



Grasping for Intraorganizational Power: A Multi-Case Study Analysis of Dysfunctional Functional Behaviours by Information Technology Personnel

Andrew J. Setterstrom

Operations Management and Information Systems, Northern Illinois University, USA

Abstract: Power plays an important role in organizations. It helps to explain why certain decisions are made and how those decisions are executed. While intraorganizational power is critical in facilitating the execution of the activities by information technology (IT) departments, it can be expected that some self-interested individuals will act in bad faith in its pursuit. Using resource dependency theory for guidance, a multi-case study of three mid-western universities was carried out to identify dysfunctional behaviours by IT personnel aimed at gaining intraorganizational power or avoiding its erosion. These behaviours are compared to the literature and strategies for mitigating these activities are offered to practitioners.

Keywords: Intraorganizational power, Resource dependency theory, Information technology, Dysfunctional behavior, Case study

1. Introduction

Intraorganizational power and politics are crucial in garnering commitment and support for IT strategy and decisions, as well as facilitating change. At the same time, academics within the fields of organization studies (Hickson et al., 1971; Pettigrew, 1973; Pfeffer and Salancik, 1974) and information systems (Kling and Iacono, 1984; Markus, 1983; Newman and Noble, 1990; Setterstrom and Pearson, 2013) have recognized the possibility that individuals and groups within an organization will act to increase or preserve personal power. This is not surprising, as members of an organization, while cooperators in a common undertaking, are rivals with each other over scarce resources and intangible rewards (Farrell and Petersen, 1982). Driven by self-interest, power is pursued as it provides the ability to influence decisions, such as resource allocation and which strategies/tactics the organization will adopt, as well as providing a sense personal satisfaction. This is problematic, as power-gaining activities are often carried out without regard to whether such behaviors compromise personal ethics, diminish organizational effectiveness, or even compromise the organization's ability to remain viable and achieve long term-goals.

Despite the important role power plays in facilitating the execution of the activities by the IT department, research that has identified dysfunctional power gaining activities by IT personnel has generally focused on only a few incidences of such behaviors, such as those that arise during systems implementation (e.g. Hussain and Cornelius 2009; Markus, 1983), resulting in a fragmentation of knowledge on the topic. Additional research in this area will help both practitioners and academics achieve a better understanding of how the pursuit of power by IT personnel can have tangible negative consequences for their organizations. Using a multi-case study methodology in conjunction with an extensive literature review, this study identifies power-gaining activities carried out by IT personnel, discusses the negative consequences resulting from these actions, and provides possible solutions for mitigating these behaviors. For the purposes of this research, resource dependency theory is adopted as a theoretical lens for understanding sources of intraorganizational power.

2. Literature Review

The study of power in intraorganizational situations has been an important pursuit for scholars, and has generated considerable interest in the information systems discipline in particular (see Jasperson et al., 2002). This is not surprising, as research suggests that intraorganizational power is critical for the execution business functions carried out by an organization's IT department. For example, Preston et al. (2008) demonstrated that CIOs need to possess some degree of power to enable the IT department to pursue initiatives that support organizational strategies, while Setterstrom (2016) found that IT project success is related to the power possessed by the IT project manager.

A basic definition of intraorganizational power is the ability of one actor within a given organization to influence the behavior of another actor within the same organization (Emerson, 1962). Emerson's conceptualization does not attribute power to the individual actors, but rather to the social relation. Emerson goes on to posit that each actor in any social relation provides resources that are valued by the other actor in the relationship, resulting in a mutual dependence. In an organization, these resources can range from fiscal or human resources to ego-support. Power then occurs in a relationship when one actor's dependency on the resources provided in the relationship exceeds the dependency of the other actor in the relationship. Importantly, Emerson notes that, regardless of whether or not a resource being provided in a relationship has substantial value to the other actor, high dependency on the relationship does not occur if the resource is readily available elsewhere. For the purposes of this paper, Emerson's view of power will be employed. This broad conceptualization of power was chosen because this research is not concerned with classifying which type of power is being observed; rather, this study is focusing on sources of power.

Using Emerson's (1962) conceptualization, the resource dependence school of thought has attempted to describe sources of power for actors, which can be individuals, departments, or entire organizations. For example, in their seminal article, Hickson et al. (1971) argue that power is a dependent variable that is influenced by three contributing variables, or sources of power: (1) coping with uncertainty, (2) non-substitutability, and (3) centrality. Also building on Emerson's conceptualization of power, Pfeffer and Salancik (1974; 1978) articulated the resource dependence theory. Resource dependence theory posits that a continuous supply of resources is needed by organizations to execute the processes and functions for which they were created. While resources include capital, raw materials, technical expertise, customers, and human resources, intangible and complex assets on which actors are dependent, such as prestige and social legitimacy, can also be considered resources. Resource dependency theory argues that an individual gains power within an organization when they are able to supply resources which are considered both critical to the organization and difficult to acquire (Pfeffer and Salancik, 1974).

Organizations can be conceptualized as collections of individuals and coalitions that contribute to a common enterprise. Importantly, academics have observed that actors within an organization do not share homogeneous aspirations and preferences (Cyert and March, 1963; Yukl, 2002). Similarly, individuals value their own needs and the needs of their departments more than the needs of the organization at large (Cyert and March, 1963; Eisenhardt and Bourgeois, 1988; Pettigrew, 1973). Actors within organizations want and need resources, such as capital, employees, or social legitimacy, to perform their job duties. However, resources are scarce, which results in several motivations for political activity to secure these resources.

3. Research Methodology

In an effort to gain a better understanding of the types of dysfunctional behaviors motivated by the desire to gain/conservate power, a multi-case study approach was adopted. Three case studies were conducted. The unit of analysis for each case was a single organization; specifically, mid-western universities. These organizations were chosen because each was large enough that their respective IT departments had a substantial annual budget (between 4 and 6 million dollars) and provided large-scale technology solutions comparable to those of other large organizations commonly examined in the IS literature (e.g., organization-wide network, large-scale client-server infrastructure, etc.). To ensure that the results are obtained through a rigorous process, I based the case study design and methods on the work of Yin (1994). The primary respondent for each case was the top IT executive at the university. When possible, interviews were conducted with project managers, additional senior IT managers, and other top managers outside of the IT department. A semi-structured interview process was used so that the data gathered had some degree of uniformity, while remaining open-ended so that the conversation could move in any unexpected direction. All interviews were tape recorded and transcribed. The data

was analyzed using the approach suggested by Marshall and Rossman (2006). First, with the use of a spreadsheet, the data was organized. Once the data matrix was completed, categories were examined across cases and the literature for patterns and themes, as suggested by Patton (2002). Lastly, I re-examined the transcripts of the interviews and conducted a review of the literature to identify possible methods for mitigating the risk of dysfunctional behaviors performed by IT personnel.

4. Results

4.1. Routinization

One type of dysfunctional behavior that was observed to one degree or another in all three of the cases was resistance by IT personnel to record the details of their job duties. Hickson et al. (1971) discuss how routinization leads the capturing of tacit knowledge possessed by an organization's workers. In the context of the IT department, routinization refers to the creation of recurrent tasks by IT personnel and documenting the details of performing those tasks. Personnel for whom resistance was documented included IT help desk personnel, as well as systems and network administrators. The interviewees observed that in many cases resistance to document job duties stemmed from more than one cause, including laziness and having higher priority duties. However, in the opinion of their supervisors, resistance on the part of one network administrator and one system administrator in particular was done in an effort to retain greater control over the domain where job duties resided and increase personal job security, respectively. Notably, it was acknowledged that these behaviors did achieve those goals to a certain degree. In another instance, a computer lab manager not falling under the formal authority of the IT department was resistant to routinizing job duties, which included the maintenance of the computers in the lab. The IT staff in the centralized IT department had developed routinized procedures for maintaining computers in other labs for the campus. These procedures substantially improved the efficiency of performing this job duty, while also ensuring that the technology standards adopted by the university were met. The respondent observed that the lab manager was very territorial of his work domain and insisted that he be contacted exclusively for issues that arise from problems within the lab. While this effort helped to retain dependence on his services, it resulted in a decrease in efficiency of his job duties and, at times, a bottleneck in the maintenance of lab computers. Interestingly, this represents an instance of a power struggle which can occur as a result of decentralizing the IT governance for an organization.

This study's interviews revealed one method for reducing resistance to routinize and documenting job duties. An IT manager reported that addressing the issue with the resisting personnel by communicating the importance of documenting their job duties and then setting a time line for the completion of documentation was effective. A review of the operations management literature provided two additional suggestions: incentivizing employees and rotating IT personnel through related job duties. Lazaric and Denis (2005) conducted a case study of a manufacturing firm that was implementing ISO norms, which included extensive documentation of job-related tasks and routinization. Management implemented an incentive system to motivate employees to produce documentation that sufficiently described the details of job duties that the employees performed and employees were rotated among related job tasks, which had the benefit of a collective definition of these job tasks.

4.2. Protection of Personal Job Domain

Another dysfunctional behavior observed in the case studies was IT personnel acting to protect their job domain. I argue that because IT personnel understand, at least intuitively, that permitting end-users to perform IT-related activities that fall within their expertise results in the organization becoming less dependent on that IT professional to perform those duties. In conversations with non-IT personnel, two instances were identified where IT personnel used policy and procedure to protect their territory. Specifically, IT personnel were identified as refusing to allow capable users to perform software upgrades, installations, or maintenance on their PCs, arguing that policy dictates that a qualified technician must carry out the work. When questioned about adhering to these types of policies, IT personnel cited numerous examples of end-users, who were in fact not qualified to perform maintenance and installations, causing considerable problems on their PCs prior to the implementation policies restricting administrative privileges. In one of these cases, end-users identified a policy created by the centralized IT department where support for technology issues will only be provided for resources provided by the IT department. This policy creates a potential situation where the IT department is depended on exclusively for information technologies. However, IT personnel indicated that this policy was important for ensuring the ability of the IT department to support the technologies utilized at the university. When end-users adopted technology not provided or supported by the IT department, it was often hardware/software that the IT personnel were not familiar with and not compatible with the current technology standards. Consequently, resolving issues that involved these

technologies took considerable resources (i.e. time). The literature identifies a similar example in which end-users were prohibited from making technology purchases without approval from appropriate IT personnel (Markus and Bjorn-Andersen, 1987).

The degree to which policies that protect job domain are enforced to prevent personal power erosion, as opposed to being implemented for the benefit of the organization, is difficult to gauge. I suggest that top-level IT managers maintain open channels of communication with end-users to attempt to identify policies and procedures that have become obsolete or are being leveraged in a dysfunctional way. Practitioner literature offers some guidance, suggesting that IT managers should encourage open discussion with any IT personnel potentially affected by policy change to create mutual understanding, while avoiding the use of coercion to minimize resistance (Koch, 2006).

4.3. Implementation Resistance

Organizational members will resist changes that they believe will result in a loss of power or status (Dent and Goldberg, 1999). Accordingly, empirical research in the context of IS has demonstrated that the implementation of IT is often resisted by individuals concerned with power erosion (Burkhardt and Brass, 1990; Lapointe and Rivard, 2005). It is worth noting that much of the literature in this area has focused on end-users of IT. However, similar threats to power and legitimacy exist for the IT personnel that will be responsible for supporting future information systems being implemented by an organization. A conspicuous dysfunctional behavior observed in one of the cases provides support for this assertion. During the implementation of a commercially-developed ERP system, a system administrator of a software solution developed in-house for which a component from the ERP new system would replace petitioned the system users to resist the implementation. The system administrator garnered support by reporting problems with the proposed system to the end-users and creating a belief that the system will be difficult to use. The project manager for the ERP system reported that these activities were carried out in an effort by the system administrator to conserve the value of the unique expertise required to administer the current information system. Unfortunately, this political activity resulted in significant resistance from the future system's users in the form of refusing to provide information about the requirements needed to configure the new system, as well as campaigning with the university's administration to cease system development. Ultimately, these resistance activities resulted in the failure of implementation for this ERP component.

Overcoming resistance to implementation by IT personnel can be a precarious task, as it is often the IT personnel whom are relied upon for identifying these types of behaviors. The project manager from the case where the ERP component implementation failed identified a lack involvement by the end-users in the several steps of the system development process, as well as relying on the resisting IT employee to act as the primary liaison to the department for which the system was being implemented. A higher level of communication with the end-users would have helped to identify the IT employees' attempt to thwart the system implementation, allowing for IT management to address the issue with the employee directly.

4.4. Undertaking System Adoption

Another type of power gaining behavior that I anticipated to be observed is the campaigning for the adoption of superfluous IT systems. I believed that some IT professionals would attempt to increase personal and departmental power by suggesting that the adoption of a given portfolio of IT solutions will be effective in improving organizational performance in some important way, when in fact the suggested IT portfolio is configured to help the IT personnel achieve personal interests (Knights and Murray, 1992; Meyers, 1994). Evidence from the literature supports this notion. In a case study by Hussain and Cornelius (2009), IT management campaigned for the implementation of an enterprise-wide IT system to support the operations of a community health care organization. The IT manager cited benefits to the organization as the primary reason for system adoption. However, evidence suggested that the primary motivations for the IT manager were establishing departmental credibility, obtaining greater resources, and increased personal power. The interviews from my research did not reveal evidence IT personnel petitioning for systems implementation for the purpose of increasing power. There are several possible explanations for this result. First, each of the case studies took place in the context of a university. As several of respondents from outside of the IT department noted when discussing an apparent lack of "technology for technology's sake," the IT department is working on a very limited budget. Moreover, major IT initiatives must pass the scrutiny of IT review committees of one kind or another, greatly hindering the ability of IT personnel to campaign for unnecessary systems. In fact, the enterprise-wide IT projects that were discussed during

the interviews were all initiated from outside of the IT department. Another possible explanation is that IT personnel mask their personal motivations for IT systems implementation with rational reasons for adoption (Brown, 1998). I agree with the argument set forth by Avgerou and McGrath (2007) that all IT initiatives adopted for rational reasons (e.g. increased efficiency) are not without political motives, and no IT initiative is completely devoid of some rationality. IT systems can be very expensive to the organization that adopts them and very disruptive to existing organizational processes. Therefore, it is crucial for organizations to take precautions to mitigate the adoption of unneeded IT systems. This study's findings suggest that adopting organizational policies and procedures for gaining system adoption approval as one effective method. For instance, establishing a review committee for new IT systems that is composed of members from outside the IT department (Shelly and Rosenblatt, 2009), using simple, quantifiable performance goals that are easily measurable as a basis for making IT investment decisions (Bensaou and Earl, 1998), and co-locating IT personnel in the functional areas that IT supports to help avoid IT departmental isolation (Bensaou and Earl, 1998) are all techniques that may reduce unnecessary system adoption.

5. Conclusion

Organizations commonly experience issues related to their IT departments, including rigid adherence to inefficient IT policies and procedures, failing to integrate user preferences into IT solutions, resistance to documenting job duties and IT outsourcing, and the adoption of technology for technology's sake, to name a few. Importantly, organizations are places where political activity takes place. The individual preferences of employees do not necessarily align with the overall needs of the organization. Consequently, many of the dysfunctional behaviors by IT personnel perceived as being irrational can be attributed to, in part, intentional efforts to gain or avoid loss of intraorganizational power.

Using a multi-case study approach in conjunction with an extensive literature review, this research demonstrates how the desire to gain/retain power by IT personnel is a motivating factor for many common problems organizations experience related to their IT functions. Drawing from solutions utilized by respondents in this study's interviews, as well as from the literature, a number of solutions for mitigating these counter-productive power gaining activities were identified and discussed. As such, practitioners have a number of possible solutions to help mitigate these behaviors. However, an important first step to addressing these issues is to recognize when power-gaining activities are occurring. It is also worth noting that many activities performed by IT personnel that are perceived to be for the purposes of increasing intraorganizational power may have alternative motivations, while activities motivated by personal interest (e.g. systems implementation) often are not devoid of rational reasoning.

Future research should attempt to support the arguments presented in our work using quantitative data. One interesting area deserving further investigation is conditions under which dysfunctional behavior is most likely to occur. Antecedents such as organizations maturity (age), technical orientation, and organizational culture could provide insight to practitioners. Another area of research is how cloud computing and outsourcing affect the power possessed by IT departments; while certain trends in the modern business landscape would be expected to increase the influence of IT departments, such as the increased adoption of enterprise-wide systems, the ability to obtain IT solutions from sources other than the IT department should theoretically make IT departments more substitutable.

References

- Avgerou, C. & McGrath, K. (2007). Power, rationality, and the art of living through socio-technical change. *MIS Quarterly*, 1(2), 295-315. [CrossRef](#)
- Bensaou, M. & Earl, M. (1998). The right mind-set for managing information technology. *Harvard Business Review*, 76(5), 118-129.
- Brown, A.D. (1998). Narrative, politics and legitimacy in an IT implementation. *Journal of Management Studies*, 35(1), 35-58 [CrossRef](#)
- Burkhardt, M.E. & Brass, D.J. (1990). Changing patterns or patterns of change: The effects of a change in technology on social network structure and power. *Administrative Science Quarterly*, 35(1), 104-127.
- Cyert, R. & March, J. (1963). *A Behavioral Theory of the Firm*. Englewood Cliffs: Prentice-Hall.
- Dent, E.B. & Goldberg, S.G. (1999). Challenging 'resistance to change'. *The Journal of Applied Behavioral Science*, 35(1), 25-42. [CrossRef](#)
- Emerson, R.M. (1962). Power-dependence relations. *American Sociological Review*, 27(1), 31-41. [CrossRef](#)

- Eisenhardt, K.M. & Bourgeois, L.J. (1988). Politics in strategic decision making in high-velocity environments: Towards a midrange theory. *Academy of Management Journal*, 31(4), 737-770. [CrossRef](#)
- Farrell, D. & Petersen, J.C. (1982). Patterns of political behavior in organizations. *Academy of Management Review*, 7(3), 403-412. [CrossRef](#)
- Hickson, D.J., Hinings, C.R., Lee, C.A., Schneck, R.E., & Pennings, J.M. (1971). A strategic contingencies' theory of intraorganizational power. *Administrative Science Quarterly*, 16(2), 216-229. [CrossRef](#)
- Hussain, Z.I. & Cornelius, N. (2019). The use of domination and legitimation in information systems implementation. *Information Systems Journal*, 19(2), 197-224. [CrossRef](#)
- Jasperson, J., Carte, T.A., Saunders, C.S., Butler, B.S., Croes, H.J.P., & Zheng, W. (2002). Review: Power and information technology research: A metatriangulation review, *MIS Quarterly*, 26(4), 397-459. [CrossRef](#)
- Kling, R. & Iacono, S. (1984). The control of information systems developments after implementation. *Communications of the ACM*, 27(12), 1218-1226. [CrossRef](#)
- Knights, D. & Murray, W.F. (1992). Politics and pain in managing information technology. *Organization Studies*, 13(2), 211-28. [CrossRef](#)
- Koch, C. (2006). Change management – Understanding the science of change. CIO. Available online: http://www.cio.com/article/24975/Change_Management_Understanding_the_Science_of_Change (accessed on 27 February 2010).
- Lapointe, L. & Rivard, S. (2005) A multilevel model of resistance to information technology implementation. *MIS Quarterly*, 29(3), 461-491. [CrossRef](#)
- Lazaric, N. & Denis, B. (2005). Routinization and memorization of tasks in a workshop: The case of the introduction of ISO norms. *Industrial and Corporate Change*, 14(5), 873-896. [CrossRef](#)
- Markus, M.L. (1983). Power, politics, and MIS implementation. *Communications of the ACM*, 26(6), 430-444.
- Markus, M.L. & Bjorn-Andersen, N. (1987). Power over users: Its exercise by system professionals. *Communications of the ACM*, 30(6), 498-504. [CrossRef](#)
- Marshall, C. & Rossman, G.B. (2006). *Designing Qualitative Research* (4th ed.). Thousand Oaks, California: Sage.
- Myers, M.D. (1994). A disaster for everyone to see: An interpretive analysis of a failed IS project. *Accounting, Management, and Information Technologies*, 4(4), 185-201. [CrossRef](#)
- Newman, M. & Noble, F. (1990). User involvement as an interaction process: A case study. *Information Systems Research*, 1(1), 89-113. [CrossRef](#)
- Patton, M.Q. (2002). *Qualitative Research and Evaluation Methods* (3rd ed.). Thousand Oaks, California: Sage.
- Pettigrew, A.M. (1973). *The Politics of Organizational Decision Making*. London: Tavistock.
- Pfeffer, J. & Salancik, G.R. (1974). Organizational decision making as a political process: The case of a university budget. *Administrative Science Quarterly*, 19(2), 135-151. [CrossRef](#)
- Pfeffer, J. & Salancik, G.R. (1978). *The External Control of Organizations: A Resource Dependence Perspective*. New York, NY: Harper & Row.
- Preston, D.S., Chen, D., & Leidner, D.E. (2008). Examining the antecedents and consequences of CIO strategic decision-making authority: An empirical study. *Decision Sciences*, 39(4), 605-642. [CrossRef](#)
- Setterstrom, A.J. (2016). IT Project Manager Decision-Making Authority: An Empirical Examination of Antecedents and Consequences. 2016 International Conference on Information Systems in Dublin, Ireland, December 11-14.
- Setterstrom, A.J. & Pearson, J.M. (2013). Bases of intra-organizational power: An analysis of the IT department. *Electronic Journal of Information Systems Evaluation*, 16(2), 86-100.
- Shelly, G.B. & Rosenblatt, H.J. (2009). *Systems Analysis and Design* (8th ed.). Boston: Thomson Course Technology.
- Yin, R.K. (1994). *Case Study Research: Design and Methods* (2nd ed.). Thousand Oaks, CA: Sage Publications.
- Yukl, G. (2002). *Leadership in Organizations*. Upper Saddle River: Prentice Hall.