University College London

Department of Information Studies

Should systems managers concentrate more on managing people or managing technology to achieve their remit? Discuss the factors which might impact on the question, and state, explain and justify your answer.

Module leader:

Kosmas Kosmopoulos

This essay is submitted as an assessment for INST0031:

Systems Management

Student ID: 19075478

Word count: 2918

March 31st 2020

TABLE OF CONTENTS

1. INTRODUCTION

An information system (IS) is an integration of Information Technology (IT), data, and people. Such key elements cooperate to acquire, manage, save and provide information for the organisation and its decision-making process (LU, et al., 2011). One of the aspects of modern systems management is a fundamental change in attitudes to management and organizational structures of current companies. Old forms of line management are slowly retreating or moving into the operating background and modern matrix organizational structures are emerging in their place. Despite research efforts and best practise recommendations from academic and industry experts, many IT projects fail, are stopped or cancelled due to poor management (LU, et al., 2011), (Strong & Volkoff, 2010). According to Thamhain (2014), human factor is one of the biggest elements of risk in any project, but also one of the most crucial elements for reducing risk. This is caused by the fact that socio-technology systems are incorrectly or rarely used by the systems managers. It is a result of growing globalization as the systems management is constantly changing and technology trends are growing rapidly (Talaba & Tajafarib, 2012). Therefore, it is difficult to keep up with all the technology development and provide the essential latest training to all the staff. In an emerging global economy, modern information technology, rapid decision-making, strategic links, but especially the quality of human capital, well-developed systems management can provide competitive advantages for most types of businesses. Hence, increasing competition leads systems managers to align the technology and people in the most efficient way to fulfil business mission, needs and objectives (Talaba & Tajafarib, 2012), (Parsons, et al., 2012), (Onuoha & Obialor, 2015). Now the question arises: *Should systems managers concentrate more on managing people or managing technology to achieve their remit?* In order to answer this question, it is important to select systems managers activities and examine whether it is more important for systems managers to focus on people or technology within the examined activity. For the aim of this essay, outsourcing and data protection activities have been selected, because the activities provide unbiased sights, vary by its tasks and nature and allow readers to look at the question from a wider point of view.

2. SYSTEMS MANAGEMENT

It is important to define this term before diving into the systems manager's tasks and responsibilities. Hence, we must first understand the word "systems management" to determine the person who is in charge of this field. According to International Organization for Standardization (ISO, 2020) by systems management we mean a summary of actions that coordinate the whole project and helps to achieve its objectives (including all its parts and sub-tasks, health and safety compliance and service quality). It is essential to mention that systems management is applicable for any type of organization and any other field, at all levels, in all areas of its activity, regardless of the territory where organizations are located and operating (Shehabuddeen, et al., 2011). The systems manager usually works for the project manager as the senior technical person, responsible for all aspects of the IT system. That means they are responsible for guiding and operating IT team, secure and effective operation of all computer systems, related applications, maintenance of accurate IT policies, system architecture, assist in developing information technology strategic plans, data protection, hardware and software or serve as the primary point of contact for outsourced information technology service providers (Thamhain, 2014), (Skulmoski & Hartman, 2010), (Ferrance, et al., 2006). In addition, systems managers should be comfortable in dealing with people, knowledgeable in the latest business trends and obviously must be technically educated (Thamhain, 2014). Interestingly, in many industries systems managers are employed under different titles such as "information architect", "business systems manager" or "systems solutions manager" but they all are connected by the same mission: achieve all of the project goals, for instance, optimize the allocation of necessary inputs and apply them to pre-defined objectives such as time, budget, quality and scope (Thamhain, 2014). According to *Anantatmula* (2008) it is a routine opinion that managers should focus on leadership and invest in people capital to fulfil the business needs. In the modern age of project development technology plays a major role in the process and it helps managers to formalize and achieve the project objectives. Hence, systems managers must align technology and people management in such way that helps them to achieve the business objectives and helps organisation to grow. By applying numerous technological tools, systems manager can improve not only the communication with stakeholders, team members and managers but also new technology trends offeribg real-time project tracking, budgeting, accounting, reporting; task scheduling workflow automation or advanced cloud solutions which may lead to increased productivity and continuous improvement in project performance (Institute, 2018). Therefore, in the following paragraphs will be examined the question, is it more important to manage people or technology?

3. MANAGING OUTSOURCED IS/IT SERVICE PROVIDERS.

This section aims to summarize the possible reasons for outsourcing and to lay out the basics of managing people and technology in the outsourcing theory. Thus, the recommendations given here can be applied to any functional area. Moreover, the following paragraphs specify the outsourcing of IS/IT and additionally answering the proposed question of this essay.

Increasing pressure on competitiveness in the business sector and cost savings in public administration leads to reflections on what steps to take to achieve the expected results. As the importance of IS and IT increases, so does the importance of the quality of IS/IT management (Bragg, 2006). However, for many organizations, it seems financially unbearable or even impossible to ensure that all IS/IT development, operation and maintenance activities are in-house. Therefore, organizations are carefully selecting activities to squeeze outside to external suppliers of IS/IT components and services. It is caused by the fact that IT field is one of the most difficult to manage, which requires much technical skills and companies are not able to keep up with the latest technological development (Fisher, et al., 2006), (Karimi-Alaghehband & Rivard, 2019). Therefore, companies must outsource many of the mentioned aspects (Keller, 2001). According to *Bragg* (2006) IT services outsourcing is widely seen as a key business strategy as the external service provider already has the appropriate technical and personnel equipment, therefore they take on responsibility for the production and implementation of all information processes and other related information assets. Nevertheless, it is keen to define the balance between the outsourced areas or activities, so the companies are not becoming overly dependent on external suppliers as well as the outsourcing makes financially sense (Kosmopoulos, 2020). The areas of outsourcing are different, most often in the field of IS/IT include: network management, planning and strategy, legacy systems maintenance, consulting, maintenance and support, software development, information systems operation, back-end operation, web services, web hosting, helpdesk, call center, IT training and education (Thamhain, 2014). As we stated above, outsourcing IS/IT might be beneficial and sometime necessary shift for companies. For this reason, the key consideration is whether to allocate their efforts on managing people or technologies.

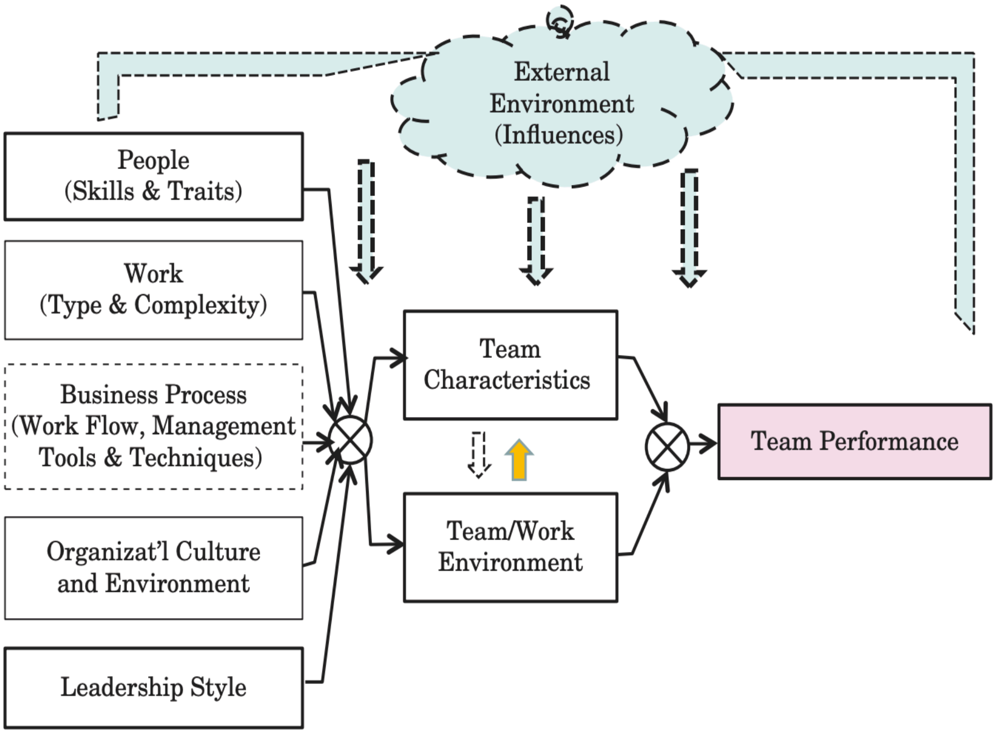
External Environment (Influences)
People (Skills & Traits)
Work (Type & Complexity)
Business Process (Work Flow, Management Tools & Techniques)
Organizat'l Culture and Environment
Leadership Style
Team Characteristics
Team/Work Environment
Team Performance

Figure 1 Influences affecting team performance in outsourcing enviroment (Thamhain, 2014)

3. 1. MANAGING PEOPLE:

The main advantage of outsourcing for companies is the save the cost associated with recruiting and training specialists. Because reputable IT companies can better exploit the potential of professionals and ensure that employees can concentrate on their knowledge, skills and overall it might support companies to become a leader in its industry (Talaba & Tajafarib, 2012), (Fisher, et al., 2006). External specialists may have a deeper specialization, smooth work flow, more experience, well-established relationships and leadership style, that directly influences team/work environment and potentially team perfomance as stated in Figure 1. All these reasons lead to handling tasks more efficiently, in terms of time and money. Hence, it is the systems managers responsibility to evaluate, observe and split / outsource the specific tasks between the right people. The usual mistake is hiring expensive specialists for routine tasks, that can be handled cheaper and more effectively (Bragg, 2006).

On the other hand, one of the most common concern about IT outsourcing is the possibility of data misuse (Photopoulos, 2011). If anyone has access to important information or technology and wants to misuse or damage it, this breach might be virtually impossible to prevent it. Therefore, the majority of companies comply with security and regulatory measures and define strong service level agreement (SLA), where the level of service (response times, agreed parameters, sanctions) and its scope are specified (Photopoulos, 2011), (Vaidya, 2019). Another usual concern to mention is the lost of control over IT functions. Although, you can request detailed monitoring and screening, but because the team is still operating off-site, it results in difficulties to implement those actions. It should be also borne in mind that the quality requirements may not be the same as those of an outsourcing company. Poor work and quality can increase the cost and may result in the loose of customers (Pankowska, 2019). There are other risks to considerate in terms of human factor in outsourcing, such as bankruptcy of the service provider, employees who are unwilling to retrain in the latest technologies, collapse of cooperation and flexibility, demotivated IT experts, which may disloyal managers (Photopoulos, 2011), (Bahli & Rivard, 2005). To conclude the above, pros and cons of managing people were stated and in the following part advantages and disadvantage of managing technology will be discussed.

3. 2. MANAGING TECHNOLOGY:

An essential benefit of outsourcing is the access to newest tools, updated techniques and latest technologies, which might be expensive to have in-house. These benefits also bind along the advantage of avoiding cost of continually re-training in-house IT professionals in such structured methodologies, procedures and documentation (Thamhain, 2014), (Photopoulos, 2011). Hence, outsourcing solves this problem in a very efficient way, resulting in reduction of operational cost. If companies aim to apply the technologies in-house, it will be inevitably connected with a continous investments in modernization. This option is also associated with a number of risks, such as the technology needed to meet the needs of the company will change over time and the supplier may no longer be able to support the new technology as well as outsourcing companies may find it difficult to pass their software licenses (Bragg, 2006), (Bahli & Rivard, 2005), (Bahli & Rivard, 2013).

To address the risks stated in the paragraphs above, these can be eliminated by a number of measures, which are clearly defined and clarified in the service level agreement (SLA). In some situations, mentioned risks may bring down the company or dramatically worsen its strategic or financial position, hence socio-technological system and its continual monitoring must be balanced carefully (Fisher, et al., 2006).

We can demonstrate that outsourcing addresses mainly personnel issues, as this dynamically evolving area requires qualified and experienced specialists, which can be find in the supplier's staff. There are not many of them in the labor market, and their full-time employment may be inefficient for organizations. This measure, however, keeps them from projects related to supporting the main activities of organizations and dilutes their expertise and specialization (Kosmopoulos, 2020). In addition to that, technology should support the decision made by systems managers who can control the technology by finding how updated the supplier's technology is, their ability to use the technology for the customer and their ability to train staff to use such technology. These options are all available to the manager who is heading into a decision to outsource.

4. MANAGING DATA PROTECTION

This section aims to summarize the possible reasons and risks of data protection and to lay out the basics of managing people and technology in the data protection theory to answer the proposed question of this essay.

Organizations collect and store large amounts of personal information about their customers, members and employees. Thus, they must pay attention to protecting privacy and reducing the growth of identity theft, through effective protections and regulations and action plan that will allow them to take informed decisions during an incident (Thamhain, 2014). This requires the development and implementation of response mechanisms for such a crisis before one occurs. It is necessary to understand what kind of data protection you are trying to solve, rather than asking what data protection you need (Buffington, 2010), (Hadlington, 2018) (Kosmopoulos, 2020). The loss of sensitive data remains a major concern for both organizations as well as individuals whose information could be at risk of breach. Organizations facing a data breach may experience reputational damage resulting in: negative publicity, loss of customer and representative confidence, legal and regulatory exposure, drop of credit rating and stock price, direct costs of handling such accident and complying with the legal requirements to inform consumers that their private information has been breached (Photopoulos, 2011), (Vaidya, 2019). In the following paragraphs will be discussed if systems managers who handle data protection may or may not put more effort on managing people.

4. 1. MANAGING PEOPLE

Loosing precious data is often caused by unproper workflow procedures and backup strategies (Photopoulos, 2011). Nevertheless, 65% of corporate information loss is caused by internal threats, which include employees, service personnel and visitors (Kosmopoulos, 2020), (Hadlington, 2018). This is due to the negligence or malevolence of employees, malicious internal or external parties, and unaddressed process of technical vulnerabilities. So-called internal attacks are one of the biggest threats facing data and systems. For the most frequent and sometimes the greatest damage due to loss or attack data is usually not hackers, but the employees themselves, who can accidentally / purposely delete the desired data, lost their storage devices, improper handle disposal data, share their organisational accounts and passwords, intentional or unintentional noncompliance with security policies (Hadlington, 2018), (Buffington, 2010), (Vaidya, 2019). Hence, following from Figure 2, systems managers are responsible for ensuring that all employees are aware, educated and trained in appropriate security policies, standards and procedures for protecting sensitive information and can becoming more aware of the consequences their actions may lead to. Activity monitoring and logging of employees will help analyse physical access to sensitive information, policy compliance, identify attacks and breaches and support an effective response program. This can be done by providing effective use of IDs for certain access purposes (Photopoulos, 2011). On the contrary, Dodke (2019) stresses that these prevention policies may contain number of risks such as interruption in workflow of employees who will be constantly with errors and notifications even when they are trying to access data in an appropriate manner. Therefore, systems managers aim to create honest work relationships and increase the trust in the workplace, which might result in less data breaches incidents (Parsons, 2016)

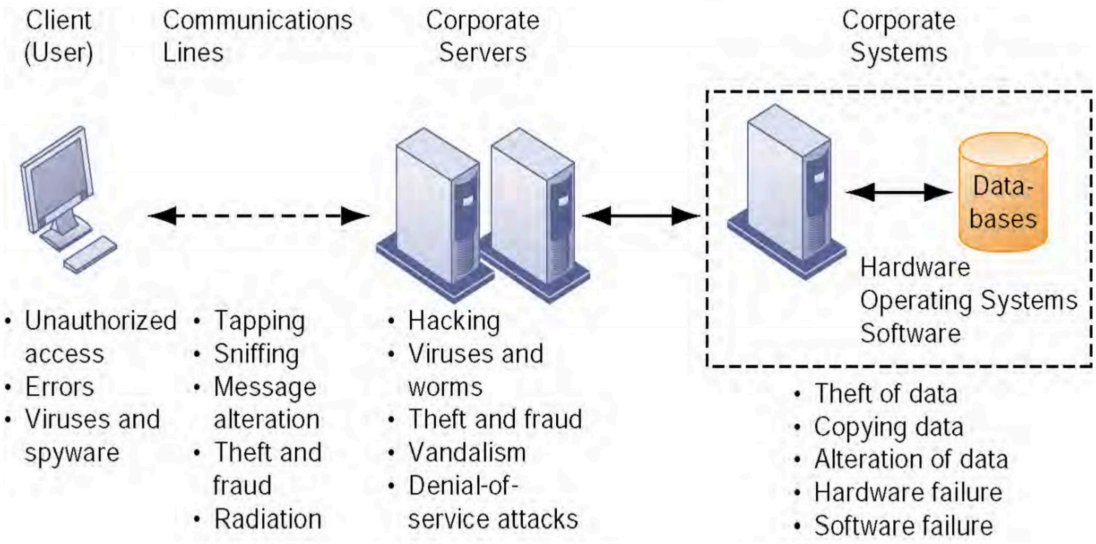

Figure 2 The weakest link in the data protection chain is poor management (Kosmopoulos, 2020)

4. 2. MANAGING TECHNOLOGY

A significant number of data loss reported by IT experts result from infection with malware, defect in the design or other malicious software code. Adding the risk of software failure or software code that creates security risks into information systems or databases, we find it to be one of the biggest potential problems resulting in unauthorized access to sensitive information. Such breaches have the ability to destroy, steal or encrypt data, and in some cases completely disable the computer hardware and penetrate the entire network (Thamhain, 2014). E-mail attacks and phishing are the one of the most common inputs to computers and subsequently computer networks today (Kosmopoulos, 2020). Hence, systems managers should prevent this from happening by implementing technical prevention system such as detection module programmed to alert staff when unauthorized software or application is trying to access sensitive data, strong data backup procedures, recovery testing, firewalls or more sophisticated password management (Photopoulos, 2011), (Vaidya, 2019).

As examined above, data breaches can have several or more root causes, including lax employees, negligent third parties, malicious internal or external parties and unaddressed process or technological vulnerabilities. Often, companies do not even know how catastrophic impacts data failures and data losses can have. Therefore, the first necessary step is to thoroughly assess the risks associated with both the company’s information architecture as a whole and its individual parts. Result of this analysis should be accurate information on the importance of each part, including their relationship to the most important processes of organizations.

5. CONLCUSION

In order to answer and conclude the proposed question *“Should systems managers concentrate more on managing people or managing technology to achieve their remit?”* the essay demonstrates that systems managers should focus on people management, developing its relationships, training employees in the best technology tools, which supports systems manager’s decision and enhances people capabilities. It is necessary for systems managers to invest their efforts into the right people and tools, which makes their decisions more accurate and strenghten project workflow to meet the objectives. As it is evident from the paragraphs above, such management consists of four main pillars in the following order: (1) staff training and education, (2) adoption of set guidelines and best practices aligned with working tools and technology, (3) best technology tools for evaluating software vulnerabilities and quality, (4) auditing and monitoring of set standards. As demonstrated in the systems managers tasks , both people and technology management should be aligned together in the most efficient way to fulfill the business needs and to resolve the potential problem together as quickly and with minimal loss as possible. Evidently in the modern era, people and technology are two inseparable parts.

6. BIBLIOGRAPHY

Anantatmula, V. S., 2008. The Role of Technology in the Project Manager Performance Model. Project Management Journal, 39(1), pp. 34-48.

Bahli, B. & Rivard, S., 2005. Validating measures of information technology outsourcing risk factors. Omega, 33(2), pp. 175-187.

Bahli, B. & Rivard, S., 2013. Cost escalation in information technology outsourcing: A moderated mediation study. Decision Support Systems, Volume 56, pp. 37-47.

Bragg, S. M., 2006. Outsourcing: a guide to — selecting the correct business unit — negotiating the contract— maintaining control of the process. New Jersey: John Wiley & Sons.

Buffington, J., 2010. Data Protection for Virtual Data Centers. canada: Wiley Publishing.

Dodke, D. N., Manmohan, S. S. & Pune Maharashtra, 2019. SYSTEMS AND METHODS FOR MANAGING DATA LOSS PREVENTION POLICIES FOR APPLICATIONS. US, Patent No. 10,191,908 B1.

Fisher, J., Hirscheim, R. & and Hirschheim, R., 2006. Delivery of IT services: a case study of outsourcing at alpha corporation. s.l., Association for Information Systems.

Hadlington, L., 2018. The "Human Factor" in Cybersecurity. Advances in Digital Crime, Forensics, and Cyber Terrorism, pp. 46-63.

Institute, Project Management 2018. PMI. [Online] Available at: www.pmi.org
https://www.pmi.org/-/media/pmi/documents/public/pdf/learning/thought-leadership/pulse/pulse-of-the-profession-2018.pdf#page27
[Accessed 20 3 2020].

21500:2012, I., 2012. ISO. [Online] Available at: https://www.iso.org/
https://www.iso.org/standard/50003.html
[Accessed 20 3 2020].

J., F., Green, S. G. & Forster, W. R., 2006. Getting More out of Team Projects: Incentivizing Leadership to Enhance Performance. Journal of Management Education, 30(6), pp. 788-797.

Karimi-Alaghehband, F. & Rivard, S., 2019. Information technology outsourcing and architecture dynamic capabilities as enablers of organizational agility. Journal of Information Technology, 34(2), pp. 129-159.

Keller, R. T., 2001. Cross-Functional Project Groups in Research and New Product Development: Diversity, Communications, Job Stress, and Outcomes. The Academy of Management Journal, 44(3), pp. 547-555.

Kosmopoulos, K., 2020. IT Outsourcing, London: UCL.

LU, Y., XIANG, C., WANG, B. & WANG, X., 2011. What affects information systems development team performance? An exploratory study from the perspective of combined socio-technical theory and coordination theory. Computers in Human Behavior, 27(2), pp. 811-822.

Onuoha, J. & Obialor, D., 2015. The Impact of Information Technology on Modern Librarianship: A Reflective Study.. Information and Knowledge Management , 5(11), pp. 52-58.

Pankowska, M., 2019. Information Technology Outsourcing Chain: Literature Review and Implications for Development of Distributed Coordination. Sustainability, 11(5), p. 1460.

Parsons, M., Rollyson, J. & Reid, D., 2012. Evidence-Based Staff Training: A Guide for Practitioners. Behavior Analysis in Practice, 5(2), pp. 2-11.

Parsons, P., 2016. Ethics in Public Relations: A Guide to Best Practice. third ed. s.l.:s.n.

Photopoulos, C., 2011. Managing Catastrophic Loss of Sensitive Data. s.l.:Syngress.

Shehabuddeen, N., Probert, D., Phaal, R. & Platts, K., 2011. Representing and Approaching Complex Management Issues: Part 1 - Role and Definition. SSRN Electronic Journal.

Skulmoski, G. J. & Hartman, F. T., 2010. Information Systems Project Manager Soft Competencies: A Project-Phase Investigation. Project Management Journal, 41(1), pp. 61-80..

Strong, D. M. & Volkoff, O., 2010. Understanding Organization—Enterprise System Fit: A Path to Theorizing the Information Technology Artifact. MIS Quarterly, 34(4), pp. 731-756.

Talaba, S. M. G. & Tajafarib, M., 2012. Impact of information and communication technology (ICT) on library staff training: A comparative study. Annals of Library and Information Studies , Volume 59, pp. 7-15.

Thamhain, H. J., 2014. MANAGING TECHNOLOGY-BASED PROJECTS. New Jersey: John Wiley & Sons.

Vaidya, R., 2019. Cyber Security Breaches Survey 2019: Statistical Release. [Online]
Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/875799/Cyber_Security_Breaches_Survey_2019_-_Main_Report_-_revised.pdf
[Accessed 20 3 2020].