Central IT or Shadow IT? Factors Shaping Users' Decision To Go Rogue With IT

Completed Research Paper

Cecil Eng Huang Chua
University of Auckland
aeh.chua@auckland.ac.nz

Veda C. Storey
Georgia State University
vstorey@gsu.edu

Langtao Chen
Georgia State University
lchen18@student.gsu.edu

Abstract

Shadow Information Technology (IT) occurs when users develop systems outside of the central information technology department. It provides both benefits and risks. Users procuring shadow IT often do not consider integration with existing enterprise architecture, privacy and security protection, maintenance cost, and legal ramifications. Problems with shadow IT must often be resolved by central IT. It is, thus, important for central IT to determine when users will consider shadow IT, and how shadow IT can be managed. This research analyzes paired interviews with CIOs and senior users to identify factors causing shadow IT. The paper finds that the form the shadow IT/central IT duality takes is based on: (a) perceptions of legitimacy of the Shadow IT by the organization and central IT; and (b) the ability of user departments to procure IT independently.

Keywords: Shadow IT, legitimacy, configuration theory

Introduction

As technology continues to evolve, functional departments become further empowered to develop systems outside the control of the central information technology (IT) department (Jones et al. 2004). Not only can users in functional departments develop personal or departmental end-user systems (Rockart and Flannery 1983), they can also obtain software or services from the cloud (Buyya et al. 2009), install information systems on portable devices (Walters 2013), or procure open source software from the Internet. Such organizationally unsanctioned IT is often referred to as shadow IT or rogue IT (Behrens and Sedera 2004; Jones et al. 2004). Shadow IT is essentially ubiquitous - 50-75% of all employees use Shadow IT (Nasuni 2013), with companies spending millions of dollars fighting it (Kiernan 2014). Given the real possibility that users can ignore central IT mandates, potentially compromising organizational performance, it would be useful for a central IT department to be able to predict when users will decide to implement shadow IT, and manage that process.

This research attempts to answer the following questions: (1) "When will shadow IT arise from a functional department?" and (2) "What form will such shadow IT take?" To address these questions, paired interviews with Chief Information Officers and information technology users were conducted to develop a configuration theory. The contribution of this research is that we identify the kinds of shadow IT that emerge from a functional department and then show that the manner in which shadow IT evolves is directly related to the legitimacy of the shadow IT to the overall organization, the central IT department, and the user function. It is also directly related to the ability of the user function to procure IT resources.

The paper proceeds as follows. The next section outlines related research on shadow IT and, especially, end user computing. This is followed by the research methodology. The interviews conducted are then

presented and analyzed. Next, we present the overall findings and implications of the research results and conclude the paper.

Related Research

Shadow IT

Shadow IT refers to information systems developed to support organizational processes that are not under the jurisdiction of a central IT department (Behrens 2009; Behrens and Sedera 2004). Behrens and Sedera (2004, p. 1713) define shadow IT as "systems which replicate in full, or in part, data and/or functionality of the legitimate systems of the organization." Although, traditionally, Shadow IT has been viewed as equivalent to end-user development (Sumner and Klepper 1987; Wulf and Jarke 2004), the two are not synonymous.

First, end-user development assumes the development of systems by users, often using a programming language (Sutcliffe and Mehandjiev 2004). However, modern users are able to procure or source systems independently of central IT, without developing such software themselves. The Internet and cloud computing, for example, provide users with access to alternatives to in-house software. A worker may choose to download and use Open Office in-lieu of the office productivity suite installed. Many people use "individual information systems" and perform work from home (Baskerville 2011). If properly configured, the home computer may access office databases and resources through Remote Desktop, Citrix or related technologies. Alternately, data can be transmitted from office to home through email, ftp, cloud storage services, or various other options. Over 1 in 4 office workers use Dropbox (a cloud storage solution) for work files in an unauthorized way (Nasuni 2013). Mobile computing with personal devices such as tablets and smartphones, similarly enables workers to perform office work with non-standard applications. This has spawned a culture of "bring your own device" (BYOD) in many offices (Walters 2013). There are even open source and cloud-based competitors to traditional enterprise systems. Compiere (www.compiere.com), and Adempiere (adempiere.org), for example, offer open source solutions for such common ERP functions as internal accounting, supply chain management, and customer relationship management (Rai et al. 2009). Similarly, shadow versions of Moodle (moodle.org) have emerged as open-source alternatives to many university learning management systems (Behrens 2009). Cloud-enabled vendors can perform the duties of a traditional IT department, including developing cloud-enabled applications, and maintaining applications and infrastructure. In short, it is possible (though not necessarily probable) for motivated organizational departments (i.e., functional departments) and individuals to employ shadow IT in-lieu of all but the most specialized applications or services that are managed by a central IT group.

Prior research has treated shadow IT as synonymous with end-user development. This may explain why research on shadow IT has been remarkably sparse and has tended to view shadow IT as small systems to work around limitations of enterprise systems (Strong and Volkoff 2004). This narrow view of shadow IT overlooks the increasing prevalence of both infrastructure-based (e.g., cloud data stores), and enterprise-scale (e.g., Compiere and Moodle) shadow IT. Furthermore, this view focuses on tensions between central IT and functional departments that need not exist. For example, there are shadow IT systems that are not workarounds of enterprise systems, but nevertheless allow user departments to perform much needed work. University faculty regularly install and implement their own systems, but central IT departments are not necessarily hostile to such shadow IT. Finally, this view carries an implicit normative perspective of shadow IT, as either good or bad. Strong (2004), for example, highlight how shadow IT can undermine the legitimacy of enterprise systems due to the barriers of shadow IT on enterprise-level information sharing. Behrens (2009) argues that shadow IT has a bad influence on organizations by promulgating a culture that includes a lack of documentation and extreme reliance on the person who develops the shadow system. Implicit in such a view is that the successful implementation and legitimacy of enterprise systems impact an organization positively. An alternate view recognizes that certain stakeholders may benefit from a successful enterprise system, in specific contexts. However, the shadow IT systems may be more organizationally useful and beneficial to the bottom line. As a result, the enterprise system is inherently not legitimate. Wulf and Jarke (2004, p. 42), for example, argue that "[End-user development, e.g., shadow systems] leads to more efficient appropriation processes by empowering users to adapt software to their local needs."

Given the lack of research on shadow IT, relevant questions arise: "When will shadow IT arise from a user/functional department," and "what form will such shadow IT take?" Even for central IT departments not hostile to shadow IT, answering these questions is critical, given that central IT often becomes involved with shadow IT issues. Examples include repairing or maintaining shadow IT when the original developer departs an organization, or when routine software upgrading causes a function, such as Excel macros, to malfunction.

The literature provides some insights into addressing these questions. Historically, end-user development was undertaken because end-users had specific needs for computer programs to support their work that central IT did not support (Ferneley 2007). Often, central IT's high level of workload, priorities, difficulty in understanding an end-user's requirements, and related reasons, prevented central IT from adequately addressing user needs (Ferneley 2007). In short, shadow IT as a phenomenon spans much more than end-user development. Furthermore, the acquisition and use of many kinds of shadow IT require substantially less technological knowledge and experience than previously required for end-user development.

Configuration Theory

This research attempts to develop a configuration theory of Shadow IT. Questions of when and what form (i.e., "When will shadow IT arise from a user/functional department," and "what form will such shadow IT take?") are more amenable to configuration theories (Doty et al. 1993) than to variance or process theories (Markus and Robey 1988; Mohr 1982). Configuration theories are especially amenable to mappings of nominal to nominal constructs; in our case, different organizational environments to distinct kinds of shadow IT.

Analogous to a variance theory, a configuration theory is a set of factors that together predict an outcome. However, the relationship between the exogeneous and endogeneous factors is often non-linear. Indeed, the factors are often nominal or ordinally measured, rather than measured on an interval scale. A configuration theory is an enumeration of the factor values and their outcomes. Well-known examples of configuration theories are the taxonomy of life, periodic table, and Minzberg's (Mintzberg 1993) theory of organizational types (Doty et al. 1993).

Configuration theories are more than atheoretical classification systems. Like other strong theories, they have constructs, establish relationships between constructs and make predictions (Doty and Glick 1994; Gregor 2006). For example, Minzberg's theory defines five ideal organizational types and predicts that organizational performance deteriorates the more an organization deviates from these ideal types (Mintzberg 1993). In chemistry, the periodic table is organized around the construct of the "electron cloud." Type I elements have one electron in the outermost shell, that move in particular ways (construct). The manner in which the electrons are organized determines properties of the element such as its conductance, and whether it will form an acid or a base when dissolved (relationship). The periodic table is also predictive. All Type I elements create a flame when immersed in water. Whereas statistical contingency theories are one kind of configuration theory, most configuration theories are non-linear. Thus, in the periodic table, the behavior of type I and type II elements does not predict how type III elements behave (Fiss 2007). From a statistical perspective, most configuration theories map nominal or ordinal constructs to other nominal or ordinal constructs.

There are two types of contingency theories, typologies and taxonomies. Typologies are theory-driven, whereas taxonomies are empirically driven (Meyer et al. 1993). Thus, for example, the taxonomy of life is continuously being revisited as new kinds of life are discovered. Given the relatively little research carried out on shadow IT, a taxonomic contingency theory appears most appropriate. Therefore, this research will attempt to develop a taxonomy of drivers to shadow IT, which will be represented as a set of trajectories.

Research Methodology

The study began as a project commissioned by an IT service provider interested in shadow IT. The IT service provider wanted to understand the shadow IT landscape, and assess whether central IT groups would be interested in procuring products associated with detecting shadow IT. The researchers were granted permission to ask more broad questions to investigate the shadow IT phenomenon. The IT service

provider gave the researchers a list of customers to contact and question as well as funds to collect data over a three-month period. At the end of the three months, the IT service provider was given an initial report. Further data collection on remaining customers occurred over a further nine-month period.

Data Collection

The intent of the original study design was to conduct paired interviews: one interview with the CIO or equivalent in an organization, and the other with a senior user. The interviewees were interviewed separately, with the CIO blind to the particular user interviewed. Both parties received similar questions to triangulate findings within the organization (Klein and Myers 1999). In one case, users declined interviews, so matches could not be obtained. In two other cases, the participants requested a paired interview with other members of the organization who were also being interviewed.

The interviews were semi-structured in that interviewers prepared a list of questions to ask prior to the meeting, but asked other questions based upon issues raised by the interviewees. Generally, interviews began with the interviewers (a researcher and an undergraduate student) explaining what shadow IT is, and stressing that the interviewers viewed shadow IT as a phenomenon that was neither good nor bad. Interviewees were then asked to state their perceived roles and duties within their organizations. Interviewees were also asked whether there was shadow IT within their organizations and, if so, to specify its nature. When inquiring about shadow IT, the interviewer would not simply accept the interviewee's statements, but would further probe for examples of shadow IT the interviewee might not normally consider, e.g., VBA macros on Excel spreadsheets, applications on mobile phones, and cloud software. For each identified example, the interviewer inquired about the relationship of that shadow IT to departmental and organizational functions. Interviews lasted approximately one hour, and were recorded and transcribed with the permission of the interviewees. In total, 19 participants were interviewed from industries which included health, manufacturing, government, financial, transport, and educational. A breakdown of the interviews conducted is shown in Table 1. A breakdown by industry is not given, as many industries have only one pair.

Table 1. Interviews Conducted

Type	Total
Total People	19
Total Interviews	17
Total Matched Pairs	9
CIOs individually interviewed	8
Users individually interviewed	7
CIO+user interviewed as pair	2

Data Analysis

The analysis of the data involved coding the interviews, creating a concept map to identify themes, and inferring a set of trajectories that would capture and represent the themes and findings from the data.

Coding Interviews. The unit of analysis was the described IT artifact. During the interviews, the interviewees would describe a specific shadow IT artifact, identify who developed it, and describe its history, which included what happened to the shadow IT artifact.

The artifacts were then clustered, based upon their similarities, into a set of trajectories. A trajectory is a sequential pattern of practices common across different individuals or organizations (Kim and Kogut 1996). For example, Chua and Yeow (2010) explored trajectories of coordination across open source software development teams. Kwee (2011) studied the effect of corporate governance orientation on a firm's strategic renewal trajectories over time. Mamanian (2013) investigated the trajectories of the use of mobile e-mail devices. A practice is a repeated behavior common across different individuals or organizations (Faraj and Xiao 2006; Orlikowski 2007). Our use of trajectories and hence a focus on the

evolving nature of shadow IT is appropriate given our questions focused on "when" and "what form" style longitudinal questions.

Three "surface" characteristics of the trajectories were employed to create the taxonomy: (1) the size of the shadow IT system, (2) who operated the shadow IT system at the end of the trajectory, and (3) whether the functional department consulted IT about the shadow system at some point. These surface characteristics were employed because, based upon the clustering, they emerged as highly distinctive differentiating characteristics of the taxonomy.

The trajectories and surface characteristics were identified through an iterative process of discussion and reclassification (Corbin and Strauss 1990). In total, a final set of seven distinct trajectories were identified. A trajectory was identified when a "steady-state" was reached that a real trajectory had been identified. This was done through a process of discussion and reclassification which aided in the identification of important qualitative differences among the trajectories.

Initially, two distinct trajectories identified were: "Shadow IT Replaces Central IT," and "Shadow IT Creates Competing IT Department." In both trajectories, a large shadow IT system is being developed. However, in the former case, the shadow IT is useful across multiple functions or departments, but users do not express dissatisfaction with the central IT department. In the second case, the IT system need not be cross-functional. However, these systems are large, expensive, and critical to the organization - so critical that funding is provided to have a vendor run the system independent of the central IT department. In the end, it appeared that organizational criticality was the essential distinguishing characteristic of both these trajectories, and so the two were merged.

As another example, we initially identified a trajectory for shadow IT that spawned independent vendor enterprises; that is, became independent IT businesses selling new products. However, given that the research focus was on organizational management of Shadow IT, this observation dealt with issues outside the scope of the study and so was not pursued further.

After the initial trajectories were identified, we analyzed them to identify factors that caused trajectory forks. Trajectory forks are factors that, when present, suggest a particular trajectory, but, when absent, suggest a different one. The concept of legitimacy (Suchman 1995) emerged from this analysis. Two kinds of legitimacy issues arose: (1) legitimacy with respect to central IT; and (2) legitimacy with respect to the overall organization. Legitimacy, however, did not explain all of the trajectories. The remaining trajectory forks appeared associated with resource constrains placed on the departments.

Findings

This section presents the trajectories which emerged from analyzing the interview data. The labelled trajectories, the surface characteristics of the trajectories, and the underlying factors that lead to the identification of each trajectory are presented as Table 2. The remainder of the section details each trajectory.

Trajectory 1: Shadow IT Not Allowed to Exist

In a small number of situations, both users and central IT interviewees agreed that shadow IT did not exist. These situations were all characterized by the criticality of the processes and data involved. In all such cases, the organizational processes were highly government regulated.

> *[Shadow IT exists] for things "on the edge," not for the core functions. The guy in Wellington built a little system that helps manage mobile [donated item] collections. And that's ok because its on the edge, its not a core system... But when it comes to basic info, like we received this [donated item] from this donor, we moved it there, it expired, was used by this etcetera, its all in the main info sys.* (CIO)

In these instances, users elected not to develop shadow IT, not because of internal IT mandates, but because users understood that the organization would be seriously harmed if external bodies discovered the Shadow IT (i.e., coercive isomorphism (Meyer and Rowan 1977)).

We actually have to be formally licensed to manufacture therapeutic goods just like a pharmaceutical company have to be to manufacture drugs... Because we have to adhere to stringent what we call GMP requirements... GMP has quite stringent requirements around all kinds of things, including computer systems and IS management and so we are probably a little more structured [than] some other organisations in the way we manage our systems (User)

Table 2. Trajectories representing Shadow IT Situations

	Surface Characteristics			**Underlying Factors**		
Trajectory	Size	Final Operation	Central IT Consulted	Legitimacy-Organization	Legitimacy-IT Dept.	User Resource Proc.
1. Shadow IT Not Allowed to Exist	None	Central IT	Yes	Yes	Yes	Irrelevant
2. Pure Shadow IT	Small	Functional Department	No	No	No	Yes
3. Re-appropriation of Existing Technology	None	Central IT	No	No	No	No
4. Central IT Assumes Maintenance.	Small - Medium	Central IT	Yes	No	Yes	User department unable to support system long-term. Central IT open to supporting system.
5. Central IT Sponsors System	Small	Functional Department	Yes	No	Yes	No
6. Central IT Replaces Shadow IT	Large	Central IT	Yes	Yes	Beginning No, At end, Yes	Yes
7. Shadow IT Replaces Central IT	Large	Central IT	No	Yes	No	Yes

Such organizations did have shadow IT, but not in these critical areas. For example, the user above readily admitted that there were a number of shadow IT systems. In the quote below, the user emphasizes how shadow IT is acceptable, but not when the core, regulated, manufacturing business is affected.

People were using laboratory reagents that were expired, because they weren't reading expiry dates on the label... So they developed a spreadsheet where when the reagent comes in the goods area, it was the goods people enter the batch number and the expiry date of the reagent into the spreadsheet. ... Every day they scan and check the reagents they have in stock against their spreadsheet and if anything is out of date, it will highlight red cell... but I can't think of any spreadsheet that are doing things that are going to have some critical impact on patient's safety.

All of our critical safety stuff is done within [central IT system], which is the exhaustively validated system. (User)

Also, in such organizations, users were mindful and considered the potential impact of their shadow IT systems on the organization.

> *So the risk with that is if it still goes wrong, then they might end up using an out of date reagent. Which is going to be no greater than the current risk of not having a spreadsheet.* (User)

In terms of the analysis, the surface characteristics of the "Shadow IT Not Allowed To Exist" trajectory are that there is "no" shadow IT. Furthermore, in these organizations, users and central IT consulted on shadow IT, with the result that users understood the danger of shadow IT and chose not to implement it. This trajectory occurs when the function, the central IT department, and the organization as a whole are all in agreement that things should be managed at a central level. Shadow IT has no legitimacy, users refuse to develop shadow IT, and hence shadow IT does not emerge.

Trajectory 2: Pure Shadow IT

Likewise, we discovered instances where shadow IT systems were constructed and persisted in the organization for a long time before being discovered by the central IT department (if at all).

> *And [an employee] left, and there was a routine left behind – this is how you maintain this Access database, then something happened to the Access database and they couldn't remember the password so we tried to hack the password, which we eventually managed to do* (CIO)

Pure shadow IT demonstrates the importance of the ability of the user function to procure or develop systems independently. If users are unable to procure resources, shadow IT cannot exist.

> *They can only choose to build Access themselves, because they've got... you know, it's on the desktop, but they can't build .NET applications because they don't have access to development tools.* (CIO)

In many cases, some user in the function procures a development environment and develops the shadow IT him/herself.

> *Because most people aren't that sophisticated. A very small percentage of people would be sophisticated enough to do [shadow IT]. But they would be able to talk to [person], our man that does this BI [Business Intelligence] type of stuff. But he's got most of the things covered.* (CIO)

Alternately, the organization allows a department sufficient budgetary discretion to buy Shadow IT from the market.

> *In some cases it can be as big as 50 thousand, 60, 70 thousand dollars. So some of those are quite significant chunks of money. They can reprioritize the definition of what's an operational expenditure versus a capital expenditure and if they have some underspend they can get a developer in and pay just an hourly rate and get some developer time.* (CIO)

Note that systems can be "shadow" within an organization, but can become significant at an industry-level, especially if similar departments across the industry have the same unsupported need.

> *Another good example is AuthorScope, or Scope solutions it's now called. Just a clever guy, a surgeon at Auckland hospital developed new software for orthopedics kind of clinical audit. Built it out a bit, it got too hard for him... Probably bumped into somebody in a function, a software company. "Ok we'll take it over we'll redevelop it in a new framework in return for you getting a free license for the rest of your life," that kind of thing...it's now used by quite a large number of orthopedics departments across the region.* (CIO)

The surface characteristics of this trajectory are, thus, that the systems are small, often going undetected. The fact that they remain secret suggests there is little consultation with central IT. Furthermore, these systems are maintained indefinitely by the functional departments (until discovered). From an underlying factors perspective, these systems are wholly in the shadows, and hence not legitimate to either the organization or central IT. Their existence alone suggests that the functional department is able to procure them.

Trajectory 3: Re-appropriation of Existing Technology

Users may adapt or re-appropriate an existing technology in new ways (Majchrzak et al. 2000; Orlikowski et al. 1995). Well-known examples include using spreadsheets for more advanced accounting purposes and scheduling, instead of procuring specialized technologies for these activities. Several examples of re-appropriated technology emerged from the interviews. For example, in one interview, a telephone dialing system (in the quote, called a dialer) was repurposed for use as a workflow management tool.

> *So what we do is we use the dialer for that, as the workflow tool... which isn't intended to be used as a workflow tool ... It's how we operate the dialer. So we haven't had to change any of the code for the dialer. But what our host system does is that it goes 'right, this account is due to be manually dialed', so it sends a list to the dialer. Then what we do, once we get that list into the dialer, is we start slicing and dicing it ... that's when we start playing with what accounts have been sent to the dialer. So we play with it there rather than in the host.* (User)

From a shadow IT perspective, repurposing of technology tends to occur when there is demand by users for a particular kind of IT-enabled tool. That tool is not provided by the Central IT department, and because of budgetary or technical constraints, users are unable to develop their own tool to perform the work. In the case of the dialer, the user admitted that, in her department, this application had lower priority than other projects.

> *Some of the stuff that we do could probably be automated, but it does fall into that, you know, 'oh, very difficult to prioritise in amongst everything else'...* (User)

The technical skillset of people in the department was also constrained to query extraction. Even simple VBA macros were beyond them.

> *Yes I've got two data analysts, who do... extract data for us out of DSS [Decision Support System], automated schedule reporting for us. They are not really doing things like creating, you know, macros for us to be able to run our operation.* (User)

In short, on the surface, shadow IT does not exist, with the IT systems operated by central IT. However, the way in which the technology is actually used would come as a surprise to central IT. Underlying the concept of appropriation of technology is that functional departments have a need that is not supported by the organization and central IT. Furthermore, the functional area does not have the capability to procure or build an application independently.

Trajectory 4: Central IT Assumes Maintenance

When shadow IT systems become large, they become difficult for the original developers to maintain. Users often have other duties, and maintaining Shadow IT is not a priority. At this point, users often approach the Central IT group to determine whether the central IT group can take over maintenance.

> *Some of these systems that someone might have built just for themselves would become quite a valuable asset for either the business group or other business groups. So what we've identified, if that's the case, then those need to be in a more secure, managed environment and we've converted a number of Access databases into .NET. So, as I said, those that have become more of a wider user base, as opposed to just an individual who just built their own database, we have converted those, as I said, .NET, where they are managed and backed up and supported by, you know, good IT practices.* (CIO)

Maintenance for Shadow IT often requires more than technical support and development. There may be administrative burdens and elements of administrative expertise that the functional departments cannot address, but Central IT can.

> *This guy, literally a guy... who built this thing and hosted it out of a literally a garage somewhere in London, and they said, "Well we'd like to trial this." And he said "fine." So, they set up a trial using that hosted environment, with ... Robb's Garage, the UK... And they did a pilot with one ward, or they were going to do it with two wards I think, for something like six months, that was supposed to be the pilot... they actually implemented it into something like 12 or 16 wards. It was just so successful that after the first month it grew like wildfire... so at that point, we sat down with that*

> *hosting company, and said look this is getting pretty critical to us. So how exactly is your server running and how robust is this thing. So that was when we started negotiating about service levels and we stayed with that service provider and we kept doing it.* (CIO)

When central IT assumes maintenance, this is indicative that the IT department is supportive of the functional area's procurement of IT. However, this procurement does not arise as a result of official channels. The typical organizational governance and approval structures (e.g., ensuring reliability, consistency of service) are not in place since the development is through informal channels.

It is then interesting to ascertain why user departments go through informal channels in-lieu of obtaining formal approval initially, especially given support from IT. One reason is that going through formal channels requires adherence to formal development and bureaucratic processes. For example, government hospitals might be required to obtain three quotes for an IT product or service. They might also be required to ensure that IT systems meet certain quality assurance criteria. It would be virtually impossible, then, to procure useful systems from startup vendors. Thus, in this trajectory, although the IT department is sympathetic to the functional area's goals, the overall organizational structure is not conducive to the function's IT requirements.

Thus, in this trajectory, the shadow system is small to medium in size. It has become too difficult for the functional department to maintain, but has existed for some time. Being undetected suggests it is not an enterprise-wide system. Central IT in the end maintains the system. Also, as the functional department seeks assistance from central IT, there is some consultation process that ensues. From an underlying factors perspective, central IT views shadow IT as legitimate because the central IT accommodates the user's request. However, there is no legitimacy organizationally; otherwise, there would not have been a shadow functional system in the first place. Users clearly had the capabilities and resources to procure the initial system.

Trajectory 5: Central IT Sponsors Development

A trajectory similar to the "Central IT Assumes Maintenance" trajectory is the "Central IT Sponsors Development" trajectory. In this trajectory, the central IT group unofficially provides resources for shadow IT to be procured or developed.

> *Because we have a panel supplier arrangement, we've got a number of vendors that have BAs [business analysts], architects, developers ... So I will say to the business, "if you need it now, all my resources are committed, but I can go out to our preferred suppliers and request a BA or a developer, that's going to cost, I don't know, 500 dollars a day, 200 dollars a day, whatever it might be, so if your business unit has the funding to pay for those external contractors, for this piece of work, then we will bring them in and sit them down with the team here, and they will do the development for you."* (CIO)

Central IT Sponsors Development only arises when the central IT group has some kind of excess capacity. Often, central IT has no spare human resource capacity. However, central IT sometimes has discretionary flexibility in the budget, and can allocate financial resources to help develop the shadow IT.

> *An elearning guy came to us and said we need more elearning. I said, absolutely, but fat chance that it is going to make the priority list based on what we are doing. And he said, look I found this online company, its an open source product. All I need is 20 thousand dollars to get started. So it seemed like a sensible idea. Here's 20 thousand dollars, and see how far you get.* (CIO)

As the quote above reveals, similar to "Central IT Assumes Maintenance," this trajectory arises when central IT is supportive of shadow IT, but the central organization is not. In this case, there is no chance of the organization approving the functional department's project. However, in addition, the functional department does not have sufficient resources to procure or develop the shadow IT on its own. Central IT provides the additional resources to make shadow IT a reality.

Thus, the surface characteristics of this form of shadow IT are that the systems tend to be small. The budget or resources transferred from central IT do not materially impact central IT operations. Central IT is clearly consulted. Otherwise, no money or resources would change hands. Finally, it is the functional department that maintains the system, not central IT. With regard to the underlying factors, the lack of an

official budget or sufficient formal resource allocation suggests a lack of legitimacy in the organization. The fact that central IT provides these resources suggests that central IT views the shadow IT as legitimate. Finally, the dependency of the functional department on central IT suggests that the functional department could not develop such a system by itself.

Trajectory 6: Central IT Replaces Shadow System With Central System

In other cases, shadow IT is detected because multiple departments develop similar or related Shadow IT systems to resolve a similar, or related, problem. This often arises, because central IT does not recognize the need for IT necessary across the organization. In these circumstances, the shadow IT emerges independently across the organization. Because the shadow IT emerges multiple times, it is detected and the central IT group replaces these systems with a new central system.

> *So previously everyone had done their own organisational charts, and we went out and overwrote all of them and said 'here's the org charts'... what those guys were using, like excel spreadsheets, or, you know, whatever tools they are using, they've all disbanded them and they just go into our org charts. And then IS picked that up to make sure that we are covered, so any sort of future improvements, updates, upgrades, IS were involved in that process. It was the right thing to do, we just needed to escalate it and really push it through quickly.* (CIO)

Why does central IT fail to recognize important organizational needs? Sometimes, this occurs if, for example, larger, more strategically critical, cross-departmental systems demand the attention of central IT.

> *We will be working on 5 of the 10 things that they decide, number 6 comes along and we start it. However then something else comes up, and that becomes number one because that has a bit of benefit for us, so we park number 6, pick up number 11, and start working on that, then come back to the group and then say 'okay, we've finished one through 6, so we've got 4 here, you brought in another 7, which of these do you know wanna take to the top 10'. And that process runs on a monthly basis. And that effectively consumes the spare capacity inside the IS function that is on the bench waiting for projects to go through the maturity cycle of concept, business case, into coding.* (CIO)

In terms of surface features, the final central system is cross-functional and hence, large. That central IT remained ignorant of a cross-functional problem suggests a lack of consultation with central IT. Finally, central IT is the final maintainer of the new cross-functional system. In terms of underlying factors, the various functional departments, and hence the organization views shadow IT as legitimate, but central IT did not initially approve the software (i.e., shadow IT was illegitimate to central IT). The individual functions had sufficient resources to independently develop their own shadow IT.

Trajectory 7: Shadow IT Replaces Central IT

The final trajectory reflects the converse of "Central IT Replaces Shadow System." In some cases, the shadow IT system actually replaced a competing central IT system.

> *Blackboard was the official system, in the teaching and learning environment. People said, "We want to bring the Moodle environment test mode and it will only be in test mode and we will see how that goes... so they started using lectures on them, so it became a production environment. But it was under their control sitting somewhere on some server and you know, we've got an organisation functionally dependent on shadow IT, literally, so it was a question of pulling that in, doing review, specifying, "are we gonna go Blackboard or Moodle?", and we did a big review, it lasted probably 6 months, we made a decision, "we are going Moodle."* (CIO)

In most cases, the replacement occurred at an application level. Here, Moodle replaced an existing courseware system. However, situations also emerged where a shadow IT vendor could potentially replace the entire IT department. In the quote below, the user seeks, not only an externally built custom application, but also provision to have the application maintained externally without liaising with IT.

> *Because obviously while I want it hosted externally... ultimately we might bring it into the [organization], but at the moment it's hosted externally for a number of reasons, such as: it's an*

> *internet based system, which means that our staff can access it anywhere... because we are only half way through implementing this, we can make changes quickly, and things like that. Stuff that doesn't happen through our centralised IT group. Well, it happens, but over a very long period of time.* (User)

Note that, when multiple departments employ an enterprise system in-lieu of an existing organizational one, or when large enterprise-level systems are hosted and supported externally, top management is aware of this situation. In this trajectory, the organization views shadow IT as legitimate, but the central IT group does not. Thus, in terms of surface features, these are large, shadow enterprise systems implemented with minimal or no consultation with central IT. Central IT eventually maintains these shadow systems.

Discussion

This research presents multiple examples of shadow IT and demonstrates where and how it thrives. Shadow IT emerges as a result of an unmet demand by a function. An analogy can be made to a wild plant that grows in the garden tended by central IT. If a plant is wild, it does not mean the gardener views the plant as a weed. A gardener may be delighted to find wild mint in his or her garden. In a similar way, central IT can fund IT systems knowing that, if such systems were to go through formal processes, they would never emerge.

Wild plants thrive in gardens for two reasons. First, there must be an opportunity - the garden itself must be conducive to the growth of the plant. The soil condition must be right, there must be sufficient sunlight and water, and other plants in the garden must afford the wild plant sufficient space to grow and thrive. In a similar way, shadow IT thrives, because the existing IT landscape does not adequately meet the needs of the function that commissions shadow IT. Second, a wild seed must land on the soil. A garden surrounded by an impermeable fence, where the gardener weeds regularly and uses clean compost is unlikely to have wild plants simply because seeds cannot take root. Similarly, shadow IT evolves and must be maintained.

The research presented seven separate trajectories that shadow IT could take. These trajectories are analogous to seven different kinds of wild plants, each of which takes root under different conditions. The trajectories ranged from shadow IT not appearing, to shadow IT remaining as applications in a function, to shadow IT replacing applications developed and maintained by central IT. The investigation also demonstrated that these trajectories could be explained by three factors: (1) legitimacy to the organization as a whole, (2) legitimacy to central IT, and (3) the capability of the function to develop or procure IT resources independently. This research, then, proposes the model depicted in Figure 1.

In identifying these factors, the research highlights that the shadow IT/central IT duality arises not only because of the dynamic relationship between the central IT group and the functional departments. Instead, the duality arises as a result of a complex interplay between the functions, IT departments, and the organization as a whole. In some trajectories, the IT department supports the functions in their quest for shadow IT. This is because the IT department approves of the function's request, but knows the organization as a whole would not develop the request through proper channels. In other cases, support is given by the organization to the functions, to the extent the organization becomes willing to pay for a shadow central IT department, i.e., an unofficial second central IT department, to operate and maintain applications for a functional department. Note that unlike a framework or classification system (what Gregor calls a Type I theory), Figure 1 is inherently testable, and explains and predicts shadow IT phenomena. It is what Gregor (2006) would call a Type IV theory.

The research also demonstrates that a key enabler of shadow IT is the ability of the function to procure or develop shadow IT. Indeed, much IT, especially open source IT, is now relatively cheap to procure. This has enabled shadow IT to become more prevalent and at an enterprise scale. An IT department that wishes to eliminate shadow IT can do so by taking such extreme measures as eliminating each department's discretionary budget, locking worker personal computers into dumb terminals, blocking Wi-Fi access to mobile and external devices, disabling macros on office productivity software, and denying worker access to the Internet. In most modern organizations, however, this is, obviously, not a feasible or acceptable option.

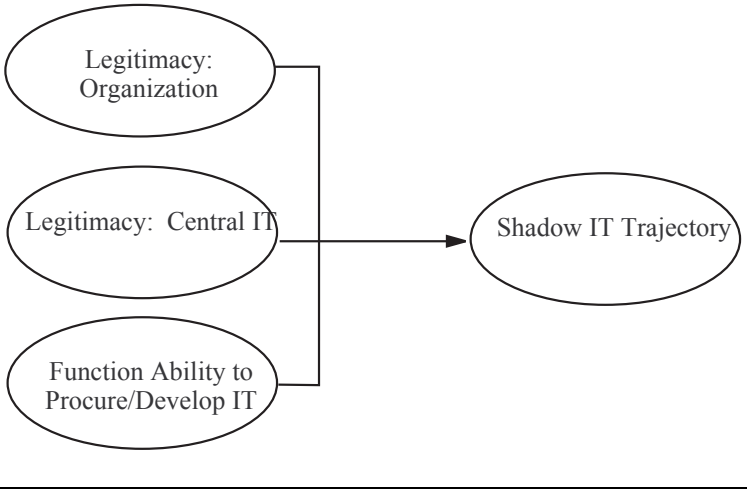

Figure 1. Factors Influencing Shadow IT Trajectory

Practical Implications

Shadow IT came to prominence largely as a result of the introduction of desktop computing. The findings reported here largely emerge as a result of a new wave of technologies and ideas including outsourcing, cloud computing, and mobility, which are reshaping the IT landscape. Increasingly, IT is becoming ubiquitous. Ironically, while the increased ubiquity of IT threatens the role of central IT, there is an increasing role for IT specialists. These new specialists are needed not within the central IT group, but within functional departments. Furthermore, the role of IT specialists in functional departments differs significantly from their role in central IT.

In almost all of the organizations in the study, obtaining approval, funding, and personnel for IT projects was a competitive process. The sole exception was a technology firm, where individual departments were expected to provide their own IT solutions. Often, the demands for IT were so great that important-to-implement IT projects were rejected on the grounds of priority and capacity. Thus, in many cases, the only viable solution for the functional departments was to develop or procure systems independently. In some cases, a sympathetic central IT group would surreptitiously provide the functional department with trained personnel or resources. Functional departments, however, cannot rely on the central IT group to be sympathetic. Thus, functional departments that want to improve their access to technological tools must independently invest in individuals with IT training.

Individuals who develop or manage shadow IT in functional departments are often qualitatively distinct from those in central IT. They might have weaker technical skills, but a more nuanced understanding of the specific needs of the functional areas. Thus, an accountant with IT skills, for example, better appreciates how depreciation works, and, as a result, can develop a more nuanced formula in his or her Excel spreadsheet. In contrast, the maintainer of an ERP system in central IT is more appreciative of how the ERP modules link together and how those modules satisfy internal and external regulatory requirements.

This research, therefore, concludes that, increasingly, if a functional area wants to get work accomplished, IT has become a mandatory skill in the functional area. As a result, every department should have at least one IT skilled employee to build the shadow IT systems the department needs.

Conclusion

This research has analyzed shadow IT initiatives in various companies based upon in-depth interviews with Chief Information Officers and information technology users involved in creating or managing IT services. A qualitative analysis was carried out to further our understanding of shadow IT, the drivers to its adoption, and the results from its adoption. A set of seven trajectories were derived which showed that

shadow IT is a continuum, as opposed to a phenomenon that is (or is not) allowed to exist within an organization. The trajectories span the gamut of possibilities from shadow IT will not emerge/persist over time, to shadow IT will remain small, to shadow IT will eventually replace central IT systems. On the surface, three factors determined the characteristics of the trajectories. These were the size of the IT system, who maintained the IT system in the long run, and whether central IT was consulted on the development/procurement of the shadow IT system.

The main contribution of this research is the development of a taxonomic configuration theory and the identification of three factors that lead to the different shadow IT trajectories. These are the legitimacy of shadow IT with central IT and the organization in general, and the ability of the functional department to procure or develop shadow IT. Also, as a practical contribution, this research demonstrates the growing ubiquity of IT, where not having an IT trained person in a functional department can disenfranchise and disempower that department within the organizational landscape.

One theme that has emerged from this analysis is the importance of legitimacy in shadow IT projects (Meyer and Rowan 1977; Suchman 1995). For example, there are significant legitimation processes that arise where shadow IT becomes enterprise level. Similarly, there are clear coercive isomorphism elements to situations where Shadow IT does not exist. Also, elements of our data resonate with the cognitive and sociopolitical legitimacy framework of Aldrich (1994). Our future work will focus on reexamining our data using a legitimacy lens.

The conclusions of this paper were drawn with a relatively small sample size. Future research with more organizations and perhaps with other methods is necessary to confirm findings found here. Also, we did not consider a number of potentially germane factors, including organizational size and number of employees. These should be considered in future research.

References

Aldrich, H.E., and Fiol, C.M. 1994. "Fools Rush in? The Institutional Context of Industry Creation," *Academy of Management Review* (19:4), October, pp. 645-670.

Baskerville, R. 2011. "Design Theorizing Individual Information Systems," *in Proceedings of the 15th Pacific Asia Conference on Information Systems*, Brisbane, Australia.

Behrens, S. 2009. "Shadow Systems: The Good, The Bad and The Ugly," *Communications of the ACM* (52:2), February, pp. 124-129.

Behrens, S., and Sedera, W. 2004. "Why Do Shadow Systems Exist after an ERP Implementation? Lessons from a Case Study," *in Proceedings of the 8th Pacific Asia Conference on Information Systems*, Shanghai, China.

Buyya, R., Yeo, C.S., Venugopal, S., Broberg, J., and Brandic, I. 2009. "Cloud Computing and Emerging IT Platforms: Vision, Hype, and Reality for Delivering Computing as the 5th Utility," *Future Generation Computer Systems* (25:6), June, pp. 599-616.

Chua, C.E.H., and Yeow, A.Y.K. 2010. "Artifacts, Actors, and Interactions in the Cross-Project Coordination Practices of Open-Source Communities," *Journal of the Association for Information Systems* (11:12), December, pp. 838-867.

Corbin, J., and Strauss, A. 1990. "Basics of Qualitative Research: Grounded Theory Procedures and Techniques." Thousand Oaks, CA: Sage.

Doty, D.H., and Glick, W.H. 1994. "Typologies as a Unique Form of Theory Building: Toward Improved Understanding and Modeling," *Academy of Management Review* (19:2), April, pp. 230-251.

Doty, D.H., Glick, W.H., and Huber, G.P. 1993. "Fit, Equifinality, and Organizational Effectiveness: A Test of Two Configurational Theories," *Academy of Management Journal* (36:6), December, pp. 1196-1250.

Faraj, S., and Xiao, Y. 2006. "Coordination in Fast-Response Organizations," *Management Science* (52:8), August, pp. 1155-1169.

Ferneley, E.H. 2007. "Covert End User Development: A Study of Success," *Journal of Organizational and End User Computing* (19:1), January-March, pp. 62-71.

Fiss, P.C. 2007. "A Set-Theoretic Approach to Organizational Configurations," *Academy of Management Review* (32:4), October, pp. 1180-1198.

Gregor, S. 2006. "The Nature of Theory in Information Systems," *MIS Quarterly* (30:3), September, pp. 611-642.

Jones, D., Behrens, S., Jamieson, K., and Tansley, E. 2004. "The Rise and Fall of a Shadow System: Lessons for Enterprise System Implementation," *in Proceedings of the 15th Australasian Conference on Information Systems*, Hobart, Tasmania.

Kiernan, S. 2014. "UXC to Combat 'Shadow IT' with Vendor Exclusive." Retrieved Apr 21, 2014, from http://www.crn.com.au/News/375998,uxc-to-combat-shadow-it-with-vendor-exclusive.aspx

Kim, D.-J., and Kogut, B. 1996. "Technological Platforms and Diversification," *Organization Science* (7:3), May-June, pp. 283-301.

Klein, H.K., and Myers, M.D. 1999. "A Set of Principles for Conducting and Evaluating Interpretive Field Studies in Information Systems," *MIS Quarterly* (23:1), March, pp. 67-93.

Kwee, Z., Van Den Bosch, F.A., and Volberda, H.W. 2011. "The Influence of Top Management Team's Corporate Governance Orientation on Strategic Renewal Trajectories: a Longitudinal Analysis of Royal Dutch Shell Plc, 1907–2004," *Journal of Management Studies* (48:5), July, pp. 984-1014.

Majchrzak, A., Rice, R.E., Malhotra, A., King, N., and Ba, S. 2000. "Technology Adaptation: The Case of a Computer-Supported Inter-Organizational Virtual Team," *MIS Quarterly* (24:4), December, pp. 569-600.

Markus, M.L., and Robey, D. 1988. "Information Technology and Organizational Change: Causal Structure in Theory and Research," *Management Science* (34:5), May, pp. 583-598.

Mazmanian, M. 2013. "Avoiding the Trap of Constant Connectivity: When Congruent Frames Allow for Heterogeneous Practices," *Academy of Management Journal* (56:5), October, pp. 1225-1250.

Meyer, A.D., Tsui, A.S., and Hinings, C.R. 1993. "Configurational Approaches to Organizational Analysis," *Academy of Management Journal* (36:6), December, pp. 1175-1195.

Meyer, J.W., and Rowan, B. 1977. "Institutionalized Organizations: Formal Structure as Myth and Ceremony," *American Journal of Sociology* (83:2), September, pp. 340-363.

Mintzberg, H. 1993. *Structure in Fives: Designing Effective Organizations*. Englewood Cliffs, NJ: Prentice-Hall, Inc.

Mohr, L.B. 1982. *Explaining Organizational Behavior*. San Francisco: Jossey-Bass.

Nasuni. 2013. "Shadow IT in the Enterprise." Retrieved April 21, 2014, from http://www6.nasuni.com/rs/nasuni/images/Nasuni-White-Paper-Shadow-IT-in-the-Enterprise.pdf

Orlikowski, W.J. 2007. "Sociomaterial Practices: Exploring Technology at Work," *Organization Studies* (28:9), September, pp. 1435-1448.

Orlikowski, W.J., Yates, J., Okamura, K., and Fujimoto, M. 1995. "Shaping Electronic Communication: The Metastructuring of Technology in the Context of Use," *Organization Science* (6:4), July-August, pp. 423-444.

Rai, A., Maruping, L.M., and Venkatesh, V. 2009. "Offshore Information Systems Project Success: The Role of Social Embeddedness and Cultural Characteristics," *MIS Quarterly* (33:3), September, pp. 617-641.

Rockart, J.F., and Flannery, L.S. 1983. "The Management of End User Computing," *Communications of the ACM* (26:10), October, pp. 776-784.

Strong, D.M., and Volkoff, O. 2004. "A Roadmap for Enterprise System Implementation," *Computer* (37:6), June, pp. 22-29.

Suchman, M.C. 1995. "Managing Legitimacy: Strategic and Institutional Approaches," *Academy of Management Review* (20:3), July, pp. 571-610.

Sumner, M., and Klepper, R. 1987. "Information Systems Strategy and End-User Application Development," *ACM SIGMIS Database* (18:4), Summer, pp. 19-30.

Sutcliffe, A., and Mehandjiev, N. 2004. "End-User Development," *Communications of the ACM* (47:9), September, pp. 31-32.

Walters, R. 2013. "Bringing IT out of the Shadows," *Network Security* (2013:4), April, pp. 5-11.

Wulf, V., and Jarke, M. 2004. "The Economics of End-User Development," *Communications of the ACM* (47:9), September, pp. 41-42.