IDEA GROUP PUBLISHING

701 E. Chocolate Avenue, Suite 200, Hershey PA 17033, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.idea-group.com

ITP4581

NETWORK RISK ASSESSMENT FOR SYSTEMS CHANGE

Philip J Irving, Principal Lecturer. philip.irving@sunderland.ac.uk
Helen M Edwards, Professor (Software Engineering). helen.edwards@sunderland.ac.uk
University of Sunderland, School of Computing and Technology, David Goldman Informatics Centre
St. Peter's Campus, SUNDERLAND, SR6 0DD. UK., Tel: +44 (0)191 5152408, Fax: +44 (0)191 5152781

ABSTRACT

Risk assessment for systems implementation (or change) normally focuses on the software development aspects of the process or user interactions with a system. However, there is an important connection between the software system and the network upon which it runs. Changes to one can have significant impact on the other. The need to consider this interaction is presented and the lack of available literature to support this activity is outlined. Examples are given to illustrate the effect of failing to evaluate networks within the risk assessment of systems change.

INTRODUCTION

Many risk assessment methods consider computer systems to be complex socio-technical systems: and thus they provide mechanisms for assessing the interaction between, for instance, the users and the software. However, the fact that such systems are frequently composed of sub-systems often seems to be overlooked. Whereas, changes to a sub-system needs to analysed not only in isolation, but also in terms if the impact on the whole. One sub-system that we believe is frequently overlooked in terms of its importance in terms of complexity of systems change is the network. However, corporate networks are, perhaps, the single most important subsystem of all: for data (often mission critical) flows through the network like blood flows through the human body. Moreover, just as the body suffers if blood ceases to flow, so the organisation may cease to function if the data doesn't reach its destination. Two examples seek to illustrate this point: consider a bank where the cash machines take half an hour per transaction, or a company trading on-line that takes 40 minutes for a customer to pass through the checkout. In either case, the software systems may function correctly, but the outcome "falls short of what was expected" (Kontio, 1997). The failure may, in such cases, be a result of ineffective networks (rather than faulty software) and issues outside the boundary set by the software project manager.

In this paper we seek to draw attention to the need for effective research into relevant risk assessment and mitigation practices for coping with systems changes in networked environments. To present our argument we outline the lack of existing literature, provide a summary of the consequences of network failures, discuss the impact of systems change on networks and network changes on systems before drawing the conclusion that further work is required in the area.

LITERATURE REVIEW

Network Risks in Systems Change

For any researcher investigating a problem area an initial task is the review of relevant literature. In this case the required literature would be both general risk literature and specific work on risk assessment for networks. Such literature was indeed acquired. However, the search for "network risk assessment" returned papers focusing simply on the aspect of security risks. This is undoubtedly an important concern, for example vulnerabilities in the area of security can lead to theft, fraud, data loss or even a Denial of Service (DoS) attack (Brooke, 2000; Myerson 1999). However, this is not the only area of risk in the networked environment: for example, preventing effective use of a network will also deny the users the services which they require. Thus a software project which causes a network to under perform will also lead to the serious situation of a DoS, yet no evidence of such research has been uncovered in literature surveys conducted by the authors. It was considered that a literature search of network design would also be useful in identifying risk assessment strategies for networks: but again, in practice, that also produced little of relevance to software development and change. The authors and a masters project student have carried out extensive searches using the digital library of the IEEE and ACM, ScienceDirect, Web of Science, Google and other search engines and have only been able to retrieve network risk assessment research covering security, results of these searches are reported in Velde (2002) and Irving (2002).

This absence of a literature review perhaps indicates a large gap in current risk thinking. Risk doesn't just apply to the development/change process, it applies to implementation of that process. Most authors in computing will recognise that failure to correctly specify the design will cause many problems in implementation; yet none seem to be considering risks arising from, for example, failure to review the network.

Consequences of Network Failures

It can be argued that failure to consider network failure is as damaging as failure to consider design problems: if the design of the project is flawed then the product may be totally unusable or require extensive re-working. Whereas, where the underlying network is incapable of supporting the project then project implementation may well bring down the entire network and all the mission and safety critical systems, which operate upon it. Indeed surveys in 1994 (Disaster Recovery Planning, 1994) in the US highlighted the following effects of computer outage:

1. The average company will lose 2-3% of gross sales within 8 days of a sustained computer outage.
2. The average company that experiences a computer outage lasting 10 days will never fully recover. 50% will be out of business within 5 years.
3. The chances of surviving a disaster affecting the corporate data processing centre are less that 7 in 100. The chances of experiencing such a disaster are 1 in 100.

This survey shows the effects of a sustained computer outage across a sample of 100 companies in the US. The companies in the survey ranged from sole traders to multi-national organisations. Whilst the authors recognise that in terms of a 2002 paper this information is dated, few would argue that the stakes (and the risks), given the prevalence of the internet, are now much higher.

Network failure can also lead to data loss, Cipriano (1994) reported that "Among companies that experience severe data loss, 43% never reopen and 90% go out of business within 2 years". Indeed the

authors have personal experience of companies that would be unlikely to survive more than a week if they lost their network.

NETWORK RISK ASSESSMENT DISCUSSION

Given the impact of network failure it might be expected that project managers would take this into account in their risk assessment. However, the limited evidence accrued thus far, from the literature and in discussion with practitioners, suggests that this factor is rarely considered. Perhaps this confirms Keil et al's assertion that "project managers believe they can control these risks" (Keil et al,1998). It is a fact that networks, although rapidly developing still lag behind computing power in terms of speed (Irving 2003); thus the effects of failure to give appropriate consideration to the network are irreversible. There may be no mitigation path available: a network cannot be simply "upgraded", this needs to be a planned change. Change here is another long project in which a careful analysis must be undertaken to determine the effects of the change to all systems. Obviously this can seriously delay the implementation of the project.

The problem is further compounded in many organisations where network management staff are often completely divorced from systems developersment staff: and are quite often under completely different management. But, rationally we can see that most applications developed are dependent upon the network. Moreover, changes made to the network will affect what the software development team are producing. Therefore, to make progress we need to assess risk within a network context from two perspectives:

i. System changes that affect networks
ii. Network changes that affect systems

The latter perspective should be the domain of the networking team, the former the domain of the development team. However, just as Kontio (1997) advocates a close working relationship with the users, the authors would advocate a close working relationship between the teams.

Systems Change: Impact on Networks

There are many situations in which a change to the software or the system will affect the operation of the network. Whilst in some cases, the network may be able to be upgraded and cope with the change, there are other instances where the network cannot be upgraded. As a means of demonstrating such points, there follows an example of a project in which risk assessment of systems change/implementation failed to recognise the impact of the changes to the network. A simple illustrative bandwidth example is given below (Figure 1). This illustrates the failure of the software developers to take into account the abilities of the company's current network, which in turn leads to the system being unusable. More details and further examples can be found at (Irving, 2002).

Figure 1: Bandwidth example

> Company 1 is a medium sized highly profitable organisation based in a listed Victorian building. Four years ago, they spent a large amount of money having a network installed and a networked sales order system developed. Whilst this software helped them to be successful, it is now found to be constraining their growth and they contracted a software consultancy to develop new software. As they are due to move to purpose built premises in one year they wish to spend very little money on the current building. The new system was much improved resulting in an increase in the amount of data to be shipped on the network. Thorough testing was undertaken on the consultant's premises and the software approved. Upon implementation at company premises, the performance of the software was so poor that it immediately had to be withdrawn. The first analysis of the problem showed that the PCs were less powerful however, a suggested upgrade failed to improve performance. The root cause of the problem was that the network bandwidth could not support the requirements of the new software.

For this example changing the network architecture was out of the question because of the huge costs imposed by constraints of the building. Therefore, the new software could not be used. Risk assessment for the network had not been undertaken resulting in catastrophic consequences for the project.

Network Change: Impact on Systems

Just as the software project manager should consider how the software changes will affect the network, so the network team should consider the problems that a network change can make to software and its users. This illustrates that the network and development teams need to maintain regular contact. An example case study can be found at (Irving, 2002).

CONCLUSIONS

Most risk assessment methods define a boundary for the system being changed: however, computer systems almost always comprise of sub-systems which need to integrate successfully with the other systems. Unfortunately the risk assessment methods that have been analysed by the authors fail to adequately recognise the impact that the network and software components of a systems can have on one another. This paper has highlighted the need to investigate this aspect of systems change further. The authors are in the early stages of a research project which will both gather empirical data from practitioners and evaluate existing risk assessment and mitigation approaches in order to develop an approach that reflects the interconnection that exists between systems and networks.

REFERENCES

Brooke, P. (2000). *Network Computing.* October 30th 2000.

Cipriano, M:.(1994). Marketing director for Mountain Network Solutions.

Disaster Recovery Planning (, 1994). Disaster Recovery Planning: Managing Risk & Catastrophe in Information Systems", 1994. ExertExtract published in *On-track Ltd Data Protection Guide* 1994.

Irving, P. (20022). *Examples of Network Risks*. o osiris.sunderland.ac.uk/~cs0pir/irma2003.

Irving, Philip .J. (2003). Computer Networks. Learning Matters, London. ISBN: 1903337062.

Irving, Philip .J. (2003). Local Area Networks. Crucial Publishing, London.

Keil M, Cule, P.E., Lyytinen, K. and Schmidt, R. (1998) "Against all odds: A new framework for identifying and managing software project risks". *Communications of the ACM*, Vol. No. 41, no. 11 pages 77-83.

Kontio, J. (1997) *The Riskit Method for Software Risk Management, Version 1.*0. CS-TR-3782 University of Maryland (can be downloaded from http://mordor.cs.hut.fi/~jkontio/riskittr.pdf)

Myerson, Judith (11999). Risk Management . *International Journal of Network Management* Vol 9, Pages 305-308.

Velde, N-H. (2002). *Risk Assessment of Network and Systems Changes*. MSc IT Management Project, University of Sunderland, UK.