Bridging the Gap between General Management and Technicians – A Case Study in ICT Security

Jabiri Kuwe Bakari, Charles N. Tarimo, Christer Magnusson, and Louise Yngström

Department of Computer and System Sciences, Stockholm University/KTH, Forum 100
SE- 164 40 Kista, Sweden
{si-jba, si-cnt, cmagnus, louise}@dsv.su.se

Abstract. The lack of planning, business re-engineering, and coordination in the whole process of computerisation, is the most pronounced problem facing organisations in developing countries. These problems often lead to a discontinuous link between technology and the business processes. As a result, the introduced technology poses some critical risks to the organisations due to the different perceptions of the management and technical staff in viewing the ICT security problem. This paper discusses a practical experience of bridging the gap between the general management and ICT technicians.

1 Introduction

The paper outlines a successful mission of how to bridge the gap between general management and ICT technicians. It is based on practical experiences obtained from an ongoing study which aims at developing guidelines for managing ICT security in developing countries' organisations. The study was guided by using the BRITS framework [1, 2, 3] where ICT risks are viewed as part of the actual business rather than primarily as part of the ICT. The framework also includes a repository of mitigation suggestions, hosted in the EMitL database, which was used together with ITIL, ISO 17799 and COBIT [4, 5, 6, 7]. The findings are organised in a list of ten initial steps or aspects of importance to successfully bridge the gap. The presentation highlights the motivation and practical experiences of each step.

2 The Ten Aspects of Importance in Bridging the Gap between the Management and Technicians

In this section, the 10 steps are outlined and discussed with respect to the experience encountered when executing each. It is a part of the findings of a study conducted at the beginning of 2005, at a government-owned service provider organisation in Tanzania. The organisation is operating in 21 out of 26 regions of the country. It has 900 staff in total and its operations are based on four main core services, where three of them are greatly dependent on ICT to meet their intended objectives. The

Please use the following format when citing this chapter:
Author(s) [insert Last name, First-name initial(s)], 2006, in IFIP International Federation for Information Processing, Volume 201, Security and Privacy in Dynamic Environments, eds. Fischer-Hubner, S., Rannenberg, K., Yngstrom, L., Lindskog, S., (Boston: Springer), pp. [insert page numbers].

organisation has approximately 2 million customers scattered throughout the country, with approximately 25% active customers. The steps included:

(i) Getting top management's sponsorship (the chief executive officer (CEO) buying into the idea first)
(ii) Getting technical management sponsorship (the technical department is the custodian of ICT in the organisation)
(iii) Set up the special ICT security project team (Start by forming a provisional ICT security task force)
(iv) Quick scan of the ICT related risks and their consequences to the organisation (Risk exposure due to ICT)
(v) Getting management's attention and sponsorship (The management as a whole needs to buy into the idea as well)
(vi) Getting the current status of ICT security documented (Take stock of the existing situation)
(vii) Conduct awareness sessions (To allow staff to recognise ICT security problems and respond accordingly)
(viii) Carry out Risk assessment/analysis
(ix) Work out the Mitigation plan (Short term plan for issues that need immediate attention and long term plan)
(x) Develop countermeasures

Step 1: Getting top management's sponsorship (the CEO buying into the idea first)

ICT security appeared to be a new concept to most CEOs in the organisations studied. As confirmed by numerous researches, management sponsorship is important in any effort to improve security in organisations [8]. However, getting an appointment to meet the CEO and talk about ICT security was not easy. In this case, we were directed to see either the IT director or chief security officer or accept a long waiting appointment to see CEO. Eventually, on succeeding, the appointment lasted for about 10 to 15 minutes in which we introduced our agenda on what ICT related risks are and the challenges in managing them. Further, the consequences of not managing such risks to the shareholder value were also discussed emphasising that today's (information age) CEOs will be responsible to their board on the state of ICT security in their organisations. The discussion was based on risk exposures such as business interruption, which can propagate through to the balance sheet with great financial implications and cause embarrassing media coverage, loss of confidence to customers, staff and hence loss of credibility.

Step 2: Getting technical management sponsorship (the technical department is the custodian of ICT in the organisation)

It was relatively hard to talk about ICT related issues in the organisation without the permission of its IT department. From most of those who were asked for an appointment, the reaction was "Have you consulted the IT department?" On the other hand, the technical staff are aware of the ICT security problems, though mostly as a technical concern and not as a business concern. In order to get their support, we had to describe the security problem more holistically, i.e. including both technical and

non-technical issues and reasons why we should include and talk to other departments as well. Our observation indicated that the difference in perception between the management and the technical department made it difficult for the technical department to address the problem adequately [1]. Getting technical staff to understand the non-technical components of the problem and how to communicate the problem to the management as risk exposures which needed management attention was yet another important step to take.

Step 3: Address the ICT Security problem as a special project (Forming a provisional ICT security taskforce)

The important question at this stage was how or where do we start? It was at this point that we formed the special ICT security project team. The composition of this team included three technical staff (software, network and hardware), one legal officer, one human resource officer, one internal auditor, one security (physical/traditional) officer, and one from operational departments (where core services of the organisation are processed). Also one more member of staff from the insurance department was in the team purposely for risk management as there was no other department than insurance that was handling/managing risks in the organisation. The main question we faced here was why then only staff from these departments and not others? Our response was based on the facts below:

Technical: Partly the ICT security problem is a technical issue which could be as a result of software, hardware or network problems.

Auditors: Traditionally, auditors are used to auditing the financial transactions or operational processes and compliance to laws and regulations, policies, standards and procedures. Given the nature of their work they can also see the risk exposure of an organisation as part of the big picture. Auditing in ICT is usually considered operational. The prime focus for ICT audit is security—evaluating whether the confidentiality, integrity and availability of data are ensured through the implementation of various controls. It also involves evaluating the realisation of benefits to the business from investment in IT.

Legal: As the dependence on ICT in an organisation grows, legal issues, in particular computer/cyber crime, are becoming an indispensable part of ICT risk management. Involvement of a legal officer in the team facilitates the need to address the ICT security problems from a legal perspective.

Physical Security: Most security departments, particularly in the studied organisations, still value physical assets. So the strategies end up taking more care of tangible assets than intangible ones. The involvement of security staff helps the re-engineering of physical security.

Operations: Operations is where the core services of the organisation are taking place and so is the main source of risk exposure which could prevent the organisation from achieving its mission. In our work we considered having a senior member of staff from the operations department who is fully knowledgeable of operation transactions. His participation in the team would assist in the risk assessment exercise.

Insurance/Risk manager: ICT security management is basically risk management focusing on ICT—mainly how to insure valuable information assets [10].

Step 4: Quick scan of the ICT related risks and their consequences to the organisation (Risk exposure due to ICT)

Before meeting the management as a whole, we needed some kind of justification and this was obtained by first working out some facts on likely consequences of ICT related risks to the organisation. We achieved this by carrying out a quick scan of such risks with the help of the ICT security team. This exercise involved capturing information on how core services are linked to the use of ICT. Face-to-face interviews with the CEO, chief financial officer (CFO), IT managers and the heads of the departments involved in the provision of the core services were conducted. This step was accomplished by using EMitL tool. The tool helped to interpret the consequences of losses in the corporate value based on financial indicators, to technical terminology. This interpretation was based on three groups of damage exposures due to ICT risks, namely liability claims, direct loss of property and business or service interruption [1,2].

Step 5: Getting Management's attention and sponsorship (The management as a whole buy into the idea as well)

The management had to be convinced and understand that their organisation was vulnerable to ICT related risks. Furthermore, we had to educate them on the magnitude of the security problem, and insist that ICT security was more than a technological issue. This means it has something to do with the kind of administration, policies and procedures that were in place; the kind of legal and contractual obligations the organisation had, particularly in delivering services, and also the ethics and culture of the individual staff. This was achieved by presenting to the management the worked out status of their ICT security from step 4 and by discussing their role in managing the identified problems with respect to their positions in the organisation.

Step 6: Getting the current status of ICT security documented (Take stock of the existing situation)

Our next step involved taking stock of what is existing in terms of systems: hardware, software, platforms, networks, applications, users and information assets; Environment: (location and services)—security threats, and countermeasures as well as policies and procedures that are currently in place. This information helped to identify the current status and also highlighted areas that may need immediate attention. In addition, we later, during the awareness sessions, used this information to help staff understand and appreciate the type of problem they have.

Step 7: Conduct awareness sessions among users (with some feedback from steps 1-6)

Our approach was top down, starting with the management, and the topic was "Managing Technology risks, the role of the management, including legal issues in a computerised environment". Along with the presentation notes, we attached the timetable of other training sessions for their departments/staff as well. This helped to get the message across to other staff through their bosses who made sure that their staff attended their respective sessions. More than 90% of the targeted staff during the awareness sessions attended in person. We made some observations during the

sessions, for example, if you look at the staff as they were getting into the awareness session room, you could read their faces indicating something like "this session is not for me". However, after some time into the session the situation changed, and you could observe that, staff were getting concerned on the discussed issues. ICT Security awareness efforts were designed to allow staff from various departments to recognise ICT security concerns and respond accordingly as detailed in [9]. Apart from the general awareness session, we also conducted special sessions with individual departments, namely legal, accounts, human resources, internal auditing, physical security and technical. These were meant to address relevant departmental-specific issues in more detail.

Step 8: Carry out Risk assessment and analysis

Using the security team, we started to conduct risk assessment and analysis starting with the operations department followed by the IT department, physical security and later other departments. Information obtained from this step was vital for the discussion we held later with individual managers, e.g. when discussing with CFO on how to financially hedge the identified risks. The obtained information was also used to estimate the security awareness and in proposing countermeasures based on the output of the EMitL tool (the output of step 4) [1].

Step 9: Work out the Mitigation plan (Short term plan for issues that need immediate attention and long term mitigation plan)

This is the step that came in with pressure from the management. Having realised how risky it was to go without proper ICT security management in place, the management was now in the forefront, suggesting to the security team that they should come up with the mitigation plan. From the risk assessment and analysis, step 8, we found that there were issues that needed immediate attention. For example, the issues of licences, patching management, training, and improvement of the infrastructure. Although there was no budget for these, the management saw the reason to re-allocate their budget immediately. A long term plan was then worked out which included among other things disaster recovery and business continuity plans, the development of countermeasures including policies and procedures on ICT security.

Step 10: Developing the countermeasures

The main question here was what set of countermeasures would provide the best protection against the identified risks and the state of ICT security in the organisation. By taking into consideration the suggestion made from the EMitL tool (what should have been in place), ITIL (why), ISO 17799 (what), COBIT (how) and finally the environment in which the organisation is operating, we started deriving the relevant countermeasures to be implemented in order to address the identified ICT risk exposure [4, 5, 6].

3 Discussion and Conclusion

Perception and interpretation of the word ICT security often leads to the misunderstanding of the actual ICT security problem and causes inconsistency in addressing it. To the management it may sound better if we could use Managing technology risks instead of Managing ICT security as detailed in [10]. The ten steps describe above were used to bring a common view to the problem of ICT security among the management and technical staff. Reviewing the steps as described here, one can easily see that they fit well with issues discussed under aspects such as Organisational information security governance and the like such as those presented in [7, 8].

Our objective to bridge the gap between the management and the technical department was achieved through the ten steps. These included, CEO buying into the idea first, recognising that technical department is the custodian of ICT in the organisation, starting it as a special project, showing where the risks and their consequences are, getting the entire management attention, taking stock of the existing situation, conducting awareness sessions to address the ICT security problem with respect to the organisation's specific environment, carrying out detailed risk assessment and working out a short term plan for issues that needed immediate attention and long term plan, and finally developing countermeasures for the identified problems. The study showed that the success of an ICT security management process begins with the management realising the importance of ICT security management.

References

1. Bakari, J. K., Magnusson, C., Tarimo, C. and Yngström, L.: Ensuring ICT Risks Using EMitL Tool: An Empirical Study, IFIP, Springer, USA. (2005) 157-173.
2. Bakari, J.K.: Towards A Holistic Approach for Managing ICT Security in Developing Countries: A Case Study Of Tanzania", Ph.L thesis, SU-KTH, Stockholm. (2005).
3. Magnusson, C. Hedging Shareholders Value in an IT dependent Business Society, THE FRAMEWORK BRITS, Ph.D Thesis, SU-KTH, Stockholm, (1999).
4. ITIL, (April, 2005); http://www.itil.org.uk/.
5. COBIT, (20th October, 2005); http://www.isaca.org/cobit/.
6. ISO 17799 Standards.
7. Solms, B. V. Information Security governance: COBIT or ISO 17799 or both? Computer & Security Vol 24 (2005) 99-104.
8. Solms, B. V. and Solms, R. V. The 10 deadly sins of information security management, Computers & Security, Vol.23 No 5 ISSN 0167 –4048, (2004) 371-376.
9. Wilson, M. & Hash, J. 'Building an Information Technology Security Awareness and Training Program' NIST Special publication 800-50, USA, (2003).
10. Blakley, B. McDermott, E. & Geer, D.: Information Security is Information Risk Management, ACM Press New York, NY, USA, (2001).