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-mharie.ahlfeldt@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*.

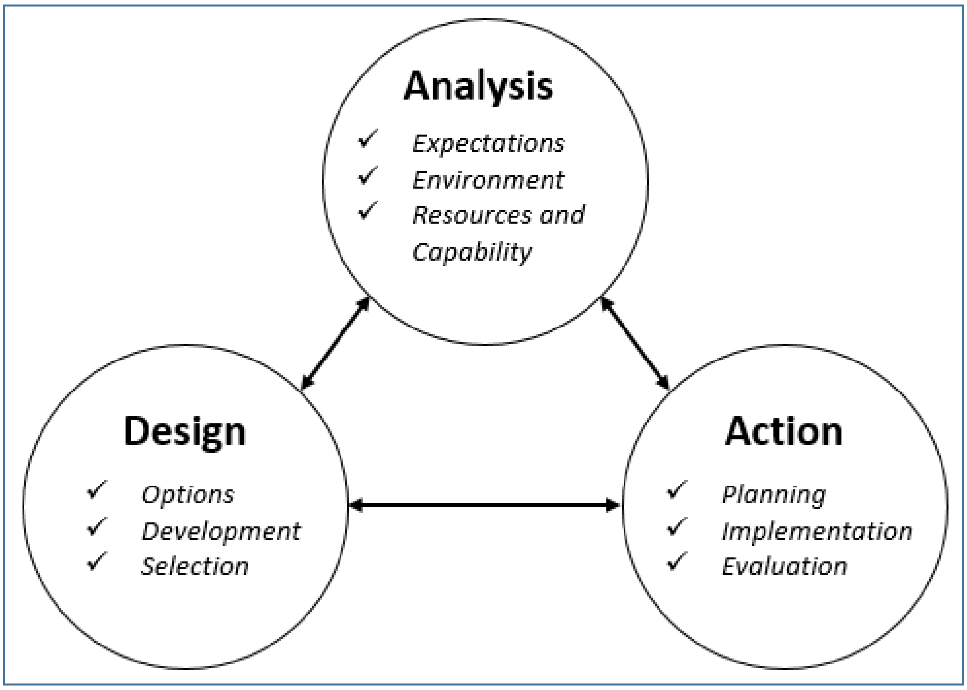

Figure 1. Framework for the analysis, adapted from Brodin (2015).

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.

Category	Number of articles
Analysis	52
• Expectations	11
• Environment	33
• Resources & capability	8
Design	31
• Options	15
• Development	13
• Selection	4
Action	0
• Planning	0
• Implementation	0
• Evaluation	1
Total	85

Table 1. Distribution of articles by category.

3 MANAGEMENT ISSUES FOR BYOD

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

3.1 Analysis

Analysis concerns the assessment of opportunities and threats involved in the adoption of BYOD, including *expectations, environment*, and *resources and capability.*

3.1.1 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 *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 *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 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 (Tokuysohi, 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. Mourmant 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.

Framework category		**BYOD management issues**	**BYOD research agenda**
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	options	*8. strategic options*	improvement of normative models of strategic options based on empirical evidence and theory
	development	*9. security policy update* *10. regulatory framework*	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

Allam S., Flowerday S.V. and Flowerday E. 2014. 'Smartphone information security awareness: A victim of operational pressures', Computers & Security, 42(2014): 56-65.

Ashenden, D. and Lawrence D. 2013. 'Can We Sell Security Like Soap? A New Approach to behaviour Change'. The 2013 workshop / New security paradigms workshop (NSPW '13), Banff, Canada.

Barbier. J., Bradley J., Maculay J., Medcalf R. and Reberger C. 2012. 'BYOD and Virtualization: Top 10 Insights from Cisco IBSG Horizons Study'. Cisco IBSG.

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

Brodin, M. 2015 'Combining ISMS with strategic management: the case of BYOD'. 8th IADIS International Conference on Information Systems (IS 2015), Funchal, Madeira, Portugal.

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

Caldwell, T. 2012. 'The dangers facing data on the move'. Computer Fraud & Security. 2012(12): 5-10.

Camp, C. 2012. 'The BYOD security challenge: How scary is the iPad, tablet, smartphone surge? '. ESET Threat Blog. URL: http://blog.eset.com/2012/02/28/sizing-up-the-byod-security-challenge (visited July 2013).

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

Gatewood, B. 2012. 'The Nuts and Bolts of Making BYOD Work'. The Information Management Journal. 46(6): 26-31.

Green, N. 2002. 'On the Move: Technology, Mobility, and the Mediation of Social Time and Space'. The Information Society, 18(4): 281–292.

Guinan, P. J., Parise S. and Rollag K. 2014. 'Jumpstarting the use of social technologies in your organization'. Business Horizons. 57(3): 337-347.

Györy, A., Cleven, A., Uebernickel, F. & Brenner, W. 2012. 'Exploring the shadows: IT governance approaches to user-driven innovation'. ECIS 2012, Barcelona, Spain.

Harris J., Ives B., & Junglas I. 2012. 'It consumerization: When gadgets turn into enterprise IT tools'. MIS Quarterly Executive. 11(3): 99-112.

Holleran, J. 2014. 'Building a Better BYOD Strategy'. Risk Management, 61(7): 12-13.

Wu, H. 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.

Intel 2012. 'Insights on the Current State of BYOD in the Enterprise – Intel's IT Manager Survey'. URL: http://www.intel.com/content/dam/www/public/us/en/documents/white-papers/consumerization-enterprise-byod-peer-research-paper.pdf (visited July 2013).

Ipass 2011. 'The iPass Global Mobile Workforce Report - Understanding Enterprise Mobility Trends and Mobile Usage'. URL: http://mobile-workforce-project.ipass.com/cpwp/wp-content/uploads/2011/11/ipass_mobileworkforcereport_q4_2011.pdf (visited January 2014).

ISO/IEC 27001 2013. ISO/IEC 27001:2013 – Information Technology – Information Security Management Systems – Requirements.

ISO/IEC 27002 2013. ISO/IEC 27002:2013 – Information Technology – Security Techniques – Code of practice for information security controls.

Johnson, G. and Scholes K. 1997. 'Exploring Corporate Strategy: Text and Cases'. Hemel Hempstead: Prentice Hall Europe

Jones, A., Martin T. and Alzaabi M. 2012. 'The 2012 Analysis of Information Remaining on Computer Hard Disks Offered for Sale on the Second Hand Market in the UAE'. SRI Security Research Institute, Edith Cowan University, Perth, Western Australia.

Kahn, W.A. 1990. 'Psychological conditions of personal engagement and disengagement at work'. Academy of Management Journal 33(4): 692-724.

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

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

Millard, A. 2013. 'Ensuring mobility is not at the expense of security'. Computer Fraud & Security. 2013(9): 11-13.

Miller, R.E. & Varga J. 2011. 'Benefits of Enabling Personal Handheld Devices in the Enterprise'. Intel Corporation.

Montaña, J. C. 2005. 'Who Owns Business Data on Personally Owned Computers'. Information Management Journal. 39(3): 36-40,42.

Mooney, J. L., Parham A. G. and Cairney T. D. 2014. 'Mobile Risks Demand C-Suite Action!'. The Journal of Corporate Accounting & Finance. 25(5): 13-24.

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

Mourmant G., Niederman F. and Kalika M. 2013. 'Spaces of IT intrapreneurial freedom'. 2013 annual conference / Computers and people research (SIGMIS-CPR '13). ACM, New York, USA.

MSB 2015. Swedish Civil Contingencies Agency. Framework for information security management systems. URL: https://www.informationssakerhet.se/sv/Metodstod/ [accessed 2015-04-12](in Swedish).

Niehaves, B., Köffer, S., and Ortbach, K. 2012. 'IT consumerization–a theory and practice review'. AMCIS 2012. Seattle, USA.

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).

Pfeffer, J. 1995. 'Competitive advantage through people: Unleashing the power of the work force' 1995: Harvard Business Press.

Readwrite 2013. 'BYOD by the Numbers'. [Infographic] Say Media Inc. URL: http://readwrite.com/2013/03/26/intel-byod-by-the-numbers (visited July 2013).

Ring, T. 2013. 'A breach too far?'. Computer Fraud & Security. 2013(6): 5-9.

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

Simkin, S. 2013. 'Cisco Security Intelligence - Annual Security Report & Cisco Connected World Technology Report'. URL: http://www.cisco.com/en/US/solutions/ns341/ns525/ns537/ns705/ns1120/ASR_CCWTR_Summary.pdf (visited July 2013).

Singh, N. 2012. 'B.Y.O.D. Genie Is Out Of the Bottle – "Devil Or Angel"'. Journal of Business Management & Social Sciences Research (JBM&SSR). 1(3): 1-12.

Skype, Norton by Symantec and Tom Tom 2012. 'Survey finds nearly half of consumers fail to upgrade software regularly and one quarter of consumers do not know why to update software'. URL: http://about.skype.com/press/2012/07/survey_finds_nearly_half_fail_to_upgrade.html (visited July 2013).

Steiner, P. 2014. 'Going beyond mobile device management'. Computer Fraud & Security. 2014(4): 19-20.

Stevenson K. 2012. 'Accelerating Business Growth through IT - 2012-2013 Intel IT Performance Report'. Intel Corporation.

Thielens, J. 2013. 'Why APIs are central to a BYOD security strategy'. Network Security. 2013(8): 5-6.

Tokuyoshi, B. 2013. 'The security implications of BYOD'. Network Security. 2013(4): 12-13.

UNICEF 2014. 'Om föräldrars tillgänglighet i mobilen efter arbetstid'. URL: http://blog.unicef.se/wp-content/uploads/2014/05/UNICEF_Faktablad_barnr%C3%A4ttsprinciperna.pdf (visited May 2014).

Van Der Meulen, R. and Rivera J. 2013. 'Gartner Predicts by 2017, Half of Employers will Require Employees to Supply Their Own Device for Work Purposes'. Gartner Inc. URL: http://www.gartner.com/newsroom/id/2466615 (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.

Walker-Brown, A. 2013. 'Managing VPNs in the mobile worker's world'. Network Security. 2013(1): 18-20.

Walters, R. 2013. 'Bringing IT out of the shadows'. Network Security. 2013(4): 5-11.

Webster, J. and Watson R.T. 2002. 'Analyzing the past to prepare for the future: Writing a literature review'. Management Information Systems Quarterly, 26(2): xiii-xxiii.

Wilson, J. 2012. 'Enterprises rate mobile device security vendors, reveal BYOD concerns. Infonetics '. URL: http://www.infonetics.com/pr/2012/Enterprise-Mobile-Security-Strategies-Survey-Highlights.asp (visited July 2013).

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(5): 9.

Yang, T. A., Vlas R., Yang A. and Vlas C. 2013. 'Risk Management in the Era of BYOD: The Quintet of Technology Adoption, Controls, Liabilities, User Perception, and User Behavior'. 2013 International Conference on Social Computing (SocialCom). Washington D.C., USA.