2015

Mobility and Security in the New Way of Working: Employee Satisfaction in a Choose Your Own Device(CYOD) Environment

Arjan de Kok
Utrecht University, The Netherlands, a.dekok@uu.nl

Yvette Lubbers
Utrecht University, The Netherlands, i.lubbers@uu.nl

Remko W. Helms
Utrecht University, remko.helms@ou.nl

Recommended Citation

de Kok, Arjan; Lubbers, Yvette; and Helms, Remko W., "Mobility and Security in the New Way of Working: Employee Satisfaction in a Choose Your Own Device(CYOD) Environment" (2015). *MCIS 2015 Proceedings*. 31.
http://aisel.aisnet.org/mcis2015/31

MOBILITY AND SECURITY IN THE NEW WAY OF WORKING: EMPLOYEE SATISFACTION IN A CHOOSE YOUR OWN DEVICE (CYOD) ENVIRONMENT

Complete Research

Arjan de Kok, Department of Information and Computing Sciences, Utrecht University, Utrecht, The Netherlands, a.dekok@uu.nl

Yvette S. Lubbers, Department of Information and Computing Sciences, Utrecht University, Utrecht, The Netherlands, i.lubbers@uu.nl

Remko W. Helms, Department of Information and Computing Sciences, Utrecht University, Utrecht, The Netherlands, r.w.helms@uu.nl; Faculty of Management, Science & Technology, Open University, Heerlen, The Netherlands, remko.helms@ou.nl

Abstract

The consumerization of IT, known as Bring Your Own Device (BYOD), is an inevitable component in the future IT infrastructure of organizations. It is not the question if employees will use consumer IT products for their work, but how and under which conditions. The use of personalized mobile devices may be beneficial for both the employee and organization, but the concern of IT executives, on corporate data residing on uncontrolled mobile devices, is often leading to a restrictive policy. Giving employees the ability to choose from a variety of secure devices, at the expense of the organization, Choose Your Own Device (CYOD), may well bring the best of two worlds. In this research 126 employees at four multinational organizations were surveyed on their perception of usability and satisfaction of devices for their knowledge tasks. The outcomes were matched against a Risk Assessment on seven identified IT threats. The results show that a majority (52%) believes their performance would improve, when given the ability to choose a device of their own. The Risk Assessment shows that IT security risks do not need to increase, provided that the proper security policies are in place. This implies that the performance and satisfaction of employee can improve in a secure CYOD environment.

Keywords: New Way of Working (NWOW), Choose Your Own Device (CYOD), Bring Your Own Device (BYOD), Consumerization.

1 Introduction

In the new world of work the use of consumer IT for business purposes, consumerization or Bring Your Own Device (BYOD), has seen a tremendous flight in the past years (Gillett, 2012; Citrix, 2013). Employees perceive personal devices to be more useful, more powerful, easier to use, and more fun than enterprise IT, and often they are (Harris et al., 2012). Personal devices have become inexpensive and the software apps are low cost or for free. On the other side, IT executives have concerns, mainly about data security, when employees view and use corporate information on their own mobiles, tablets and other personal devices. Also, BYOD confronts IT departments with a wide variety of software platforms that are used to connect to the corporate network, on devices that are renewing at a much faster pace than upgrades that were rolled out in the past. The reaction is often a push towards tight control, imposing restrictive, and often performance-taking, software on employees' devices. The question that is now raised by employees is: "Should I be the one to pay for working more effective and pleasurable, while receiving corporate control over my privately owned hardware?" This results in a situation that makes both parties feel uncomfortable.

A solution that seeks to find a 'middle-way' in this impasse is Choose Your Own Device (CYOD). Choose Your Own Device enables employees to choose, against no personal costs, the devices that they feel suit them best in the tasks they need to perform, whilst allowing the organization to supply enterprise-controlled technology. Having the benefits of both worlds, CYOD is growing in popularity, especially in larger organizations. Where there is existing research on BYOD, research in the field of CYOD policies, especially in the light of IT security, and in the context of the New Way of Working, is scarce if not at all absent.

The research question is: Can a CYOD policy contribute to a perceived improvement in employee performance and satisfaction, in a secure way? In this research 126 employees were surveyed at four large organizations, that had chosen for a CYOD policy, whilst seeking the optimum of IT security and user satisfaction. The context of this CYOD environment (at least for the Dutch divisions of these companies), was the New Way of Working. The following chapter (2) briefly describes the context of the New Way of Working and CYOD, the tasks of knowledge workers and threats in IT security. The research method is explained in chapter 3 as well as the Technology Acceptance Model that is used for the determination of the device usefulness and user satisfaction. Chapter 4 discusses the research results. This leads to a number of conclusions and recommendations for future research in chapter 5.

2 Theoretical background

2.1 The New Way of Working

Where in the past many authors e.g. Hammer & Champy (1993) envisioned a 'New World of Work', with information technologies as rule-breaking for the way business processes would change, the last decade has shown an increase in pace in which new ways of working are being adopted in organizations. Bødker & Christiansen (2002) were one of the first to observe that 'new work is characterized by a mobile, networked technology, project-managed organization, and new office designs. The office designs are explicitly motivated by the wish to facilitate creativity, knowledge sharing and communication, carried out across a variety of settings: office, home, airports, coffee shops and cars' The creation of new office spaces that are breaking with all traditional rules and design concepts is probably one of the most visible effects of the New Way of Working (NWOW). Offices transform from dull production facilities to inspiring meeting places, in which no effort is spared to create a new sense and experience of work (Waber et al.,2014). At the same time employees enter into new working relations in which they have the freedom to decide when and where to work, and become responsible for their results instead of being measured by their 'presenteeism' at the office (Johns & Gratton, 2013).

Baane et al. (2010) add: 'The work principles of The New Way of Working give maximal freedom to employees, on the basis of mutual trust. This trust is expressed in the freedom that employees have for carrying out their work in ways, times and locations that suit them best. The employees are evaluated based on their personal or team contribution, rather than their presence. Thus the employees can engage in a working relationship that fits in terms of ambition, skills, lifestyle or stage of life'. The context of NWOW can be divided into three dimensions: Bricks, Bytes and Behavior. (1) Bricks, the physical dimension, addresses all aspects of the physical work environment, (2) Bytes, the technological dimension, that addresses all aspects concerning the use and application of ICT, and (3) Behavior, the personal dimension, which addresses all aspects concerning the manager-employee relationship and the way the employee works and experiences his or her work.

2.2 Knowledge tasks

The work principles of NWOW are best applied in the work environment of the 'knowledge worker' (Greene & Myerson, 2011). The term knowledge worker is not new: already in 1969 Drucker used the term knowledge worker for 'the man or woman who applies productive work ideas, concepts and information rather than manual skill or brawn'. The question is: which tasks are performed in the work environment of the knowledge worker, and which device would suit the execution of this task well, in the perception of the knowledge worker? Reinhardt et al. (2011) researched the roles and actions knowledge workers perform. In their literature review they analyzed all the knowledge actions described by different authors (e.g. Davenport & Prusak, 1998) and combined them to one coherent list of knowledge actions. These tasks were used in the Employee Survey in this research. For an overview of the knowledge tasks and their description see Appendix 1.

2.3 Consumerization of IT

Mobility is an important aspect in the vision of the New Way of Working to work anywhere and anytime. For employees it is important to work with the devices that are best suited for their work, adding the 'work with anything' aspect to working anywhere and anytime. Moschella et al. (2004) were probably the first ones to coin the term Consumerization of IT (Ruch & Gregory, 2014). They concluded employees were often so frustrated with the existing IT infrastructure, that they chose to bring and use their own devices for their work. The work with personal consumer devices for business means is since called IT consumerization or Bring Your Own Device (BYOD). Giddens & Tripp (2014) define BYOD as 'the use of personal devices at work, on the workplace, to complete work-related activities'. Ingalsbe et al. (2011), Holtsnider et al. (2012), and Harris et al. (2011) use similar definitions for the dual use of devices for private and business purposes. The use of consumer IT devices for business purposes is expected to contribute to work performance and greater autonomy for employees (Niehaves et al., 2012, 2013). Murdoch et al. (2010) and Harris et al. (2011) add that employees using the technology of their own find it easier to use and important for their job satisfaction.

Though many companies struggle with this phenomenon, and often do not have a BYOD program in place, the reality is that employees already bring their personal devices to work (Gillett, 2012; Citrix, 2013). Forrester Research found that 52% of the information workers use three or more devices for work (Gillett, 2012). They predict that by 2016 there will be 760 million tablets in use, most for use both at work and at home (Gillett, 2012). As companies reap the benefits, but employees pay the cost, of the improved work performance, a number of companies decided to sponsor the use of personal devices. Sometimes this sponsoring goes under the condition of allowing company security controls on one's personal device. In particular the security aspects of protecting business data fragmentation on a broad range of personal devices is challenging to implement. ICT managers however realize this trend cannot be stopped, and therefore needs to be managed. Because of the security aspects, a number of organizations consider a Choose Your Own Device (CYOD) policy in which employees are allowed to choose from a range of mobile devices with pre-installed security management software in place, at no personal cost.

A CYOD policy can optionally be combined with a BYOD policy, for instance when users agree to have security software installed on their personal device as well, but often it is restrictive in the form of a Don't Bring Your Own Device (DBYOD) policy. In this case personal devices are not allowed to connect to the corporate network. In practice this means that employees in a DBYOD environment can only access the restricted guest network from their own device.

2.4 IT threats

An IT risk can be defined as the damage or impact an event or threat will cause, against the chance or probability of its occurrence (Baskerville 1993; Peltier, 2005). The chance of occurrence may be both erroneous human actions and attackers who attempt to abuse weaknesses in technical solutions. Mobile devices e.g. notebooks, tablets and smartphones are often used outside the corporate network. Mostly users are able to install software or apps, and connect to multiple public domains. Often users do not realize the potential damage this may cause. Morrow (2012) found that around 40% of the employees admit they do not update their (security)software, while unauthorized access to and information theft from endpoints has increased by malware, key loggers and cyber-attacks. Even when antivirus software is present, mobile malware can be effective, and steal user credentials.

Security risks constantly change over time, making research in this area time-bound. Whitman (2003) identified twelve categories of IT security threats of both human and technical ground. In the light of this research some categories were identified as not applicable (e.g. force of nature), or not essentially different for the types of researched devices. The results was the following list of seven IT security threats that were identified for this research:

	Threat	Examples
1	Act of Human Error or Failure	accidents, employee mistakes
2	Compromises to Intellectual Property	piracy, copyright infringement
3	Deliberate Acts of Espionage or Trespass	unauthorized access and/or data collection
4	Deliberate Acts of Theft	illegal confiscation of equipment or information
5	Deliberate Software Attacks	viruses, worms, macros, denial of service
6	Technical Hardware Failures or Errors	equipment failure
7	Technical Software Failures or Errors	bugs, code problems, unknown loopholes

Table 1. IT security threats (Whitman, 2003)

There are roughly three mechanisms to cope with IT security risks: (1) authentication, (2) network security and (3) device security. (1) Authentication is ‘the process of determining whether someone or something is, in fact, who or what it is declared to be’ (Rouse, 2007). When a user is authenticated, identity and access management can be applied. This security discipline ‘enables the right individuals to access the right resources at the right times for the right reasons.’ (Gartner, 2015). (2) Network security is the policy to prevent unauthorized access to the corporate network. Almost all corporate laptops nowadays use a VPN connection to access corporate data from an external connection. Information from a virtual private network is securely transported over a public network by encrypting the data to keep it confidential (Govcert, 2009). (3) Device security. This can be enforced using software such as a Mobile Device Management (MDM) tool. This software is installed on the mobile device and encrypts the (corporate) data. It enables the employer to monitor the entire device, push software updates, and remotely kill data stored on the device in case of loss or theft (Gajar et al., 2013). Ideally, organizations are able securely deliver corporate data to employees, without interfering with their access to personal apps and data. However, the ability to separate corporate data from personal data on a mobile device has its limits. E.g.: Was the picture taken by the camera a business whiteboard or holiday picture? Information security will therefore always be a balancing act of business interest versus personal freedom.

3 Research method

3.1 User acceptance models for IT

To determine the user acceptance of information technology, multiple models have been developed. In this section two models are discussed: the Person-Artifact-Task (PAT) model from the Flow theory, and the Technology Acceptance Model (TAM).

The Flow theory originates from Phychology. The psychologist Csikszentmihalyi (1975, 1988, 1990) found that people can be so absorbed in an activity, such as chess playing or rock climbing, that they excel in performance and lose track of time, without being aware of it. When personal computers were introduced, the Flow theory was used to address user experiences in computer-mediated environments (CMEs), such as the satisfaction and acceptance of information technology (Ghani, 1991). Based on the Flow theory, Finneran & Zhang (2002) defined the Person-Artifact-Task (PAT) model, in which activities are broken down into tasks and artifacts (tools), that need to be mastered by the user. The likelihood of an optimal (flow) experience depends on the interplay between the person, the task and the artifact. Kiili (2004) presents a framework of the factors in each stage of flow with the components of the PAT model, see Figure 1.

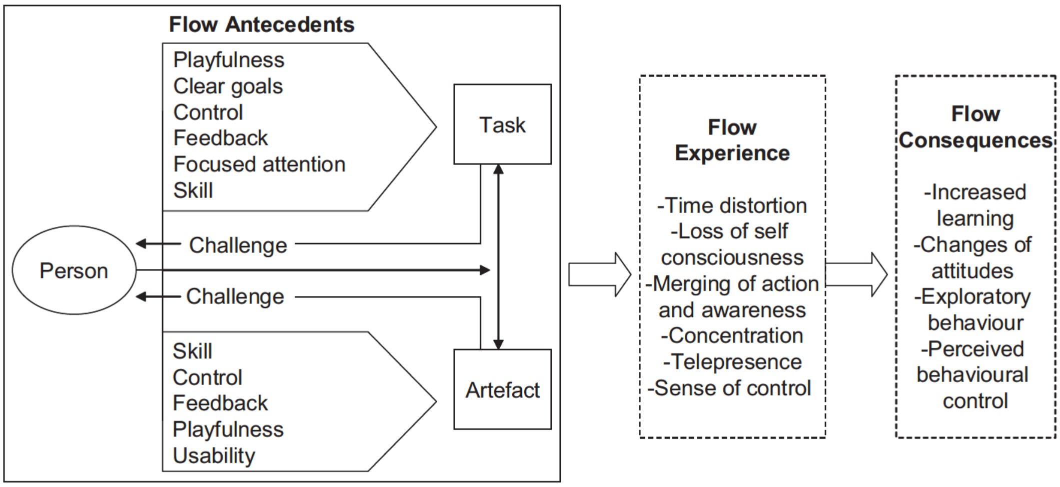


Figure 1. Person-Artifact-Task (PAT) model (Finneran and Zhang, 2002, Kiili, 2005)

In this framework the antecedents Speed and Ease of use (Skadberg & Kimmel, 2004), are combined as the Usability factor. Perceived ease of use (PEOU) is an established and validated construct in MIS literature (Davis, 1998; Venkatesh & Davis, 1996, 2000).

Based on the Theory of Reasoned Action (TRA) of Ajzen & Fishbein (1980), which suggests that people form intentions to adopt a behavior or technology based on their beliefs about the consequences of adoption, Davis (1998) builds the Technology Acceptance Model (TAM). In this model two major variables determine an individuals' information system acceptance; Perceived usefulness and Perceived ease of use. In the extended Technology Acceptance Model (TAM2), Venkatesh & Davis (2000) incorporate several additional attributes that influence system acceptance, e.g. Output quality. Figure 2 shows the extended Technology Acceptance Model.

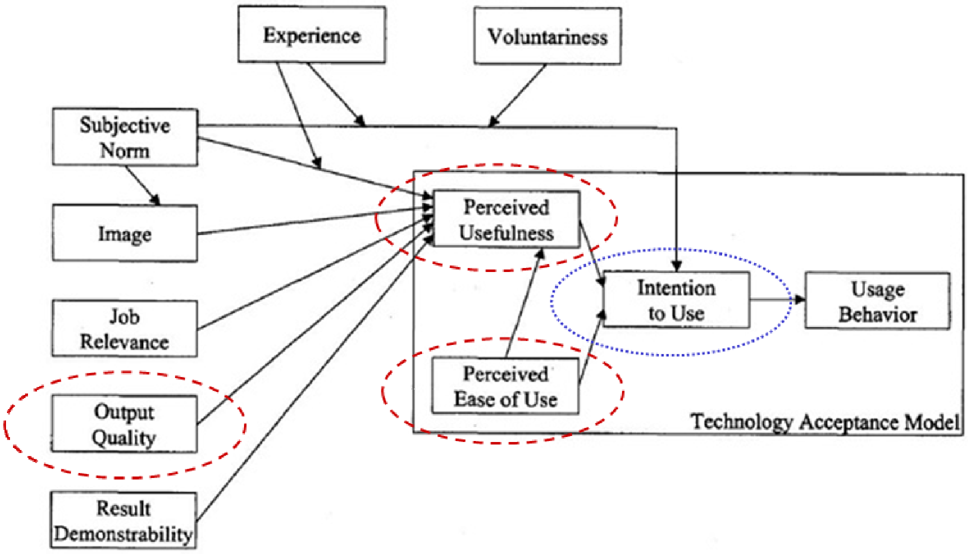


Figure 2. Extended Technology Acceptance Model (TAM2) (Venkatesh and Davis, 2000)

In Figure 2 the first three constructs, that are used in this research, have been circled with a red dashed line. They are defined by Venkatesh & Davis as follows: Perceived usefulness is the extent to which a person believes that using the system will support or enhance his or her work job performance. Perceived ease of use is the extent to which a person believes that using the system is or will be free of effort. Perceived usefulness is influenced by Perceived ease of use because, other things being equal, the easier the system is to use the more useful it can be. Output quality is the degree to which a person believes the system performs his or her job tasks well.

The fourth construct that is used in this research is (perceived) satisfaction. This construct is not as such in the TAM2 model, but it is related to the Intention to use, which therefore has been circled with a dotted blue line. Wixom & Todd (2005), who tried to combine the attributes from user satisfaction literature with the Technology Acceptance literature, warn that user satisfaction is limited in its ability to predict system usage. The question is therefore what leads to satisfaction and intended system use.

Giddens & Tripp (2014) suggest that device self-efficacy, personal innovativeness and device competence are the reasons for more job performance and satisfaction. They base their view on the Social Cognitive Theory of Bandura (1977), who defines self-efficacy as the extent to which a person believes in one's own ability to complete a task or reach a goal. In the context of CYOD, device self-efficacy is defined as 'the belief a certain device will enable a person to perform his or her task'. In this research satisfaction is defined as the combination of the perceived satisfaction (device self-efficacy) with the device preference. The device preference is measured by the number of people that would choose a certain CYOD device for a task (device competence). For an overview of the used constructs see the Employee Survey section on the left in Figure 4.

3.2 Employee Survey and Risk Assessment

For this research 126 respondents in four multinational organizations were surveyed. In order to observe corresponding findings across the companies, an overall study protocol was created (Yin, 2009). Besides the questionnaires on the use of devices and satisfaction, context interviews were held at the participating companies, to determine the (type of) CYOD policies. The four companies were:

Company 1 – a Dutch-headquartered Financial Accountancy firm, with 155.000 employees in 144 countries worldwide.

Company 2 – a 20.000 employee Media and learning multinational, headquartering in Finland.

Company 3 – a US-based multinational with business in Trading, Purchasing, Distributing grain and other Agricultural commodities, with 143.000 employees in 67 countries worldwide.

Company 4 – a Dutch-headquartered multinational producer of alcoholic beverages, with worldwide over 90.000 employees in 178 countries.

n the first section of the Employee Survey the respondents were asked which knowledge tasks they perform, and how their current device supports this task. Next, they were asked if they felt having a device of their own choice would improve their task performance, and if so, which device they would choose. Finally they were asked if they were willing to contribute in the device cost (see Figure3).

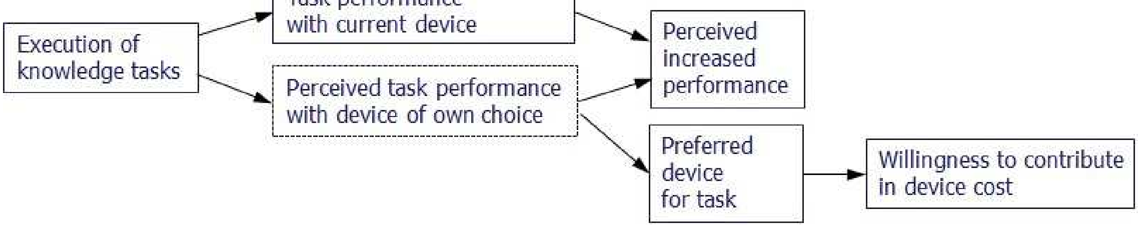
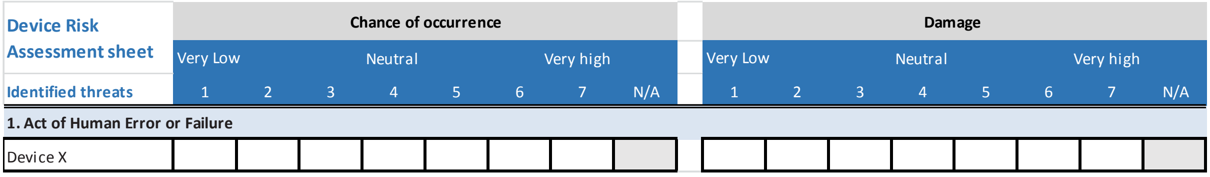

Execution of knowledge tasks
Task performance with current device
Perceived task performance with device of own choice
Perceived increased performance
Preferred device for task
Willingness to contribute in device cost

Figure 3. Employee Survey on tasks performance and preferred device

To determine the IT risks associated with the preferred CYOD devices, interactive Risk Assessments sessions were held with the IT Experts / Security Officers of the participating companies. For each device the IT risk was determined and calculated, using two variables: the chance a threat can occur and the damage it will cause when it occurs. For the 7 before mentioned identified threats, in each participating company the IT expert or Security Officer evaluated the IT threats per type of device. The chance of occurrence and damage were rated on a 1 to 7 point Likert scale, meaning the highest risk for a specific threat for a device could be 49. The overall IT risk per device was determined by taking the average of all multiplications. The table below shows part of the used Device Risk Assessment sheet.



Device Risk Assessment sheet	Chance of occurrence								Damage							
	Very Low			Neutral			Very high		Very Low			Neutral			Very high	
Identified threats	1	2	3	4	5	6	7	N/A	1	2	3	4	5	6	7	N/A
1. Act of Human Error or Failure																
Device X																

Table 2. Structure Risk Assessment sheet

In the second section of the Employee Survey the usefulness and satisfaction were investigated. The usefulness was determined based on the average of the first three constructs: Perceived usefulness, Perceived ease of use, and Quality of output. For the satisfaction, the fourth construct, Perceived satisfaction was combined (multiplied) with the score on preferred devices. The results of the Employee Survey were then combined with the Risk Assessment. This leads to the following analysis model:

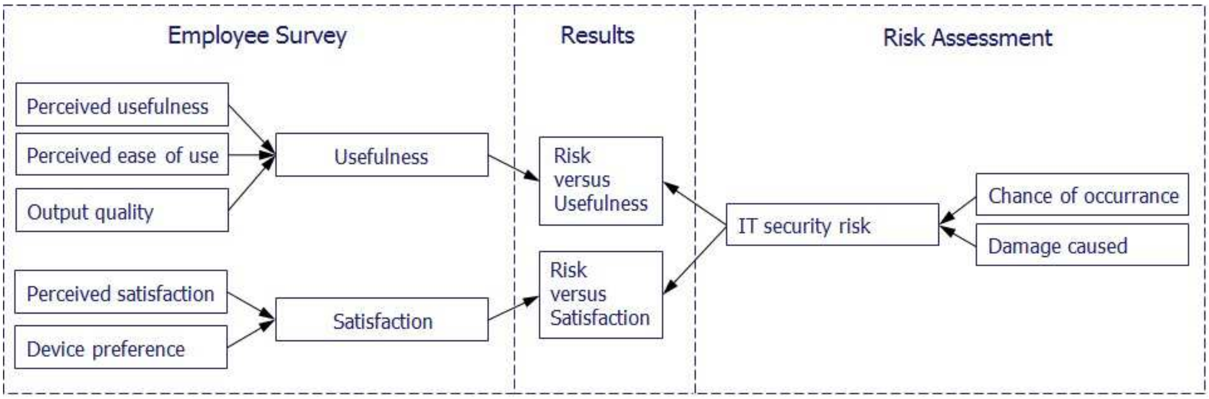
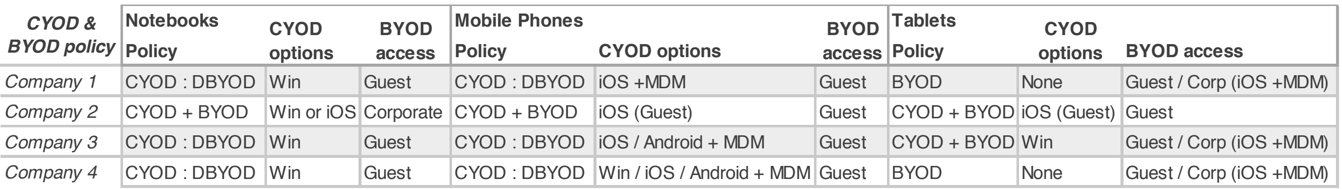


Figure 4. Analysis model

4 Research results

4.1 CYOD and related policies

In the context analysis, the CYOD policies were analyzed. All four companies have a CYOD policy in place, but the choices per device type differ. Also the use of own devices brought to the workplace differs per company. In most companies the use of own devices is restricted: Don't Bring Your Own Device (DBYOD), meaning personal devices can only be used on the guest network. Table 3 gives an overview of the CYOD policy and related policies at the participating companies.



CYOD & BYOD policy	Notebooks Policy	CYOD options	BYOD access	Mobile Phones Policy	CYOD options	BYOD access	Tablets Policy	CYOD options	BYOD access
Company 1	CYOD : DBYOD	Win	Guest	CYOD : DBYOD	iOS +MDM	Guest	BYOD	None	Guest / Corp (iOS +MDM)
Company 2	CYOD + BYOD	Win or iOS	Corporate	CYOD + BYOD	iOS (Guest)	Guest	CYOD + BYOD	iOS (Guest)	Guest
Company 3	CYOD : DBYOD	Win	Guest	CYOD : DBYOD	iOS / Android + MDM	Guest	CYOD + BYOD	Win	Guest / Corp (iOS +MDM)
Company 4	CYOD : DBYOD	Win	Guest	CYOD : DBYOD	Win / iOS / Android + MDM	Guest	BYOD	None	Guest / Corp (iOS +MDM)

Table 3. CYOD and related policies

Table 3 shows that companies 1,3, and 4 have a CYOD & DBYOD policy in place for notebooks and mobile phones. For tablets they have a BYOD policy in place, at company 3 combined with the CYOD option. These three companies use a Mobile Device Management, MDM, tool to control the IT security risks. Company 2 has no MDM software in place, but is nevertheless allowing BYOD notebooks on the corporate network. The company has recognized this is an IT risk. For mobile phones and tablets there is both a CYOD and BYOD policy, but all devices are excluded from the corporate network. This makes company provided CYOD devices (as well as BYOD devices) relatively useless to perform business tasks on.

4.2 Tasks and performance

The overview of the tasks (knowledge actions) the respondents perform is in Appendix 1. As knowledge workers often perform more than one task, the total number of tasks is higher than the number (126) of respondents; in total 405 tasks were mentioned, meaning the average respondent performs a bit more than three (3,2) tasks. Analysis, Acquisition and Information search are the most performed knowledge tasks. These observations (multiple tasks per user/role and most frequent tasks/knowledge actions) are in line with the research results of Reinhardt et al. (2011).

When asked if the respondents believed their tasks could be performed well with the device they currently use, 53% of the respondents agree and 18% strongly agree that their current device supports the execution of their tasks well. Yet, when asked if they believe that having a device of their own choice, would increase their task performance, the response is as follows (Figure 5):

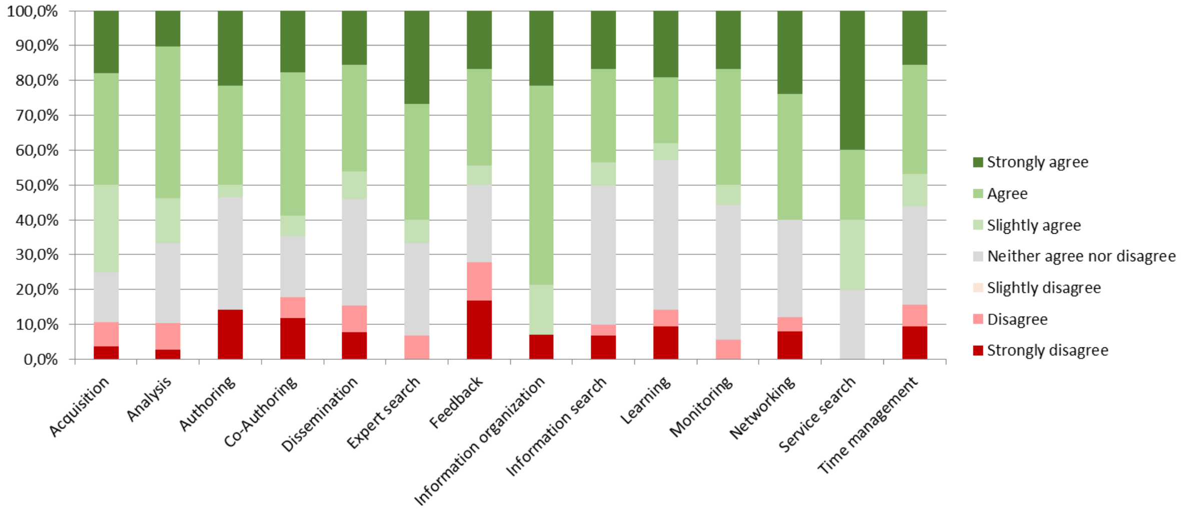


Figure 5. Perceived performance improvement per task with CYOD

Figure 5 shows that 52% of the respondents agree or strongly agree that having a device of their own choice would improve their task performance. This is an interesting outcome in the light of the first question, where over 70% of the respondents indicated to be able to perform their work well on their current device. The outcome does however fall in line with the research of Harris et al. (2012), who state that if employees were to choose their own hardware and software for work, they (strongly) agree that they would complete more tasks on time (49%), be more innovative (50%), and would be a happier employee (53%).

For each task, the respondents were asked whether they would rather use another device than the one they currently use, and if so, which device. The results of this analysis is in Appendix 2. The results show that a vast majority of the respondents would prefer another device, if given the choice in a CYOD environment. In general notebooks are preferred over desktops, provided they perform well enough. While only 2 respondents currently use an Apple notebook, Macbooks are preferred by most respondents over Windows notebooks. For the more mobile tasks light (and thin) notebooks or tablets are preferred. Overall, the Apple iPad the is most preferred CYOD device, especially for reading and viewing data.

Appendix 3 gives an overview of the current devices in use for the tasks. The table in Appendix3 also contains the sum of the preferred devices that were mentioned. Figure 6 shows the relative spread of the current device use as well as the spread of the preferred devices in a CYOD environment.

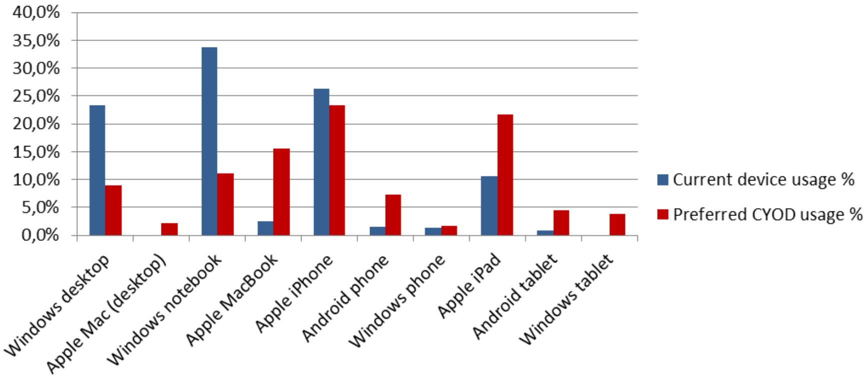


Figure 6. *Current and preferred device usage*

Figure 6 shows that in CYOD environment, there is less need for Windows desktops and notebooks, and more need for Apple notebooks, and in particular Apple iPad tablets. In general this means that, when implementing a CYOD policy that fits the preferences of the users, the number of operating systems and the number of different sorts of devices the ICT department has to manage, will rise.

Finally, the respondents were asked if they were willing to pay fully or partially for the device or their own preference. When it comes to paying, almost 75% (74,8%) of the respondents is not willing to contribute anything for the device of their choice. A group of around 15% is willing to pay up to 50% of the device cost. When the respondents are correct about the perceived improvement of their performance with the device of their choice, this would justify a CYOD policy (above a BYOD policy), as most of the employees are not willing to contribute personally to their improved business performance, but there is a lot of potential to gain.

4.3 Risk Assessment

The detailed results of the Risk Assessment can be found in Appendix 4. Though the Apple Mac desktop is not used in one of the case companies, the device was included in the Risk Assessment as it was one of the preferred CYOD devices. The risks that were determined are the net risks of the devices, meaning that the risk degree already includes a proper security policy with technical controls in place. The overall IT risk of the devices is determined by calculating the average of the outcomes of all participating companies. This result is shown in Figure 7.

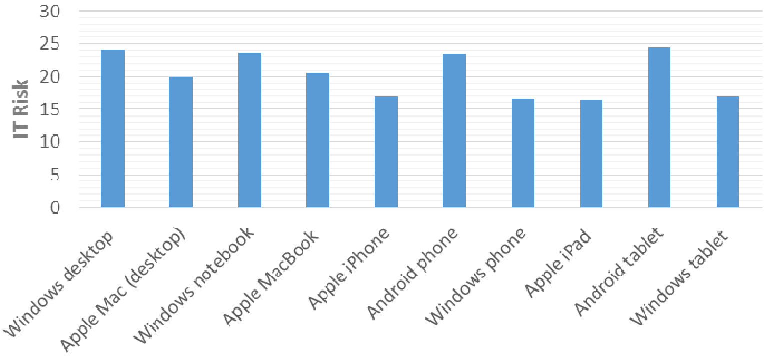


Figure 7. *IT Risk for devices*

Figure 7 shows that Windows desktops and notebooks, and Android phones and tablets, are the devices with the highest IT risks. Windows phones and tablets, and Apple devices in general, are the devices with the lowest IT security risks.

4.4 Usefulness and satisfaction

In the second section of the Employee Survey, the respondents were asked to score devices on Perceived usefulness, Perceived ease of use, and Output quality for each knowledge task. The results of this analysis is in Appendix 5. Overall, Windows notebooks score well on Perceived usefulness, Perceived ease of use, and Output quality. The iPad is less suitable for tasks e.g. Authoring and Analysis, but more suitable for reading and viewing tasks. Both laptops and tablets are suitable for Information search; tasks where mobile phones (iPhone and Windows phone) score lower. Finally, the respondents were asked to score the device of their own choice on Perceived satisfaction. Figure 8 shows the overall results of the Usability and Perceived satisfaction outcomes for with the different devices.

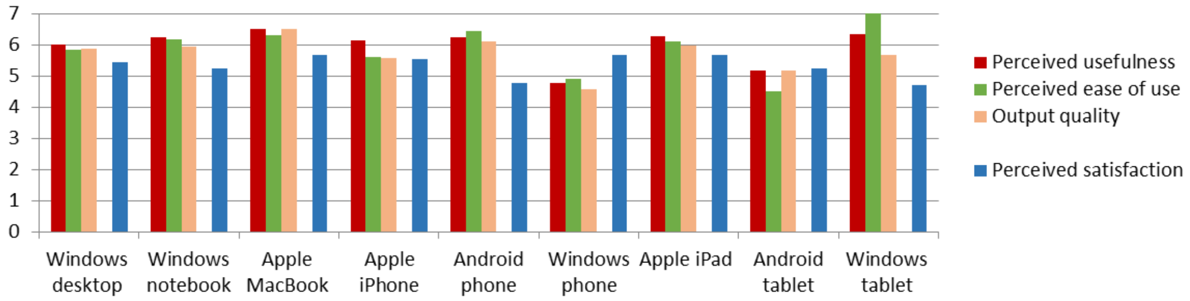


Figure 8. Usefulness and perceived satisfaction per device

In general, the perceived satisfaction scores lower than usability (the three constructs), except for the Windows phone. Possibly this is because the respondent were cautious of being over-optimistic.

4.5 IT Risk versus usefulness and satisfaction

When the Risk Assessment result is plotted against the Usefulness, being the average of the constructs: Perceived usefulness, Perceived ease of use and Output quality, the following picture appears.

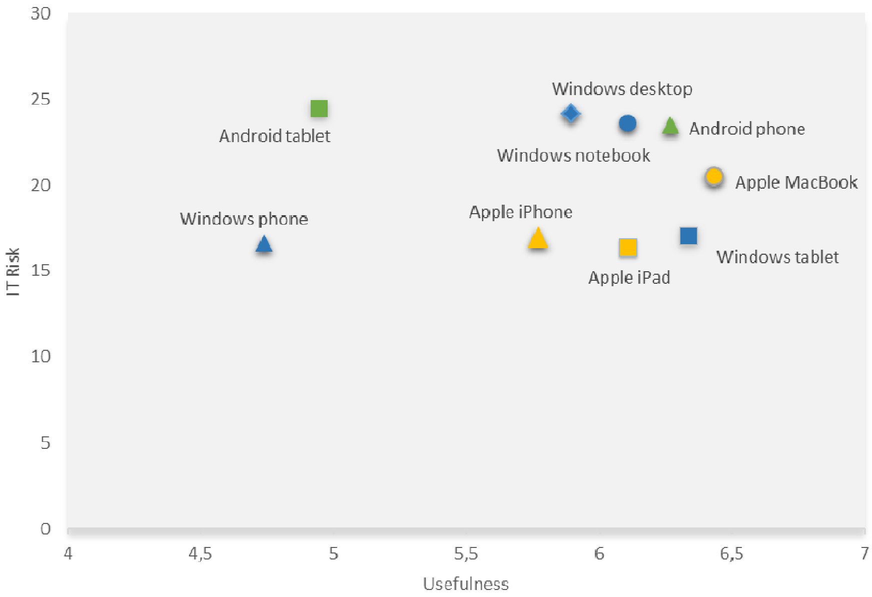


Figure 9. Usefulness versus IT Risk

Figure 9 shows the Android tablet and Windows phone score lowest on usefulness, while the Apple MacBook and Windows tablet score highest. From an IT security point of view, Windows desktops and notebooks and Android tablets and phones score worst.

When the IT Risk is plotted against the Satisfaction, being the combination (multiplication) of the Perceived satisfaction with the number of choosers of a preferred device, a quite different picture appears.

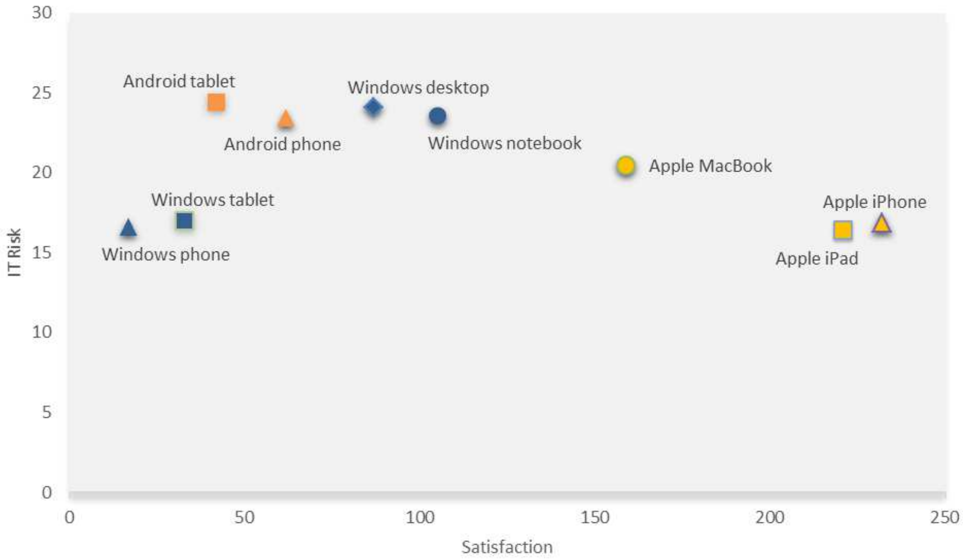


Figure 10. Satisfaction versus IT Risk

Figure 10 shows that Apple devices score by far best when it comes to satisfaction (preferred device and perceived satisfaction). Windows desktops and notebooks are somewhere in the middle, while Android and Windows phones and tables are at the bottom of the preference list. From an IT security point of view the preferred CYOD devices are less vulnerable than the Windows devices, that are often currently in use. This leads to an interesting conclusion: enabling employees to improve their task performance, whilst experiencing a higher job satisfaction, by giving them the opportunity to use a device or their own choice in a CYOD environment, does not increase, but instead reduces, the overall average IT security risks. A precondition for the above situation is that the proper security policies with technical controls are in place. This means that the implementation of a CYOD policy (with more Apple devices) does not raise the IT risk level, but it does mean the management of more platforms and software.

5 Discussion, conclusions and future research

5.1 Discussion

As mentioned in the introduction, research on Choose Your Own Device (CYOD) policies in the area of an implementation of the New Way of Working is scarce. Comparable literature on NWOW and CYOD can hardly be found, if any. This research on IT security risks versus usability and device satisfaction, in a NWOW and CYOD environment, is possibly one of the first steps in this area. Some critical notes are however at its place.

Having four companies with 126 respondents is reasonable, but the respondents were not evenly distributed across the organizations. This made intra-company comparisons unreliable if not impossible, and has the risk of over-emphasizing company-related viewpoints.

The perceived satisfaction and number of preferred devices for a task are subjective user-perceptions. It may well be that an Apple iPad is in reality not the best device for the given task, even if respondents believe it is. This effect (likability versus reality) has not been measured, but is realistic in both this research as in daily business practice. This may mean that, though in reality a Windows tablet could be more useful for executing a task than an Apple iPad, most users would still prefer an iPad, when given the choice, to perform their task on.

Having the IT Experts and Security Officers of four multinationals available for the Risk Assessment is good, but estimating risks remains a subjective and human exercise. The results should therefore be seen as a first indication of the possible effects of CYOD on job performance and employee satisfaction.

5.2 Conclusions and future research

Organizations struggle with the phenomenon of employees using consumer devices for business purposes. In an optimal situation the use of these personalized mobile devices would be beneficial for both the employee and organization, rendering higher employee satisfaction with higher performance on task execution. The question is how this optimum can be reached. Having researched the IT security risks against the effects and possible gains of a CYOD policy, this study shows that:

- Though over 70% of the respondents agree they can perform their tasks well with their current device, a majority (52%) of the respondents (strongly) agrees, having the ability to use a device of their own, will increase their task performance.
- The vast majority of employees, almost 75%, is however not willing to contribute to the costs of personal devices. Combined with the first conclusion, this implies that a CYOD policy is to be preferred over a BYOD policy, and can be beneficial for the organization.
- Introducing a CYOD environment in an organization will lead to a shift in the types of devices used. Desktops are likely to be replaced by (powerful) notebooks, preferably in combination with optional large monitors, and where suitable for the task, tablets will be used instead of notebooks.
- The introduction of the CYOD environment will lead to the mandatory management of more platforms and software. Besides Windows devices, Apple devices and the use of (iOS) apps will need to be fully supported by the corporate IT strategy.
- Under the precondition that the security policies with technical controls are in place, the introduction of a CYOD policy does not necessarily increase the level of IT security risk. The average net IT risk may even decrease when introducing CYOD, e.g. in this research with the preferred Apple devices.

Enabling employees to improve their task performance whilst experiencing a higher job satisfaction, by giving them the opportunity to use a device or their own choice and preference, in a CYOD environment, does not by definition increase the overall average IT security risks. Organizations that know which devices employees need to best perform their tasks, can balance out the business risk requirements and meet the employee expectations to maximize employee satisfaction without giving up on corporate data protection. In doing so, the consequence will be the management of more platforms and operating systems in a controlled CYOD environment.

This research is only a first step towards a future of effective CYOD policies in a NWOW environment. There will always be more information to explore and describe. For instance: the aspect of the usefulness of software in combination with (preferred) hardware was not researched in this study, but is certainly an aspect worth investigating in future studies of CYOD in a NWOW environment. Also the cost of a CYOD program against the possible business gain could be a field of future study, as well as the actual performance gain from implementing CYOD in real business practice. The results of this study should therefore be used with care, as more future research should support these first findings, and add more insights.

References

Ajzen, I. & Fishbein, M. (1980). Understanding attitudes and predicting social behavior. Englewood Cliffs, NJ: Prentice-Hall.

Baane R., Houtkamp P.,& Knotter M. (2010). The new world of work unravelled – Het nieuwe werken ontrafeld – over Bricks, Bytes & Behavior. 1-168. Koninklijke Van Gorcum BV. ISBN 9789023245858.

Bandura, A. (1977). Self-efficacy: Toward a unifying theory of behavioral change. Psychological Review (84:2), pp. 191–215.

Baskerville, R. (1993). Information systems security design methods: implications for information systems development. ACM Computing Surveys, 25(4), 375–414. http://doi.org/10.1145/162124.162127

Bijl, D.W. (2011). Journey towards the New Way of Working - creating sustainable performance and joy at work. Par CC. ISBN: 978-94-90528-00-3

Bødker, S., & Christiansen, E. (2002). Lost and Found in Flexibility. University of Aarhus, Center for New Ways of Working. Retrieved from http://pure.au.dk/portal/en/publications/lost-and-found-in-flexibility(cd3361c0-983b-11da-bee9-02004c4f4f50).html

Citrix. (2013). Best practices to make BYOD simple and secure. Citrix Systems.

Csikszentmihalyi, M. (1975). Beyond boredom and anxiety. San Francisco, CA: Jossey-Bass.

Csikszentmihalyi, M. (1988). The flow experience and human psychology. In M. Csikszentmihalyi & I. S. Csikszentmihalyi (Eds.) (1988). Optimal Experience: Psychological studies of flow in consciousness (pp. 15-35). New York: Cambridge University Press.

Csikszentmihalyi, M. (1990). Flow: the psychology of optimal experience. New York: Harpers Perennial.

Davenport, T.H., & Prusak, L. (1998). Working knowledge: How organizations manage what they know. Boston: Harvard Business School Press.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quarterly, 13(3), 319-342.

Finneran, C. M., & Zhang, P. (2002). The Challenges of Studying Flow within a Computer-Mediated Environment. Paper presented at the Americas Conference on Information Systems, Dallas, TX.

Gajar, P. K., Ghosh, A., & Rai, S. (2013). Bring Your Own Device (BYOD): Security risks and mitigating strategies. Journal of Global Research in Computer Science, 4(4), 62–70.

Gartner. (2015). Identity and Access management (IAM). Retrieved from http://www.gartner.com/it-glossary/identity-and-access-management-iam/

Ghani, J. (1991). Flow in human computer interactions: test of a model. In J. Carey (Ed.), Human Factors in Information Systems: Emerging Theoretical Bases. New Jersey: Ablex Publishing Corp.

Giddens, L., & Tripp, J. (2014). It's My Tool , I Know How to Use It : A Theory of the Impact of BYOD on Device Competence and Job Satisfaction. Proceedings of the Twentieth Americas Conference on Information Systems, pp. 1–8.

Gillett, F. E. (2012). Tablets Will Rule The Future Personal Computing Landscape. Forrester Research.

Govcert (2009). Security of mobile devices and data carriers – Dutch title: Beveiliging van mobiele apparatuur en datadragers. National Cyber Security Center. The Hague. Retrieved from: https://www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/whitepapers/whitepaper-beveiliging-van-mobiele-apparatuur-en-datadragers.html

Greene, C., & Myerson, J. (2011). Space for thought: designing for knowledge workers. Facilities, 29(1/2), 19-30.

Hammer, M., & Champy, J.A. (1993) Reengineering the Corporation: A Manifesto for Business Revolution. Ch. 4 & 5. HarperCollins Publishers Inc. ISBN 0-06-662112-7.

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

Holtsnider, B., and Jaffe, B. D. (2012) IT Manager's Handbook: Getting Your New Job Done. Morgan Kaufmann.

Ingalsbe, J. a, Shoemaker, D., & Mead, N. R. (2011). Threat Modeling the Cloud Computing, Mobile Device Toting, Consumerized Enterprise – an overview of considerations. AMCIS 2011 Proceedings, 1–6.

Johns, T., & Gratton, L. (2013). The Third Wave Of Virtual Work. Harvard Business Review, January-February 2013, pp. 66-73.

Jones, P., & Jordan, J. (1998). Knowledge orientations and team effectiveness. International Journal of Technology Management, 16, 152-161.

Kiili, K. (2005). Digital game-based learning: Towards an experiential gaming model. Internet and Higher Education, 8(1), 13–24. http://doi.org/10.1016/j.iheduc.2004.12.001

Kok, A. de, Bellefroid, B.E.W. & Helms, R.W. (2013) Knowledge Sharing and Channel Choice: Effects of the New Way of Working. Proceedings of the 14th European Conference on Knowledge Management, ECKM 2013.

Kok, A. de, Koops, J. & Helms, R.W. (2014) Accessing the New Way of Working: Bricks, Bytes and Behaviour. Proceedings of the 18th Pacific Asia Conference on Information Systems, PACIS 2014.

Morrow, B. (2012). BYOD security challenges: Control and protect your most sensitive data. Network Security, 2012(12), 5–8. doi:10.1016/S1353-4858(12)70111-3

Moschella, D., Neal, D., Opperman, P., and Taylor, J. 2004. The "Consumerization" of Information Technology. El Segundo, California, USA: CSC.

Niehaves, B., Köffer, S., & Ortbach, K. (2012) IT Consumerization – A Theory and Practice Review, AMCIS, paper 18.

Niehaves, B., Köffer, S., & Ortbach, K. (2013) The Effect of Private IT Use on Work Performance - Towards an IT Consumerization Theory. International Conference on Wirtschaftsinformatik: Leipzig.

Peltier, T. R. (2005). Information Security Risk Analysis. Auerbach Publications, CRC Press, Taylor & Francis Group. ISBN 0-8493-3346-6.

Reinhardt, W., Schmidt, B., & Sloep, P. (2011). Knowledge worker roles and actions - Results of two empirical studies. Knowledge and Process Management, 18(3), 150–174. http://doi.org/10.1002/kpm

Rouse. (2007). Authentication.
Retrieved from http://searchsecurity.techtarget.com/definition/authentication

Ruch, T., & Gregory, R. (2014). Consumerization of It – Where Is the Theory? Proceedings of the 18th Pacific Asia Conference on Information Systems, PACIS 2014.

Venkatesh, V., & Davis, F. (1996). A Model of the Antecedents of Perceived Ease of Use: Development and Test. Decision Sciences, 27(3), 451-481.

Venkatesh, V., & Davis, F. (2000). A theoretical extension of the Technology Acceptance Model: Four longitudinal field studies. Management Science, 46(2), 186–204.

Waber, B., Magnolfi, J., & Lindsay, G. (2014). Workspaces that move people. Harvard Business Review, Oktober 2014, pp. 68–77.

Whitman, M. E. (2003). Enemy at the Gate: Threats to Information Security. Communications of the ACM, 46(8), 91–95. Retrieved from http://portal.acm.org/citation.cfm?id=859675

Yin, R.K. (2009). Case Study Research. Thousand Oaks , California, USA, Sage Publications.

Appendix 1 Knowledge tasks

Typology of knowledge actions / tasks of Reinhardt et al. (2011) and their description. In this research the task 'Time management' was added to the list of Reinhardt, because managing time was identified as an important part of the tasks of a large number of the respondents (e.g. in consulting work).

Knowledge action	Description
Acquisition	The gathering of information with the goal of developing skills or project or obtaining an asset.
Analyze	The examining or thinking about something carefully, in order to understand.
Authoring	The creation of textual and medial content using software systems, for example word processing systems/ presentation systems.
Co-authoring	The collaborative creation of textual and medial content using software applications, for example, word processing systems/ presentation software.
Dissemination	The spreading of information or information objects, often work results.
Expert search	The retrieval of an expert to discuss and solve a specific problem.
Feedback	The assessment of a proposition or an information object.
Information organization	The personal or organizational management of information collection.
Information Search	The looking up of information on a specific topic and in a specific form. Often we search using the folder structure of a file system or we search using an information retrieval service.
Learning	The acquiring process of new knowledge, skills or understanding during the execution of work or based on formalized learning material.
Monitoring	Keeping oneself or the organization up-to date about selected topics, for example, based on different electronic information resources.
Networking	The interaction with other people and organizations to exchange information and develop contacts.
Service search	The retrieval of specialized web services that offer specific functions.
Time management	The planning, recording and invoicing of time spend on work activities.

Table 4. Typology of knowledge actions / tasks (Reinhartdt et al., 2011)

Overall number of tasks performed by the respondents.

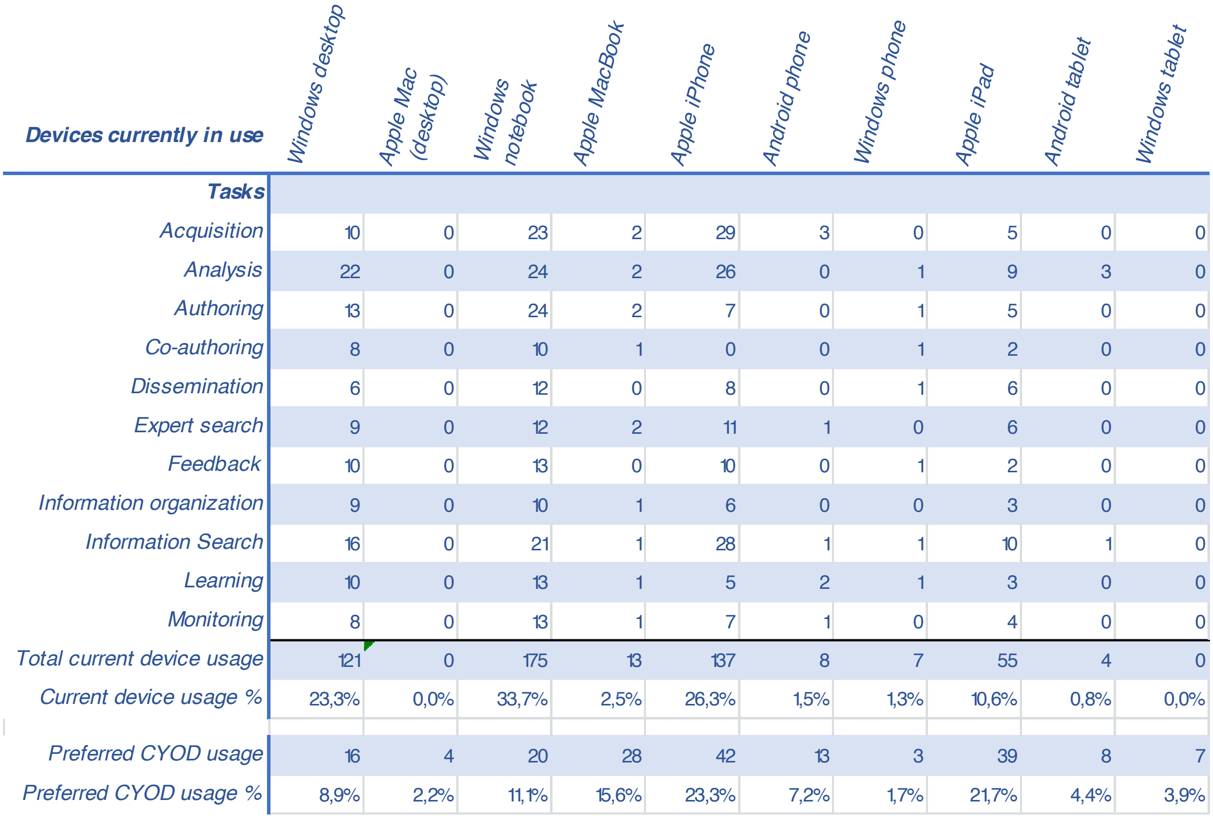
Task	#Respondents	%	Task	#Respondents	%
Acquisition	45	11,1%	Information organization	22	5,4%
Analysis	53	13,1%	Information Search	41	10,1%
Authoring	40	9,9%	Learning	24	5,9%
Co-authoring	18	4,4%	Monitoring	23	5,7%
Dissemination	19	4,7%	Networking	27	6,7%
Expert search	23	5,7%	Service search	5	1,2%
Feedback	25	6,2%	Time management	40	9,9%

Table 5. Number of tasks (knowledge actions) performed by respondents

Appendix 2 Preferred CYOD devices

- For Acquisition, 28 (out of 35) respondents indicate they would prefer another device for their task. The type of preferred device varies. Respondents with a desktop computer prefer a notebook (Apple or Windows). Some respondents using notebooks or iPhones prefer larger screens than an iPhone, but smaller screens than their notebook. Performing acquisition tasks on an Android phone is perceived by them as useful and easy, though they see the output quality as low. Overall, the device that is perceived as best for Acquisition tasks is an Apple notebook.
- For Analysis a fast computer (e.g. a desktop) is often preferred over the current devices (Windows notebooks). A thin laptop (Windows or Apple) or a tablet is perceived as useful for traveling and out-of-office work. Performing Analysis on an Apple notebook is questioned as respondents didn't find the device useful and easy to use, and the output quality not high. The Windows notebook scores low on perceived usefulness and perceived ease of use, though the output quality scores high. Overall, the Windows desktop scores best for performing analysis tasks.
- For Authoring and Co-authoring, many respondents consider a laptop as the best device for their task. Also a tablet (iPad with supporting apps) is preferred, because it is easier to carry. Some respondents prefer a thin and light laptop (Windows or MacBook Air). For authoring tasks both Windows notebooks and Apple MacBooks score high. Although mobile devices are also used for authoring, those devices are perceived as less suitable than laptops.
- For Dissemination of information respondents currently use desktop devices, but prefer an Apple or Windows notebook. Respondents already using a notebook prefer a faster and thinner laptop. Also a tablet (iPad) was indicated as a (more) useful device for this task.
- For Expert search, 20 (out of 23) respondents would rather use another device. Different devices are mentioned, such as Apple and Windows notebooks. Also a newer version of the iPhone device is preferred, with the bigger screen for mobile apps such as LinkedIn.
- For Feedback, 20 (of 25) respondents indicate to prefer another device. Suggestions include a thinner and smaller Windows notebook or Apple MacBook Air. Also iPads and Android tablets were suggested as useful.
- For Information organization a light laptop (e.g. MacBook Air) is preferred, or a notebook instead of a desktop. Also iPads are mentioned several times. One respondent (now using a notebook) replied; "A windows notebook is fine, but I do not have the software to manage disparate flows of data information. A device with such software would be my preferred device."
- For Information search, some respondents emphasized that the devices hardly matters, provided that is has a good way of conveying the information. It is the search software that matters to them. Though the hardware is said to not matter, still 35 out of the 41 respondents prefer other devices than they currently use. All types of other devices are mentioned: Apple MacBooks, Windows notebooks, larger Phones/iPads, Android tablets, and Windows tablets.
- For Learning, all (24) respondents indicate to rather use other devices. They prefer an Apple MacBook or Windows notebook over their current desktop computer. Also a tablet (iOS or Android) is mentioned a as preferred device.
- For Monitoring, 19 (of 23) respondents prefer other devices. They differ from Apple MacBooks to Windows notebooks or tablets instead of mobile phones due to the screen size.
- For Networking, 26 (of 27) respondents rather use another device than they currently use. One respondent rather uses a Blackberry phone, another rather uses an Android (Samsung) smart phone or tablet instead of iPhone. A tablet is mentioned several times, including iPad, Android tab and a Windows tablet.
- For Service search, all (5) respondents preferred another device for searching services. The only mentioned devices are Apple MacBook and Windows notebook.
- For Time management, 37 (of 40) respondents prefer another device. Tablets are in favor (iPad, Android, or Windows).

Appendix 3 – Current and preferred use of devices



Devices currently in use	Windows desktop	Apple Mac (desktop)	Windows notebook	Apple MacBook	Apple iPhone	Android phone	Windows phone	Apple iPad	Android tablet	Windows tablet
Tasks										
Acquisition	10	0	23	2	29	3	0	5	0	0
Analysis	22	0	24	2	26	0	1	9	3	0
Authoring	13	0	24	2	7	0	1	5	0	0
Co-authoring	8	0	10	1	0	0	1	2	0	0
Dissemination	6	0	12	0	8	0	1	6	0	0
Expert search	9	0	12	2	11	1	0	6	0	0
Feedback	10	0	13	0	10	0	1	2	0	0
Information organization	9	0	10	1	6	0	0	3	0	0
Information Search	16	0	21	1	28	1	1	10	1	0
Learning	10	0	13	1	5	2	1	3	0	0
Monitoring	8	0	13	1	7	1	0	4	0	0
Total current device usage	121	0	175	13	137	8	7	55	4	0
Current device usage %	23,3%	0,0%	33,7%	2,5%	26,3%	1,5%	1,3%	10,6%	0,8%	0,0%
Preferred CYOD usage	16	4	20	28	42	13	3	39	8	7
Preferred CYOD usage %	8,9%	2,2%	11,1%	15,6%	23,3%	7,2%	1,7%	21,7%	4,4%	3,9%

The current device usage % is the relative spread of the current devices in use, in relation to the total number of current devices.

The preferred CYOD usage % is the relative spread of the number of preferred devices, in relation to the total number of preferred devices.

Appendix 4 – Risk Assessment

Risk Assessment	Threat 1			Threat 2			Threat 3			Threat 4			Threat 5			Threat 6			Threat 7				
	Chance	Damage	Risk	Chance	Damage	Risk	Chance	Damage	Risk	Chance	Damage	Risk	Chance	Damage	Risk	Chance	Damage	Risk	Chance	Damage	Risk	Totals	Total average
Windows desktop																							
Company 1	5	5	25	6	3	18	5	5	25	2	1	2	6	6	36	0	1	0	5	5	25	131	18,7
Company 2	5	5	25	7	6	42	7	7	49	7	7	49	7	7	49	4	4	16	4	4	16	246	35,1
Company 3	5	6	30	6	5	30	6	5	30	5	5	25	7	7	49	6	5	30	6	6	36	230	32,9
Company 4	5	2	10	2	6	12	3	4	12	3	1	3	5	3	15	4	2	8	4	2	8	68	9,7
Totals			90			102			116			79			149			54			85	675	**24,1**
Apple Mac (desktop)																							
Company 1	7	5	35	5	3	15	4	5	20	3	2	6	3	6	18	0	2	0	6	5	30	124	17,7
Company 2	5	5	25	6	6	36	6	7	42	6	7	42	6	7	42	4	4	16	4	4	16	219	31,3
Company 3	4	4	16	5	6	30	4	4	16	5	5	25	3	5	15	5	5	25	4	5	20	147	21,0
Company 4	5	2	10	2	6	12	3	4	12	3	1	3	5	3	15	4	2	8	4	2	8	68	9,7
Totals			86			93			90			76			90			49			74	558	**19,9**
Windows notebook																							
Company 1	5	5	25	6	3	18	5	5	25	6	1	6	6	6	36	0	1	0	5	5	25	135	19,3
Company 2	5	5	25	7	6	42			0	7	7	49	7	7	49	4	4	16	4	4	16	197	28,1
Company 3	5	6	30	6	6	36	6	5	30	6	5	30	7	7	49	7	7	49	6	6	36	260	37,1
Company 4	5	2	10	2	6	12	3	4	12	3	1	3	5	3	15	4	2	8	4	2	8	68	9,7
Totals			90			108			67			88			149			73			85	660	**23,6**
Apple MacBook																							
Company 1	6	5	30	5	3	15	4	5	20	7	2	14	3	6	18	0	2	0	6	5	30	127	18,1
Company 2	5	5	25	6	6	36	6	7	42	6	7	42	6	7	42	4	4	16	4	4	16	219	31,3
Company 3	4	5	20	5	6	30	4	4	16	7	6	42	3	5	15	4	4	16	4	5	20	159	22,7
Company 4	5	2	10	2	6	12	3	4	12	3	1	3	5	3	15	4	2	8	4	2	8	68	9,7
Totals			85			93			90			101			90			40			74	573	**20,5**
Apple iPhone																							
Company 1	4	5	20	4	3	12	3	6	18	6	4	24	4	6	24	0	4	0	4	5	20	118	16,9
Company 2	5	5	25	5	5	25	5	7	35	7	7	49	5	7	35	3	4	12	4	4	16	197	28,1
Company 3	3	4	12	3	4	12	3	4	12	4	5	20	3	5	15	3	4	12	3	3	9	92	13,1
Company 4	4	2	8	2	6	12	3	6	18	2	6	12	2	4	8	2	2	4	2	2	4	66	9,4
Totals			65			61			83			105			82			28			49	473	**16,9**
Android phone																							
Company 1	5	5	25	4	3	12	6	6	36	6	4	24	6	6	36	0	3	0	5	5	25	158	22,6
Company 2	5	5	25	7	5	35	7	7	49	7	7	49	3	4	12	3	4	12	4	4	16	198	28,3
Company 3	6	6	36	6	5	30	6	6	36	5	5	25	6	6	36	5	6	30	6	5	30	223	31,9
Company 4	4	2	8	2	6	12	3	6	18	2	6	12	4	4	16	3	2	6	3	2	6	78	11,1
Totals			94			89			139			110			100			48			77	657	**23,5**
Windows phone																							
Company 1	4	5	20	4	3	12	4	6	24	4	3	12	5	6	30	0	3	0	4	5	20	118	16,9
Company 2																							
Company 3	4	5	20	5	5	25	5	5	25	5	5	25	4	5	20	4	5	20	6	5	30	165	23,6
Company 4	4	2	8	2	6	12	3	6	18	2	6	12	2	4	8	2	2	4	2	2	4	66	9,4
Totals			48			49			67			49			58			24			54	349	**16,6**
Apple iPad																							
Company 1	4	5	20	4	3	12	3	6	18	6	5	30	4	6	24	0	4	0	4	5	20	124	17,7
Company 2	5	5	25	5	5	25	5	7	35	7	7	49	5	7	35	3	4	12	4	4	16	197	28,1
Company 3	3	4	12	3	4	12	3	4	12	0	0	0	3	5	15	3	4	12	3	3	9	72	10,3
Company 4	4	2	8	2	6	12	3	6	18	2	6	12	2	4	8	2	2	4	2	2	4	66	9,4
Totals			65			61			83			91			82			28			49	459	**16,4**
Android tablet																							
Company 1	5	5	25	6	3	18	6	6	36	5	4	20	4	6	24	0	3	0	5	5	25	148	21,1
Company 2	5	5	25	7	5	35	7	7	49	7	7	49	7	7	49	3	4	12	4	4	16	235	33,6
Company 3	6	6	36	6	5	30	6	6	36	5	5	25	6	6	36	5	6	30	6	5	30	223	31,9
Company 4	4	2	8	2	6	12	3	6	18	2	6	12	4	4	16	3	2	6	3	2	6	78	11,1
Totals			94			95			139			106			125			48			77	684	**24,4**
Windows tablet																							
Company 1	4	5	20	4	3	12	4	6	24	5	4	20	5	6	30	0	3	0	4	5	20	126	18,0
Company 2																							
Company 3	4	5	20	5	5	25	5	5	25	5	5	25	4	5	20	4	5	20	6	5	30	165	23,6
Company 4	4	2	8	2	6	12	3	6	18	2	6	12	2	4	8	2	2	4	2	2	4	66	9,4
Totals			48			49			67			57			58			24			54	357	**17,0**

Appendix 5 – Evaluation of usefulness of devices

Device in use Task	Windows desktop	Windows notebook	Apple MacBook	Apple iPhone	Android phone	Windows phone	Apple iPad	Android tablet	Windows tablet
Acquisition									
Usefulness	6	5,9	6,5	7	5,3	-	5,8	-	-
Ease of use	5,7	5,6	6,5	6,7	5,3	-	5,4	-	-
Output quality	5,8	5,5	7	4,7	5,3	-	6	-	-
Analysis									
Usefulness	6,2	5,7	5	-	5,6	2	5,8	4,3	-
Ease of use	6,2	5,3	4,5	-	5,6	1	5,6	4	-
Output quality	6,1	6,3	4,5	-	5,6	1	5,7	4,3	-
Authoring									
Usefulness	6,2	6,4	6,5	-	5,8	5	5,6	-	-
Ease of use	5,8	6,2	6,5	-	5,6	5	5	-	-
Output quality	5,7	6,2	6,5	-	5,1	4	4,8	-	-
Co-authoring									
Usefulness	6,1	6,5	7	-	-	4	6,5	-	-
Ease of use	5,8	6,4	7	-	-	5	6,5	-	-
Output quality	6	6,2	7	-	-	4	6,5	-	-
Dissemination									
Usefulness	6,2	6,3	-	-	5,3	5	6,2	-	-
Ease of use	6	6,5	-	-	5,8	5	6,2	-	-
Output quality	6	6,3	-	-	5,5	5	6,2	-	-
Expert search									
Usefulness	5,9	6,3	6,5	7	5,5	-	6,2	-	5
Ease of use	6	6,2	6	7	5,2	-	6,2	-	-
Output quality	6	5,8	6	7	4,9	-	5,7	-	3
Feedback									
Usefulness	5,9	6	-	5	5,9	5	6,5	-	-
Ease of use	5,9	6,1	-	6	5,8	6	6,5	-	-
Output quality	6	5,1	-	6	5,8	5	6,5	-	-
Information organization									
Usefulness	5,8	5,9	6	5,5	5,5	-	6	-	-
Ease of use	5,7	5,6	6	6	5,8	-	6	-	-
Output quality	5,7	5,4	6	6	5,5	-	6,7	-	-

Appendix 5 - Evaluation of usefulness of devices (continued)

Device Task	Windows desktop	Windows notebook	Apple MacBook	Apple iPhone	Android phone	Windows phone	Apple iPad	Android tablet	Windows tablet
Information Search									
Usefulness	5,9	6,4	7	5	5,5	5	6	6	7
Ease of use	5,5	6,3	6	6	5,4	5	5,9	5	7
Output quality	5,6	6	7	6	5,7	5	6,2	6	7
Learning									
Usefulness	5,9	6,3	7	5,5	6	5	6,7	-	-
Ease of use	5,8	6,3	6	6	6	5	7	-	-
Output quality	5,8	6,3	7	6	6	5	6	-	-
Monitoring									
Usefulness	6	6,3	7	7	6	-	6,5	-	-
Ease of use	5,8	6,2	7	7	5,9	-	6,3	-	-
Output quality	5,8	6,1	7	7	5,9	-	6	-	-
Networking									
Usefulness	5,8	6,3	7	6	6,2	5	6,5	-	7
Ease of use	5,6	6,3	7	6	6,1	5	6,5	-	7
Output quality	5,8	6,3	7	6	6,1	5	6,3	-	7
Service search									
Usefulness	-	6,5	7	-	5,7	-	7	-	-
Ease of use	-	6,5	7	-	4,7	-	6	-	-
Output quality	-	6,5	7	-	5,3	-	5	-	-
Time management									
Usefulness	6,1	6,3	6	-	6,1	7	6,5	-	-
Ease of use	6	6,3	6	-	5,7	7	6,3	-	-
Output quality	5,8	6,1	6	-	5,7	7	6,2	-	-

Device Task	Windows desktop	Windows notebook	Apple MacBook	Apple iPhone	Android phone	Windows phone	Apple iPad	Android tablet	Windows tablet
Overall									
Usefulness	6,0	6,2	6,5	6,0	5,7	4,8	6,3	5,2	6,3
Ease of use	5,8	6,1	6,3	6,3	5,6	4,9	6,1	4,5	7,0
Output quality	5,9	6,0	6,5	6,1	5,6	4,6	6,0	5,2	5,7