A Paradigm Shift For Bring Your Own Device (BYOD)

Completed Research

Donald Kerr
University of the Sunshine Coast
Australia
dkerr@usc.edu.au

Amir Talaei-Khoei
University of Nevada Reno, USA
University of Technology Sydney, Australia
atalaeikhoei@unr.edu

Amir Hossein Ghapanchi
Victoria University, Australia
amir.ghapanchi@vu.edu.au

Abstract

The present paper aims to understand the effectiveness of the current adoption models in newly-built concept of Bring Your Own Device (BYOD) and also the role of IT departments in adopting BYOD in organizations. The paper extends the literature on adoption and combines them with the body of work on BYOD. The paper compares these two concepts to build a theoretical framework in which BYOD can be examined. The paper presents the lessons learned from four different case studies in Australia, United Kingdom and Denmark. It was found that BYOD requires adaptation as opposed to adoption of technologies. Adaptation is a process in which an employee customises software in a way that allows them to do their task on their own device, at their own place and in their own time. The paper also reports that the adaptation process dictated by BYOD can lead to either innovation or errors and difficulties made by inconsistent use of technologies. The article informs IS researchers that there is a need to study the phenomena of technology adaption further. The research also rises awareness among practitioners on the significant changes that need to be implemented to run BYOD practices.

Keywords

Bring your own device, Adoption, Cloud computing.

Introduction

There are strong indications from the literature (Kerr and Houghton 2010, Spierings, Kerr and Houghton 2016) that employees are developing IT artefacts outside the accepted ICT infrastructure of their organization, usually as a workaround to existing systems. In the past, this has been controlled to some extent, as these developments have been confined to corporately condoned software applications using devices provided by the organisation. While these artefacts have caused some concern to centralized IT departments, they have been able to be accessed from time to time and this has usually resulted in a purge of these systems. In this paper we are referring to these workarounds as feral information systems (FIS), based on the work of Kerr and Houghton 2010. These audits of FIS have resulted in a better understanding of what people have developed and why they were developed, and decisions are made whether to keep the system or remove them. However, we contend that the game is changing and that greater access to the internet and cloud computing has lead to the increased use of mobile apps being accessed and modified on employee’s personal devices (Kerr and Koch 2014). This along with an ever-increasing number of employees using their own devices at work has made it harder for IT departments to exercise the same amount of control over FIS applications as they have in the past. This paper builds on earlier work by Kerr and Koch (2014) that looked at the BYOD phenomena from a “workplace tension” perspective and expands it to the concept of a paradigm shift.

We suggest that this represents a major paradigm shift for corporate computer technology in both usage and how these ‘innovations’ affect corporate IT governance and systems security. The large-scale personal
use of devices such as iPads and smartphones for example, has shown that individuals are very quick to accept new consumer based technology. In many cases these “digital natives” are able to adapt software about to their own work situation using their own devices. However, whether this adaptation is in the best interests of the organization can be debated. There may well be advantages with respect to greater agility for the organization and this could lead to innovation, however there could also be problematic situations with unbridled adaption without proper controls leading to errors in software outputs and subsequent reporting. Examples of this can be shown in work by McGill (2005) who showed that user developed Excel spreadsheets had many errors.

In the context of this paper, adaptation is defined as a process in which an employee customises software in a way that allows them to do their task on their own device, at their own place and in their own time. Adaptation is an unstructured customization of software at the level of tasks relevant to the employee or his/her workgroup and limited to an individual’s IT expertise. Adoption on the other hand is a structured customization at the process level of an organization and is related to the IT expertise of the organization’s implementation group. We contend that the adaption of technology to fit the task is in contrast to the technology adoption models presented in the past and may require a re-think on how effective the technology adoption models are in today’s ever changing, cloud based world. There is increasing evidence that employees are pretending to adopt the enterprise software but are in fact adapting to the corporate sanctioned software through the use of third party software and using their own devices. Therefore, the research questions we pose in this paper are:

1. How effective are the technology adoption models in the new environment of bring your own device, internet-based applications and cloud computing?
2. How does the new approach of technology adaption through the use of BYOD influence the roles of IT departments in organizations?

This paper is divided into the following sections. The next section looks at the history of technology adoption models and how successful they have been in the past with some concerns expressed about how effective that may be in the future. The next section identifies inconsistencies in the adoption model’s predictive capabilities, this followed by an analysis of the adaptation process couched in terms of a paradigm shift to BYOD. The section that immediately follows provides examples of software adaptation from cases studies conducted in various countries. This is followed by a discussion and conclusion section.

**Literature Review**

Research on IS adoption started following the work of Davis (1989) that proposed Technology Acceptance Model (TAM). TAM was developed based on the Theory of Reasoned Action (Fishbein and Ajzen 1991) and it is one of the most influential IS theories that explains users’ adoption of technology (including information technology). TAM posits that the acceptance of technology is driven by two main factors: perceived usefulness (PU) and perceived ease of use (PEOU). Davis (1989) defines perceived usefulness as “the degree to which a person believes that using a particular system would enhance his or her job performance”. Perceived ease of use is also defined as “the degree to which a person believes that using a particular system would be free of effort” (Davis et al. 1989). Perceived ease of use and perceived usefulness are behavioural beliefs and lead to an individual’s behaviour intention and actual behaviour.

There are various extensions to the Technology Acceptance Model. For instance, some scholars proposed adding further factors into the equation, such as subjective norm, perceived behavioral control, and self-efficacy to the main model (Hartwick and Barki, 1994; Taylor and Todd, 1995). Other scholars brought some further belief factors like trialability, visibility, and result demonstrability into the model from the diffusion of innovation literature (Agarwal and Prasad, 1997; Karahanna et al., 1999). Others suggested the addition of some moderating variables into the model, such as demographic characteristics and personality traits (Gefen and Straub, 1997; Venkatesh and Morris, 2000). Among researchers who have suggested extensions to TAM, Wixom and Todd’s (2005) model adds additional belief factors, factors from related models and some external factors.

TAM2 was introduced by Venkatesh and Davis (2000) sought for drivers other than PU and PEOU. TAM2 added social influence factors (such as subjective norm) and cognitive instrumental processes (such as job relevance and result demonstrability) as antecedents to PU to enable a better prediction of information.
technology acceptance. According to TAM2, “people use a mental representation for assessing the match between important work goals and the consequences of performing the act of using a system as a basis for forming judgments about the use-performance contingency (i.e., perceived usefulness) [p. 191]” (Venkatesh and Davis, 2000). There have been recent attempts to factor in BYOD using modifications of the traditional acceptance models (Weegner and Gewald 2014), however presently these are not well known and as we will demonstrate throughout this paper, may not be as applicable due to the clandestine nature of FIS development and the use of BYOD as demonstrated in the cases studies that follow.

**Evidence Inconsistent with Extant TA models**

The paper herein presents evidence for the areas in which technology acceptance models failed to predict. Conducting a qualitative meta-analysis on existing TAM models, Legris et al. (2003) found that, in many cases, TAM failed to predict users’ adoption. For example, in Davis et al.’s (1989) study Perceived Ease of Use was not found to impact user attitude. Taylor and Todd (1995a) and Taylor and Todd (1995b) found no effect of attitude on Behavioural Intention. Hu, Chau, Sheng, and Tam (1999) could not support the impact of Perceived Ease of Use On Perceived Usefulness and attitude. Gefen and Keil (1997) found no influence of Perceived Ease of Use On the Actual Use. We suggest that the adaptation of both existing and introduced software through ubiquitous access of Internet based software and the cloud computing environment has not been considered to be a factor in the adoption or not of enterprise wide systems in the past.

**Evidence of adaptation rather than adoption of software in the workplace**

Several case studies have been conducted the area of understanding why end users develop workarounds (in this context called Feral Information systems – see Kerr and Houghton 2010) in order to adapt their work to the workplace information systems rather than completely adopting the system as intended by the corporation at the time of implementation. We suggest that this adaptation provides end users with enough flexibility to allow them to use the system (apparent adoption) yet only use components they are comfortable with or to circumvent components they do not understand or are uncomfortable with. In order to test this, four case studies designed to investigate workarounds are reported in this paper. With all these cases, the research approach was the same; namely an interpretative case study approach (Klein and Myers 1999, Walsham, 1993) using semi structured interviews that were subsequently transcribed and subjected to thematic analysis using the software package Leximancer. The objective was to provide insights into the social aspects of ICT usage in a mandated ICT environment. The case study approach (Stake 1995; Yin 1994) was selected and qualitative methods were used as the investigation centred on exploring how stakeholders adapted their ICT usage to “get the job done”. As we were concerned with organizational rather than technical issues, the case method (Stake 1995; Yin 1994) was considered highly appropriate for our purposes. All four case studies took an explorative approach (Yin 2004) since the adaptation of the mandated ICT was considered to be local and emergent rather than a priori (Deetz 1996). Therefore, the approach to understanding is primarily abductive, looking to existing theories to provide plausible explanations but not aiming to build or test theory. The cases were all qualitative in nature and included Australian, United Kingdom and Danish organizations and business; see Table 1.

<table>
<thead>
<tr>
<th>Pseudonym</th>
<th>Location</th>
<th>Type of enterprise</th>
<th>Type of research</th>
</tr>
</thead>
<tbody>
<tr>
<td>TRANS</td>
<td>Australia</td>
<td>Transport company</td>
<td>Qualitative – interviews and thematic analysis of transcripts</td>
</tr>
<tr>
<td>UNI</td>
<td>Australia</td>
<td>Tertiary Education</td>
<td>Qualitative – interviews and thematic analysis of transcripts</td>
</tr>
<tr>
<td>DOT</td>
<td>United Kingdom</td>
<td>A UK training organization associated with a UK University</td>
<td>Qualitative – interviews and thematic analysis of transcripts</td>
</tr>
<tr>
<td>DEN</td>
<td>Denmark</td>
<td>A series of small to medium manufacturing businesses</td>
<td>Qualitative – interviews and thematic analysis of transcripts</td>
</tr>
</tbody>
</table>

*Table 1 – Research undertaken with respect to adaptation of technology*
Transcripts from research conducted on all four research locations have been used to gain some insights to the adaptation of existing information systems from a variety of perspectives and cultures. The following extracts from transcripts demonstrate the various examples of how end users attempt to adapt technology to suit their own work needs rather than attempt to adopt the technology as expected by the organization.

In addition to the thematic analysis, we use an approach described by Brodin (2015) within the BYOD research area. Using this approach of analysis, design and action, we analyse each case. Brodin (2015) suggested that the first step (analysis) should present the present state of the organisation and this involves understanding culture, capabilities and the organisational goals. The idea is to determine the gap between the present and desired state (Brodin 2015). In the design phase, the current policies should be looked at as well as the overall business strategy including regulations etc. (Brodin 2015). The action step should include a risk assessment and a plan for implementation.

This research has demonstrated that the use of BYOD was very much ad hoc and in many cases clandestine in all four case study organisations and it is evident that none of the steps outlined by Brodin (2015) steps were undertaken and that each case simply had an unplanned, individualistic growth in the use of BYOD. The use of a framework similar to that described by Brodin would have assisted these cases immensely. In the following cases we will attempt to retrofit the approach that Brodin recommends in order to identify the problems associated with an unplanned, ad hoc introduction of BYOD in organisations.

**Case 1 – TRANS**

Analysis – This organisation had just implemented an ERP system (SAP). The decision to adopt SAP was controversial with the accounting section winning the day. The engineering section wanted a different ERP that was more focused on the safety and engineering aspects of the organisation. This battle left the organisation ripe for the pickings with respect to developing workarounds and by default, opening up the BYOD environment to the development of FIS.

Design – This was not done at all and there were many examples of the potential to develop workarounds through the adaptation of various technologies in this organization. For example; there appeared to be extensive adaptation of technology through the use of other applications other than the mandated system (in this case the enterprise system, SAP). This is confirmed through statements by workers (in this case an engineer) such as “... we've got a diary that tracks all material usage on a daily basis so it will have on there [the IT system] how [much product] we unloaded today so Bruce will come in write in the diary in that section, how many items of [product] he does. That diary then goes into a database internally within here and onto a spreadsheet...” These databases and spreadsheets were developed internally and away from the SAP system. They were examples of adaptation of technology to either supplement the SAP system or replace it. This adaptation uses traditional technology (Spreadsheets on workplace computers), however the expectation is that more technology aware employees will adapt the spreadsheet to a cloud based application in the future to enable more remote applications of the technology. In another example an employee expanded on a common theme throughout this research, namely the perceived need for a complete analysis of SAP and its role within the organization, for example the quote “Better metrics needed – that is better ways to apply models of analysis etc.” indicate a degree of discontent with the organisation and the ERP implementation and a possible lead into software adaptation further down the track.

Action – the organisation has no action plan other than adapting their IT infrastructure to cloud based solutions and depending on third party software providers to help integrate their own IT into cloud based solutions. In many cases these FIS’s were completely unknown to senior management.

**Case 2 – UNI**

Analysis - The university case was based on questioning security issues and how employee computer usage (access to the cloud and adaptation of software) affected the governance and security of the organization.
Design – This was not done well and the transcripts reflected the views of the information technology manager’s perspective on security and cloud computing. All three people were interviewed at the same time. They were the Director of information technology services, the manager of Information Technology Services (ITS) and the ICT Infrastructure Team Leader and data security manager.

With respect to the current policies, the director of suggested that “The most fundamental aspect of security is accountability through the audit function of the institution, we are held responsible for the custodianship of financial data” and “ICT security at the most fundamental level in terms of being audited as an organisation”. The Director further asserts that “The place that the auditors will go is IT to determine how secure the financial data is…. This is extended to all assets associated with the university’s core business” She then posed the question “Does increased use of non-corporate cloud-based applications affect the organization’s ability to provide auditable secure financial data?”

The Data manager indicated that a major challenge for the University was maintaining information security in a mobile world and this is not so much the technology but the behaviour pattern of staff and students. He went on to ask the question “How do we know if the person accessing the information is the person they claim to be?

The director went on to suggest that cloud computing is the next threat because although systems can be locked down within your own environment, the problem is the accountability the University has when a service that is not housed on the campus. IT staff have no capability to control over what is done “in the cloud” by academic staff and students. The director was concerned that nothing is done about “the cloud” until there is a security problem and then it is fixed but the industry is always in catch-up mode.

Action - This case example demonstrates the concern the centralized IT function has with respect to employees and students adapting technology to suit their own requirements. The industry appears to be always in “catch up mode”

**Case 3 – DOT**

Analysis - The adaptation of technology to “fit” within the existing system was prevalent in this organization and there did not appear to be any other approach other than a complete lock down of IT within the organisation. For example, USB thumb drives were completely banned.

Design – There were many design issues in this organisation because all data was treated as confidential. For example, the deputy director of DOT had concerns about the financial system and how the lack of feedback was particularly problematic for him. He stated that “Financial systems are an example where the financial information is entered and stored and managed by a separate finance department …… They give us a printout which is designed to suit their purposes and not necessarily designed to suit our purposes in managing the team …..The finance department have produced an outline spreadsheet which is very course in the way that the data is presented so we have short courses that we budget so much – then they ask us “does that look OK?” and we don’t know what assumptions underpin that particular number [and] what courses are included [and] what the associated risk of these courses. Does it include courses that are 100% certain to run or does it include aspirations and to what level so our interpretation of that can be difficult – it could also mean that other department’s interpretations can be different to ours which means that they’re not getting a good picture of what our financial situation is and as a result we are not getting the right information in which to manage our activities to best effect to deliver the financial performance targets of [DOT]”. [Deputy Director of DOT]

Action – There were no actions here either. This is an example of the frustration expressed about systems lacking in feedback capability and how the adaptation of the existing system is more acceptable solution rather than the adoption of a flawed system (at least perceived to be flawed by the respondent).

**Case 4 – DEN**

Analysis – This was a large supermarket chain in Denmark. The respondent was a mid-level manager in one of the supermarket’s stores. In this example the company did not offer a calendar management system. In this case the manager tool it upon himself to use his own device and cloud services to provide a workaround solution for himself.
Design – This example involved the downloading of software from the Internet. He elaborated “…downloaded from the Internet as you could say public software available on the Internet that we download and integrate with our own systems in order to have an easier day. An example of that, we have our Notes calendar and email. So, calendar, as today my meetings are wall to wall, all morning. So, I’m very dependent on knowing where to go next and at this point of time the business or the organisation doesn’t offer [an] electronic calendar that you could carry around. We only have the calendar here. But it's pretty convenient to have the calendar on your mobile phone. So, when the organisation doesn’t offer that, what do we do? It’s only top management who has this feature. So, middle management like me and a lot of my colleagues, we find [a] work-around. It’s not authorised, but we do it anyway. So, I downloaded this application here called AweSync. It’s a product that can take my Notes ID Calendar here and put it into my Google account. Okay? So, when it’s on Google Calendar, I can set up my smartphone and that I can hook up with Google. So, now I have an updated calendar on my phone with business information.”

Action - This demonstrates a situation where a prevalence of Internet based software makes it easy for end users to adapt their corporate system to suit their own needs. However, this was not condoned by the central IT department and issues such as security and governance must be considered.

**Lessons learnt from the Cases**

The TRANS case showed examples of adaptation of software and the use of their own devices to fit individual tasks in order to make their work easier (in this case the development of an Excel spreadsheet application). There appeared to be a clear case of SAP not being able to emulate the material usage process within this work group effectively or the task associated with the process was not aligned with the standard approach developed during the implementation and adoption of the SAP software (see table 2). In addition, the statements about looking for “better ways to apply models of analysis” appeared to be a further indication that the SAP system did not fit the requirements of the workgroup. The lessons learnt from this case relate to the people directly involved with specific tasks and how well those tasks reflect the enterprise wide process that the ERP was supposed to cater for (see table 2).

The UNI case provided an example of how IT management were concerned about the adaptation process with employees’ computer usage possibly effecting governance, security and risk management profiles of the University. The director of IT services considered the IT infrastructure to be a vital component of the University’s governance structure and suggested that any audit of any aspect of the University will start at the IT services level and that the university executive needs the system to be accurate and accountable. Therefore, the concern about adaptation of software and cloud computing is that there may be some inadvertent or even deliberate attempts to alter the integrity of the IT systems in place. Naturally there are safeguards in place and the technology is very good, however the IT director was more concerned about the behaviour pattern of staff and she posed the question “How do we know if the person accessing the information is the person they claim to be? “. The lessons learnt from this case are related to adaptation causing possible concerns about governance, security, privacy, liability and risk management.

The DOT case provided an example of the problems with inter-organizational information systems and how an inter-organizational IT application did not provide the required level of detail. This resulted in a temptation to adapt the application to suit the specific requirements of the case study department. Lessons learnt from this case relate to the IT abilities of the individuals concerned. In this particular case the individuals have very limited knowledge and expertise in spreadsheet development and this situation could have led to a risk of inaccurate calculations, inadequate privacy and problematic security (see table 2). Because the IT infrastructure was so locked down in this case example, all this work was undertaken on their own devices. This goes against the “single point of truth” mantra of ERP systems as there are at least two or may be more copies of the Excel spreadsheet and these cannot be linked or updated.

The DEN case provided us with an example of adaptation from a true BYOD perspective. In this case the person actually downloaded an app to allow him more flexibility in his appointment scheduler. The lesson learnt from this case is in relation to a requirement for flexibility in tasks and a need for the BYOD ideal of access to his diary and scheduler at any time, any place and on any device. In this particular case it was his smartphone. The implications to security and privacy are unknown at this point in time, however there were no security checks on the software for malware or keyloggers etc.

*Twenty-fourth Americas Conference on Information Systems, New Orleans, 2018* 6
While the first three case examples may have been related to the workplace environment, they could have equally been achieved under a BYOD environment. For example, an Excel spreadsheet can be easily developed and/or edited on any device, at any time and at any place. It is entirely possible that these adaptations were done at home on an iPad, smartphone or a personally owned notebook computer. In fact it would seem more likely that these adaptations were done in a BYOD environment thus allowing for more flexibility and freedom from the pressures of work in a home setting.

**Adaptation: A Paradigm Shift towards Bring Your Own Device (BYOD)**

The recent advances in ubiquitous technologies have brought the attention of some businesses into the concept of anywhere, anytime and any device, as a possible promise to reduce cost and seek more efficiency by asking employees to use their own devices and in a time and place they feel most comfortable in with respect to the given task. On the other hand, many other businesses are struggling with the BYOD concept due to many factors, associated with the old model of a centralised IT department and the perceived need to have tight IT controls to ensure proper governance structures and to ensure the network is secure. Regardless of how conservative the organization is with respect to governance and security issues, employees from all walks of life and industries are embracing the concept of BYOD because it provides them with benefits such as work satisfaction, and a flexible working environment. This has led to a growing trend among employees looking to gain access to their workplace networks on their own devices, in their own place and at their own time to get their tasks done.

Employees, having brought their own devices, may no longer seek corporately purchased technologies, rather they may look for adapting the given task with the technology that they are already familiar with and use regularly. According to the above described cases and the lessons learned from them, Table 2 provides a comparison between adaption and adoption.

**Discussion**

This paper has provided examples of how employees adapt existing, adopted and usually mandated software to suit their own requirements or download Internet based applications to adapt to their own work-related tasks. This trend appears to be much more prevalent over the past few years and we argue that this is possibly due to employers wishing to continue with the implementation of enterprise wide systems that some employees consider inflexible systems. Frameworks have been suggested to cater for the BYOD phenomena (Bordin 2015, Lee, Warkenin, Crossler and Otondo 2016) however these frameworks do not seem to be well known and where not used in the cases described in this paper.

Work by Weegner and Gewald (2014) looking at the factors of employee decision-making with respect to BYOD indicated that to many employees, the perceived benefits of BYOD adoption outweighed the risks. It was also noted that in the Weegner and Gewald research that the innovativeness of the employee was a strong influential factor for the adoption of BYOD. This research appears to indicate that the trait of innovativeness is an important determinant for the desire to develop FIS through the use of BYOD.

In this research we have described the customization process in terms of adaptation and adoption. We suggest that adaptation is becoming more prevalent with increased knowledge of the technology and the BYOD phenomena and that employees have a desire to innovate outside the mandated IT infrastructure provided by their employer. We also suggest that adoption is related to enterprise wide applications and is mostly done in the work environment by trained IT professionals. On the other hand, the adaption process is much less controlled with developments being undertaken by people who may not be professionally trained but have adequate knowledge. This adaption process is likely to occur at home or some other non-work related location using their own personal devices. We asked two questions, namely:

1. How effective are the technology adoption models in the new environment of bring your own device, internet-based applications and cloud computing?
2. How does the new approach of technology adaption through the use of BYOD influence the roles of IT departments in organizations?

In answer to our first research question, we suggest that the traditional adoption models outlined in the literature review may have inherent problems as they are not able to cater for this adaption process. In
the situations we outlined in our case studies, employees did not actively reject the technology but on the other hand they did not actively adopt it either. The adoption model may indicate acceptance and adoption of a certain technology but in fact end users are happily using adapted or even alternative technologies in order to get their work done and due to the clandestine nature of many of these systems, they may not be detected by the centralized IT department at all. In addition, the specific BYOD adoption models described by Weegner and Gewald (2015) may not be useful because the organisation doesn’t even know there is a BYOD problem.

The adaptation rather than adoption could in part explain the negative results reported by Legris et al. (2003) and Gefen and Keil (1997). It would therefore be interesting to see if the TAM models are able to accurately predict adoption in more recent examples shown in our case studies. The research undertaken by Weegner and Gewald (2014) does provide a model for BYOD adoption. However, the fact that employees may appear to be happy with the mandated IT system and that FIS developments using BYOD may be clandestine, management may not even be aware of potential problems. We also suggest that many adoption models predict a satisfactory adoption by end users but do not detect that employees have in fact only adapted the measured IT system and are using other technologies to suit their specific job requirements or tasks. It may also be that actors are adapting technology in order to more fully understand and complete their tasks because of other external factors such as: fears of job security, shifts in global markets, increases in layoffs and other related issues.

In answer to our second research question, we suggest that this new world of digital natives and their ability to adapt software to their own requirements needs to be accounted for by managers and IS researchers. Managers need to be aware of and either stamp out the resultant software adaptations or cater for the new approach. There are obvious risks with catering for adapted technologies (although there may be no other option), for example the adapted software is only as good as the IT abilities of their author and they may contain errors. Research by McGill (2005) demonstrated that spreadsheets in particular can be problematic with respect to end user errors (McGill 2005). On the other hand, the adaptation of software can bring agility and innovation for the organization and can lead to new ideas and

### Table 2 Adaptation versus Adoption

<table>
<thead>
<tr>
<th>School of thought</th>
<th>Adaptation</th>
<th>Adoption</th>
</tr>
</thead>
<tbody>
<tr>
<td>BYOD: Characteristics</td>
<td>- Any time</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Any place</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Any device</td>
<td></td>
</tr>
<tr>
<td>Enterprise software Characteristics:</td>
<td>- During working hours</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- At the place of work</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- On a work station</td>
<td></td>
</tr>
<tr>
<td>Definition of Customization</td>
<td>Who</td>
<td>Individuals or local work groups</td>
</tr>
<tr>
<td></td>
<td>What</td>
<td>Tasks</td>
</tr>
<tr>
<td></td>
<td>How</td>
<td>- unstructured</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- kept secret</td>
</tr>
<tr>
<td>IT abilities</td>
<td>IT expertise of employees</td>
<td></td>
</tr>
<tr>
<td>Governance</td>
<td>No support of governance processes</td>
<td></td>
</tr>
<tr>
<td>Security</td>
<td>Low level of security</td>
<td></td>
</tr>
<tr>
<td>Privacy</td>
<td>Determined by individuals</td>
<td></td>
</tr>
<tr>
<td>Liability</td>
<td>Individuals’ responsibility</td>
<td></td>
</tr>
<tr>
<td>Risk management</td>
<td>- handled by individuals</td>
<td></td>
</tr>
<tr>
<td>Ownership</td>
<td>Who owns the work?</td>
<td></td>
</tr>
<tr>
<td>Efficiency</td>
<td>Highly related to the context of development</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Implications</td>
<td>Governance processes are strategically supported</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Highly secured (relevant security software and policies are in place etc.)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Determined by enterprise policies</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Supported by the legal infrastructure of the enterprise</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- handled by enterprise</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- reactive</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Enterprise wide ownership</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Highly related to the context of development</td>
<td></td>
</tr>
</tbody>
</table>
ways of doing business. From an IS research perspective, there appears to be a need to reconsider the adoption of technology models to cater for digital natives and their natural affinity to adapt rather than adopt the technology. From an organizational perspective, this phenomenon could be particularly problematic if the board and upper management is expecting reports and forecasts to be obtained from the “a single point of truth”, namely the implemented ERP system.

The adaptation of mandated enterprise systems may also be of concern to centralized IT departments with rigid command and control structures. However, if a less rigid structure is adopted, a more flexible workforce could lead to greater agility and innovation for the organization. Companies such as Intel have demonstrated an awareness of this phenomenon through their acknowledgement of a BYOD workplace (Intel 2012). Intel has suggested this is the future of IT and that, by our inference, the adaptation.

Conclusions

Although this research is looking at emergent behaviours, we suggest that it does provide enough evidence to suggest that the present TAM type models may be lacking in providing an explanation for the adaptation process and that this phenomenon may be subsumed within the model and simply assumed to be genuine adoption of the technology under study. In this research we are suggesting therefore that the TAM type models be modified to allow for adaptation as another factor in the adoption process. This has been done to some extent, however there could still be a potential problem with the status of BYOD usage being largely unknown by the relevant authorities.

With respect to the first research question regarding the effectiveness of the technology acceptance models, we suggest that this adaption process should be catered for as mentioned above, the existing technology adoption models may be reporting complete adoption by employees yet many employees may be adapting technology to suit their purposes and giving researchers and management the impression that they have adopted the system completely. This could be a flaw in the model with quite serious repercussions for both the company and the end users if the non-recognized software purchases and/or modifications cause problems further down the track. This is apart from our obvious position of requiring models that can accurately predict outcomes and allow for as many contingencies as appropriate. In this research we are suggesting that an understanding of the nature of software adaptation is an important consideration when applying adoption models in the real world.

With respect to the second research question regarding the influence on IT departments, the adaptation of corporate software could lead to innovation for the organization, or it could lead to erroneous reporting due to spreadsheet errors or problems with downloaded software (for example). Whatever the case, the adaption of software is here to stay and both managers and IS researchers need to be aware of the phenomena and any implications it may have on the organization. In relation to potential errors, it is important that consideration be given to the quality of work that may come from adaptation of software by people who do not have a deep understanding of software development processes. Although digital natives may be very familiar with the technology, it does not mean that they are necessarily very good at the process. It may be that they have knowledge a mile wide but only an inch deep and end up developing inappropriate or flawed software. This is an area that could warrant further research.

In concluding our analysis of we argue that there is a need to study the phenomena of technology adaption further. In particular, more research is needed to understand how modern software platforms increase the problems of risk, software adaptation and FIS creation. This research leads to the question, what are the implications of these issues on the modern enterprise? We have argued here that these systems are a natural response given that technology to facilitate these actions is increasingly available through the internet and that the new generation of employee is much more technologically aware of possible digital solutions. However, more research needs to be conducted so we can understand the phenomena of technological adaption better.

References


Deetz S. 1996 “Crossroads—Describing Differences in Approaches to Organization Science: Rethinking Burrell and Morgan and Their Legacy”, Organization Science 7(2) 191-207


Kerr, D; Koch, C (2014) A creative and useful tension? Large companies using “bring your own device”. IFIP Advances in Information and Communication Technology, Aalborg, Denmark, 2014.


