IDEA GROUP PUBLISHING
701 E. Chocolate Avenue, Suite 200, Hershey PA 17033-1240, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.idea-group.com
ITB12587

This paper appears in the book, *Emerging Trends and Challenges in Information Technology Management, Volume 1 and Volume 2* edited by Mehdi Khosrow-Pour © 2006, Idea Group Inc.

Potential Weaknesses in Risk Assessment for Business Data Communications

Philip Irving, Sonia Tindle, & John Tindle
University of Sunderland, School of Computing & Technology, David Goldman Informatics Centre, St. Peter's Campus, SUNDERLAND, SR6 0DD, UK, T: +44 (0)191 5152752, F: +44 (0)191 5152781, {philip.irving, sonia.tindle, john.tindle}@sunderland.ac.uk

ABSTRACT
Initial research presented by the authors in 2003 suggested that a particular area in ICT is excluded from current risk assessment processes - the point where Systems Development (SD) and network engineering overlap. Extensive on-going research has confirmed this gap and risks it poses to both Business Data Communications and SD. The lack of existing relevant literature supports this view. Preliminary results from an empirical survey indicate that neglect of this area allows risks to threaten SD/change.

INTRODUCTION
Current RA methods often approach the evaluation of computer systems from a socio-technical perspective, overlooking sub-systems. One sub-system that we believe is often neglected is the network. Corporate networks are arguably the single most important sub-system of all; data flows represent the life-blood of an organisation and any interruption will have serious implications. While such network failures normally fall outside the project manager's influence, they may cause his software systems to under-perform or fail to operate. This paper updates previous work by Irving and Edwards (2003).

RA AREA OF OMISSION
The IT industry has an unenviable record for unsatisfactory systems development projects. In 1995 US companies alone spent an estimated $59 billion in cost overruns and another $81 billion on cancelled software projects (Johnson, 1995). Five years after publication of Boehm's (1987) initial work, equally surprising was that few organisations used formal RA (Griffiths & Wilcocks, 1994). Software RA attempts to address these issues.

Literature within network RA is mostly security related (Myerson, 1999), reflecting the priority most organisations assign to maintaining data privacy and security. However, equally important is the need to ensure easy access to that data. One of the most feared security threats is the Denial of Service (DoS) attack where the organisation is denied access to its network and data (Irving, 2003 and 2005; Myerson, 2002), usually with catastrophic effects (Glennen, 1997). Preventing such attacks is one of the key objectives of network security (Lewis et al., 2003).

An application which requires more than the available bandwidth will flood the network with data, forming queues at key networking devices. As the buffers fill, packets will be dropped in an attempt to throttle back the network traffic, giving the same symptoms as a DoS attack (Cisco, 2004). Quality of Service (QoS) would be unlikely to aid the problem unless the offending application is given a lower priority (Cisco, 2004b).

It is unlikely too that network design would highlight the problem. After initial design, maintenance of the network is a somewhat iterative process: reviewing traffic flows, then predicting and planning for network growth.

FAILURE OF CURRENT RA METHODOLOGIES
Effective control relies upon network failure being identified as part of the software or systems change RA process. Extensive literature searches by the authors and MSc students indicate that it is unlikely that current SD/change RA methods would identify such risks (Velde, 2002; Irving and Edwards, 2003; Irving, 2004; Chew, 2005). Similarly, it is unlikely that acceptance testing would flag up problems. While network impact may be included in the test criteria, it would be difficult to assess before the end product had been produced (Zeed, 1996).

Of the main published software RA methods, only RiskIT and SERUM could possibly identify the networking risks. Even here, specialist knowledge would be required by the teams. Unfortunately, these methods don't mandate such knowledge or staff in the project teams (Irving 2004).

PRELIMINARY FINDINGS
The literature surveys confirmed the need for RA identified by Hall (1998) and the authors have clearly shown that there is a gap where network and software RA overlap. An empirical survey is currently being undertaken in a large not-for-profit organisation in the North East of England to determine practice in this area. Stratification (Kendall and Kendall 1992) was used to determine appropriate layers to survey and the investigation was undertaken via interviews over a one month period.

All software bought or developed runs on the network, making network performance critical to project success. At the organisation level, all major business systems are procured. Of the non-major business systems, 50% were developed in-house with the remaining 50% being bought in. Budgets ranged up to £300,000 (including hardware) with the typical budget being between £15k and £50k. Larger systems (up to £2m) were procured by specially formed project teams. As with most organisations, the financial risks of a failed project are formidable.

It was found that RA was unusually high on the agenda of the organisation as a result of recent audit criticism. Such RA was mainly operational but some had filtered down to project level.

A client-led project focussed approach is used; the client department establishes the project and the central IT team work as "contractors". Control is via fortnightly progress meetings. Projects are managed through a subset of the PRINCE methodology (Prince 2005). Risks are identified through brainstorming and recorded on a risk identification sheet very similar to the SEI/SRE model (Sisti 1994). There is no specific toolkit for the identification of risks such as that found in the RiskIT method (Kontio 1997). Further, RA takes place as part of the project rather than before its inception, unlike methods such as RAMESES (Edwards 2000). The brainstorming technique is not iterative and relies on all risks being identified by team members. Risks are then graded by their impact and likelihood of occurrence for subsequent management. Such an RA technique would be unlikely to identify networking risks which is evidenced even with the inclusion of a networking professional

in the project team. There is evidence to suggest that not all risks are identified.

Nevertheless, this approach seems to be successful, with the majority of projects coming in on time and in budget compared to only 30% found by OTR (1992). However, funding and timescales are tightly linked to specific budgets which is likely to be jeopardised if the project overruns.

At the departmental level SD was undertaken piecemeal with no formal RA. Whilst the projects developed at this level weren't mission critical, they did reside on the network alongside mission critical applications and had the potential to wreak havoc.

It was found that network RA appears to be limited to verifying that the proposed solution speaks IP and will operate with the network devices. No attempt is made to determine how much additional traffic will be placed on the network and whether the network will be able to cope with the additional load. Where the system is a replacement, there is an assumption that the new system will use the same amount of bandwidth as the old. As we are moving more towards web based applications and seeing a change from the old 80/20 rule where 80% of network traffic was local to the new 80/20 rule where 80% of traffic traverses the corporate backbone (Irving 2005), this is an unreliable assumption. Additionally, no baseline data exists of network performance (other than the network backbone) and no trials are carried out to determine bandwidth required by the new application.

Even during installation no measurements are taken pre/post installation. Although there have been no catastrophes, there is evidence to suggest that some applications are performing worse on the live network than they were on a private network, despite backbone measurements suggesting a maximum of 40% utilisation. This was identified during one large project which trialled the software on a private network first. Fortunately the new system, even though impeded by the network, still performed better than the system it replaced. To the users, therefore, it represents a step forward.

CONCLUSIONS

Clearly RA is desirable in SD/change (Hall, 1998). Yet evidence (Standish 1995), suggests that it is not widely practised and that software projects continue to be a problem. There are many reasons for this from the difficulties inherent in SD projects (BSI, 1995) to the difficulties in applying the RA techniques, yet there are clearly enormous benefits to their application.

Since the beginning of the 1990's a number of RA methods have been developed which address a wide range of SD problems. A thorough review of each of these methods found that there was a general lack of support for network RA for systems change. Similarly, thorough reviews of network RA revealed almost no treatment apart from minor consideration by Myerson (2002). In today's competitive environment, organisations cannot afford to be risk averse; instead, they are forced to take risks to gain a competitive advantage (Neumann 2000). Thus RA and management are crucial to the well being of the organisation.

Early evidence from our empirical survey clearly demonstrates that even a formal project management method and the addition of a member of networking staff to the project team is insufficient to identify all of the networking risks. This suggests the need for a formal method or toolkit such as that in the RiskIT approach (Kontio 1997).

Overall we conclude that there is a need for network consideration during the RA phases of SD projects, that risks do go unnoticed by current practice and do impact upon end system performance. The results obtained so far in this survey have led us to believe this is indeed a weakness in the SD/change process worthy of further investigation.

REFERENCES

Boehm, B.W. (1987), "Improving Software Productivity", IEEE Computer, pp 43-57, May, 1987.

Chew, B. (2005). Network Risk Assessment. MSc Dissertation, University of Sunderland 2005.

Cisco Systems (2004). Building Scalable Cisco Internetworks. Cisco Press 2004.

Cisco Systems (2004b). Building Cisco Advanced Switched Networks. Cisco Press 2004.

Edwards et al. (2000) "The RAMESES method: Decision support for systems change in SMEs (a guide for SMEs). University of Sunderland.

Glennen, A. (1997) Computer Insurance – the only constant is change. Insurance Brokers' Monthly and Insurance Adviser 47, 12 (1997), 11-13.

Griffiths, C. and Willcocks, L. (1994) Are Major Information Technology Projects Worth the Risk?, Oxford Institute of Information Management/IC-PARC, Imperial College, 1994.

Hall, E. M. (1998) Managing Risk: Methods for Software Systems Development.1998 Addison Wesley.

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

Irving, P. J. and Edwards, H.(2003) Network Risk Assessment for Systems Change. International Research Management Association (IRMA) 2003.

Irving, P. (2004). Network Risk Assessment for Systems change. MSc thesis. University of Sunderland.

Irving, P. (2005) Computer Networks 2nd Edition. Lexden Publishing, Ipswich, UK. ISBN: 190499508X

Johnson, J. (1995) Chaos: The dollar drain of IT project failures. Applic. Dev. Trends 2, 1 (1995), 41-47

Kendall, K. E. and Kendall, J. E. (1992). Systems Analysis and Design. 2nd Edition. Prentice-Hall editions. Prentice-Hall International ISBN: 0-13-880907-0.

Kontio, J. (1997) *The Riskit Method for Software Risk Management, Version 1.00*. CS-TR-3782 University of Maryland (can be downloaded from http://mordor.cs.hut.fi/~jkontio/riskittr.pdf)

Lewis, W. (2003) An Empirical Assessment of IT Disaster Risk. Communications of The ACM September 2003/Vol. 46, No. 9ve.x

Myerson, J. (1999). Risk Management . *International Journal of Network Management* Vol 9, Pages 305-308.

Myerson, J. M. (2002) Identifying Enterprise Network Vulnerabilities. International Journal of Network Management. Volume 12, Pp 135-144.

Neumann, P. G. (Editor) (2000). Risks to the Public in Computers and Related Systems. ACM Sigsoft, Software Engineering Notes vol. 25 No. 4. July 2000 Pp 7-11.

OTR Group, Computer Weekly, Dec 12th, 12, 1992.

Prince 2005. http://www.ogc.gov.uk/prince2/ last accessed 22/11/05.

Sisti, F. and Joseph, S. (1994) "Software Risk Evaluation method v 1.0", Software Engineering Institute Technical Report, CMU/SEI-94-TR-19, SEI, Pittsburgh, PA., Dec. 1994.Standish Group, "CHAOS report", 586 Olde Kings Highway, Dennis, MA 02638, USA, 1995.

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

Zeed, HM (1996) *Modelling the maintenance process at Zurich Life Insurance*. 12th International Conference on Software Maintenance (ICSM'96)