EMERGING FROM THE SHADOWS: SURVEY EVIDENCE OF SHADOW IT USE FROM BLISSFULLY IGNORANT EMPLOYEES

Research Paper

Mario Silic, Swiss School of Business and Management Geneva, Switzerland

Dino Kolak, Swiss School of Business and Management Geneva, Switzerland

Marijana Leontic, College of Environmental Health and Safety, Croatia

Abstract

Current research dealt with various aspects of Shadow IT. However, we still do not have an evidence of how much the phenomenon is widespread in organizations. Are employees really using Shadow IT and how much? We conducted an online survey of 450 employees in 5 organizations to understand how much Shadow IT is used by employees. Our research found that Shadow IT phenomenon is widespread in the organizational context. We found that 52% of "Blissfully ignorant" employees, despite their 75% awareness of information security policy, do use Shadow IT to satisfy their job needs, increase their productivity and efficiency. These illegal activities are conducted as employees miss clarity on the proper compliance behaviors regarding Shadow IT but also because they believe that IT department cannot meet their needs in terms of the approval speed. Our study has several important insights for practitioners and offers some future directions for researchers.

Keywords: Shadow IT; software; organizational IT; shadow systems; information security

1 Introduction

According to Gartner (2014) by 2015 "35 percent of enterprise IT expenditures for most organizations will be managed outside the IT department's budget". While this can be seen as scary prediction, on the other side, it is also not a very surprising one as employees do not anymore want the technology to be contextualized for them by an IT department. Instead, they want to work faster, be more efficient and more productive (Silic & Back, 2014). These reasons led to the birth of the Shadow IT phenomenon which empowered employees by providing them tools, services and systems for which an official IT department approval was needed. Shadow IT represents all hardware, software, or any other solutions used by employees inside of the organizational ecosystem which did not receive any formal IT department approval (Silic & Back, 2014). At its origins, Shadow IT was perceived as a security risk (D'Arcy & Marketing, 2011) which could endanger organizational systems by the non-compliant employees behaviors. Moreover, Shadow systems could also undermined the official systems (Strong & Volkoff, 2004) or jeopardize the organizational information and data flows (Oliver & Romm, 2002). Many other challenges are accompanying Shadow IT use such as compliance issues, wasted time, inconsistent business logic, increased risks for data loss or leaks, wasted investment (Silic & Back, 2014).

The 2012 French survey[1] of 129 IT managers classified top shadow applications as follows: Excel Macro 19% software 17% Cloud solutions 16% ERP 12% Business Intelligence (BI) systems 9% Websites 8% hardware 6% VoIP 5% Shadow IT project 3%. Another case study of a large international company revealed that Greynet (networking applications – e.g. Skype), Content apps (e.g. PDF viewer) and Utility tools (e.g. Video converter) are the most used Shadow IT applications in the organizational context (Silic & Back, 2014).

Despite the previous literature findings on the “the good, the bad and the ugly” (Behrens, 2009) of the Shadow IT, interestingly we still do not have any evidence of how much Shadow IT phenomenon is really present among company’s employees. How many employees are really using Shadow systems? Reason for this knowledge gap probably lies in the fact that access to data is rather limited. Indeed, similar to some other contexts such as the black hat research - hacking practices (Mahmood, Siponen, Straub, Rao, & Raghu, 2010), there is no an easy way to gather necessary information on illegal employee practices. Many practitioner studies provide usage numbers. For instance, (McAfee, 2013) estimates that 35% of all Saas (Software as a Service) applications in organizations are purchased and used without oversight. But, one of the challenges with these studies is that they usually do not follow the scientific rigor where the results could be biased by the vendor interests.

However, we believe that better understanding of how much Shadow IT is really used by employees could bring important insights about the Shadow IT phenomenon. In this research paper we aim to investigate the Shadow IT use by employees from five different organizations. Therefore, our core guiding research question is:

How much is Shadow IT used by employees in organizations?

[1] RESULTATS DE L’ENQUETE SUR LE PHENOMENE DU « SHADOW IT » par Thomas Chejfec : http://chejfec.com/2012/12/18/resultats-complets-de-lenquete-shadow-it/

To answer our research question, we are using an online survey that was run in different types of organizations at national and international level. Our study has important implications for practitioners as it offer valuable insights on the Shadow IT phenomenon use within the organizational boundaries. Also, from the theoretical standpoint, our study provides new facts that help to further understand and theorize about the employee compliance with IT security policies.

In the next section we will review the literature and then we will present our results. Finally, we will proceed with the discussion and conclusion sections

2 Literature review

There are several different terms to describe the Shadow IT phenomenon. Rogue IT, shadow systems, workaround systems, or feral systems are just some of them. We use Shadow IT term in this study as it seems to be the most widely accepted in the literature. Shadow IT defines the same autonomous developed system, process, and organizational unit developed without the awareness, acceptance, knowledge, or support of an IT department (Rentrop, van Laak, & Mevius, 2011). It is often seen as a security threat (Györy, Cleven, Uebernickel, & Brenner, 2012) or even as an 'insider-threat' where a non-malicious employee uses and installs non approved software and where there is strong non-compliant behavior from the employees related to information security policies (Merrill Warkentin & Willison, 2009). 'If users do not comply with ISsec policies, ISsec measures lose their efficacy' (Puhakainen & Siponen, 2010). Shadow IT has an important dual-use context (Silic, 2013; Silic & Back, 2014) where it can have positive effects on the organizational ecosystem but it can also bring negative consequences. On the negative side, Shadow IT is said to undermine the official system (Strong & Volkoff, 2004) or even damage organizational data and processes (Oliver & Romm, 2002). On the positive side, Shadow IT systems can be very efficient and effective when used in place of the formal and standard systems already present (Behrens & Sedera, 2004; Harley, Wright, Hall, & Dery, 2006).

Similar to past studies and relying on the ISsec threats taxonomy (M Warkentin, 1995), we define Shadow IT as an insider threat which is caused by employee or the human factor. This insider driven threat is considered to be a non-malicious one as employee does not have any intention to commit any damage. From that perspective, Shadow IT can be situated on the fringes of organizations, where it fills the existing gap between users and the solutions provided by an IT department (Behrens, 2009). This is typically a business and IT alignment domain which should reveal the organizational capability to fulfil business needs with IT abilities (Henderson & Venkatraman, 1993). In this context, IT should be the enabler of business objectives and should have as an objective to reach the goals in the most efficient way possible (Luftman & Kempaiah, 2007). This clear gap in the alignment between business and IT created a context and provides justification to employees to use shadow systems. Past studies have investigated the role of social media software that enables faster business communication (Jones, Behrens, Jamieson, & Tansley, 2004) or Excel/Access self-made macros that provide better productivity outcomes (Sherman, 2004).

More recently, the Shadow IT phenomenon got significant boost with the appearance of new technologies and the ongoing mobile revolution (Rentrop et al., 2011). However, currently only a few studies have investigated the Shadow IT phenomena; a fact that can be largely explained by the fact that access to data is rather challenging (Silic & Back, 2014). For (Behrens, 2009), due to their informality, shadow systems are rarely obvious, which is the major obstacle in getting access to them. Several past studies have already highlighted this 'insider-threat' (Willison & Warkentin, 2013) and the way it can be reduced. One of the questions that still pertains is why there is this strong misalignment between business and IT. Scholars explain this misalignment by : 1) a significant lack of communication between IT and business (Campbell, 2005; Reich & Benbasat, 2000), decreased responsiveness (Teo & Ang, 1999) , or even a lack of support from IT staff when there is a gap in shared knowledge(Earl, 1989).

Recently, studies investigated the link between the IT Governance and Business IT Alignment (Zimmermann & Rentrop, 2014) or even proposed a method (Fürstenau & Rothe, 2014) to detect and evaluate Shadow IT systems.

However, we are still missing a more simplistic understanding of the importance of the phenomenon in the organizational context. How much is Shadow IT used by employees in organizations? Or, is practiced and how much knowing that organizations usually do have very sophisticated measures to prevent Shadow systems use?

3 Research Methodology

Current research lacks a complete understanding of how much Shadow IT is used in organizations. One of the main reasons for this gap is that access to data is very difficult. We used an online survey method to understand the Shadow IT use among employees in 5 different organizations.

Research setting

In order to minimize bias we opted for different organizations operating at national and international level as well as having different cultural backgrounds. In Table 1. Details about participating organizations are presented. An important point to highlight is that most of the organizations (except O2 which had Windows XP) had Windows 7 operating system which is known to have advanced security features that can prevent users without the administrator rights to install any software. This means that any new software installation can be very difficult (not impossible) for non-tech savvy users without the IT department involvement.

Table 1. Survey participant details

	O1	**O2**	**O3**	**O4**	**O5**
Type	Private	Public	Public	Private	Private
Industry	Auto.	Non-profit org.	Gov.	Eng.	Finance
IT dep.	Central	Central	Central	Central	Central
IT dep. size	50	12	15	25	100
# of employees	4200	350	1500	1200	7500
Org. type	International	National	National	International	International

Data collection

To collect data on the employees' shadow systems usage practices, in alignment with the company IT department, we used an online survey method. Our research was done with 5 organizations in which an online survey was running for 2 months. Survey link was sent by email randomly (organizations had internal mechanisms on how to randomly send email invitations to employees) to approximately 10% of all employees from the participating organizations. In total, there were 3 reminders sent out to employees encouraging them to complete the anonymous survey and assuring that their identity cannot be revealed at any point. This was necessarily taking into account the survey topic.

4 Results

Out of 1400 e-mail invitations sent in 5 different organizations we received a total of 480 responses. We eliminated 30 responses mainly due to implausible response times (less than 1 minute) or because of the incomplete answers.

Demographics

In Table2. participants demographics are detailed. We can see that there is very good distribution between male and female participants.

Table 2. Demographics of the participants

Experience	**N**	**in %**	**Gender**	**N**	**in %**
Less than 1 year	24	5%	Male	237	53%
1 - 3 years	73	16%	Female	213	47%
3 - 8 years	176	39%			
Over 8 years	176	39%			

Table 3 provides more details about functions from which participants originate.

Table 3. Participant details per functions

Function	N	In %
Administration	103	23%
Finance and Human Resources	37	8%
Information Technology	66	15%
Management	96	21%
Operations and Manufacturing	74	16%
Other	44	10%

Sales and Marketing	30	7%

Shadow IT use

Through the survey we asked participants to indicate if they ever used or installed any non-approved Shadow system. At the beginning of the survey we clearly explained what Shadow system is and provided several examples. The same approach was used in the e-mail invitation where all the terms were explained. Hence, in Table 4. Shadow IT usage is detailed for Software and Hardware (example of Shadow Software was Dropbox or Skype; example of Hardware is an employee owned USB stick).

There were 37% employees that have installed and used a non-approved Shadow system in their organization. For the Hardware Shadow IT use 52% of employees confirmed positively.

Table 4. Shadow IT usage

Q: Have you every install and use and non-approved Shadow system?			
	Answer	Number (N)	In %
Software	Yes	166	37%
	No	284	63%
Hardware	Yes	233	52%
	No	217	48%

Further, we asked what were the main reasons for using Shadow IT and reasons for not asking an approval from the IT department. Employees affirm that the main reasons for using Shadow IT is because they need it to do their job (42%), to complete it faster (38%) and efficiency (28%) and productivity (20%) are also figuring among the top reasons. Interestingly, 35% of employees are not aware that they need the IT department approval for using the shadow systems. Approval process is too slow (32%) is another reasons why employees do not turn to IT department to obtain the needed system. It also seems that employees believe that their request would be refused (20%) or they are unsure to whom to talk in IT department (12%). Trust in IT department (2%) do not seem to be an issue for employees.

Table 5. Reasons for using Shadow IT

Reason for using Shadow IT	**N**	**In %**	**Reason for not asking IT dept. approval**	N	**In %**
Because I needed it to do my job	191	42%	I did not know that I needed any formal approval	158	35%
To complete my job tasks faster	169	38%	Approval process it too slow	146	32%
To be more efficient	124	28%	Because it would be refused	90	20%
To be more productive	90	20%	I don't know to whom to talk to within IT dept.	56	12%
[I do not think I did anything illegal	45	10%	I do not trust IT dept	11	2%
For fun	23	5%			

Several participants provided also more insights about reasons for using Shadow IT and for not asking the IT department approval. One participant said "*IT Dept guys are normally closed minded and not open to new ideas & suggestions and prone to always follow only what is written in black & white*" and another one added "*I know my USB stick is virus free*".

Information Security policy

We asked participants to provide more insights about the information security policy. Majority of participants (91% or 409) affirmed that they are aware of the information security policy existence. Moreover, 75% (337) of participants did read the policy and 65% (292) claim that Software and Hardware parts regarding the approval process is explained in the policy.

Type of Shadow IT

In Table 6. and Table 7. Software IT usage per software and hardware categories (software categories were identified through synthesis of categories available in the online open source software repositories such as sourceforge.org; for hardware categories we used various online sources) are detailed. Overall, 3 categories are indicated as the most used ones for software: Audi & Video (28%), Business & Enterprise (26%) and Excel Macros (17%). For hardware

USB sticks (59%), External hard drives (20%) and Cell phone (16%) categories seem to be the most used ones.

Table 6. Shadow IT software usage per category

Software category	**N**	**In %**
Audio & Video (ex: VLC media player)	135	28%
Business & Enterprise (ex: OpenOffice, PDF creator, CRM	126	26%
Communications (ex. FTP tools, Bittorent)	36	8%
Development (ex. Eclipse, XAMPP and similar programming tools)	18	4%
Excel Macros (ex self-crated excel macros)	81	17%
Home & Education (ex. Ghostscipt, Moodle)	0	0%
Games (ex. ny non approved game)	27	6%
Graphics (ex. Cam Studio, Inkscape, FreeCAD,etc.)	36	8%
Science & Engineering (ex. matplotlib or similar scientific libraries)	9	2%
Security & Utilities (ex. Nmap or similar security tools)	0	0%
System Administration (ex. shell tools)	9	2%

Table 7. Shadow IT hardware usage per category

Hardware category	**N**	**In %**
USB sticks / tokens / flashdrives	203	59%
External hard drives	70	20%
Optical drives	0	0%
Cell phone / PDA / SIM Card reader	56	16%
Contactless cards / RFID	0	0%
Smartcards	7	2%
Mice / Fingerprint	7	2%

Overall, when asked to indicate which type of Shadow IT they most use, employees indicated that Hardware (27%), Software (25%), Mobile phone (21%) and Excel macro (12%) are the most used types of shadow systems.

Table 8. Shadow IT usage

Shadow IT category	**N**	**In %**
Mobile phone (example: install apps on company mobile phone)	119	21%
Business Intelligence systems	7	1%
Cloud solutions (example: docs.google.com	21	4%
Enterprise Resource Planning - ERP	0	0%
Excel Macro (example: you created your own excel macro)	70	12%
Hardware (example: USB stick)	154	27%
Software (example: PDF creator)	140	25%
Voice over IP - VoIP (example: Skype)	21	4%
Websites (example: access to unauthorized websites)	35	6%

5 Discussion

Our research study aimed at answering the following research question: How much is Shadow IT used by employees in organizations? By conducting an online survey with 5 organizations we found that Shadow IT is very present in the organizational information ecosystem. We could see that 37% and 52% of surveyed employees use software or hardware Shadow systems, respectively. While for hardware part this is not that much a surprising result as USB stick is also part of this category, and USB use is often ‘silently’ approved by the IT department. Moreover, it is not that easy to put countermeasures against plugging-in USB or hard drives. However, software Shadow IT result is quite unexpected and we consider it as rather high. Our research found that 37% of employees do use some type of software Shadow IT. This implies that in most of situations employees have to 1) either install an application or 2) access external service (e.g. cloud solutions). However, most of the surveyed organizations do have Windows 7 which has advanced security features where administrator rights are needed to install a new application. So does it mean that employees are rather tech savvy and somehow bypass these restrictions? This was found to be one of the actions that employees do and bypass restrictions by installing portable apps (e.g. portableapps.com) that do not require any administrator rights (Silic, 2013). Moreover, companies can easily put counter-measures against using external services such as cloud solutions. Still, it seems that employees, despite the fact that large majority is aware of the information security policy existence, are not stopping the Shadow IT use. And what is even more interesting are the reasons why employees are doing so. Our research confirms some previous findings where Shadow IT is used to increase productivity (Sherman, 2004) and efficiency (Jones et al., 2004) or just to do their job. However, we find also an interesting result where the main reason of not asking for IT department is not because of the slow approval process or low level of trust, but due to the fact that employees did not know that they needed to ask for a formal approval. This could be explained by the fact that information security policies are often difficult to read and understand (Bulgurcu, Cavusoglu, & Benbasat, 2010). But, this could also be seen as an opportunity to avoid and fix the existing misalignment (Györy et al., 2012) between users and IT department. Training employees on Shadow IT practices could be another direction that can be explored to lower the potential security risks behind shadow practices.

Overall, employees also believe that the approval process when submitting a new request to IT department is very slow. This could be a call for action for organizations to rethink what kind of role the IT department should play in today's digital transformation of organizations we are witnessing. Organizations are impacted by the all recent technological advances (e.g. mobile, cloud, etc.) and IT department role has to evolve to become much more user centric rather than what it is today.

Finally, our research reveals that high number of employees is fully aware of the information security policy which deals with security behind software/hardware use, but employees are still "blissfully ignorant" and continue their Shadow IT practices despite the sanctions they may experience.

Our research has some limitations. We used randomly chosen sample of employees and did not target the entire population. This could have some effects on the final results.

Implications for practice are manifold. Our research, to our best knowledge, for the first time reveals the importance of the Shadow IT phenomenon (Silic et al. 2004, Silic et al. 2017, Silic 2019, Silic et al. 2016) in organizational context. This is an important learning for practitioners as Shadow IT realities are still ignored in many organizations. We shed some light on Shadow IT practices and its importance for employees. Further, novel insight on why employees do not ask for IT department for a formal approval is revealed. There is a clear gap in the current knowledge as employees are simply not fully of what is allowed and what is not. This is a call for action for all decision makers responsible for the internal communication flows within organization where information security policy does not seem to be either 1) accurately explained or 2) it is not self-explanatory so that employees can receive a better knowledge on security practices surrounding Shadow IT use.

Finally, researchers can use our study as starting point to further theorize and explain the role of Shadow IT in the existing business misalignment between different stakeholders as it is very clear that the current gap is not sitting only within the IT department. Moreover, future research could try to further analyze the role of Shadow IT in the organizational innovation processes and shed light on the Shadow IT positive side, which, so far, did not receive adequate focus in academia.

6 Conclusion

Our research found that Shadow IT phenomenon is widespread in the organizational context. “Blissfully ignorant” employees, despite their awareness of information security policy, do use Shadow IT to satisfy their job needs, increase their productivity and efficiency. These illegal activities are conducted as employees miss clarity on the proper behaviors regarding Shadow IT but also because they believe that IT department cannot meet their needs in terms of the approval speed. Our study has several important insights for practitioners and offers some future directions for researchers,

7 References

Behrens, S. (2009). Shadow systems: The good, the bad and the ugly. *Communications of the ACM, 52*(2), 124-129.

Behrens, S., & Sedera, W. (2004). *Why do shadow systems exist after an ERP implementation? Lessons from a case study.* Paper presented at the 8th Pacific Asia Conference on Information Systems, Shanghai, China.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS quarterly, 34*(3), 523-548.

Campbell, B. (2005). *Alignment: Resolving Ambiguity within Bounded Choices.* Paper presented at the PACIS.

D’Arcy, P., & Marketing, L. E. (2011). CIO strategies for consumerization: The future of enterprise mobile computing: Dell CIO Insight Series.

Earl, M. J. (1989). *Management strategies for information technology*: Prentice-Hall, Inc.

Fürstenau, D., & Rothe, H. (2014). SHADOW IT SYSTEMS: DISCERNING THE GOOD AND THE EVIL.

Gartner. (2014). Gartner Reveals Top Predictions for IT Organizations and Users for 2012 and Beyond.

Györy, A., Cleven, A., Uebernickel, F., & Brenner, W. (2012). *Exploring the Shadows: IT Governance Approaches to User-Driven Innovation.* Paper presented at the ECIS.

Harley, B., Wright, C., Hall, R., & Dery, K. (2006). Management Reactions to Technological Change The Example of Enterprise Resource Planning. *The Journal of Applied Behavioral Science, 42*(1), 58-75.

Henderson, J. C., & Venkatraman, N. (1993). Strategic alignment: Leveraging information technology for transforming organizations. *IBM Systems Journal*, *32*(1), 4-16.

Jones, D., Behrens, S., Jamieson, K., & Tansley, E. (2004). The rise and fall of a shadow system: Lessons for enterprise system implementation. *Hobart*, *Tasmania. ACIS*.

Luftman, J., & Kempaiah, R. (2007). An Update on Business-IT Alignment:" A Line" Has Been Drawn. *MIS Quarterly Executive*, *6*(3).

Silic, M., & Back, A. (2014). Shadow IT–A view from behind the curtain. *Computers & Security*, *45*, 274-283.

Silic, M., Barlow, J. B., & Back, A. (2017). A new perspective on neutralization and deterrence: Predicting shadow IT usage. *Information & management*, *54*(8), 1023-1037.

Sillic, M. (2019). Critical impact of organizational and individual inertia in explaining non-compliant security behavior in the Shadow IT context. *Computers & Security*, *80*, 108-119.

Silic, M., Silic, D., & Oblakovic, G. (2016). Influence of Shadow IT on innovation in organizations. *Complex Systems Informatics and Modeling Quarterly CSIMQ*, (8), 68-80.