BYOD VS. CYOD – WHAT IS THE DIFFERENCE?

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

ABSTRACT

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

KEYWORDS

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

1. INTRODUCTION

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

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

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

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

1.1 Ways to Manage Devices

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

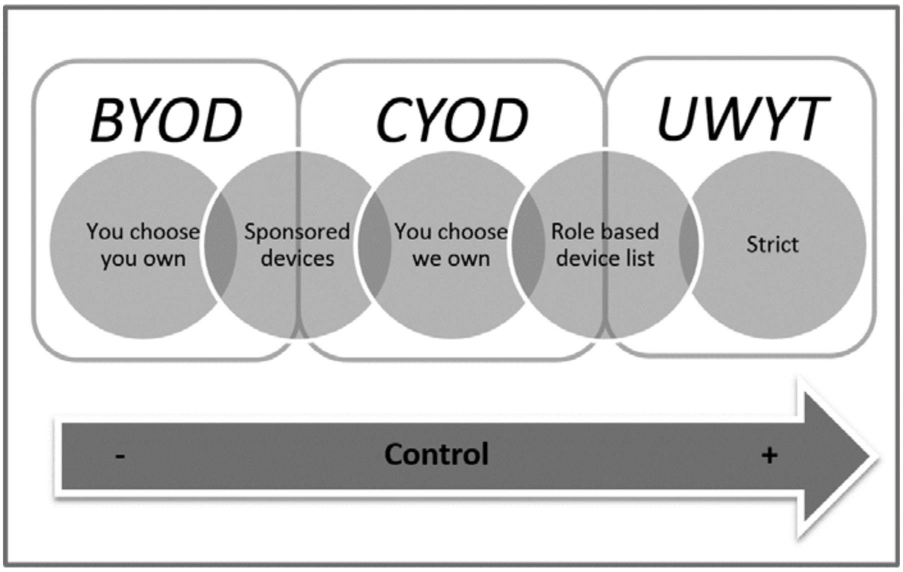


Figure 1. Strategies for mobile devices and the amount of control from the organisation

2. METHOD

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

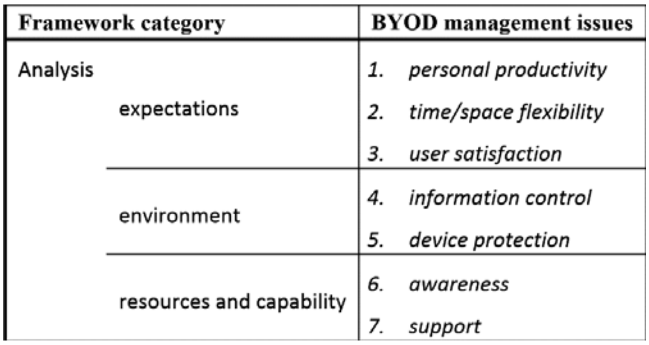
1. An extensive literature search using the WorldCat search engine with different search terms connected to BYOD.
2. Manual screening for relevance (where relevance requires that the article both falls within the mobile/dual-use definition and focuses on policy, management or strategic issues, rather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

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

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

2.1 Analysis Framework

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



Framework category		BYOD management issues
Analysis		*1. personal productivity*
	expectations	*2. time/space flexibility*
		3. user satisfaction
	environment	*4. information control*
		5. device protection
	resources and capability	*6. awareness*
		7. support

Figure 2. The framework used in this analysis, adapted from Brodin et al. (2015)

3. BYOD

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

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

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

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

Table 1. Management issues for BYOD

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

4. CYOD

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

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

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

When it comes to user satisfaction, it is more about convenience than who owns the device. If the user is allowed to use the device for private purposes as well and do not need to carry, for instance, two smartphones the satisfaction level will increase. On the other hand, the satisfaction rate depends on what the user got before. Almost all respondents say that their employees do not want to go from CYOD to BYOD. One respondent replied to the question about BYOD with; “Yes, though it's not interesting in Sweden. It adds nothing. There is not potential for it. There is no way for it financially and no incentive to do that so it's not a fact as I see it.”

Although CYOD brings a lot of positive things there are some concern. The concerns are based on the mobility and the increased exposure of information and devices. Or as one respondent expressed it: “The most dangerous thing we have, we'd rather not use mobile devices. But we have to, because otherwise we need to sit at the customer at all times. Sometimes we have to take some risks but we try to avoid mobile media as far as possible.”

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

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

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

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

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

Table 2. Management issues for CYOD

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

5. COMPARISON AND DISCUSSION

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

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

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

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

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

Table 3. Comparison of management issues for BYOD and CYOD

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

6. CONCLUSIONS

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

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

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

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

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

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

REFERENCES

Anderson, N., 2013. Cisco Bring Your Own Device - Device Freedom Without, San Jose: Cisco Systems, Inc.

Barbier, J. et al., 2012. Cisco IBSG Horizons Study. , p.5.

Berelson, B., 1952. Content analysis in communicative research, New York: Free Press.

Brodin, M., 2015. Combining ISMS with Strategic Management: The case of BYOD. IADIS International Conference Information Systems, pp.161–168.

Brodin, M., Rose, J. & Åhlfeldt, R.-M., 2015. Management issues for Bring Your Own Device. , 2015, pp.1–12.

Brooks, T., 2013. Classic enterprise IT: the castle approach. Network Security, 2013(6), pp.14–16. Available at: http://linkinghub.elsevier.com/retrieve/pii/S1353485813700709 [Accessed November 22, 2013].

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

Cisco, 2013. Cisco Security Intelligence - Annual Security Report & Cisco Connected World Technology Report,

Harris, J., Ives, B. & Junglas, I., 2012. IT Consumerization: When Gadgets Turn Into Enterprise IT Tools. MIS Quarterly, 2012(September), pp.99–112.

Intel, 2012. Insights on the current state of BYOD in the Enterprise – Intel’s IT Manager Survey,

iPass, I., 2011. iPass Global Mobile Workforce Report 2011Q3. Workforce, pp.1–27.

Jenkins, A.M., 1985. Research Methodologies and MIS Research. In E. Mumford, ed. Research Methods in Information Systems. Amsterdam, Holland: Elsevier Science Publishers B.V.

Kane, C. et al., 2014. Building The Business Case For A Bring-Your-Own-Device (BYOD) Program,

Krippendorff, K.H., 2004. Content Analysis: An Introduction to Its Methodology, Thousand Oaks, CA: Sage Publications Ltd.

Miller, R.E. & Varga, J., 2011. Benefits of Enabling Personal Handheld Devices in the Enterprise - Intel, IT@Intel White Paper.

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

Orlikowski, W.J., 2007. Sociomaterial Practices: Exploring Technology at Work. Organization Studies, 28(9), pp.1435–1448. Available at: http://oss.sagepub.com/cgi/doi/10.1177/0170840607081138.

Pettey, C. & Van Der Meulen, R., 2012. Gartner identifies three security hurdles to overcome when shifting from enterprise-owned devices to BYOD. Gartner Inc. Available at: http://www.gartner.com/newsroom/id/2263115 [Accessed July 20, 2013].

Silverman, D., 2001. Interpreting qualitative data, London: SAGE Publications Ltd.

Skype, Norton & TomTom, 2012. Survey finds nearly half of consumers fail to upgrade software regularly and one quarter of consumers do not know why to update software. Available at: http://about.skype.com/press/2012/07/survey_finds_nearly_half_fail_to_upgrade.html [Accessed October 19, 2015].

Walters, R., 2013. Bringing IT out of the shadows. Network Security, 2013(4), pp.5–11. Available at: http://linkinghub.elsevier.com/retrieve/pii/S1353485813700497 [Accessed November 22, 2013].

Webster, J. & Watson, R.T., 2002. Webster and Watson literature review. MIS Quarterly, 26(2), p.11.

Wilkinson, S., 1997. Focus group research. In D. Silverman, ed. Qualitative research: Theory, method and practice. London: Sage Publications Ltd.

Yun, H., Kettinger, W.J. & Lee, C.C., 2012. A New Open Door: The Smartphone’s Impact on Work-to-Life Conflict, Stress, and Resistance, *International Journal of Electronic Commerce*, *16*(4), 121-152. doi:10.2753/jec1086-4415160405