy – the action phase. The resulting research agenda identifies twelve management issues for further research and four overall research directions that may stimulate future research.

Keywords: BYOD Bring Your Own Device, information security management, strategic management.

1 INTRODUCTION

During the last decade it has become commonplace for employees to have dual-use computing devices (devices used both at home and at work) - often for a mixture of private and professional purposes. One popular way of labelling this trend is Bring Your Own Device (BYOD). A recent survey indicates that 95% of companies allow employees some use of their own devices, that 36% offer full support for all employee-owned devices, and that 48% support selected devices (Barbier et al., 2012). Harris et al. (2012) report that one third of organisations allow privately owned devices (a result confirmed by Disterer & Kleiner (2013)) - and another third deploy company-owned dual-use devices. Some large companies sanction extensive BYOD programs; for instance Intel’s program involves 10,000 personal devices (Miller & Varga, 2011). The use of privately owned devices may also be widespread in companies that do not sanction them. Harris et al. (2012) report that 36% of employees ignore company policy and choose to use the device they feel appropriate. BYOD is predicted to be ubiquitous in the near future (van der Meulen & Rivera, 2013).

Though dual-use of devices is widespread, the term BYOD covers several different interpretations in the literature. BYOD implies that the employee owns the device and transports it to the workplace, a phenomenon associated with consumerization (Niehaves et al, 2012). However it may be more common for companies to supply consumer devices (for example a mobile phone) and allow home use (Oliver, 2012). Dual-use also implies that the device is used for a variety of work and personal tasks, implying shared or duplicated data, software and network connections. Where the device is used at home it may be connected to the computing environment of the workplace (Stevenson, 2012), and to external third party services. The nature of the device may be less significant than the extension of access to webmail, cloud services and content management systems (Morrow, 2012). BYOD in this study refers to computing devices which are mobile (used in the office and outside it, including the home) and/or dual-use (used both for professional and private purposes), whether provided by the employer or the employee.

The rapid spread of BYOD probably has many causes, including the popularity of mobile devices, efficiency gains for users in synchronising home and work resources, and productivity gains for employers in the expansion of the work sphere and better integration of information resources.
Employers may hope to transfer some of the device costs to their employees, or use the devices as attractive perks. However, both IT managers and information security experts express concern (ReadWrite, 2013; Intel, 2012). Whereas most information management approaches strive for standardization, consolidation and reduction of complexity (Disterer & Kleiner, 2013), widespread adoption of BYOD implies reduced standardization and increased complexity. There are major problems concerning integration with existing infrastructures, device support, and increased exposure to a variety of information security hazards, such that BYOD should be considered an issue of strategic importance for information security managers - and probably also for the senior managers of information-dependent organisations. Research indicates the importance of choosing an appropriate model for governance and support (Barbier et al., 2012). Strategic management of BYOD covers both the determination and execution of policy.

An early, but rapidly accelerating literature studies these phenomena, so that the management of BYOD may be considered an emerging research area. The objective of this article is to investigate how this literature deals with these issues using literature study techniques. We will address the following research questions:

- **RQ1:** Which managerial issues are highlighted in the emerging literature?
- **RQ2:** What are the research gaps in the early BYOD literature, from a strategic management perspective?

The paper is structured as followed. In section 2 the research method and analysis model are explained. Section 3 presents the analysis of the literature according to the model. Finally, section 4 gives the results and conclusions of the analysis, and offers directions for future research.

## 2 Research Method

The search for relevant literature in this review was derived from Webster and Watson’s (2002) structured approach for determining the source material. These were the principal steps:

1. An extensive literature search using the WorldCat search engine with the search terms: Bring Your Own Device, BYOD, BYOT, BYOS, Bring Your Own, office-home smartphone, smartphone+information management, smartphone+policy, personally owned, consumerization, shadow IT and mobile computing, in combinations with information management, policy, security management, private, privacy, user-driven and dual-use. The search was filtered for peer-reviewed articles in English. This step resulted in 2865 article abstracts.

2. Manual screening for relevance (where relevance requires that the article both falls within the mobile/dual-use definition and focuses on policy, management or strategic issues, rather than technical issues). The articles were screened first by reading the abstracts. This screening removed many articles where BYOD had a different meaning (for instance a term in chemistry), articles which were tangential to the theme of the paper (for instance concerned with pedagogics and BYOD) and articles dealing with primarily technical issues. The remaining articles were downloading in full text and screened again, resulting in 69 unique articles.

3. Backward chaining by reviewing the citations in the articles identified as relevant in step 2. This step revealed many white papers and non peer-reviewed articles but only one new article.

4. Complementary forward chaining search in Web of Knowledge, Academic Search Elite, ScienceDirect, ACM, Emerald, Springer, IEEE and Wiley. This revealed 15 new relevant articles, leaving a total of 85 articles as the literature selection.

The search was considered complete since the complementary searches revealed few new articles of relevance.
2.1 Analysis framework

Webster and Watson (2002) also require that a literature review be concept-centric, where the concepts determine the ‘organizing framework’ of the review. Concepts may derived from the analysis, but a common practice is to adopt a suitable conceptual framework from the literature. The chosen BYOD management framework (Brodin, 2015) is adapted from Jonson and Scholes (1997) seminal work on strategic management, and the international standards ISO/IEC 27001 (2013) and ISO/IEC 27002 (2013) Information Security Management Systems (ISMS. The three main categories in the model are analysis, design and action.

![Diagram of Analysis, Design, and Action]

**Figure 1. Framework for the analysis, adapted from Brodin (2015).**

*Analysis* concerns the assessment of opportunities and threats involved in the adoption of BYOD, where *expectations* refer to the opportunities in the form of BYOD benefits that are targeted, *environment* points at BYOD threats originating from outside the organisation (for example information security threats) determined through risk assessment, and *resources and capability* indicate the organisation’s current ability to realise benefits and mitigate environmental threats.

*Design* concerns the development of strategic information and security governance strategies or policies for BYOD, where *options* represent distinct strategic directions, *development* refers to the adaptation and enumeration of options, and *selection* refers to choosing the appropriate strategy or policy.

*Action* concerns the operationalization of the chosen BYOD strategy, where *planning* precedes the policy *implementation*, and *evaluation* is carried out to determine the success of the BYOD strategy and its implementation.

Most articles in the literature selection covered several of these areas, but in table 1 they are classified according to their primary, or dominant purpose.
3 \textbf{MANAGEMENT ISSUES FOR BYOD}

In this section the principal management issues investigated in current BYOD research are analysed.

3.1 \textbf{Analysis}

\textit{Analysis} concerns the assessment of opportunities and threats involved in the adoption of BYOD, including \textit{expectations}, \textit{environment}, and \textit{resources and capability}.

3.1.1 \textbf{Expectations}

Researchers point to many expectations for BYOD related to benefits for both employee/users and management. The main expectations are for increased personal productivity, flexibility of time and place and increased user satisfaction.

IT Managers rank \textit{increased personal productivity} as the most important expectation for BYOD (Intel, 2012). The BYOD-program at Intel reports that personal device users saved on average 47 minutes per day, amounting to more than 2 million hours per year (Miller & Varga, 2011). iPass (2011) claim that a dual use mobile user works longer than other employers: 240 hours more per year. In cash terms, productivity benefits may amount to between $300 and $1300 per year per employee, depending on job role (Barbier et al., 2012). One reason for increased productivity may be that employees who are able to satisfy their psychosocial needs at work invest more of themselves (Kahn, 1990; Pfeffer 1995). However many of the existing studies of BYOD benefits are sponsored by large industry players (Intel, Cisco) with vested interests in promoting BYOD, and these results should be treated with caution.

BYOD \textit{increases flexibility of time and place}, allowing employees to work outside the office and normal working hours. Some managers expect this to be the most significant BYOD benefit (Singh, 2012). One way this can be measured is by monitoring business related emails and access to corporate resources from non-corporate devices after office hours. Harris et al. (2012) refers to a study where 14% of employees connected to corporate resources after work hours and 22% used a private mobile phone to check corporate emails before they went to bed. Logically BYOD also helps the employee to

\begin{table}[h]
\begin{center}
\begin{tabular}{|c|c|}
\hline
\textbf{Category} & \textbf{Number of articles} \\
\hline
Analysis & 52 \\
\quad Expectations & 11 \\
\quad Environment & 33 \\
\quad Resources & capability & 8 \\
Design & 31 \\
\quad Options & 15 \\
\quad Development & 13 \\
\quad Selection & 4 \\
Action & 0 \\
\quad Planning & 0 \\
\quad Implementation & 0 \\
\quad Evaluation & 1 \\
Total & 85 \\
\hline
\end{tabular}
\end{center}
\caption{Distribution of articles by category.}
\end{table}
manage their personal affairs from the office, but this is not investigated. Increased freedom to manage personal work in terms of time and place may have positive health effects (iPass, 2011). However constant work availability facilitated by BYOD is implicated in increased personal stress (Green 2002), and the extension of work into home life, may affect family relationships, for example the amount of time spent with children (UNICEF 2014).

A secondary expectation for BYOD is increased user satisfaction (Miller & Varga, 2011). This is associated with the convenience of reducing the number of devices; for example one mobile phone for both private and business use (Disterer & Kleiner, 2013). Harris et al. (2012) report that many users enjoy having advanced technology devices at work and home, but relatively few believe that it contributes significantly to work satisfaction.

3.1.2 Environment

In the BYOD literature the organisational environment is largely perceived as an information security threat, in which dual use devices are at greater risk. Threats are assessed through risk assessment, and increased risk stems from user behaviours and expectations for their devices, particularly when they also use them for personal purposes and consider that they own them. Thus the principal managerial issues for BYOD in relation to environmental threats are data control and device protection.

A major BYOD concern is control of corporate data, especially where data is stored outside company premises, when the device that it is stored on is lost or stolen, or if the employee leaves the company. Particularly difficult is the question of who is accessing corporate data, since BYOD devices (which may connect to confidential corporate data systems) are seldom physically secure, and may be attached to multiple networks. A company owned device can be retrieved when an employee leaves, or remotely wiped if it is stolen. The data, if stored, may be encrypted, and the company’s information security policies enforced by the IT department. Even with these precautions, sensitive corporate data is routinely recoverable from second-hand hard disks (Jones et al. 2012). Dual use device owners tend to resist the installation of encryption and remote wipe software (or other kinds of software associated with managerial control) since they consider that it encroaches on their privacy (Pettey & Van Der Meulen, 2012). Only a third of private device owners use encryption for company data (Camp, 2012). Private device owners freely install software of their own choice and join networks other than the company’s protected network. If it is too complicated to access the secure network, users may go for the less secure guest network instead (Kehoe, 2013). They may store data on multiple hard disks, including their private cloud (Dropbox, OneDrive, iCloud, Google Drive). A particular problem arises when the key or password protecting the data is personal, whereas the data is corporately owned (Walters, 2013). How can this data be monitored and audited? An employee leaving a company takes their privately owned device with them – how does the company ensure that sensitive corporate data is removed?

A related managerial issue is protection of BYOD devices, since devices storing sensitive corporate data are routinely lost, stolen or hacked (Wilson, 2012). If the IT department does not control the device they cannot force operating system updates or ensure that the antivirus program is up to date (Morrow, 2012). Most private users have poor protection habits: they do not update software regularly (Skype et al. 2012), or use the auto-locking facilities provide for them. Researchers expect those behaviours to remain when their device is used for work-related purposes (Disterer & Kleiner, 2013). Camp (2012) estimates that “less than half of all devices in the BYOD category are protected by the most basic of security measures”. Users should back-up their own devices (Wong 2012) since the organisation cannot be responsible. IT managers are thus required to protect corporate data they may not even control (Walters, 2013). Faced with non-standard devices and non-compliant users (Tokuyoshi, 2013) they may give up. Difficulties in supporting security, encryption and remote wipe are the most common explanations for not restricting BYOD use.

3.1.3 Resources and capability

Resources and capabilities represent the organisation’s current ability to realise benefits and mitigate environmental threats from BYOD. Two significant managerial issues here are awareness and support.
Awareness describes an organisation’s capacity to monitor and react to the BYOD threats in its environment. Allam et al. (2014) propose a model for smartphone information security awareness based on accident prevention techniques. The model is designed to help monitor the information security position and tailor security policies and procedures to threats. However Ashenden and Lawrence (2013) believe that awareness programmes are limited and their effect on behavioural change doubtful. Instead, they propose a social marketing framework that will be more effective. They identify the user behaviour they want to change, analyse why users exhibit those behaviours, identity benefits for users from potential change which increase security, design an intervention, and evaluate the impact.

A significant resourcing and capability issue for BYOD is support. BYOD devices run many operating systems on many platforms, with diverse software. IT managers anticipate many compatibility problems with existing IT infrastructures (Intel, 2012). However, users expect the same level of support they had with their standardised company-owned devices (Brooks, 2013). IT professionals experience the frustration of increasing support costs and administration time, which reduces productivity in other areas (Walters, 2013). Intel (2012) claims that BYOD comes with no impact on support and with relatively low cost (Miller & Varga, 2011). Organisations that transferred purchase costs for devices to their users saved some money. However Harris et al (2012) report that these savings were eaten up by the increased cost of managing the IT environment.

3.2 Design

Design concerns the development of strategic information and security governance strategies or policies for BYOD, where options represent distinct strategic directions, development refers to the adaptation and enumeration of options, and selection refers to choosing the appropriate strategy or policy.

3.2.1 Options

Strategic options represent different choices that managers have in relation to the adoption of BYOD, where the two extreme positions are (i) to forbid any kind of dual use device, and (ii) to allow each and every form of BYOD without restrictions. Mournant et al. (2013) do not examine BYOD as an independent option, but as part of their model for intrapreneurial freedom; BYOD is part of freedom of materials and resources. Harris et al. (2012) present a model for IT consumerization with 6 strategic options that range from strict (tight control, few standard devices) to complete freedom. The only option that allows privately owned devices is laissez-faire, where management allow external devices and applications without any restrictions. However no research advocates this strategy, although some researchers and standards discuss trade-offs and the acceptance of risk. Holleran (2014) proposes a compromise option, where BYOD is prohibited, but in return employees are allowed to use their mobile devices for personal purposes. Another way of developing strategic options is through analysis of the managerial control space. Yang et al., (2013) proposes a risk management quintet, which looks at the mechanisms for technology adoption, control, liabilities, user perception, and user behaviour.

One prominent article genre in this category was the opinion piece from an acknowledged industry expert (e.g. Millard (2013); Steiner (2014); Thielens (2013); Walker-Brown (2013)). Though apparently peer reviewed, these articles are based on personal experience and do not display any conventional research method. They are not considered further here.

3.2.2 Development

Regardless of choice of strategic option, there is universal agreement that the first development step is information security policy update (Oliver, 2012; Harris et al., 2012; Wong, 2012; Gatewood, 2012; Caldwell, 2012; Simkin, 2013; Montana, 2005; Vickerman, 2013; Yang et al., 2013). Though these researchers identify the policy as central to the success of BYOD, research in the information security management field indicates that policies are often broken. Younger people seldom obey information security policies (Simkin, 2013), though more than half of IT professionals believe they do. Users have poor understanding of policies (Oliver, 2012; Wong, 2012), if they are even aware of them.
Consequently, it is not enough to update a policy; it must also to be communicated (Wong, 2012; Gatewood, 2012; Oliver, 2012).

Wong (2012) points out the need for users to understand the regulatory framework: for example which information is owned by the organisation and which is personal information that they may freely use. This problem is compounded by role confusion: when, and in what situations, is a user acting as a private person, and when they are acting as an organisational representative. Is it acceptable to post sensitive corporate information on a social network where you are profiled as a private person, or if you are no longer working for the company? Other central aspects in the development area are risk assessment, clarification of ownership of information, right to audit, privacy rights, security of business information, and registration of assets (Vickerman, 2013).

3.2.3 Selection

BYOD strategy decisions should be made by the appropriate people in the organisation after weighing benefits against information security risks: the business/security balance. Ring (2013) identifies organisations that gave BYOD both green and red lights after evaluating the risks. He concludes that the choice is ultimately “a business decision, not a security decision”. Borrett (2013) agrees, arguing that senior management target increased flexibility and/or cost-savings. Mooney et al. (2014) suggest that the entire c-suite (chief executives) should be involved in the process. Guinan et al. (2014) disagree, arguing that, depending on the organisation, the process may be top-down, middle-out or bottom-up, and that knowing where and with whom to begin may be the key to success. Silic and Back (2013) identify two must-win areas when selecting a strategic option: mobile strategy and security framework. Furthermore, they argue that stakeholder support is critical, both for making the change and for rooting new information security procedures in the culture.

3.3 Action

Action concerns the operationalization of the chosen BYOD strategy, where planning precedes the policy implementation, and evaluation is carried out to determine the success of the BYOD strategy and its implementation.

3.3.1 Planning, Implementation and evaluation

BYOD is a relatively new phenomenon, and few researchers directly address the action phase. Those that do, agree on the need for training. Walters (2013) focuses on the human and informational, rather than technologies, since a lot of the traditional layered approach to enterprise security do not apply anymore. What definitely apply is the human layer with information security education and awareness. Furthermore, Walters (2013) state that functional and organisational roles for data access must be determined before a BYOD implementation can start.

Gatewood (2012) emphasises information security training for all employees and points out that a forgotten and unlocked phone can lead to a disaster. The technical mechanisms are not worth as much if employees do not comply with the BYOD strategy and policies. Studies indicate that proper security training must be in place to get employees to adopt the new strategy (Hu, 2013; Markelj & Bernik, 2012).

When the policies and procedures are implemented it is important to evaluate opportunities and threats with respect to organisational context to determine if an update is needed (Niehaves et al, 2012).

4 DISCUSSION AND DIRECTIONS FOR FUTURE RESEARCH

Two research questions were posed for this review. In response to the first question: What managerial issues are highlighted in the emerging literature on BYOD, twelve issues were identified (represented in italics in the next sections).

Managerial expectations for BYOD include increased personal productivity, time/space flexibility and increased user satisfaction. These benefits coincide with expectations for mobile devices in general,
and researchers need to understand what the specific impact of dual use, personal ownership and personal choice of device have on these outcomes. In addition the methodological approach of this research requires more consideration, and there is a need to separate independent research investigations from those of major industry players. Researchers should also establish costs (and particularly hidden costs) of BYOD programs which may result from infrastructure integration, support and extra information security demands, the costs of information security breeches, and employees organising their personal affairs in work time, amongst other things. There is also need for research into employees’ dual use (home and work) patterns.

Environmental information security threats highlighted the need for improved approaches for information control and device protection. Many of these threats are known in the mobile security field, and researchers need to understand how (partial) loss of organisational control of information and devices, less standardization and transfer of responsibilities for protection/backup to users affect these threats. Important questions for researchers may be: which known threats are amplified by BYOD (and by how much) and have known responses that can be scaled up; which threats are amplified to the point where they can no longer be managed with known responses; and which threats are new and require improved management approaches. Many of these questions require empirical investigation and quantification. An unexplored question is whether there are information security threats that are reduced or removed by BYOD. A further issue that is not yet investigated is the effect of BYOD on employee privacy. Users have information rights (many of them are backed by law), as well as organisations.

Issues relating to organisational resources and capabilities include awareness and support. Organisational information security awareness may come to depend more on user-led reporting, manufacturer alerts and monitoring the information security communities. Patterns for support may change when there are many different devices and little standardization, with more reliance on users’ own capabilities and lower levels of information (which might also focus on information security guidance and instructions). Crowd-sourced solutions to these problems, with users doing much of the work themselves and IT professionals co-ordinating are not yet researched. A further issue needing investigation is information classification; this may facilitate many differentiated strategic options.

With respect to the design of BYOD strategies, researchers need to improve already established models of strategic options in order to complement the partial offerings available. Such models should offer differentiated BYOD strategies to managers, explaining the potential benefits, costs, risks and information security responses of different courses of action. Such strategic option models should be based on quantitative and qualitative evidence, with a theoretical departure point. Since development of new strategic positions involves an information security policy update, researchers may investigate how current information security standards (such as ISO/IEC 27000-series and methodological support for information security (MSB, 2015)) manage BYOD. However, at the same time they should investigate how the take-up of the information security regulatory framework as a whole can be improved, especially in the BYOD environment where users may perceive the regulatory framework as voluntary. Selection of options is based on the business/security balance. This is a particularly complex area for organisations and need to be researched, as it involves cross-disciplinary comparative assessments of benefits and risks, where neither organisation-wide benefits nor a complete empirically based picture of information security threats are yet available. Moreover the development of strategic options implies comparative assessments for several scenarios or contingencies. Most of the BYOD literature focuses on personal productivity, and its influence on team communication, group work, customer management, and at the organisational level information flow, workflow and management communication are not yet studied. Managers should understand what they could expect to achieve for their organisations with BYOD programs. Organisations with structured information security programs already in place are better placed to handle emerging BYOD difficulties. However many organisations lack information security classification and security risk management that might provide a firmer foundation for strategic decision-making. Managers should also be helped to understand the scale of risk to which their organisations are exposed by authorised (or unofficial employee-led) BYOD programs.
The action or implementation of strategies is not much investigated in current BYOD literature (see below), but researchers can translate BYOD compliant information security standards and methods into training materials and contribute more effective learning strategies.

Research directions for BYOD management issues are summarized in table 2.

<table>
<thead>
<tr>
<th>Framework category</th>
<th>BYOD management issues</th>
<th>BYOD research agenda</th>
</tr>
</thead>
</table>
| Analysis expectations| 1. increased personal productivity  
2. time/space flexibility  
3. increased user satisfaction | benefits and costs should be established empirically by independent researchers using methodologically sound techniques. |
| environment          | 4. information control  
5. device protection | cataloguing of known mobile information security threats and responses for BYOD area, and identification of new threats and responses; protection of employee privacy. |
| resources and capability | 6. awareness  
7. support | investigation of distributed and user-led information security awareness and support; information classification. |
| Design development   | 8. strategic options  
9. security policy update  
10. regulatory framework | improvement of normative models of strategic options based on empirical evidence and theory  
development or improvement of policy and regulatory frameworks from existing information security standards and methods, and investigation of improved user compliance |
| selection             | 11. business/security balance | cross-disciplinary comparative assessments of organisational benefit and information security risk |
| Action planning       |                                                                                  | (under researched area requiring further investigation) |
| implementation        | 12. training | materials, methods and tools for communicating and disseminating regulations within organizations, (under researched area requiring further investigation) |
| evaluation            |                                                                                  | (under researched area requiring further investigation) |

Table 2. Research directions for BYOD management issues

In response to the second question (what are the research gaps in the early BYOD literature, from a strategic management perspective), the current distribution of research over the BYOD management framework (Brodin, 2015) is skewed. Table 2 shows that the largest part of the research concerns strategic analysis (expectations, environment, resources and capabilities), where the majority deals with information security threats. A smaller proportion concerns strategy design, with many recommendations based on experiential evidence and a widespread concern with information security policies. Much less research covers action – the operationalization of strategy phase. One reason for this absence may be that BYOD is an emerging phenomenon, so there are relatively few well-designed implementations to investigate. Another possibility is that BYOD presents relatively few new strategic challenges, and can be managed with incremental changes to information management and mobile security strategies within existing frameworks. Regardless, this still has to be investigated. Therefore it seems necessary to take the following steps to provide sound research that is helpful to practitioners.
1. Ground BYOD research in existing mobile security research in order to specify what can be inherited from existing research and what the new parameters are, such as ownership, decreased standardization etc.

2. Develop theory-based strategic options frameworks with suitable research methods (for instance design science).

3. Focus on strategic action (planning, implementation, evaluation) research by encouraging the empirical investigation of BYOD implementations using case studies, action research, and other qualitative methods, supplemented by for instance quantitative evaluation methods.

4. Encourage cross-disciplinary research to broaden the base of the research beyond the information security communities (see Györy et al., (2012)).

5 CONCLUSIONS

In this article we investigated the emergence of the widespread empirical phenomenon of Bring Your Own Device in research literatures. BYOD is linked to consumerization, as computing devices for personal use become widespread in affluent societies. Much of the research discussion is located in the mobile security research area, since data and device security is a major concern. There are technical strands of research (for example in chip design); however we chose to focus on the managerial implications of BYOD for companies. Though BYOD is difficult to separate from other aspects of dual use computing, two aspects of BYOD may become crucial for the development of computing in organisations. The first is the shared understanding that the user owns their device (regardless of who actually pays for it); the second is the consequent understanding that they have free choice – of device, the software that they install on it, and what they use it for. These factors effectively move the locus of control of the device (and the information accessed by it) away from the organization and towards the individual employee - a change widely assumed to be unstoppable and non-reversible. Such changes often require a strategic response from organisations. We analysed 85 articles focusing on these phenomena using a framework developed for the purpose from the strategic management and security standards literature. We identified 12 BYOD core management issues addressed by the literature and provided a focused research agenda for each of these existing issues. We also analysed prominent gaps in the literature and identified four overall research directions which can help address those gaps. The twelve management issues, together with these four overall research directions provide a basis for a stimulating and useful programme of research.

References


Harris, J. 2013. 'A survey of security risks of mobile social media through blog mining and an extensive literature search'. Information Management & Computer Security. 21(5): 381-400.


Kehoe B. 2013. 'BYOD - Proceed with caution'. Hospitals and Health Networks. 87(6): 17.


Oliver, R. 2012. 'Why the BYOD boom is changing how we think about business it'. Engineering and technology. 7(10): 28.
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. URL: http://www.gartner.com/newsroom/id/2263115 (visited July 2013).


Vickerman, J. A., 2013. 'Managing the Risks of BYOD With the line between work and home increasingly blurred, companies must establish a policy that embraces progress'. Risk Management, 60(1): 38-41.


COMBINING ISMS WITH STRATEGIC MANAGEMENT:
THE CASE OF BYOD

Martin Brodin
University of Skövde
Box 408, S-541 28 Skövde, Sweden

ABSTRACT
Bring Your Own Device (BYOD) (where employees use their private devices for work) causes problems for organisations since their management systems are seldom designed for this purpose. If BYOD is not adequately regulated, many security and privacy issues may result. This paper proposes an analysis-design-action framework for designing a suitable security management strategy by combining Johnson and Scholes’ strategic management model with the ISO/IEC 27000-series.

KEYWORDS

1. INTRODUCTION
ISO/IEC 27000-series focus on what to do when it comes to information security management (ISM), not how it can be done. The step from knowing what to do to understand how to do it has proved to be overly complex and costly for many organisations (Gilles, 2011). The ISO/IEC 27000-series is intended to assist organizations of all types and sizes with implementation and operation. Through the use of the standards, organizations can develop and implement a framework for managing the security of their information assets, it can also be used to prepare for an independent assessment (ISO/IEC 27000, 2014).

Although the standard is general and can be applied to different organisations in different situations it may cause some problems. A general problem with information security management standards are the focus on the existence of policies and processes, and not how they can be accomplished in practice (Siponen, 2006). When dealing with a specific problem, standards are too general to easily be applied (Doherty & Fulford, 2005).

In the last years evolution of mobile devices has gone in a high-speed, the devices are getting more and more like computers. Organisations are having a hard time to keep up with this pace; at the same time the demands from users, to get the newest devices to make their job easier, are increasing. When organisations fail to adopt the latest technology, more and more users start to bring their personal devices and use them in the work. This trend is called Bring Your Own Device, or simply BYOD, and is in many ways the opposite to popular information management approaches; which strive for standardization, consolidation and reduction of complexity (Disterer & Kleiner, 2013). At the same time it is important to find the right model for governance since 86 % of the costs connected with BYOD adoption are non-hardware (Barbier, et al., 2012).This is not a security or technicians decision, it is something that has to be decided by senior management (Borrett, 2013; Ring, 2013).

This article will introduce a method to adopt to phenomenon like BYOD into an organisation with the help from ISO/IEC 27000-series and strategic management. The work is based on a literature study in the field of BYOD. The research question is:

RQ: How can BYOD be adopted to an organisation?

In section 2 a short introduction to BYOD is presented while section 3 discusses how mobile devices and BYOD are managed in ISO/IEC 27000-series. In section 4 a model for strategic management is introduced and section 5 proposes a framework for adapting to BYOD.
2. **BRING YOUR OWN DEVICE**

BYOD is growing fast and by 2016 will 38% of companies stop providing their employees with devices, according to a survey by Gartner, and the predicted number for 2017 is 50% (van der Meulen & Rivera, 2013). Some major companies already got their own bring-your-own-device program, for instance Intel got 10 000 personal devices involved in their program (Miller & Varga, 2011). However, many organisation do not have a strategy for devices or got old strategies that are ignored by a lot of the employees. Harris et al. (2012) found in their study that 36% of employees stated that they do not care about their organisations current policies and will use what they feel is right for them. Without clear, communicated strategies and education, there is a great risk that a lot of security issues will occur (Silic & Back, 2014; Walters, 2013). By highlighting the problem and make a strategy for BYOD organisations can get the benefits and at the same time reduce the risks.

By allowing BYOD organisations hope to gain one or more benefits; the top benefits are increased productivity, improved flexibility and high level of user satisfaction (Miller & Varga, 2011). Another benefit that is mentioned when talking about BYOD is cost savings, as the user will take some of the cost from the device budget (Buchholz, 2012). Although there has been studies which show that cost savings from devices got eaten by increased cost to manage and secure the new IT environment (Harris et al. 2012; Walters, 2013).

Risks that commonly are connected to BYOD are decreased control and security. When the device is private the employee will keep it even after the employment, but what will happen to organisational data (Walters, 2013)? Even if the former employee will delete or keep all data safe, at some point the device will end its life, what then? Analysis of information remaining on disks offered for sale on the second-hand market showed that 47% of the readable disks could be easily recovered (Jones et al. 2012). Even if the data is removed from the disk it can still be recovered.

With no or little control over the device, it is hard to force updates and make sure that the antivirus program is up to date (Morrow, 2012). It is likely that a private device that is used for work purpose as well will be managed as other private devices (Disterer & Kleiner, 2013). A survey by Skype, Symantec and Tom Tom revealed that 40 % of users do not update their software when prompted to do so (Skype et al. 2012). Another study concluded that less than half of all devices in the BYOD category got at least the most basic protection (Camp, 2012).

In order to identify problems and benefits with BYOD, a systematic literature review was conducted on BYOD (in WorldCat, ACM, IEEE, ScienceDirect, Academic Search Elite, Web of Knowledge, Springer and Emerald). The review showed that research studies with focus on management for adoption to BYOD, from it first appears to fully implemented and supported, is missing. There are studies that point out benefits (Barbier, et al., 2012; Miller & Varga, 2011; Singh, 2012), threats (Disterer & Kleiner, 2013; Morrow, 2012; Pettey & Van Der Meulen, 2012), solutions to part of the problem (Allam, et al., 2014) and importance of policies (Gatewood, 2012; Oliver, 2012; Wong, 2012).

3. **THE ISO/IEC 27000-SERIES**

ISO (International Organization for Standardization) is an independent, non-governmental membership organization and the world’s largest developer of voluntary International Standards, supported by 165 countries. The 27000-series are developed in cooperation with IEC (International Electrotechnical Commission) and are still under development. ISO/IEC 27000-series is a standard for information security management systems, which is defined in ISO/IEC 27000:

*An Information Security Management System (ISMS) consists of the policies, procedures, guidelines, and associated resources and activities, collectively managed by an organization, in the pursuit of protecting its information assets. An ISMS is a systematic approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an organization’s information security to achieve business objectives. (ISO/IEC 27000, 2014)*

The established standards in the 27000-series that are of interest in an adoption to BYOD are shown in table 1.
Table 1. ISO/IEC standards of interest in this article.

<table>
<thead>
<tr>
<th>Standard</th>
<th>About</th>
</tr>
</thead>
<tbody>
<tr>
<td>ISO/IEC 27000</td>
<td>Information security management systems -- Overview and vocabulary</td>
</tr>
<tr>
<td>ISO/IEC 27001</td>
<td>Information security management systems -- Requirements</td>
</tr>
<tr>
<td>ISO/IEC 27002</td>
<td>Code of practice for information security controls</td>
</tr>
<tr>
<td>ISO/IEC 27003</td>
<td>Information security management system implementation guidance</td>
</tr>
</tbody>
</table>

ISO/IEC 27000 defines terms that are used in the series and provides an overview of information security management systems. ISO/IEC 27001 specifies requirements for the establishment, implementation, maintenance and continuous improvement of an information security management system. ISO/IEC 27001 also includes requirements for the assessment and processing of information security risks. ISO/IEC 27002 provides best practice recommendations on information security management and ISO/IEC 27003 gives some guidance for implementation.

ISO/IEC 27001 (2013) states that the organisation shall determine the external and internal issues that are relevant to its purpose and that affect the intended results when it comes to security. It is also important to understand which stakeholders are relevant and which of these stakeholder requirements that are relevant to information security. Senior management are responsible for information security policy, it is up to date and communicated in the organisation. When planning, it is important to prevent and reduce the unwanted effects and assess whether the measures had the intended effect.

3.1 BYOD in ISO/IEC 27002

The ISO/IEC 27002 has two advices for BYOD: separate private and professional use and sign an agreement where the user more or less waives his rights. The standard also gives some code of practice for mobile devices in general, which of some can be adopted to BYOD, see table 2.

Table 2. Mobile device guidelines that can be applied to BYOD.

<table>
<thead>
<tr>
<th>Advice in ISO/IEC 27002</th>
<th>How to manage with BYOD</th>
</tr>
</thead>
<tbody>
<tr>
<td>Register all mobile devices</td>
<td>Access policy</td>
</tr>
<tr>
<td>All devices shall have physical protection</td>
<td>BYOD policy</td>
</tr>
<tr>
<td>List accepted versions and prompt for updates.</td>
<td>IT-policy</td>
</tr>
<tr>
<td>Limit access to information</td>
<td>Technical</td>
</tr>
<tr>
<td>Controlling access</td>
<td>Technical</td>
</tr>
<tr>
<td>Protection against virus</td>
<td>IT-policy</td>
</tr>
<tr>
<td>Backup</td>
<td>IT-policy</td>
</tr>
</tbody>
</table>

The standard also present guidance for the introduction of teleworking, which also can be applied to BYOD. Things that should be considered for teleworking, and also for BYOD:

- Security requirements for communication, with regard to remote connection.
- Use of virtual desktop to avoid processing of information on private devices.
- How to deal with the possibility of family and friends are using the same device.
- Access from private networks.
- The right to access private devices during investigations and updates.
- Does the licenses allow use on private devices?
- Requirements for anti-virus and firewall.

4. A MODEL FOR STRATEGIC MANAGEMENT

Strategic management can be summarized in three steps; strategic analysis, strategic choice and strategic implementation, each step consists of several activities. Figure 1 is not a picture of what it looks like in practice, nor an ideal way to work. It is more a model to be used when thinking through strategic problems.
The starting point is the strategic analysis where the management has to look deeper into the culture, stakeholder expectations, resources, strategic capability and the environment. What opportunities and threats are there? Analyses that can be used here are:

Culture and stakeholder expectations
- Cultural context analysis – identify taken-for-granted beliefs from both in- and outside.
- Stakeholder analysis - who has an interest in and expectation of the organisation’s performance?
- Business ethics – how the organisation influence the behaviour and values of people and society.

Resources and strategic capability
- Resource audit – identify available resources to support the strategy.
- Value chain analysis – how resources are being utilised, controlled and linked together.
- Comparison and balance of strategic capability against industry norm, best practise or historical data.
- Identification of key issues – summarization of performed analyses.

The environment
- Identify the status of the environment, static or about to change.
- What elements has affected the development and performance in the past?
- Identify key forces.
- Strategic position – how does the organisation stand against competitors?

When all analyses are done, it is time for strategic choice; develop, evaluate and select a strategy. While developing a new strategy, it is important to get the answers to three questions regarding the development:
1. What basis?
2. Which direction?
3. How?

When strategic options are identified, they should be evaluated; useful criteria for evaluation is suitability, feasibility and acceptability. After evaluating the strategies a choice has to be made, helpful analyses here can be:
5. A FRAMEWORK FOR BYOD ADOPTION TO A MANAGEMENT SYSTEM

Using a model for strategic management in the BYOD implementation gives a clearer picture of what needs to be done. By adapting the model to ISO/IEC 27000-series, many of the security concerns around BYOD will be managed. Adopting BYOD does not necessarily represent a strategic change in business direction for an organisation. However, it may have implication on strategic information management and ISM, which is why the model has to be modified to suit this purpose. This framework gives both the security and strategic way of thinking and acting. The proposed framework is shown in figure 2 and explained in more details in this section. The main structure is from Johnson and Scholes (1993) with the security focus from ISO/IEC 27000-series. Information security management and strategic management permeate the entire framework.

![Diagram of BYOD framework]

Figure 2. The proposed framework for BYOD adoption.

Table 3 shows, which tasks should be performed at each step, the source is either ISO/IEC 27000-series (ISO) or Exploring corporate strategy by Johnson and Scholes (1993; 2012) (J&S).
Table 3. Tasks in the proposed framework, italic text show main contributions from each source.

<table>
<thead>
<tr>
<th>Tasks</th>
<th>Source</th>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Analysis</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Environmental analysis</td>
<td>J&amp;S</td>
<td>Environment</td>
</tr>
<tr>
<td>Risk assessment</td>
<td>ISO</td>
<td>Environment</td>
</tr>
<tr>
<td>Business ethics</td>
<td>J&amp;S</td>
<td>Expectations</td>
</tr>
<tr>
<td>Stakeholder analysis</td>
<td>ISO and J&amp;S</td>
<td>Expectations</td>
</tr>
<tr>
<td>Cultural context analysis</td>
<td>J&amp;S</td>
<td>Expectations</td>
</tr>
<tr>
<td>Information classification</td>
<td>ISO</td>
<td>Resources &amp; Capability</td>
</tr>
<tr>
<td>Resource audit</td>
<td>J&amp;S</td>
<td>Resources &amp; Capability</td>
</tr>
<tr>
<td>Value chain analysis</td>
<td>J&amp;S</td>
<td>Resources &amp; Capability</td>
</tr>
<tr>
<td>GAP analysis</td>
<td>ISO and J&amp;S</td>
<td>Resources &amp; Capability</td>
</tr>
<tr>
<td><strong>Design</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cost/benefit analysis</td>
<td>J&amp;S</td>
<td>Option</td>
</tr>
<tr>
<td>Shareholder value analysis</td>
<td>J&amp;S</td>
<td>Option</td>
</tr>
<tr>
<td>Risk elimination</td>
<td>ISO</td>
<td>Development</td>
</tr>
<tr>
<td>Development of the strategy</td>
<td>J&amp;S</td>
<td>Development</td>
</tr>
<tr>
<td>Selection</td>
<td>J&amp;S</td>
<td>Selection</td>
</tr>
<tr>
<td><strong>Action</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Planning &amp; allocating resources</td>
<td>ISO and J&amp;S</td>
<td>Planning</td>
</tr>
<tr>
<td>Risk assessment for implementation</td>
<td>ISO</td>
<td>Planning</td>
</tr>
<tr>
<td>Managing change</td>
<td>J&amp;S</td>
<td>Implementation</td>
</tr>
<tr>
<td>Evaluation</td>
<td>ISO and J&amp;S</td>
<td>Evaluation</td>
</tr>
</tbody>
</table>

5.1 Analysis

During the analysis phase a number of analyses will be conducted and summarised in order to provide a picture of the present state in the organisation. The organisation has to determine which issues that are relevant and affects overall strategy and information security (ISO/IEC 27001, 2013). It is also necessary to analyse the effect on culture, strategic capability and organisational goals (Johnson, et al., 2012). The environmental analysis includes identification of the status of the organisation, important elements for development and key forces. The analysis phase ends with a GAP analysis where the present state compares with the desired state, which is set by the management or from best practice.

Johnson and Scholes (1993; 2012) model leaves out information classification and risk assessment important parts of a BYOD adoption. On the other hand; ISO/IEC 27000-series misses cultural context analysis and business ethics.

5.2 Design

The design phase starts with more analyses and continues with the development of strategies. Updating current policies is a very important step in this phase (Gatewood, 2012; Harris, et al., 2012; Montaña, 2005; Oliver, 2012; Simkin, 2013; ISO/IEC 27001, 2013; Wong, 2012; Yang, et al., 2013). The information security policy should address the requirements derived from the business strategy, regulations, contracts, and the current, and expected, overall threat (ISO/IEC 27002, 2013). A Cost/Benefit analysis will be performed, but since financial return is not the main focus a profitability analysis will not be necessary.

The main contribution from ISO/IEC 27000-series here is the risk elimination; Johnson and Scholes (1993; 2012) add a focus on the benefits and values for shareholders.

5.3 Action

When turning the strategy into action it is, according to ISO/IEC 27001 (2013), important to perform risk assessment. This is done associated with the planning of the implementation. When planning the implementation, an education for the employees should be planned in conjunction with implementation.
(ISO/IEC 27002, 2013). Organisation structure and design, which appear in Johnson and Scholes (1993; 2012) model is left out because a reorganisation is not necessary for this kind of adaptation. After the implementation it is very important to evaluate if the strategy delivered the expected result (ISO/IEC 27001, 2013).

6. CONCLUSION

BYOD is a phenomenon that is not well managed in business management systems and creates concerns among security experts and IT technicians. It is time for the senior management to act and get a structure so they can determine how BYOD should be handled in the business. Without a strategic decision, BYOD will exist in the organisation but unregulated. This may lead to information being compromised and without control.

As with any strategic change, the work has to be methodical and with substance behind the decisions to be sustainable. In this case, information security plays an important role and the strategic work need support from information security management. The proposed framework combines the strategic management process with the information security management from ISO/IEC 27000-series. Even though BYOD is used as an example in this paper, the framework can be used to any adoption to new phenomenon that not fit into the existing management system.

Future work should focus on further analysing and extending this framework and evaluate it in practice. A way to extend the framework is to develop guidelines for BYOD or similar phenomena.

REFERENCES


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


Wong, W., 2012. BYOD: The Risks of Bring Your Own Device: Five things to keep in mind when it comes to employees using their own hardware in the workplace. Risk Management, 59(9).

ABSTRACT
During the last years mobile devices have become very popular to use both for work and pleasure. Different strategies have evolved to increase productivity and to satisfy the employees. In this paper, we look at the two most popular strategies and look at the strengths and weaknesses of those. This is done by a systematic literature review and semi-structured interviews with CIO’s or equivalent roles. We conclude that BYOD and CYOD comes with similar strengths, but CYOD brings a little fewer security risks.

KEYWORDS
BYOD, CYOD, Information Management, Mobile Devices, Mobile strategy, Smartphone, Bring Your Own Device.

1. INTRODUCTION
During the last years Bring Your Own Device (BYOD) has gained in popularity and opportunities, and threats have been discussed widely in both scientific and business articles (Brodin et al. 2015). But lately its popularity in the USA has decreased and in Europe, it has never really taken hold. Choose Your Own Device (CYOD) is a more popular approach in Europe and is gaining in popularity in the US (Kane et al. 2014).

The objective of this article is to investigate the difference between BYOD and CYOD issues using literature study techniques and interviews with CIOs. The following research questions will be addressed:

- **RQ1:** Which managerial issues are connected to both BYOD and CYOD?
- **RQ2:** What is the difference between BYOD and CYOD from a managerial perspective?

The paper is structured as follows. In section 2 the research method and analysis model are explained. Section 3 presents an introduction to BYOD, section 4 presents an introduction to CYOD and section 5 presents a comparison and discussion. Finally, section 6 gives the conclusions of the analysis, and offers directions for future research.

1.1 Ways to Manage Devices
Traditionally, when it comes to ISIT-devices, the employer received their working tools with the words: use what you are told (UWYT). IT then got a pre-determined list of approved devices which they control and has configure for work purpose. A variation is a list of allowed devices that depends on the role of the employee, where some roles can get much freer choice than others. The role based list approach is a mix of UWYT and CYOD. When moving from UWYT to CYOD the IT-department leave the choice of device completely to the user, but still buy and control the device. In this category, there are some variations between level of private use and control. When the organisation lets go even more of the control they let the employee buy the device by themselves, but with money from the organisation, if it will be a private or proprietary device may vary. The final step in device freedom is when the organisation is completely left outside the devices and the employee use their own private device even at work. This gives us three ways to see manage these devices, figure 1. In this article, the strategies that fall under BYOD or CYOD are of interest.
2. METHOD

This study uses a qualitative research methodology. First, a literature review was conducted with an approach from Webster and Watson (2002). The steps used in the literature review were:

1. An extensive literature search using the WorldCat search engine with different search terms connected to BYOD.
2. Manual screening for relevance (where relevance requires that the article both falls within the mobile/dual-use definition and focuses on policy, management or strategic issues, rather than technical issues).
3. Backward chaining by reviewing the citations in the articles identified as relevant in step 2.

After a literature review, 12 semi-structured interviews were conducted with CIO, CSO, CFO, CSIO or head of IT in food industry, manufacturing industry, defence industry, health care, municipality and different types of consulting firms. The size of their organisations goes from 50 to 15 000 employees. The objective is ‘to gather data on attitudes, opinions, impressions and beliefs of human subjects’ (Jenkins 1985).

Data analysis was conducted using content analysis (Silverman 2001; Berelson 1952; Krippendorff 2004). As a technique, content analysis yields ‘a relatively systematic and comprehensive summary or overview of the dataset as a whole’ (Wilkinson, 1997;170). It operates by observing repeating themes and categorizing them using a coding system. Categories can be elicited in a grounded way or can (as in our case) originate from an external source such as a theoretical model (Wilkinson 1997). The coding scheme was developed from the framework presented in the next section.

2.1 Analysis Framework

Webster and Watson (2002) also require that a literature review be concept-centric, where the concepts determine the ‘organizing framework’ of the review. Concepts may derived from the analysis, but a common practice is to adopt a suitable conceptual framework from the literature. Brodin (2015) created a framework for BYOD adoption which later was used by Brodin et al. (2015) to identify management issues for BYOD. The chosen framework for this paper derived from the seven BYOD management issues, figure 2, that Brodin et al. (2015) identified before moving on to designing a strategy.
3. **BYOD**

In literature about BYOD there are three main benefits that usually are highlighted; increased personal productivity, increased flexibility of time and place and increased user satisfaction (Brodin et al. 2015). Studies show that users which are allowed to use the same device for both private and work purpose works a lot more than others and saves hundreds of hours each year for their company (Miller & Varga 2011; iPaaS 2011; Barbier et al. 2012). This is due to the flexibility to work whenever and wherever the employee wants. This flexibility may not only be a benefit, not to the private life at least. In a study the respondents talks about how their partners are planning holidays where there is no mobile coverage or caught them in the middle of the night reading e-mails (Orlikowski 2007). Another study concluded that this flexibility is proven to increase work overload (Yun et al. 2012). While the increased use of mobile devices may harm the family life, a life without mobile devices could be painful for the user. In a study by iPaaS, 52 percent gave a negative emotional response to a week without their mobile device and almost 50 percent said that their mobile work environment contributed positively to their overall health (iPass 2011).

The mobile work climate will lead to a work and private life overlap and if the user do not have to switch between a personal and a work device the satisfaction will increase. A side effect will be that personal and work data may be mixed and questions about privacy may be raised. (Anderson 2013) Users tend to resist functions like encryption and remote wipe, when they are forced to them by their organisation, they consider that it encroaches on their privacy (Pettey & Van Der Meulen 2012). This makes it more difficult for the organisation to make sure that all devices that contain organisational data are secured to a minimum level. With devices all around the world with questionable security level the control over the information gets harder to keep. What will happen to the data when the device that it is stored on is lost or stolen, or if the employee leaves the organisation?

The security awareness is a problem in a lot of organisations. In a survey, 40 % said that they do not update their software and 25 % did not understand why you should update at all (Skype et al. 2012). Another study showed that even if the device is updated the security level is low; only 10 % of all tablets and 25 % of all smartphones got auto-locking and for laptops the share is 33 % (Camp 2012). Walker-Brown (2013) observes that “users only think about security when they either lose their data, or are blocked from accessing it”, which seems to be true according to the surveys above. Another awareness problem comes with the policies, there are a lot of studies that shows that users do not obey and in many cases not even aware of BYOD and security policies (Cisco 2013; Oliver 2012)

Support for BYOD is a tricky question, the users expect the same level of support as they had with their company owned standard devices (Brooks 2013). At the same time causes the new flora of devices, with different operating system, problem for IT managers and their existing IT infrastructures (Intel 2012). This gives an increasing cost for support and administration, which reduces productivity in other areas for the IT professionals (Walters 2013). In the end, the saved money from devices were eaten up by increased cost of managing the IT environment (Harris et al. 2012).
Table 1. Management issues for BYOD

<table>
<thead>
<tr>
<th>Management issues</th>
<th>BYOD</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. <em>personal productivity</em></td>
<td>Increase since the employees can work from any place at any time and go a device that they are familiar with.</td>
</tr>
<tr>
<td>2. <em>time/space flexibility</em></td>
<td>Very high</td>
</tr>
<tr>
<td>3. <em>user satisfaction</em></td>
<td>High, since they use a device they know and like. Although lower if they used to CYOD.</td>
</tr>
<tr>
<td>4. <em>information control</em></td>
<td>Unsure, organisational data may remain on private devices.</td>
</tr>
<tr>
<td>5. <em>device protection</em></td>
<td>Up to the user.</td>
</tr>
<tr>
<td>6. <em>awareness</em></td>
<td>More important since private, uncontrolled devices are used.</td>
</tr>
<tr>
<td>7. <em>support</em></td>
<td>Problem mainly for the network. Complex with a lot of different devices with no control software.</td>
</tr>
</tbody>
</table>

4. CYOD

When the users are allowed to choose their own devices without having to pay for them, a lot of the benefits from BYOD occur and a bit more control remains in the organisation. A key here is that the employer own the device and got the right to some control in exchange, the employee is allowed to, to some extent, also use the device for private purpose. The respondents, which uses CYOD, had a problem to see any argument for changing to BYOD. As one of the respondents said: “Yes, we would have saved some hundred dollars every year if we had asked staff to bring their own devices, get the installations and the images they need to do their job. But then we lose a competitive advantage that we have over our competitors. Then the staff would say; okay, I’ll now have to pay €1500 every two years out of my own pockets, just to get the right tools to do my job. And then they start at our competitors instead.”

So, what are the benefits with CYOD? Compared to a non-mobile or strictly on workplace strategy we got, just like BYOD, flexibility of time and place. That comes, of course, with every strategy that allows the user to bring their device outside the organisation wall. Almost all respondents said that one of the most important benefits with go-mobile is that their users can work whenever and where ever they like. Although not everyone sees this as a pure benefit, four of the respondents highlighted this as a problem, if the employees start to work more or less 24 hours a day and gets available even after regular working hours. In one of these organisations they just implemented a system where the employees got two phone numbers, one which the colleagues and clients gets and that is turned off after work hours and one for friends and relatives. The other three had had discussions about turning off mail-sync on evenings and weekends or instructing managers to think about the time they send email to their employees.

Personal productivity is raised both as a benefit and a threat. Most of the respondents can see an increased productivity connected to the new flexible way to work, although one respondent could see a risk that the users started to pay more attention to private social media and games during work hours and thus reduces productivity. Two of the respondents thought that the benefit of employees working on private time is eaten up by the time they spend on private internet browsing and mailing during work hours.

When it comes to user satisfaction, it is more about convenience than who owns the device. If the user is allowed to use the device for private purposes as well and do not need to carry, for instance, two smartphones the satisfaction level will increase. On the other hand, the satisfaction rate depends on what the user got before. Almost all respondents say that their employees do not want to go from CYOD to BYOD. One respondent replied to the question about BYOD with; “Yes, though it's not interesting in Sweden. It adds nothing. There is no potential for it. There is no way for it financially and no incentive to do that so it's not a fact as I see it.”
Although CYOD brings a lot of positive things there are some concern. The concerns are based on the mobility and the increased exposure of information and devices. Or as one respondent expressed it: “The most dangerous thing we have, we'd rather not use mobile devices. But we have to, because otherwise we need to sit at the customer at all times. Sometimes we have to take some risks but we try to avoid mobile media as far as possible.”

A major concern is control of information and the fact that information gets more exposed when it get outside the organisations walls. The biggest concern in this context is crosstalk and shoulder surfing while working on trains and other public places. The concern goes also to the private time: “You do not carry around on a computer when you are at the pub, but a phone, you can actually take with you to the pub.” One of the respondent said that their work with a mobile device strategy was motivated by taking back control. “We had said no to tablets and saw that we had 5-600 linked to our network, though we said no. It was just a paper policy, nothing else that ruled… This one had just grown freely. So the focus of making mobility was that we felt that we must take control over our mobile devices and ensure that the data stays at the company.”

Related to the concern about control is the one about device protection -how to keep information safe even if a device is lost or stolen. Some of the respondents felt safe with their MDM-tool and PIN-lock while others did not fully trust the safety functions on the phone in the same manner as the ones on the laptops. Although very few had experienced this threat in reality in any significant way.

Almost all respondents believed more in training than policies. “Since we think that the human is the weak link, we push hard on education.” It was a common sense that users do not fully understand and know the content of long policies. A lot of the respondent tries to keep their policies on one page and focus to work with education and the culture, at least in the SME. One example is to integrate the security in other context, like when introducing something new or at an internal annual sales conference. “We try and get it as an integral part, and not just a bunch of requirements and horrible policies, read 20 pages and sign you will get your... It should rather hang together and be natural in my opinion. And then we try to introduce it in a selling mode as well.”

One respondent thought that the employees are good at policies that concern them. “But it's just like, I do not know all the regulations surrounding shapes and colours that you can use, I have been reprimanded for that. ... Nah, I don't think it is possible, we have our field and must be clear in our communications and show good examples and be able to follow up. We have a mission to ensure information rivers, computers and data.” In one of the companies they try to avoid policies and believed in another form of communication. “From the company, we have said that we do not want to throw us into and become structurally organized in every detail, but we want the be a company that keeps our flexibility and employee's ability to think and make their own decisions, but if we notice that there is a problem, many make a mistake or in a way that is not good or many begin to come to me with questions, many are asking questions about the same thing. Then we see that there is a need to structure the information and make a policy to clarify things.”

The introduction of mobile devices has not increased the workload for the support team. Even though the total number of different devices in the organisation has increased, most of the respondents still got the same amount of employees in their service desk. This is due to smother synchronization tools and easy to use operating systems on the devices. And since all devices are owned by the organisation they can make sure that all accounts work, synchronization is in place and the device is connected to the right network before it is handed out to the user.
Table 2. Management issues for CYOD

<table>
<thead>
<tr>
<th>Management issues</th>
<th>CYOD</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. personal productivity</td>
<td>Increase since the employees can work from any place at any time and go a device that they are familiar with.</td>
</tr>
<tr>
<td>2. time/space flexibility</td>
<td>Very high</td>
</tr>
<tr>
<td>3. user satisfaction</td>
<td>High, since they choose device by themselves and do not have to pay for it.</td>
</tr>
<tr>
<td>4. information control</td>
<td>Information may be stored outside the organisation.</td>
</tr>
<tr>
<td>5. device protection</td>
<td>Organisation control the device.</td>
</tr>
<tr>
<td>6. awareness</td>
<td>Important</td>
</tr>
<tr>
<td>7. support</td>
<td>Organisation configure and control the device. Same pressure on service desk as before mobile devices.</td>
</tr>
</tbody>
</table>

5. COMPARISON AND DISCUSSION

In many ways, BYOD and CYOD are quite similar. The perceived benefits are the same, both solutions provide increased productivity, flexibility, and user satisfaction. In the interviews the respondent felt that a user that can choose any device they like but do not have to pay for it do not want to start pay for the same device. A company owned device, which the user is allowed to use for private purposes as well gave a higher value than if the user had to bring their own device. Although using only a private device are better than a strictly work device.

The main difference is found in what the literature describes as concerns, in this case the control and protection of information and devices. The control part is largely the same, when the information leaves the organisation's safe embrace creates a concern. Where is the information? Regardless of whether the unit is private or not, there is a high risk that the organisation's data is mixed with private data, and in the end, it will be difficult to distinguish on who owns what. For BYOD there is an extra factor which creates even more concern; what will happen to the data when the employee leaves the organisation? The person will still keep the device where the data is stored.

When a device is private, the responsibility for the protection of it are handed over to the user. The move from organisational control of the device to private raises a lot of security concerns and increases the demand on the user for security awareness. This concern still exists for CYOD, but since the device, in a broader sense, are controlled by the organisation the concern is more related to the trust on the technology.

Security awareness has always been important and with the new mobile climate it is even more important, no matter who owns and controls the device. Since the organisation can force the user to adjust to a minimum level of security on the device the organisation control the awareness is even more important for users of private devices. They have to understand why the security is needed and what can happen if the device not meet the requirement.

The impact on the support has been discussed in literature about BYOD and it goes from very little to major impact. The problem is not the devices by themselves, most of the users know their device and how to handle them. The problem is more about making them work in the organisational infrastructure and connect to the right resources. For CYOD, this become less of a problem since the IT department configure the device and make sure it works in the environment before handing it over to the end user. With BYOD there may be a lot of devices in the network, since a single user may bring a lot of private devices, for CYOD the organisation know exactly how many devices each employee got and how much pressure the network has to handle.
Table 3. Comparison of management issues for BYOD and CYOD

<table>
<thead>
<tr>
<th>Management issues</th>
<th>BYOD</th>
<th>CYOD</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. personal productivity</td>
<td>Increase since the employees can work from any place at any time and go a device that they are familiar with.</td>
<td>Increase since the employees can work from any place at any time and go a device that they are familiar with.</td>
</tr>
<tr>
<td>2. time/space flexibility</td>
<td>Very high</td>
<td>Very high</td>
</tr>
<tr>
<td>3. user satisfaction</td>
<td>High, since they use a device they know and like. Although lower if they used to CYOD.</td>
<td>High, since they choose device by them self and do not have to pay for it.</td>
</tr>
<tr>
<td>4. information control</td>
<td>Unsure, organisational data may remain on private devices.</td>
<td>Information may be stored outside the organisation.</td>
</tr>
<tr>
<td>5. device protection</td>
<td>Up to the user.</td>
<td>Organisation control the device.</td>
</tr>
<tr>
<td>6. awareness</td>
<td>More important since private, uncontrolled devices are used.</td>
<td>Important</td>
</tr>
<tr>
<td>7. support</td>
<td>Problem mainly for the network. Complex with a lot of different devices with no control software.</td>
<td>Organisation configure and control the device. Same pressure on service desk as before mobile devices.</td>
</tr>
</tbody>
</table>

6. CONCLUSIONS

In this article we investigated the difference between BYOD and CYOD from a management perspective. We have conducted a structured literature review and interviewed 12 CIO’s in different organisations, both private and public. Our findings is that most of the benefits that come with BYOD also come with CYOD, but the concerns may not give the same impacts.

• RQ1: Which managerial issues are connected to both BYOD and CYOD?

Our findings are that it is mostly the benefits that are connected to both approaches. The personal productivity does apply to both, although for inexperienced users it may be a greater profit with BYOD. This since they will use something they already know, on the other hand, with CYOD, they will probably select the kind of device that they already are familiar with. If a CYOD device is allowed to be used even for private purposes the increased flexibility of time and space will be the exact same for both BYOD and CYOD. These two benefits will, in both cases, lead to an increased user satisfaction.

• RQ2: What is the difference between BYOD and CYOD from a managerial perspective?

Most of the differences appear around the security aspects, how to protect information on mobile devices. When a device is owned by the organisation they have more control of the device and can apply policies to it. On a privately owned device, it is up to the user to secure the device and its information. When an employee leaves the organisation a CYOD device can be completely erased, but for a BYOD device, it is up to the user to remove all data that belongs to their former employer. If the user allows the employer to use an MDM-tool on their device, the control gap between CYOD and BYOD decreases. Another issue that separates CYOD from BYOD is the possibility of deeper investigation in cases of suspected policy violation. If the device is CYOD the employer can take the device and commit a forensic investigation, if it is BYOD the employer has no right to apprehend the device and cannot carry out the investigation. Furthermore, the workload for the IT-department increases when handling BYOD. With BYOD the user can have more than one device on the network, which requires more network capacity and secondly, more devices require more help from the IT-Support.

Our conclusion is that, even if the cost of the devices themselves are higher with CYOD, the increased level of security and information control outweigh the economical disadvantages.
REFERENCES

Kane, C. et al., 2014. Building The Business Case For A Bring-Your-Own-Device (BYOD) Program,
Oliver, R., 2012. Why the BYOD boom is changing how we think about business it. Engineering and technology, 7(10), p.28.
Management of Mobile Devices – How to Implement a New Strategy

Martin Brodin, University of Skövde, Skövde, Sweden, martin.brodin@his.se

Abstract.

Since smartphones entered the market the need for them has exploded, today 85% believe that their mobile is a central part of their life. Despite the major focus on mobile devices and increased budgets, there are still many organisations missing a strategy for mobile devices. This article investigates the most important steps to take when implementing a mobile device strategy by conducting an empirical study with interviews with CIO or equivalent roles in 13 organisations with 50 to 15 000 employees. The result is an improved framework for mobile device implementation.

Keywords: Information Management, Mobile Device, 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 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 (Muth 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.

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. This is something which 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 CIO or equivalent roles. 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 CIO or equivalent roles in 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
Mobile device strategy in literature

Brodin (2015) has developed a framework (figure 1) for managing strategies for mobile devices from the first analysis to completely 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** – 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 comes 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 & Phil 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**

Literature that falls under 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; get one and keep it up to date (Oliver 2012; Harris et al. 2012; Gatewood 2012; Montañá 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**

Apart from some articles that 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 introduction of mobile devices.

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.

In our literature review, we found a major gap when it comes to 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 CIO, CSO, CFO, CSIO or head of IT in the 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. All interviews were recorded and transcribed and lasted approximately 45 minutes. The information provided by participants is kept strictly confidential. The coding was conducted using a qualitative data analysis software with codes from the framework, in section 2. The codes from the framework were then complemented with additional codes 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 our interviews we instead found three new categories; communication, training and adjustment.

Not planning, but communication

Although our theoretical model said planning, we found that communications is a more central thing in the 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 he 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 with technology; it must be solved with methods.”

Another respondent testified that a policy without anchoring of the staff is useless. “When we looked at how many 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 theoretical model indicate.
Not implementation, but training

Although it is not just about communication of a new strategy or policy, the employees also need to understand the core value of it and how they are expected to use their device to gain the most benefits and minimizing risks. One organisation with a lot of 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 respondents’ 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 gets differs between organisations, five of the respondents said that their organisation provide 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 just provide some training and think everyone will do as you told them. 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 the change in approach.”

In some cases, the training is done on a regular basis, mostly with a focus on security. Usually the reason behind it are demands of customer 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 did not arrange any kind of training connected to the mobile devices.

Having a subtitle in action called implementation could be confusing since most of the things in action is about implementation. Training on the other hand is an important task that needs to be highlighted and performed.

Not evaluation, but adjustment

Our theoretical model highlights the importance of evaluation, but in our empirical study only four did an evaluation after the implementation. Some did a proof of concept, before the implementation, which were 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 do frequently.”

That could be a way to evaluate, a problem with evaluation is in some case 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 can I control how many completed the course and you can put controls on control issues on how well people understand these questions.” Since it is so hard to evaluate it is more common to with follow-ups, informal discussions and topic on the agenda at management meetings than a full evaluation and analysis again after the strategy is implemented. Or 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 done in general. More common are small, 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 theoretical and based on standards and well known literature. In literature, there is a gap when it comes to the implementation of mobile device strategies, in this study we have looked at implementation in practice to reduce that gap and 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 appears in the strategy, adjustments are made.

This gives us the framework in figure 2, were Analysis and Design remain the same as in the original framework. After the initial work with analysis and design the work move into an iterative process where the strategy is communicated and training are 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 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.](image)

**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 the culture and to educate and communicate. Of course there are policies in the organisation, but they are often short and more general. It is well known from the literature that employees seldom read, understand and follow policies and with that in mind it seems to be a good plan to focus on the humans instead of writing a document if you really want a 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 paces and they do tend to forget. That is why the communication needs to be supported with training and this is not just 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 the organisation in all Europe. Further we only conducted 13 interviews, we can see a trend but not make any general 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 new strategy for mobile devices.

References


Salesforce, 2014. 2014 Mobile Behavior Report,


PUBLICATIONS IN THE DISSERTATION SERIES
PUBLICATIONS IN THE DISSERTATION SERIES

Martin Brodin is an industrial PhD student at Actea Consulting AB and the University of Skövde. When he is not working on his thesis he is helping organisations with issues related to information security.