



Research article

The impact of enterprise systems on organizational resilience

Ioannis Ignatiadis¹, Joe Nandhakumar²

¹School of Management, University of Bath, Bath, UK;

²Warwick Business School, University of Warwick, Coventry, UK

Correspondence:

I Ignatiadis, School of Management, University of Bath, Bath BA2 7AY, UK.

Tel: +44 1225 383699;

Fax: +44 1225 386473;

E-mail: I.Ignatiadis@bath.ac.uk

Abstract

Enterprise systems are used to facilitate the seamless integration and exchange of data between the various departments within an organization. In order to achieve this, rigidly defined control mechanisms must be in place in the system, which safeguard the company's data and protect the company against unauthorized and unintended uses of the system. This is ideal for total control; however, is only achievable to a certain extent. The configuration of controls in the enterprise system may have unintended organizational implications, due to organizational necessities. The purpose of this paper is to present the findings from a company case study, where an enterprise system is being used. We suggest that the introduction of an enterprise system creates power differentials, which serve to increase control in the organization. This results in increased rigidity, and a possible decrease in organizational flexibility and resilience. On the other hand, enterprise systems can also cause drift, resulting from the unexpected consequences of these power differentials, as well as from the role of perceptions of people in solving a problem within the enterprise system. This reduction in control may serve in some circumstances as an enabler to organizational resilience.

Journal of Information Technology (2007) **22**, 36–43. doi:10.1057/palgrave.jit.2000087

Published online 5 December 2006

Keywords: enterprise system; resilience; power; control; drift

Introduction

Enterprise systems are used by large companies and small- and medium-sized enterprises (SMEs) to reorganize and streamline their internal and external operations. One particular type of enterprise system examined in this paper is that of the enterprise resource planning (ERP) system. The installation of an ERP system usually entails major business process reengineering issues (Boudreau and Robey, 1999; Al-Mashari and Al-Mudimigh, 2003), as companies often have to adapt their work practices to the ERP system. Consequently, new forms of controls need to be in place in order to ascertain the prescribed and efficient working of employees within the ERP system.

The main purpose of this paper is to conceptualize the way that organizational control is aided with the use of an enterprise system within a company, and how drift can result from the use of such a system. The relationship between control and organizational resilience is also proposed. The outcome of this research is twofold. On

the one hand, results from this research contribute to a better theoretical understanding of the impact of enterprise systems on control and resilience in a company. As research on enterprise systems tends to move away from initial implementation concerns and success factors, the paper offers an important dimension by presenting more critical reflections on the actual use of enterprise systems and their impact on a company. On the other hand, the findings also help practitioners to become more aware of the impact of enterprise systems within their organizations, highlighting areas where the system can have unintended consequences and can function contrary to their expectations.

In the following section, we briefly review the previous research on the issues of power and control and their relevance to information systems. We then present the theoretical underpinnings of this study, followed by a presentation of the research approach employed. We follow this with the presentation of the impacts of the enterprise

system in the case study company. We then discuss and categorize the results of our research, and develop the theoretical conceptualization that arises from this discussion. We conclude this paper with the theoretical and practical implications of our study.

Information systems, power, and control

For Finnegan and Longaigh (2002), information is seen to be at the core of both control and coordination processes. They define control as the process by which one entity influences to varying degrees the behavior and output of another entity, through the use of authority and a wide range of bureaucratic, cultural, and informal mechanisms. Finnegan and Longaigh (2002) mention that technology facilitates control in three ways: changing decision-making structures, formalization of behavior, and monitoring activities.

Markus's (1983) work focuses on the link between power, politics, and the implementation of a management information system (MIS). She argues that as many MISs are designed to distribute information to individuals in a certain way, MISs can alter the basis of power. In addition, Coombs *et al.* (1992) mention that control is used to draw attention to the intended and unintended consequences of the exercise of power, and the use of knowledge in social and organizational relations. They note that some people may willingly identify and subjugate themselves to the control effects of power relations, whereas others may wilfully resist them. In that sense, IT is seen as the response to competitive pressures to enhance control over processes of production and distribution (cf. Bruns and McFarlan, 1987).

In similar lines, Bloomfield *et al.* (1994) argue that, paradoxically while IT is seen to increase decentralization of decision-making, at the same time it makes possible a centralization of control (see also Bloomfield and Coombs, 1992). This premise is also acknowledged by Orlikowski (1991), who states that '[information technology] facilitates decentralization and flexible operations on the one hand, while increasing dependence and centralized knowledge and power on the other' (p. 10). From her field study of a large multinational software consulting firm, Orlikowski concluded that IT tends to reinforce the existing structures of power and domination. Clegg and Wilson (1991) also mention that managerial control can be increased through technological change. In this case, the individual's opportunities for resistance can be reduced or eliminated when the technology makes redundant discretion, decision-making, and judgment. Clegg and Wilson, however, argue that technology is not the sole source of control: controls can be embedded in the physical structure of the labour process, producing *technical* control, or can be found in the social structure, producing *bureaucratic* control.

In relation to ERP systems, Sia *et al.* (2002) have examined the issues of empowerment and panoptic control (Foucault, 1977) of ERP systems in the case of a restructured public hospital in Singapore. Their findings tend to indicate that although an ERP implementation has the potential for both employee empowerment and managerial control, management power seems to be perpetuated through an ERP implementation. In addition

to Sia *et al.*, Hanseth *et al.* (2001) argue that ERP systems, with their emphasis on integrating business processes, streamlining, and standardization, are an ideal control technology. More generally, they argue that IT is a control technology, and the IT revolution is a control revolution. In that sense, Robinson and Wilson (2001) see three ways in which the work regime within an ERP system is enforced.

- First, the integrated approach to control within an ERP model allows for its automation in a way that replaces traditional forms of hierarchical supervision.
- Second, ERPs can strengthen corporate cultures so that employees are encouraged to identify themselves with the organization's products and values.
- Third, ERPs also specify the ways in which work is to be carried out, by defining the business processes, and hence the job content of one's work.

Boudreau and Robey (2005) claim that when looking at an organizational change arising from the use of IT, an agency perspective may mean limited possibilities for radical IT-induced change. An agency perspective of IT in this case takes the position that IT is socially constructed and open to a variety of social meanings and potential uses (cf. Ciborra, 2002). Boudreau and Robey argue that certain technologies allow for a greater degree of human agency and others to a lesser degree. Their research looked at ERP systems, which are seen as inflexible software packages constraining user-inspired action (human agency). Their results, however, indicate that although ERP systems are seen as rigid control mechanisms, there is still scope for human agency to take place within such systems. Their findings agree with Orlikowski (2000), who acknowledges that while users can and do use technologies as they were designed, they also can and do circumvent the intended uses of technology, either by ignoring certain properties, working around them, or inventing new ones. The concept of agency is also applicable to the current research. Agency here refers to the appropriation of the enterprise system by end users, and their use of it. The meanings that users attach to the workings of the enterprise system in this case, and their interpretation of it, can cause drift in the company, or can reinforce the controls imposed by the system.

In summary, the impact of power and control aspects of information systems has been investigated quite extensively in the literature. We build on the literature described above, as well as the theoretical lenses described in the following section, in order to enhance our understanding of how power and control impacts organizational resilience.

Theoretical lenses: embedding–disembedding and control determinants

This study draws on Giddens's (1990) notion of embedding and disembedding. These two constructs fall within the larger concept of modernity. Giddens defines disembedding as 'the lifting out of social relations from local contexts of interaction and their restructuring across indefinite spans of time-space' (p. 21). Conversely, embedding (or reembedding) is, according to Giddens, 'the reappropriation or recasting of disembedded social relations so as to pin them down (however partially or transitorily) to local conditions

of time and place' (pp. 79–80). In the current context of information systems, the social relations that are being disembedded and reembedded are the power differentials that arise from the use of information provided by the information system, and the access to this information that is provided to disparate individuals by the control mechanisms in the information system (in this case the ERP system).

In addition to the notions of embedding–disembedding as theoretical lenses, this paper also draws on three determinants that impact on control. In that sense, Hanseth and Braa (2000) use Giddens's analysis on modernity to claim that even more knowledge can in some cases decrease control. This paradox can occur because knowledge is filtered, among others, by the following three determinants:

1. *Differential power.* Knowledge in this case is more available to those in positions of power.
2. *Role of values.* Different perceptions and values of different settings in this case imply a different approach to knowledge and, consequently, on ways to solve a problem.
3. *Impact of unintended consequences.* This refers to the case where no amount of accumulated knowledge can include all circumstances of its implementation, leading to unintended outcomes.

We will use the above determinants as sensitizing devices (Walsham, 1993) in our research.

Because of the uncertainty and possible decreased control of modernity, Giddens likens it to a juggernaut, a runaway engine of enormous power that humanity can collectively drive to a certain extent, but which can easily get out of control and rend itself asunder. Hanseth *et al.* (2001) use Giddens's concept of a juggernaut to parallel it with ERP installations in global organizations. Although ERPs are seen as extended control mechanisms in this case, their size and complexity can threaten an organization if they are not managed correctly and allowed to get out of control. The following section discusses the research approach adopted for the examination of a company where such an ERP system is installed.

Research approach

This research adopts the interpretive case study approach (Walsham, 1993). Interpretive approaches assume that the reality is socially constructed by human agents (Walsham, 1995). According to Yin (2003), 'case studies are the preferred strategy when how or why questions are being posed, when the investigator has little control over events, and when the focus is on a contemporary phenomenon within some real-life context' (p. 1). As this research examines the question of *how* enterprise systems affect the control and resilience aspects in a company, case study research is an appropriate method. The investigator in the current research was an outsider to the company, had no consultancy or other financial interests in it, and could not influence the events studied, as he did not take part in them. The focus of the research is a contemporary one, and the real-life context is the use of an enterprise system within a company.

The case study company is TransCom (a pseudonym). TransCom employs more than 74,000 people in over 70 countries worldwide. It has more than 100 years of experience in its sector. Four offices of TransCom in the UK were visited. The ERP system installed at TransCom is SAP R/3, and it was fully installed in January 2002. It is currently implemented in the UK, France, Spain, Romania, Sweden, Chile, and the United States, with an emphasis on global deployment in the future. Prior to installation of the SAP system, another ERP system (BAAN) was used, as well as a standalone finance system.

Data collection for the research was carried out between February and August 2005 (i.e., post-ERP implementation), using semi-structured interviews and non-participant observation. For the semi-structured interviews, a list of topics was prepared for discussion with the interviewees (office-level staff and managers), but the interviewees were free to elaborate on their own understandings, and digress when it was necessary. All the interviews were tape-recorded and transcribed verbatim. For the non-participant (passive) observations, the researcher observed the subjects' daily interaction with the ERP system and the problems encountered. In addition, notes were kept after informal discussions with participants, as well as writing down observations from the field. Semi-structured interviews and non-participant observation are positioned by Nandhakumar and Jones (1997) in the middle of the spectrum analyzing distance and engagement of data-gathering methods. This means that in the current research, data collection did not involve full engagement with the company as a consultant; but on the other hand, there was a fair amount of interaction with it, in order to fully appreciate the context of ERP use. Table 1 shows the positions of the people that were interviewed and the number of interviews carried out.

Data analysis for this research was carried out using techniques from grounded theory (Strauss and Corbin, 1998). Certain levels of coding (open, axial) were performed on the collected data in order to group them into categories. The codes and categories emerged from the data, keeping in mind the theoretical lenses of embedding–disembedding and control determinants, which were described previously. In order to assist our coding, the interview transcripts were imported into NVivo, a computer-aided qualitative data analysis software package. NVivo was used simply as a tool for organizing, structuring, and familiarizing with the data, and the analysis was primarily done by the researchers. The codes and categories were conceptually linked with each other, with the use of mind-maps that explored their interrelationships.

Indicative codes developed in NVivo included 'Role of Values in Problem-Solving' and 'Impact of Unintended Consequences' (from the control determinants identified in the 'Theoretical Lenses' section), and others such as 'Authorisation Levels', 'System Expertise', and 'Monitoring Capabilities'. The last three were grouped into the higher-order category of 'Differential Power' (one of the control determinants in the 'Theoretical Lenses' section), while the other higher-order categories included 'Control', 'Drift', 'Disembedding', and 'Reembedding'. Although resilience did not appear in the codification *per se*, it was involved in the analysis on the understanding that excessive control can

Table 1 Interviews carried out

<i>Positions interviewed</i>	<i>Number of interviews</i>	<i>Area</i>
Assistant Accountant	2	Finance
Accounting Reports Manager	1	Finance
Billing Clerk	1	Finance
Accounts Payable Clerk	2	Finance
Materials Controller	2	Materials management
Materials Planner	2	Materials management
SAP Facilitator	4	Service management
Flow Repairable Controller	1	Service management
Head of Production	1	Service management
Maintenance Policy Leader	2	Service management
Production Planner	1	Service management
Purchasing Manager	1	Purchasing
Logistics Director	1	Warehouse and distribution
Business Improvement Coordinator	2	Warehouse and distribution
Inventory Planner	2	Warehouse and distribution
Business Process and Global Information System Director	1	IT management
IT Manager	3	IT management
Total Interviews	29	

inhibit resilience. The following section describes the case study company, including some level of analysis. The codes and categories are then used to inform the discussion and theory development.

Case description and analysis: impacts of enterprise system in TransCom

Use of an enterprise system generally entails definition of authorization levels, or access control mechanisms, that specify who has access to different types of data and screens in the system. In TransCom in particular, as users were given different access levels depending on their needs, some of them were given more authority to carry out tasks in the system, and hence gained power. Other users were given less authority, and hence their power was diminished. In addition, these access control mechanisms were configured at a global level in TransCom, at a central location that had the responsibility for the overall configuration of the system, including the assignment of authorization levels.

However, the fact that controls in the system can be enabled does not mean that they are automatically put in place. The system must be appropriately configured to correctly implement these controls, which is not always the case. The way that the system was actually configured in TransCom depended on the organizational necessities, as well as the perspective of the company regarding the assignment of access rights to individuals. As one interviewee mentioned:

I think, at the moment, I would say, the controls are very sort of lax, are very easy, because people have got authorizations to do nearly everything in some cases. It would help if the authorizations were limited to the actual transactions that people were meant to be doing, rather than giving them an awful lot in case they might ever need it (Business Improvement Coordinator).

From an organizational perspective, as a result of the assignment of authorization profiles, users at local company offices could abuse these authorizations and carry out work they should not be doing.

Training was carried out when the system was first installed in TransCom. However, the system users considered most training that was given to them as incomplete, and they required more thorough and continuous training on the system. In some cases, training was not organized at all, but depended on people picking up things as they worked with the system.

I didn't have any formal training. I started in 1999, when we first introduced SAP to the business, and I sat with the consultants, learning the system, saying, right, if I do this, how does that happen, how do I do this, and things like that. One thing led to another, and I became one of the, sort of, SAP experts within the business (Business Improvement Coordinator).

As a result of technical knowledge, certain users within the business (the Business Improvement Coordinator in this case) seemed to gain authority, even though this person's main business role was in Logistics and not in SAP consulting. Other employees in the company regarded the Business Improvement Coordinator as an ERP expert, and his help was sought whenever possible. Although there was a dedicated helpdesk to help users having problems in the system, people still tended to bypass this helpdesk and seek the help of the perceived expert instead.

We have a UK SAP team, that is basically the helpdesk, but the people within the offices here tend to come to me first, because more often than not I can give them a quick solution or answer to solve their problem, rather than them logging it to the helpdesk, and the helpdesk then trying to identify what the problem is (Business Improvement Coordinator).

The organizational consequence of this increase in authority was that certain business rules were not observed, and people tended to overlook the prescribed ways of solving a problem. This bypassing of business rules had the

additional organizational consequence that people from non-technical backgrounds had difficulty in understanding the technical jargon of the ERP system.

Power in the system could also arise because of the monitoring capabilities of an enterprise system. In this sense, users who had the authorization to monitor other peoples' work in the system had power over the latter. From a personal perspective, some interviewees expressed their discontent about the monitoring or panoptic (Foucault, 1977; Sia *et al.*, 2002) features of enterprise systems and the possible consequences of these features.

I think people can use [monitoring] to their own advantage. Sometimes there's too much information there, if you make a mistake or whatever, it can be used to the wrong advantage, which I am not too happy about.... It's there; it can be done. That's the worrying thing (Shift Planning Coordinator).

During the interviews, various work-arounds in the system were also mentioned. Those were employed in order to achieve something that could not be done in the prescribed way, and the workings of the system had to be reinvented, or the system had to be used in other than the usual ways. In most of these cases, the intended and established controls in the system (as implemented with the relevant authorization levels) were bypassed.

There are other screens, like for example, the stores people don't actually amend the material master. But there are certain fields where you actually go through on SAP, which the stores have access to, which if you follow through the fields, it'll actually take you to the material master, which you can actually go and change it... You can actually go through the back door and change things (Materials Controller).

Another example is that we put a block in the system to stop us using source list, basically so that we can't really amend a source list and buy stuff from other suppliers. But it doesn't really work, because all you do is still go in and create a new source list yourself (Materials Controller).

Using the system in those unintended ways had certain side effects in some cases. From an organizational perspective, this could result in data inconsistencies, which would impact various departments in the organization. From a personal perspective, people expressed their discontent about the impacts of those side effects.

I can sit here and create orders from my site. But I can also sit here and create orders for any other sites. There's nothing in stopping me in the system that says, this is not your site, you need some permission or something other to do work in their plant. Somebody from the other sites went and built some transaction on my site the other day, which messed up my stock basically.... [The impact of this transaction would be] financial, because the figures wouldn't have matched (Materials Controller).

These unintended consequences were mostly seen in a negative way; in some cases, however, there was a business

rationale behind the configuration of the system that allowed these consequences to occur.

There are benefits to being able to do it, like for example, if say, the person who places the order in another site is off sick, and there's only say, somebody here who can place the order, then that means that he can carry out the transaction. But what he should have there is that he ought to be able to go through some authority steps to do it (Materials Controller).

Discussion and theory development: embedding and disembedding aspects of enterprise systems and their impact on resilience

In this section, we draw on the three determinants (differential power, role of values in problem solving, impact of unintended consequences) outlined before as theoretical lenses, in order to interpret the results from the case study and to develop our theoretical conceptualization. The differential power determinant is presented in the following subsection, where the sources leading to it are discussed. Following this, the impacts of those power differentials are discussed, in terms of the 'role of values in problem solving' and 'impact of unintended consequences' determinants. We follow this with a discussion on disembedding and reembedding in enterprise systems, before presenting the model arising from this research.

Sources of power

The case description of TransCom illustrates that people are given decreased or increased authority, as a result of assignments of different authorization levels to carry out tasks in the system. In addition, people with increased knowledge of the system seem to gain authority as more people depend on their expertise in order to carry out their functions. Monitoring is another source of power, where the person carrying out the monitoring is seen to control what the subordinate is doing in the system. Monitoring in this case depends on the correct assignment of authorization levels to the right individuals.

It was also mentioned in the previous section that the assignment of authorization levels is carried out centrally, at a location where the global configuration of the system is implemented. Training can be done globally or locally; however, training that produces expertise in multiple areas of the system has to be carried out as a lengthy process requiring continuous interaction with the system at various levels. In the observed company, such training was self-administered and carried out by interaction with the system at a global level, while the system was being rolled out to the offices. This in turn equipped the relevant person with advanced knowledge of the system, and consequently, he gained authority because of his expertise.

In summary, the creation of authorization level profiles in the system, together with the monitoring capabilities of the system and the creation of expertise by various actors, resulted in the creation of power differentials. These power differentials then served to increase the control in the company, by empowering different users with different levels of capabilities.

Impacts of power

In the case presentation, the impact of certain aspects of power arising from the configuration of authorization levels, the generation of expertise, as well as the monitoring capabilities was mentioned. The configuration of authorization levels in some cases encompassed more authority than was necessary, either because of organizational requirements or because the system was too strict to allow intermediate levels of authorizations. As a result, there were *unintended consequences* of these configurations, which had a business impact on the company. The way to overcome those consequences was by specifying extra business rules, outside the ERP system, which defined acceptable behavior of users in the system, in the case where they were allowed to carry out tasks beyond their responsibilities in the system. However, these business rules were not always followed, and they were rather informal, as a consensus between peers, thereby decreasing the expected control offered by the ERP system.

Also, the perception of power differentials caused different people to see different ways in which to solve a problem. In the case where people were allocated increased authorization levels, and hence increased power, they tended to try and solve any issues in the system themselves, rather than talking to the experts who had more knowledge. Similarly, people regarded the perceived expert in SAP as their first point of call when encountering difficulties in the ERP system. This was quite informal, however, and the business rules clearly indicated that in cases of problems with the system, the helpdesk should be the first point of call. The *role of values* in this case was important in bypassing the business rules, as people had different perceptions on what was the best way to get help with solving a problem in the system.

In summary, the creation of power differentials resulted in unintended consequences in the company. In addition, people saw different ways of solving a problem according to their perception of those power differentials. Both those reasons served to decrease control in the company.

Disembedding in enterprise systems

An enterprise system can be disembedded, or lifted out, from social relations from local contexts of interaction, and restructured them across time space. This is achieved with the global nature of the enterprise system, which is configured in a central location. The social relations in this case, that are the outcome of the enterprise system, are power differentials that result from the global nature of the system, and the distribution of various pieces of information (of differing importance) to disparate actors. The disembedding process then results in increased control, caused by the centrality of the configuration of the enterprise system, and the concentration of power in the hands of selected individuals. As control increases, rigid mechanisms are put into place to make the organization more rigid and robust. As such, the processes and procedures in the company are solidified, and strict rules apply regarding access to and manipulation of company data. Depending on the degree of this rigidity in rules (enforced by the enterprise system), the company may become too inflexible to respond

efficiently to conditions of change and stress, and therefore become less resilient. Manipulation or relaxing of those rules may, however, lead to more flexibility (with the cost of partial loss of control), and hence resilience can actually increase.

Reembedding in enterprise systems

On the other hand, an enterprise system can also be seen to be reembedded, or reappropriated or recast, the disembedded social relations so as to pin them down to local conditions. This is achieved with the distributed nature of enterprise systems, which can be deployed in many locations across time space. The social relations that are reembedded in this case are the same power differentials (resulting from distribution of information in the enterprise system) that were the outcome of the disembedding process. As a result of the reembedding of these power relations, there may be drift because of the impact of unintended consequences of the system and the role of values of people in solving a problem. This reduction in control may serve to increase the resilience of the company, because the employees appropriate the system for their own use and are, therefore, able to respond more to change when this occurs. On the other hand, when the employees fully follow the processes and procedures dictated by the system, then there is less or no drift, and the control structures imposed by the system are reenacted. In this case, as mentioned above and depending on the degree of rigidity imposed by the enterprise system, resilience may actually decrease.

Conceptualization of disembedding and reembedding in enterprise systems

Figure 1 depicts our theoretical conceptualization of the disembedding and reembedding aspects of enterprise systems and their impact on control and resilience. Development of this conceptualization employs the embedding-disembedding concepts presented previously, and uses as sensitizing devices the three determinants on the ways knowledge (in this case information in the enterprise system) can impact control. The development of the framework in Figure 1 is based on data gathered during examination of the case study company, as well as the understanding generated on the impact of enterprise systems on organizational resilience.

Disembedding, as shown in the figure, occurs as part of the global nature of an enterprise system with a centralized configuration. What is disembedded in this case are various pieces of informational data in the system that are made available to authorized users. This leads to increased control as a result of the creation of power differentials. Reembedding then occurs as part of the distributed nature of an Enterprise System, which can be deployed across time space. What is reembedded in this case is the same information that was disembedded previously, which can now be used and processed by authorized users. This may lead to drift, stemming from unintended consequences of the system, and the perception of users regarding their use of the system.

Too much control in this case can make the organization too inflexible to absorb strain and recover from untoward

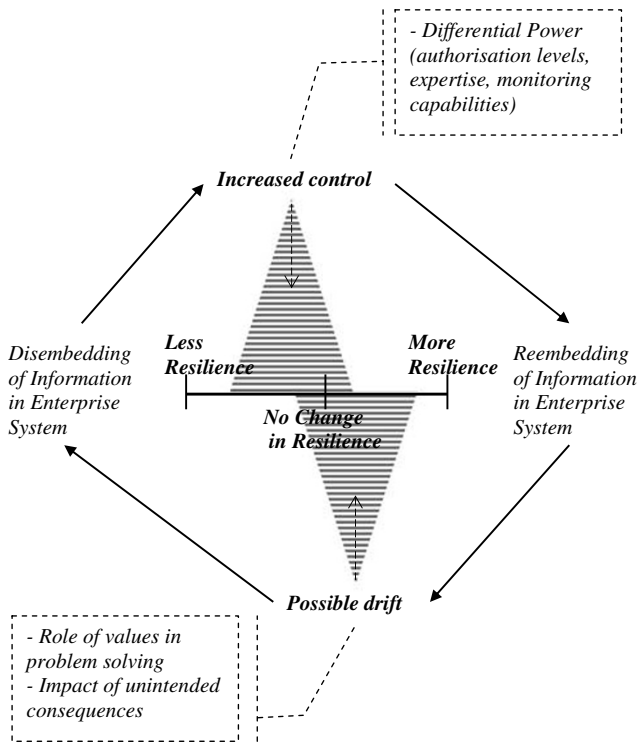


Figure 1 Embedding and disembedding aspects of enterprise systems and their impact on control and resilience.

events that may occur. As a result, the organization may become less resilient. On the other hand, if control is appropriately implemented to match the organizational needs, the company may become more resilient to change. This may come together with some possible drift from the original company's goals and objectives, but in the end, this drift, if managed correctly, may serve to make the company more flexible and resilient to future events that it may encounter.

Conclusions and implications

The purpose of this paper has been to present the findings of a study on the impact of enterprise systems on organizational resilience through processes of embedding and disembedding, and the creation of control and drift. Our conceptualization offers a way of examining changes in resilience offered by the use of an enterprise system. Although the focus of this study was an ERP system, the results can similarly be generalized for other enterprise-wide information systems.

The results of this research shed a new light on the way that enterprise systems can impact the organizational resilience of a company. Our findings agree with the literature (e.g. Hanseth *et al.*, 2001) that enterprise systems can get out of control if not managed correctly. The contribution of this research has been to refine and conceptualize the ways in which this can occur, through the embedding and disembedding of information, and the creation of power differentials. We agree with the view of Coombs *et al.* (1992), whereby control is used to draw attention to the intended and unintended consequences of the exercise of power and the use of knowledge in social

and organizational relations. We further refine their concepts to argue that the exercise of power within an enterprise system happens as part of a disembedding process, whereas unintended consequences happen as part of the consequent reembedding process. The disembedding process can lead to increased control, which if done excessively can stifle resilience. On the other hand, the consequent embedding process can lead to drift, which, if not left to get out of control, can serve to increase organizational resilience.

Our results here also complement those by Bloomfield and Coombs (1992), Bloomfield *et al.* (1994), and Orlikowski (1991), who argue that while IT can facilitate decentralization, at the same time, it can make possible a centralization of control and knowledge. We argue that decentralization may offer the opportunity to increase the resilience of a company by relaxing centralized control and rigidity. On the other hand, centralization of control and knowledge, if not managed correctly and done excessively, can decrease organizational resilience.

The implications of the findings from the current research for managers and practitioners are an increased awareness of the ways that definitions of control in an enterprise system can increase or decrease organizational resilience. This implies that increased attention should be paid to the levels of authority given to individuals in the system, according to organizational needs. Too much control can serve to streamline the operations of the company, but at the same time can decrease the resilience of the company to respond to future changes. Too little control can cause excessive drift, which can be harmful to the company. The middle and best way is to allow for the required controls to be implemented, but at the same time, not stifle the ability of the company to respond to future challenges.

The implication of this research for designers and developers of enterprise systems is that they should work closely with managers and end users of the system to make sure that the appropriate levels of authorizations and access profiles are built in and available in the system. In the opposite case, users may be given too much or too little authority through those access profiles, which can respectively lead to either the users abusing the system, or them not being able to carry out all of their functions in the system. In the first case, control is lost; in the second case, the company underperforms. In neither case, however, does resilience increase.

A limitation of the current research is that only one instance of enterprise-wide information systems has been examined, that of an ERP. Future research may investigate other (intra- or interorganizational) systems such as the customer relationship management or supplier relationship management systems. Although the boundaries between the latter and that of an ERP start to blur, it would be beneficial to examine the degree to which those systems strengthen or weaken the potential for organizational control and flexibility.

Acknowledgements

We thank the participants from the case study company for their time and cooperation. We would also like to acknowledge the valuable comments provided by Patrick Stacey on a previous version of this paper.

References

- Al-Mashari, M. and Al-Mudimigh, A. (2003). ERP Implementation: Lessons from a case study, *Information Technology & People* 16(1): 21–33.
- Bloomfield, B.P. and Coombs, R. (1992). Information Technology, Control and Power: The centralization and decentralization debate revisited, *Journal of Management Studies* 29(4): 459–484.
- Bloomfield, B.P., Coombs, R. and Owen, J. (1994). The Social Construction of Information Systems – The Implications for Management Control, in R. Mansell (ed.) *Management of Information and Communication Technologies – Emerging Patterns of Control*, London: Aslib, pp. 143–157.
- Boudreau, M.C. and Robey, D. (1999). Organizational Transition to Enterprise Resource Planning Systems: Theoretical choices for process research, in 20th International Conference on Information Systems (Charlotte, North Carolina, United States, 1999). 291–299.
- Boudreau, M.C. and Robey, D. (2005). Enacting Integrated Information Technology: A human agency perspective, *Organization Science* 16(1): 3–18.
- Bruns Jr., W.J. and McFarlan, F.W. (1987). Information Technology Puts Power in Control Systems, *Harvard Business Review* 65(5): 89–94.
- Ciborra, C.U. (2002). *The Labyrinths of Information: Challenging the Wisdom of Systems*, Oxford: Oxford University Press.
- Clegg, S. and Wilson, F. (1991). Power, Technology and Flexibility in Organizations, in J. Law (ed.) *Sociology of Monsters – Essays on Power, Technology and Domination*, London: Routledge, pp. 223–273.
- Coombs, R., Knights, D. and Willmott, H.C. (1992). Culture, Control and Competition: Towards a conceptual framework for the study of information technology in organizations, *Organization Studies* 13(1): 51–72.
- Finnegan, P. and Longaigh, S.N. (2002). Examining the Effects of Information Technology on Control and Coordination Relationships: An exploratory study in subsidiaries of pan-national corporations, *Journal of Information Technology* 17(3): 149–163.
- Foucault, M. (1977). *Discipline and Punish: The Birth of the Prison*, London: Lane.
- Giddens, A. (1990). *The Consequences of Modernity*, Cambridge: Polity Press.
- Hanseth, O. and Braa, K. (2000). Globalization and ‘Risk Society’, in C.U. Ciborra, K. Braa, A. Cordella, B. Dahlbom, A. Failla, O. Hanseth, V. Hepso, J. Ljungberg, E. Monteiro and K.A. Simon (eds.) *From Control to Drift – The Dynamics of Corporate Information Infrastructures*, Oxford: Oxford University Press, pp. 41–55.
- Hanseth, O., Ciborra, C.U. and Braa, K. (2001). The Control Devolution: EPR and the side effects of Globalization, *The DataBase for Advances in Information Systems* 32(4): 34–46.
- Markus, M.L. (1983). Power, Politics, and MIS Implementation, *Communications of the ACM* 26(6): 430–444.
- Nandhakumar, J. and Jones, M.R. (1997). Too Close for Comfort? Distance and Engagement in Interpretive Information Systems Research, *Information Systems Journal* 7(2): 109–131.
- Orlikowski, W.J. (1991). Integrated Information Environment or Matrix of Control? The Contradictory Implications of Information Technology, *Accounting, Management and Information Technologies* 1(1): 9–42.
- Orlikowski, W. (2000). Using Technology and Constituting Structures: A practice lens for studying technology in organizations, *Organization Science* 11(4): 404–428.
- Robinson, B. and Wilson, F. (2001). Planning for the Market? Enterprise Resource Planning Systems and the Contradictions of Capital, *The DataBase for Advances in Information Systems* 32(4): 21–33.
- Sia, S.K., Tang, M., Soh, C. and Boh, W.F. (2002). Enterprise Resource Planning (ERP) Systems as a Technology of Power: Empowerment or panoptic control? *The DataBase for Advances in Information Systems* 33(1): 23–37.
- Strauss, A. and Corbin, J. (1998). *Basics of Qualitative Research – Techniques and Procedures for Developing Grounded Theory*, Beverley Hills, CA: Sage Publications.
- Walsham, G. (1993). *Interpreting Information Systems in Organizations*, Chichester: John Wiley & Sons.
- Walsham, G. (1995). The Emergence of Interpretivism in IS Research, *Information Systems Research* 6(4): 376–394.
- Yin, R.K. (2003). *Case Study Research-Design and Methods*, Thousand Oaks: SAGE.

About the authors

Ioannis Ignatiadis is a Research and Teaching Associate at the University of Bath, School of Management, England. He received his Masters degree in Technology Management from UMIST, England. He also holds a Masters degree in Information Technology from Imperial College, England, and a Bachelors degree in Computer Science from the same University. He worked in the industry as a software consultant in Information Technology projects for big multinational companies in the UK, Germany, and Greece, covering the pharmaceutical, logistics, energy, and IT services sectors. He also worked as a project manager/analyst in the implementation of European Union-sponsored Information Society Technologies (IST) projects. His research interests evolve around the selection, implementation, and use of enterprise systems within an organization.

Joe Nandhakumar is a Professor of Information Systems at Warwick Business School, University of Warwick, England. He gained his Ph.D. from the Department of Engineering, University of Cambridge. Dr. Nandhakumar’s research focuses on the human and organizational aspects of information systems development, organizational consequences of information technology use, and theoretical and methodological issues in information systems research. He has widely published in these areas.