Complex Systems Informatics and Modeling Quarterly
CSIMQ, Issue 8, September/October 2016, Pages 68-80
Published online by RTU Press, https://csimq-journals.rtu.lv
https://doi.org/10.7250/csimq.2016-8.06
ISSN: 2255-9922 online

Influence of Shadow IT on Innovation in Organizations

Mario Silic[1], Dario Silic[2] and Goran Oblakovic[2]

[1] Institute for Information Management, University of St Gallen, Dufourstrasse 50, 9000 St. Gallen, Switzerland
[2] Zagreb School of Economics and Managemen, Jordanovac 110, 10000, Zagreb, Croatia

mario.silic@unisg.ch, d.silic@bina-istra.hr, goblakov@zsem.hr

Abstract. Shadow IT is relatively new and emerging phenomenon which is bringing number of concerns and risks to the organizational security. Past literature has mostly explored the "negative" effects of the Shadow IT phenomenon, including, for example, the security aspect where Shadow systems are said to undermine the official systems and endanger organizational data flows. However, the question of how Shadow IT can contribute to leverage user's innovation has not been adequately addressed. We used three methods to understand if Shadow IT can be an important source of innovation for firms: 1) Single case study with international firm that adopted Shadow IT; 2) Interviews with 15 IT executives and 3) Focus group using twitter as enabling tool to interact with 65 IT professionals. We offer a new perspective on how Shadow IT practices can leverage user's innovation. The study offers novel insights on the role of Shadow users in the organizational innovation process and how they contribute to new innovations by using Shadow IT. Not only this user led innovation through Shadow IT brings positive outcomes for the employee, but it also reveals the path to follow for organizations to increase their innovation capabilities.
Keywords: Shadow IT, software, organizational IT, shadow systems, information security, innovation.

1 Introduction

Shadow IT represents all software, hardware, or any other solutions used by employees inside of the organizational ecosystem which did not receive any prior formal IT department approval. "I got to do my job, I have to do it fast and I'm confident that the benefits will outweigh the risks." - is a typical answer to the question of why employees are using something that is non-approved and consequently, is not compliant.

User of these Shadow systems can be any employee that is looking to solve its own needs. Sometimes, this user innovation can be source of a successful commercial product. Sports equipment such as the rodeo kayak [1], mountain bike [2], snowboard [3], and surfboard [4], medical equipment [5], juvenile products such as the baby jogger [6], services such as computerized commercial banking services [7], computer games [8], and films in the animation genre [9] are few examples where user innovations was a success.

Can Shadow IT really be considered as an important source of innovation for firms? When Flowers [10] talked about hackers (someone who seeks and exploits weaknesses in a computer system or computer network) he argued that growth of knowledge workers resulted in a community of users that is able to modify or hack existing products [11].

Shadow IT is relatively a new and emerging phenomenon which is bringing number of concerns and risks to the organizational security. Past literature has mostly explored the "negative" effects of the Shadow IT phenomenon, including, for example, the security aspect where Shadow systems are said to undermine the official systems [12] and endanger organizational data flows [13]. But, they are also said to increase productivity and innovation. However, the current literature does not provide any evidence of a possible innovation increase. We are missing a deeper understanding of the phenomenon and its link with innovation. Therefore, our core guiding research questions is:

What is the influence of Shadow IT on innovation in organizations?

The objective of this paper is understand whether IT managers accept usage of shadow IT and that shadow IT creates innovations. To achieve our objective we are using a triangulation approach combining three different methods 1) revelatory qualitative case study [14] with a global firm that had successfully adopted Shadow IT innovation process; 2) Interviews with Chief Information Officers (CIOs) and 3) Online focus group using Twitter as enabling tool.

Our research contributes to the existing body of knowledge with three central contributions. Firstly, we contribute substantively to an understanding of the Shadow IT phenomenon as source of innovation for organizations. Our study establishes a clear link between the Shadow users (employees using Shadow IT) and innovation where employees by using Shadow IT can be an important source of innovation for their organizations. Secondly, our paper provides an empirical justification and solid grounded basis for further theorizing around the phenomenon of Shadow IT. Thirdly, Shadow users can be seen as employees who are usually considered as threats to Information Systems (IS) and as such they are seen as benign non-malicious insiders that violate IS security policies with benevolent intentions [15]. However, our study suggests that if organizations leverage there IS policies by incorporating mechanisms that would enable, encourage and promote Shadow IT and Shadow users to be compliant, benefits for organizational innovation could be manifold. This opens doors for new theoretical understandings of the employee computer abuse where new insights regarding IS security policies should be further theorized.

The remainder of the paper is organized as follows. First, the concept of Shadow IT is introduced. Next, the study's multi-method research design is outlined, followed by a qualitative exploratory study that examined the Shadow IT innovation phenomenon. Finally, the paper concludes with a discussion of the implications of the study, limitations, and suggestions for future research.

2 Theoretical Background

2.1 Innovation

Innovation refers to invention and exploitation [16] of useful, new (or modified) offerings [17]. It is a process that includes design, manufacturing and marketing of a new product [18].The new product can be a result of a radical or incremental improvement [19]. Closed innovation model where companies traditionally relied on their internal R&D departments was for a long time the best way to approach the innovation process. Open innovation model [20] saw new realities appearing where firms were not relying anymore uniquely on their own R&D efforts, but went outside of their standard organizational boundaries. For [11] the boundary between the firm and other external actors is much less distinct than in the closed innovation model. User, in the innovation literature, is often taking a shape of an upstream, supplier-centric, perspective [11]. In our context, the open innovation model will refer to an internal user that is the final user or end user (learning by using). These final or end users saw an important democratization of the

innovation process enabling them to share their innovations and create rich intellectual commons [21]. The Open Source Software movement is a good example of this democratization phenomenon where user is free to modify and change the source code [22].

In our specific context the user of the Shadow IT is an outlaw user. [11] defines an "Outlaw User" as someone "who, either individually or as part of a group, actively opposes or ignores the limitations imposed on them by proposed or established technical standards, products, systemss or legal frameworks. Outlaw Users may create or use novel hardware or software modifications to existing products, or exploit security loopholes to gain unauthorized access to systems".

We extend this definition by introducing the concept of the "Shadow user" which we define as someone who creates, modifies, or uses any system, process, or organizational unit without any prior awareness, approval, or support from the IT department. This system, process, or organizational unit can be any software, hardware, or any other solution. One example is use of Excel/Access self-made macros that provide better productivity outcomes [23]. Another example of Shadow IT induced innovation could relate to developing productivity or workflow processes outside of the corporate network by using third party applications such as Trello. Shadow users, by using shadow systems, may produce and create new forms of software or hardware that would enhance the existing procedures or processes. Shadow users are at the origin of the Shadow Innovations, which we define as novel system, process, or procedure that extends the typical use of the underlying artefact.

2.2 Shadow IT

Shadow IT defines the same autonomous developed systems, processes and organizational units developed without awareness, acceptance, knowledge and support of the IT department [24]. Shadow IT phenomenon can be seen as an important security threat [25]. It is also an "insider-threat" where there is strong non-compliance behavior of employees related to the information security policies [26]. "If users do not comply with ISsec policies, ISsec measures lose their efficacy" [27]. Furthermore, Shadow IT has an important dual-use context [28], [29], [30] where its use can have positive and negative consequences. On the possible negative consequences there is the possibility to undermine the official system [12], endanger organizational data and processes [13]. On the positive side, Shadow IT can be very efficient and effective when used instead of the formal and standard systems in place [31], [32]. Shadow IT is usually situated at the organization borders where it fills the existing gap between users and the solutions provided by the IT department [33]. This is typically business and IT alignment domain which should reveal the organizational capability to fulfil business needs with IT capabilities [34]. That means that IT should be the enabler of business objectives and should strive achieving them in the most efficient way [35]. The lack of alignment between business and IT creates an ideal environment for Shadow users for the creation of the Shadow Innovations. One such example relates to the unauthorized use of social media platforms [36], [37]. Past literature mainly focused on the role of social media software that enables faster business communication [38] or the productivity impact on employees of self-made Excel or Access macros [23].

In the recent technology era, the Shadow IT phenomena got a significant boost as new number of new disrupting technologies appeared [24]. Despite this fact, only small number of studies investigated Shadow IT phenomenon. This can be explained by the difficulty to access the data. For [33] due to their informality the Shadow IT systems are rarely obvious, which is the major obstacle in getting access to them.

Similar to the white and black hat IS research studies [39], Shadow IT can be seen as "black IT" and as such more profound understanding of the phenomena will lead to a better understanding of the surrounding mechanisms related to Shadow Innovations. Still, the important question is: Can Shadow users really drive Shadow Innovations? In the next sections, we will answer this question and analyze if Shadow users drive Shadow Innovations.

All tables and figures (graphs, illustrations, line drawings, pictures, etc.) must be referred to in the text (Figure 1). Figures must be centered, captions format see in Table 1. Number the figures consecutively with Arabic numerals. Do not abbreviate the word "Figure" in the caption or in the text.

3 Research Design

This paper utilizes a triangulation approach that combines three different methods in order to improve accuracy and strengthen our findings. The research design follows similar approach from the study done by [40].

Firstly, we wanted to collect insights from real-life examples where Shadow IT has been implemented. As currently, Shadow IT studies in the innovation context are scarce, we wanted to study one case in depth that would provide us rich understanding of the phenomenon. Single case studies allow researchers to get unique and deep insights of the case under study, especially if the case is extreme, unique, or revelatory [14]. The organization that we studied was an appropriate case as it openly adopted Shadow IT by incorporating it within its information systems (IS) policies. Organization is a. medium size international company that has 1,500 employees.

Secondly, we aimed to understand the practitioner's perspective about the Shadow IT topic. We used qualitative method which was appropriate given the high degree of uncertainty surrounding the phenomenon under study. That means, not enough was known a priori about Shadow IT usage and its impact on Shadow Innovations to quantitatively measure it or pre-specify its outcomes. Therefore, qualitative method provided a very rich understanding of the underlying mechanisms, activities, and behaviors that define Shadow IT use actions by Shadow users. This involved the collection and analysis of empirical data using a qualitative research approach. Qualitative research is defined as "the use of qualitative data such as interviews, documents, and participant observation data to understand and explain social phenomena" [41]. [41] observed that qualitative research methods are designed to help researchers understand people and the social and cultural contexts within which they live. [42] also notes that "interviews can be useful tools for unpacking motives and experiences".

Thirdly, as we wanted to leverage the generalizability of our findings we created an online focus group by using Twitter platform. With this approach we were able to target and involve high number of CIOs (already members of the highly visited CIO web portal).

3.1 Data Collection

We conducted semi-structured interviews for the single case study (1 interview with CIO and 1 with Vice President of IT) and the interviews with executives (15 interviews) that were selected from different organizations: large firms (40%), security companies (20%), governmental agencies (20%), and independent experts (20%). Out of 15 interviewee, 12 were CIOs and 3 were IT executives (1 IT director, 1 VP of IT and 1 Chief Technical Officer - CTO).

For the focus group study we used Twitter as a platform where any CIO was able to post its comments. We had 65 different CIOs that posted at least one tweet (post on Twitter) with a total of 320 unique tweets.

Interviews were designed as a set of open ended questions with an idea to cover the Shadow IT topic in depth. Overall, the interviews duration was between 38 and 72 minutes, with an average of 53 minutes. Interviews were conducted between February 2013 and September 2014. All interviews were recorded except one (interviewee declined to be recorded – notes were taken). Total of 78 pages of text were collected.

Regarding the focus group, data was collected using Twitter platform. Twitter is a social networking service that enables registered users to post messages that are limited to 149 characters. On the one side, this can be seen as a limiting factor as it could decrease the richness of the information and data provided, but on the other side, it could also be perceived positively as the participant has to compress the information and thus, unnecessary and low quality information can be avoided leading participant to provide essential and key insight about his view on the given topic.

Once data were collected we used the NVivo software (version 10) to code the interviews and the focus group tweets. We used exploratory analysis as suggested by [43] where we analyzed the data by reading through all of the transcripts, quickly identifying and highlighting the ideas in order to get the big picture. Nvivo further enabled us to visually code different patterns, data, phrases and words so we can group them into defined categories and themes. In this preliminary analysis several themes emerged that are further analyzed and discussed in the next sections. Finally, common themes were interconnected and we extracted different levels of abstraction as per Creswell's suggestion [43].

3.2 Demographics and Interview Protocol

In Table 1. detailed demographics of the participants can be found.

Table 1. Summary of participant demographics

	Respondent	**Position**	**Location**	**Gender**	***Date and duration of interview***
Single Case study	C1	CIO	USA	Male	March 2013; 45min
	C2	VP	USA	Male	February 2013; 38min
Interviews With CIOs	A1	CIO	USA	Male	May 2013; 44min
	A2	CIO	France	Female	May 2013; 52min
	A3	CIO	France	Male	June 2013; 61min
	A4	CIO	Germany	Male	July 2013; 65min
	A5	CIO	Portugal	Male	September 2013; 44min
	A6	CIO	Croatia	Female	October 2013; 41min
	A7	IT dir.	UK	Male	November 2013; 59min
	A8	CIO	UK	Male	December 2013; 40min
	A9	CIO	UAE	Male	January 2014; 67min
	A10	VP	Russia	Female	March 2014; 66min
	A11	CIO	Finland	Male	June 2014; 65min
	A12	CIO	USA	Female	July 2014; 43min
	A13	CTO	Sweden	Male	July 2014; 46min
	A14	CIO	Spain	Female	September 2014; 72min
	A15	CIO	Spain	Male	September 2014; 58min

For Focus group participants we are using FG abbreviation with corresponding participant number (e.g. FG1 corresponds to participant number 1). Overall, we aimed to get a deeper understanding of innovation process at the organizations to which participants belonged and what are the challenges related to employee non-compliant Shadow IT use. Moreover, we wanted to understand how Shadow IT was implemented in the case organization (case study) and what are the key learnings and challenges. Also, we were interested to understand the role of IT

department and the relationships between employees, innovation and IT processes and procedures.

The entire interview protocol was reviewed by three independent researchers. We also did pre-tests with five selected participants to identify any misunderstandings and in order to further adjust the final interview protocol. Overall, we had four main sections in the interview protocol: 1) Background/context – information about the interviewee where we asked questions such as: What is your position within [organization]? or What is you your understanding of the current information systems setup?; 2) Innovation at [case organization] – where we asked questions related to innovation processed, structure and organization of the innovation within the case organization. An example question is: Can you describe current innovation processes in your organization?; 3) Shadow IT – we wanted to understand more how is Shadow IT phenomenon threated and perceived within the organization. A sample question was: How is Shadow IT threated within the organization?; and 4) open remarks – sample questions were: Did we forget anything? Is there anything else you would like to discuss?

4 Results

In this section, we will present the results.

4.1 Single Case Study

Results from the single case study clearly pointed out that Shadow IT is an important source of innovation. For interviewee (C1): "*Shadow IT is innovative. We are pioneering new ways for employee to do their Job. Their job tasks are no more restrictive by the IT tools deployed by IT.*

With shadow IT, the methods of collaboration with outside clients, the ability to share files and use mobile devices to communicate whilst integrating with our infrastructure anywhere are innovative ways of how employees are doing their jobs. Their jobs scan be done anytime, anywhere and most of the time by any devices are all possible because of Shadow IT tools and services.". However, as pointed out by (C2) Shadow IT needs to be promoted and encouraged with the organization as by doing so new innovation solutions will appear: "*With the proliferation of social media and rich media contents, creation and distribution of media assets are now done beyond the confines of an IT local infrastructure. To allow employees to work beyond the boundaries of the local infrastructure and systems, Shadow IT will need to be encouraged. This will further enable the IT organization within a media organization to collaborate with shadow IT clients to build innovation IT solutions to meet users/clients expectations*."

Implementation of Shadow IT did not go without any challenges. Security and risk management of such practice where employees are allowed to use Shadow Systems is still a grey zone where the control and risk mitigation play key roles. For (C1) "*The greatest challenge is the enforcement and control of policies. [case organization] created and is enforcing policy that governs the use of shadow IT products. We created a BYOD policy. For file sharing, security policies are built around applications that are BYOD centric.*". And (C2) added "*Here are some risks associated with IT: IT Security risks, Data loss, Lack of controls for IP assets, Time consuming*".

Still, perception of Shadow IT in light of all the risks remains relatively negative and organizations tend not to unleash the potential behind Shadow IT and enable Shadow employees to be freer in the employee-IT relationships when it comes to leveraging shadow practices. Indeed, for (C1) companies are still reluctant to adopt Shadow IT "*because most of the products that are used in Shadow IT are consumer graded and the security modules that are in the free offerings are not sufficient for data security. Additionally, when users are involved in technology selection, business processes are not necessarily taken into consideration.*".

Overall, case organization provided an evidence of a successful Shadow IT implementation where Shadow IT is actively promoted within the organization and employees are encouraged to use Shadow IT. This led to new and innovative ways of how job is performed by employees where positive effects were threefold: 1) for employees as they were allowed to propose new innovative ways of performing their job; 2) for IT as better communication and alignment was done with the users, and 3) for external partners and customers as employees could match their requirements by adopting Shadow tools and services needed to effectively communicate, collaborate, and work with their partners.

4.2 Interviews

From the interviews it became clear that Shadow IT is not really such a new phenomenon in itself as users were always trying to bypass IT to come up with their own solutions and tools enabling faster job processes. However, what has recently changed is the arrival of the new technologies such as cloud services, software-as-a-service tools, mobile apps that enabled people to be more innovative through the technology. For example, (A4) says that *"…the phenomenon is nothing really new…however we are witnessing a plethora of new tools and services. Hence, it is more about your job performance and how to optimize it using the innovative technologies available out there. But also, what is the role of IT in this new structure – how IT should be positioned: to allow or disallow?*".

For most of the interviewees the right question is how to expand the innovation teams to a wider population of all employees as good idea can come from any employee and not just from a limited number of people. (A9) argues that "…*in our organization we count over 50,000 employees and if I compare that number with a limited number of people working in innovation labs, it is clear that the focus should shift to the entire organization.".* Overall, all interviewees (except one) agreed that Shadow IT needs to be encouraged and that without the push from the organizational stake holders it may stay at the boundaries of illegally performed activities. One interviewee (A12) provided an example of how in her organization Shadow IT is encouraged: "*we allow anyone to develop any mobile app. We then check the app for security and privacy issues to be sure it meets all required security standards. Once this is done, we put it on the company App store and track the performance: downloads, activity, etc. If it becomes viral – bingo – we may have an app that, after further evaluation, may be used as company standard. And this is innovative.*".

Another interviewee (A9) added: "*we are a technology company with over 60,000 employees and I assume all employees speak the technology language. The approach we took is that we are going out there and speak to our business partners and help them to develop their own business applications. But also, to tell them to come to IT so we can secure it. Our goal is to have an IT department that is a partner and not something you avoid. Of course, we always keep in mind that security is our main concern*".

There was an overall consensus that this new way of approaching the Shadow IT clearly opens the doors to innovation from unexpected angles. In other words, any department, any employee may have hidden talents that can turn to be very innovative. One example came from (A2): "*we just had an employee from the financial department who had some very advanced IT programming skills…he came with a small application that automated a process where 6 people were previously involved to have it done….it saves us huge amount of time but also money…he was using unauthorized programs to build the App…but nobody really questioned that part*".

While majority of the interviewees agreed that Shadow IT does bring a number of security issues, they also confirmed that for a successful Shadow IT integration the role of IT department needs to shift from the old style governance to a new governance mode where new and appropriate governance policies, security controls and the overall awareness need to be rebuilt and adapted to the new needs. For instance, (A7) said that "*the way to go is for example to allow*

employees to come up and suggest Apps or process improvements that is not part of the standard IT architecture.". Another interviewee (A13) added *"…the mentality has to change. CIOs have to start to think strategically and take a much broader view of the IT and redefine the relationship between employees and the IT department*".

One interviewee (A1) was strongly against Shadow IT arguing that risks behind Shadow IT are simply too high and cannot compensate any innovation driven activities or processes. Benefits, according to (A1), are not that high compared to all external and internal risks associated with the Shadow systems use.

4.3 Focus Group

Overall, participants noted that the time for change has arrived and there is a need for IT departments to adapt to the new realities brought by the latest technological advances which can unleash and spark employee innovation. Clearly, Shadow IT should be driven, explained and encouraged by CIOs.

For (FG1) IT department is not innovating "*IT dept. today is still on run mode with lost resources just maintaining. NOT innovating*" and one possible reason for this non innovation driven direction is because there is a breakdown in the communication flow between different partners – e.g. (FG20): "*Shadow IT is clearly an indication of the breakdown in communication or trust w/IT*". For (FG12) it is time so shed light on what Shadow IT is and what it can bring "*I argue CIOs should not prohibit shadow IT but rather shed a light on it*". Another tweet from (FG32) pointed out the need to embrace and not to block the Shadow users.

Overall, there was a general consensus about the benefits of encouraging Shadow IT where majority of participants said that Shadow IT can spark the innovation which in this new context would come not only from one single department or lab, but could be generated and driven by a much larger group of people. One participant commented (FG62) "*SIT sparks innovation. And it is now available to anyone*" and another one (FG55) added "*security could be an issue. But benefits could be simply very high*".

Many participants pointed out that security and lack of organizational support will remain strong arguments against promoting and encouraging Shadow IT use. For (FG37) "*clearly, security is a top concern*" and (FG15) added "*lot of orgs will not move. Too dangerous. Too risky*".

5 Discussion

Is Shadow IT an important source of innovation for firms? We tackled this research question by using three different methods: 1) single case study; 2) interviews and 3) focus group. By triangulating the findings from these three methods we can see that Shadow IT can be an important source of innovation for firms. While, these Shadow users are considered to be benign non-malicious insiders threatening Information Systems (IS) and violating IS security policies with benevolent intentions [15], they can also be important and new source of innovation. Indeed, so far, organizations were typically mostly relying on their innovation departments or labs to produce innovations. Interestingly, these user driven innovations benefit innovators (Shadow users) themselves. Hence, users tend to develop fundamentally different innovations because they will alone have benefits from using the innovation [44]. Typically, when Shadow user, for instance, creates a new excel-macro the first user of this newly innovated tool will be the Shadow user. However, many other forms of organizational innovation-driven practices can also contribute to unleash user's innovation ideas. Indeed, Shadow IT can be seen just as one area where employees' find an opportunity that brings them productivity.

Our research reveals that Shadow IT is an important driver of innovations within an organization. From the single case study, where we analyzed a global firm which openly adopted

Shadow IT use, we could see that encouraging employees to propose and suggest their innovative processes led to creating new benefits to the entire organization. This was achieved through an active promotion of Shadow practices where strong alignment between different stakeholders was created in order to have the process secured from end to end. And benefits were manifold. Not only employee's creativity was unleashed but also IT benefited from this end user empowerment as IT department in the newly created environment was much more consulted and became a much stronger gatekeeper for all processes related to Shadow practices. Also, external customers had seen positive effects as tools or services they were using to work with the organization (e.g. using skype to communicate with employees), with the new Shadow IT approach, are now marked as allowed. This opened new and more efficient ways for communicating, increasing productivity, and enabling fast job task execution. On the other side, results suggest that the costs of implementing Shadow IT can also be rather high, which was highlighted by the majority of the participants. Despite this fact, interviews revealed that companies do not have really the choice as the benefits seem to be higher rather than the associated costs. Hence, most of them are thinking of how to make Shadow IT part of their strategy despite all the costs that are behind it. However, not all participants were unanimous on the benefits taking over the costs. Several interviewees pointed out high risks and uncertainties behind Shadow IT practices, highlighting that the boundaries where Shadow IT starts and stops are not clear and will be difficult to define.

Interviews with IT executives were particularly useful as they revealed that Shadow IT phenomenon is currently in a strong expansion with a plethora of new products, services, or tools. And it is not a question anymore how to prevent the Shadow use, but rather how to cooperate and free employees innovation. It is evident that organizations in order to stay competitive or to keep their competitive advantage need to innovate, and one possible direction is to rely on the entire population of employees. Interestingly, when we asked IT executives about existing innovation strategies they have within their organizations, majority (except 1) indicated that their organizations do have various innovation strategies on how to increase innovation among employees. They also highlighted that these strategies are updated on annual basis.

Focus group approach provided a bit higher level of the relationship and risks behind Shadow IT. It is clear that for innovation to happen it has to be further encouraged and this process should be top-down driven. IT department needs to be strongly involved in this transformational process. On the other side, it was also pointed out that Shadow IT is still relatively an unknown phenomenon despite the fact it is nothing really new. And when something is unknown it tends to bring certain risks that are actual risks. Mostly, it relates to how to efficiently handle security challenges behind these "external" systems or processes use such as, for instance, cloud services [45]. More than anything it is the question of trust. In cloud context the question is "*who would trust their essential data out there somewhere?*" [46]. Same applies to Shadow IT where risks related to such practices could also be very high and may diminish all the positive effects behind the innovation idea.

However in order for Shadow IT to be effective and create new innovation opportunities a very strong alignment across the entire organization is needed before any Shadow IT practices are implemented. Past research showed that users innovate as they expect benefits [44] or due to their expertise and knowledge [47], [48]. In Shadow IT, users innovate as they have to fulfill their job needs by doing the job faster and more efficiently. To achieve that Shadow users mostly use greynet (communication applications such as Skype), content apps (e.g. PDF tools), or various social tools (e.g. Facebook chat) to satisfy these job needs [40].

Finally, how to approach Shadow IT user driven innovation process is already a burning topic as it is not a question anymore whether organizations should promote, encourage, and implement the phenomenon, but rather, how to do it. As not only, if done smartly, the already pending risks

may be decreased, but above all, organizations may spark innovation from unexpected places and people.

5.1 Theoretical Contributions

Our research offers several novel contributions to the Information Systems (IS) innovation literature. Firstly, in the existing IS innovation literature, the Shadow IT user driven innovation was not adequately addressed. Our research contributes to the existing knowledge gap by clearly establishing a link between the Shadow IT and innovation where we discover that Shadow IT can be an important source of innovation for organizations. In this context, we tackled also the theoretical question of "why users innovate" [49], by revealing that users are pushed to innovate when organizations do not provide sufficient tools, processes, or procedures to help them to be more efficient or productive. In that context, users innovate by following Shadow IT practices. This is where our research advances existing theoretical understandings of the illegally performed actions. In other words, there is an ongoing challenge in better understanding these "illegal activities" (e.g. similar to black hat (hackers) IS research studies [39]) where employees usually do not want to share or reveal their activities. Hence, Shadow IT can be seen as "black IT" and as such more profound understanding of the phenomena will lead to a better understanding of the surrounding mechanisms related to Shadow Innovations. Therefore, our research provides valuable insights for further theorizing and building upon the Shadow innovation processes phenomenon. Secondly, our study offers new theoretical perspectives in management as it could lead to exploring innovation from a wider population perspective and "illegal" use context. Up to now, these illegally performed activities by employees were mostly sanctioned and discouraged, but better understanding of the theoretical antecedents of Shadow IT usage can help to leverage the entire organizational innovation ecosystem.

5.2 Practical Implications

Our study offers several implications for practitioners. Firstly, our study shows that organizations can benefit from new sources of innovations: potentially entire population of their employees. Moreover, any position or any department can tomorrow be source of innovation. This can be an important learning for organizations that want to transform their business processes. Secondly, there has to be a strong alignment between all stakeholders using the top-down approach when leveraging Shadow IT practices across the organization. Without that approach, the entire process may bring important security risks. Thirdly, organizations may benefit from the very low cost user innovations as the main reason why employees innovate is because they need fast and efficient solutions to satisfy their job needs. In this context, the created innovation may be adopted at organizational level if, after the security assessment, it becomes viral or is widely adopted by potential users. Fourthly, our study shows that Shadow IT is a reality and should not be ignored. On the contrary, with plethora of existing, new, and upcoming technological tools and services, organizations should take this opportunity to create better, safer, and more innovative environment where user tasks would be done faster, better, and in a more efficient way. However, the process of switching from an old-fashioned IT department to a new governance model and control style should be done with care as number of points have to be taken into consideration such as improving the security protocols. To start with, security awareness will have to be redesigned to better communicate the security risks. By doing so, organizations will not only sensitize their employees to all risks that Shadow IT practices may bring, but it will also help to better tackle the security knowledge of their employees. In this context, IT departments should focus more on managing people and not processes/devices as the challenge seems to sit with employees.

5.3 Limitations and Future Research

Our study has several limitations. Firstly, we relied on a single case study where Shadow IT was implemented. This can cause some generalizability issues that we tried to tackle by interviewing several organizations. While many of the interviewed organizations did not officially confirm that Shadow IT is also widely accepted in their organizations, it would have been better if we had more cases under study and from different countries and cultures. Secondly, we used twitter as enabling tool for the focus group which is not a typical way to conduct a focus group. While, with this approach we received high number of responses, we recognize that responses in itself were not very rich as they were limited in number of characters. This could have some effect on the overall interpretation of focus group data. Thirdly, user perspective on Shadow IT is missing as the data was collected from CIOs and higher management levels.

There is couple of avenues for future research. We believe that we opened a Pandora's box when it comes to the Shadow IT phenomenon in the innovation context. Indeed, in future studies we could try to better understand why users innovate when they are clearly committing an illegal action. This opens many questions of users as innovators in the Shadow IT context. Another possible direction could be to further understand the impact of Shadow user driven innovation and try to measure its effectiveness.

5 Conclusion

Our research investigated the Shadow IT being an important source of innovation for firms. We offer a new perspective on how Shadow IT practices can leverage user's innovation. Not only this user led innovation through Shadow IT brings positive outcomes for the employees, but it also reveals the path to follow for organizations to increase their innovation capabilities. Finally, we provide several theoretical directions that could benefit from and build upon our theoretical findings. Also, practitioners may benefit from the study as it offers interesting insights on the role that Shadow IT may have when encouraged, promoted, and implemented in the entire organizational ecosystem where innovations may come from unexpected places and people.

6 References

[1] C. Baldwin, C. Hienerth, E. Von Hippel, "How User Innovations Become Commercial Products: A Theoretical Investigation and Case Study," Research Policy, vol. 35, issue 9, pp. 1291–1313, 2006. Available: http://dx.doi.org/10.1016/j.respol.2006.04.012

[2] C. Luthje, C. Herstatt, E. Von Hippel, "The Dominant Role of "local" Information in User Innovation: The Case of Mountain Biking," 2003.

[3] S.Shah, "Sources and Patterns of Innovation in a Consumer Products Field: Innovations in Sporting Equipment," Sloan Working Paper, 2000.

[4] N. Franke, S. Shah, "How Communities Support Innovative Activities: an Exploration of Assistance and Sharing Among End-users," Research Policy, vol. 32, no. 1, pp. 157–178, 2003. Available: http://dx.doi.org/10.1016/S0048-7333(02)00006-9

[5] C. Lettl, C. Herstatt, H. G. Gemuenden, "Learning from Users for Radical Innovation," International Journal of Technology Management, vol. 33, no. 1, pp. 25–45, 2006. Available: http://dx.doi.org/10.1504/IJTM.2006.008190

[6] S. Shah, M. Tripsas, "The Accidental Entrepreneur: The Emergent and Collective Process of User Entrepreneurship," Strategic Entrepreneurship Journal, vol.1, pp. 123–140, 2007. Available: http://dx.doi.org/10.1002/sej.15

[7] P. Oliveira, E. von Hippel, "Users as Service Innovators: The Case of Banking Services," Research Policy, vol. 40, no. 6, pp. 806–818, 2011. Available: http://dx.doi.org/10.1016/j.respol.2011.03.009

[8] L. B. Jeppesen, M. J. Molin, "Consumers as Co-developers: Learning and Innovation Outside the Firm," Technology Analysis & Strategic Management, vol. 15, no. 3, pp. 363–383, 2003. Available: http://dx.doi.org/10.1080/0953732031000160153 1

[9] S. Haefliger, P. Jäger, G. Von Krogh, "Under the Radar: Industry Entry by User Entrepreneurs," Research Policy, vol. 39, no. 9, pp. 1198–1213, 2010. Available: http://dx.doi.org/10.1016/j.respol.2010.07.001

[10] Open source software getting better. Network Security. 2008, 6:1-2. Available: http://dx.doi.org/10.1016/S1353-4858(08)70070-9

[11] S. Flowers, "Harnessing the Hackers: The Emergence and Exploitation of Outlaw Innovation," Research Policy, vol. 37, no. 2, pp. 177–193, 2008. Available: http://dx.doi.org/10.1016/j.respol.2007.10.006

[12] D. M. Strong, O. Volkoff, "A Rroadmap for Enterprise System Implementation," Computer, vol. 37, no. 6, pp. 22–29, 2004. Available: http://dx.doi.org/10.1109/MC.2004.3

[13] D. Oliver, C. T. Romm,"ERP Systems in Universities: Rationale Advanced for Their Adoption," Idea Group Publishing, Hershey, PA, 2002. Available: http://dx.doi.org/10.4018/978-1-931777-06-3.ch003

[14] L. Dubé, G. Paré, "Rigor in Information Systems Positivist Case Research: Current Practices, Trends, and Recommendations," MIS quarterly, vol. 27, no. 4, pp. 597–636, 2003.

[15] R. Willison, M. Warkentin, "Beyond Deterrence: an Expanded View of Employee Computer Abuse," MIS quarterly. vol. 37, no. 1, pp. 1–20, 2013.

[16] C. Roberts, "Biometric Attack Vectors and Defences," in Computers & Security, vol. 26, no. 1, pp. 14–25, 2007. Available: http://dx.doi.org/10.1016/j.cose.2006.12.008

[17] T. M. Amabile, "Motivational Synergy: Toward New Conceptualizations of Intrinsic and Extrinsic Motivation in the Wworkplace," Human resource management review, vol. 3, no. 3, pp. 185–201, 1993. Available: http://dx.doi.org/10.1016/1053-4822(93)90012-S

[18] C. Freeman, L. Soete, "The Economics of Industrial Innovation," in Psychology Press, 1997.

[19] P. Gardiner, R. Rothwell, "Tough Customers: Good Designs," in Design Studies, vol. 6, no. 1, pp. 7–17, 1985. Available: http://dx.doi.org/10.1016/0142-694X(85)90036-5

[20] H. Chesbrough, "Open Business Models: How to Thrive in the New Innovation Landscape," Harvard Business Press, 2013.

[21] E. Von Hippel, "Democratizing Innovation: the Evolving Phenomenon of User Innovation," International Journal of Innovation Science, vol. 1, no. 1, pp. 29–40, 2009. Available: http://dx.doi.org/10.1260/175722209787951224

[22] V. D. Serafim, R. F.Weber, "Restraining and Repairing File System Damage Through file Integrity Control," Computers & Security, vol. 23, no. 1, pp. 52–62, 2004. Available: http://dx.doi.org/10.1016/S0167-4048(04)00066-5

[23] R. Sherman, "Shedding Light on Data Shadow Systems," Information Management Online, April. 2004.

[24] C. Rentrop, O. van Laak, M. Mevius. "Schatten-IT: ein Thema für die Interne Revision," Revisionspraxis–Journal für Revisoren, Wirtschaftsprüfer, IT-Sicherheits-und Datenschutzbeauftragte, vol. 2, pp. 68–76, 2011.

[25] A. Györy, A. Cleven, F. Uebernickel, W. Brenner W, Eds., "Exploring the Shadows: IT Governance Approaches to User-Driven Innovation," ECIS, 2012.

[26] M. Warkentin, R. Willison, "Behavioral and Policy Issues in Information Systems Security: The Insider Threat," European Journal of Information Systems, vol. 18, no. 2, pp. 101–105, 2009. Available: http://dx.doi.org/10.1057/ejis.2009.12

[27] P. Puhakainen, M. Siponen. "Improving Employees' Compliance Through Information Systems Security Training: An Action Research Study," MIS Quarterly, vol. 34, no 4, pp. 757–778, 2010.

[28] M. Silic, "Dual-use Open Source Security Software in Organizations – Dilemma: Help or hinder?" Computers & Security, vol. 39, Part B(0), pp. 386–395, 2013.

[29] M. Silic, A. Back, "Information Security and Open Source Dual Use Security Software: Trust Paradox," Open Source Software: Quality Verification, Springer, pp. 194–206, 2013. Available: http://dx.doi.org/10.1007/978-3-642-38928-3_14

[30] M. Silic, "Emerging from the Shadows: Survey Evidence of Shadow IT Use from Blissfully Ignorant Employees," Available at SSRN 2633000, 2015.

[31] S. Behrens, W. Sedera, Eds., "Why do Shadow Systems Exist After an ERP Implementation? Lessons From a Case Study," 8th Pacific Asia Conference on Information Systems, Shanghai, China; 2004.

[32] B. Harley, C. Wright, R. Hall, K. Dery, "Management Reactions to Technological Change The Example of Enterprise Resource Planning," The Journal of Applied Behavioral Science, vol. 42, no. 1, pp. 58–75, 2006. Available: http://dx.doi.org/10.1177/0021886305284857

[33] S. Behrens, "Shadow Systems: The Good, the Bad and the Ugly," Communications of the ACM, vol. 52, no. 2, pp. 124–129, 2009. Available: http://dx.doi.org/10.1145/1461928.1461960

[34] J. C. Henderson, N. Venkatraman, "Strategic Alignment: Leveraging Information Technology for Transforming Organizations," IBM Systems Journal, vol. 32., no. 1, pp. 4–16, 1993. Available: http://dx.doi.org/10.1147/sj.382.0472

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

[36] M. Silic, A. Back, T. Sammer, "Employee Acceptance and Use of Unified Communications and Collaboration in a Cross-Cultural Environment," International Journal of e-Collaboration, vol. 10, no. 2, pp. 1–19, 2014. Available: http://dx.doi.org/10.4018/ijec.2014040101

[37] M. Silic, A. Back, "Factors Driving Unified Communications and Collaboration Adoption and Use in Organizations," Measuring Business Excellence, vol. 20, no. 1, pp. 21–40, 2016. Available: http://dx.doi.org/10.1108/MBE-05-2015-0026

[38] D. Jones, S. Behrens, K. Jamieson, E. Tansley, "The Rise and Fall of a Shadow System: Lessons for Enterprise System Implementation," Hobart, Tasmania ACIS, 2004.

[39] M. A. Mahmood, M. Siponen, D. Straub, H. R. Rao, T. Raghu, "Moving Toward Black Hat Research in Information Systems Security: An Editorial Introduction to the Special Issue," MIS Quarterly, vol. 34, no. 3, pp. 431–433, 2010.

[40] M. Silic, A. Back, "Shadow IT–A View rom Behind the Curtain," Computers & Security, vol. 45, pp. 274–283, 2014. Available: http://dx.doi.org/10.1016/j.cose.2014.06.007

[41] M. D. Myers, D. Avison, "Qualitative Research in Information Systems," Management Information Systems Quarterly, vol. 21, pp. 241–2, 1997. Available: http://dx.doi.org/10.2307/249422

[42] J. Hardman, "An Exploratory Case Study of Computer Use in a Primary School Mathematics Classroom: New Technology, New Pedagogy?: Research: Information and Communication Technologies," Perspectives in Education: Recearch on ICTs and Education in South Africa, Special Issue 4, pp. 99–111, 2005.

[43] J. W. Creswell, "Educational Research: Planning, Conducting and Evaluating, Quantitative," 2002.

[44] E. Von Hippel, "The Sources of Innovation," Springer, 2007. Available: http://dx.doi.org/10.1007/978-3-8349-9320-5_10

[45] H. Takabi, J. B. Joshi, G.-J. Ahn, "Security and Privacy Challenges in Cloud Computing Environments," IEEE Security & Privacy, vol.8(6), pp. 24–31, 2010. Available: http://dx.doi.org/10.1109/MSP.2010.186

[46] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, et al, "A View of Cloud Computing," Communications of the ACM, vol. 53, no. 4, pp. 50–58, 2010. Available: http://dx.doi.org/10.1145/1721654.1721672

[47] C. Lüthje, C. Herstatt, "The Lead User Method: an Outline of Empirical Findings and Issues for Future Research," R&D Management, vol. 34, no. 5, pp. 553–568, 2004. Available: http://dx.doi.org/10.1111/j.1467-9310.2004.00362.x

[48] C. Lüthje, C. Herstatt, E. Von Hippel, "User-Innovators and “local” Information: The Case of Mountain Biking," Research Policy, vol. 34, no. 6, pp. 951–965, 2005. Available: http://dx.doi.org/10.1016/j.respol.2005.05.005

[49] M. Bogers, A. Afuah, B. Bastian, "Users as Innovators: a Review, Critique, and Future Research Directions," Journal of management, 2010. Available: http://dx.doi.org/10.1177/0149206309353944