CAN WE TUNE INFORMATION SECURITY MANAGEMENT INTO MEETING CORPORATE GOVERNANCE NEEDS? (INVITED PAPER)

Louise Yngström
Department of Computer and Systems Sciences, Stockholm University/KTH

Abstract: This paper intends to stimulate discussion, research and new points-of-action for IS/IT security management from the background of corporate governance, contemporary debates of how to express observable consequences of IT and IT security, and of didactic issues. It is concluded that empirical research within IT security management is rare as compared to theoretical approaches but needed in order to have IS/IT security management on par with general management.

Key words: IS/IT Security Management, Corporate Governance, Holistic Approach.

1. BACKGROUND

Having been in the IS/IT security area for two decades following closely the development of thoughts, theories and practices from being seen and handled as a purely technical area into being seen and handled at least multidisciplinary the quest from von Solms&von Solms (2005) to start calling 'Information Security' 'Business Security' intensely focused my attention. The background to their quest is that in Corporate Governance Executive Management and Boards have started realizing their underlined responsibilities to asses how IT is providing added values and increased efficiency of IT to the organization. Governance does this by sets of policies and internal controls, of which information security policies and controls will be subsets (A Call to Action 2000). Also in the background are demands for compliances of controls to legal frameworks such as the Sarbanes-Oxley(SoX) Act and Basel II.

Would re-naming the core concept of the area make a difference? And in that case, does changing "information" to "business" make enough of a difference? How come management does not see that a lot of what is asked for is already there – or at least, that competences, insights and tools exist to be used given that IS security professionals are offered the opportunity to provide their services to the organizations? Have our proposals for communications and requests for funding through presenting elaborate risk analyses not been heard or understood? Have international efforts to develop standards and establish procedures of best practices passed unnoticed? Have current research on the need for users' awareness and abilities been neglected? The list of questions can be made much more exhaustive leaving most of us with a feeling of wading in a mesh of complex dependabilities between concepts where each piece of knowledge has infinite possible relations with other pieces of knowledge.

At the same time there is a feeling of being unjustifiably mistreated and misjudged as an area of proficiency; R&D including practices in IS/IT security has underlined, problematized, suggested, developed, used and evaluated working solutions for decades now. Schultz(2004) comments on these efforts in relation to the US SoX Act 2002; as the audit community studied the provisions of the Act it become clear to them that adequate controls sought for rest on well known and already existing IS/IT security control methodologies. His hopes are that even if it takes time for senior managers to understand the implications – that even financial /information/ systems have to show evidences of compliance originating from IS/IT security controls – their understanding will boost the practice of IS/IT security.

It is obvious that our understanding and conceptualization of the area 'Information Security Management' as compared to 'Corporate Governance' does not come through as equal/useful/sufficient/comparable/complementary to general management; changing 'information' to 'business' would hypothetically underline the similarities and usefulness.

This presentation intends to stimulate discussion in looking for aspects on IS/IT security management as viewed from inside and outside hoping to uncover points of action and research questions to further strengthen the IS/IT security management in relation to corporate management.

2. SOME OBSERVATIONS IN RELATION TO IS/IT SECURITY MANAGEMENT

In 2003 the Harvard Business Review published an article called "IT Doesn't Matter" by Nicholas Carr (2003) which excited a large part of the IT business community. Carr's main argument was that IT no longer gives competitive advantages to business – that is selectively adds value to business - but should be looked upon as any infrastructure similar to railroads or telegraphs. After all, everybody is using Internet – it does not add any values to the business just by the mere use. So IT is not a strategic resource but a part of the tactical cost structure of the business - and as such in need of being managed defensively watching costs and avoiding risks. Thus IT is seen primarily as vulnerabilities and only secondarily as opportunities. In classifying IT as an infrastructure the following traits were listed: governed by standards, not customized, scalable and replicable, one standardized delivery channel, and ubiquitous.

The counterarguments from the IT industry were active; even if IT partly can be viewed as an infrastructure that which matters is what you do with technology as such or the inherent information itself. IT has indirect effects such as creating new possibilities and options, new business models, use new information or old information in new ways, and use stable homogenized and standardized functionalities as platforms for new business (Sarup 2005). An example discussed was Amazon.com; using a common infrastructure as a stable platform created a new business model. However, since the concept as such could be copied the business model could not stay unique for very long thus successively degrading to tactical level. While tactics means efficiently and effectively controlling and protecting what you have, strategic means creating added value in such a way that the full procedure cannot easily be seen through from the outside. For Amazon.com, most of the value adding procedures built on being an early adapter of existing technology, while other examples build on value chains, where the full procedure cannot be mimicked. Dell was mentioned as such an example, where Dell through selling directly to customers got competitive advantaged through distributing goods more efficiently and obtaining information for managing inventories more efficiently, all in all leading to lower total costs as compared to competitors.

Value chains are structures and tools defining how to integrate and evaluate activities enabling a business to create unique over time lasting and not easily copied values. Typically a value chain model includes generic activities; in M Porter's model (Porter 1996) the generic activities are inbound logistics, operations, outbound logistics, marketing and service. The

model helps organizing analyses and evaluations of values of strategic choices/activities for competitive advantages. There are unlimited choices possible – to use it efficiently an understanding of the economic levers existing within one's business area and how the strategy intends to exploit them is needed, together with knowledge about temporal interdependencies between value chain processes. There are examples in the literature of how value chains add value to IT (see for instance Burg and Singleton, 2005), but the same procedures for IS/IT security have hardly emerged.

Contrary, the IS/IT security area has a history of needs emerging – or rather mushrooming - from the technical area rather than from business. There were urgent operational needs along with developing control functionalities which later were divided between machines (technical) and humans (procedural). To balance results from using technical and procedural control structures the area was gradually understood as interdisciplinary – to meet demands of not only technical criteria but also human, organizational, and legal. How to define, construct, implement and evaluate these aspects of IS/IT security have been and is researched since long; in essence generally accepting that IS/IT security has to be viewed and handled holistically and inter- or multidisciplinary. Early on the need for management's support and interactions was identified using risk analysis as communication media to demonstrate in monetary units advantages reachable through efficient IS/IT security. Efficient and effective use of IS/IT security methodologies and functionalities were seen as facilitating competitive advantages apart from securing the assets of the organization. Especially all e-models in distributed environments were and are discussed from point of view as adding value to organizations and nations from the fact that without security functionality, e-applications hardly work. However, the value chain concept is not a generally used term in presenting claims.

Most often the communication device with general management is the risk analysis, intending to give a holistic picture of added values and cost/benefits to the organization. Repeatably costs are charged to IS/IT security while benefits and added values are accredited elsewhere in the organization. This seems to give general management the idea that security is only costs – thus of tactical rather than of strategic value to the company. Few studies underline these facts by figures and most models used do not provide such elaborations. I believe this has to do with that IS/IT security professionals hesitate to measure anything inexactly and risk estimates are in that aspect in the "grey zoon". However, two examples using system theory as scientific base come to my mind: one from Gothenburg City (Eriksson 1995, commented in Yngström 1996 p66-67) where costs for (new) security functionality made it possible to use e-invoices with the benefits of lowering

costs of handling invoices by 20%. Expected outcomes were tactical as well as strategic which could not be seen solely in the ordinary charts. The second is a much more elaborate model, Business Requirements of Information Technology Security, BRITS, by Magnusson (1999) facilitating to balance IS/IT risks within and together with the ordinary corporate risk environment expressed by procedures and formulas familiar to corporate management. Contemporary research goes towards adapting the ROI (Return On Investment) for IS/IT security sector into ROSI, (Return On Security Investment). Similar discussions occur within the auditing community; Burg& Singelton(2005) claim neither ROI and TCO(Total Cost of Ownership) based methodologies nor the qualitative IE (Information Economics) methodologies avoid being subjective while stating the monetary value benefits. They suggest developing a balanced scorecard to map the intangible benefits identified in the value chain to observable consequences.

No doubt awareness and knowledge of consequences of IS/IT sec functionalities is difficult to grasp for non specialists, including corporate management. Research about usability aspects of security functionality is focused, for good reasons, on end-users. However, we stumbled over managers' understanding of business usefulness of a PGP resembling application while researching how non-linear teaching methods may facilitate users with learning and understanding of using an electronic ID-card as compared to contemporary linear teaching methods (Näckros 2005). While developing and testing the non-linear approach – a computer game – on a group of managers we had some very interesting informal feedback in their comments such as "now I know what's so good about the idea", "aha, this is how it works", "now I understand why everybody is talking about it". Unfortunately we could not go on experimenting with this group due to lack of time on their behalf, but general findings indicated that non-linear teaching methods within IS/IT security facilitate users to operate security functionalities safely – that is to understand the consequences of their actions - no matter which learning preferences or prior practical experiences they have. This exemplifies in one way the essence of holism, where subjective understanding of complex phenomena through some – often unknown – processes form a base for handling /defined parts of/ reality in such a way that the total outcome is acceptable as preferred/assessed by others. Whatever the definition of holism, it seems generally accepted that <complex phenomena> "have to be treated holistically".

During the curricula development of academic programs in information security in the 1990's the holistic aspect was much discussed. It was acknowledged that there were computer professionals lacking knowledge in

security, and auditors and security managers lacking knowledge in computing. As an amalgamation of European universities' efforts to suggest a postgraduate academic program three tracks building on four mandatory courses were suggested; one track each for

- Information Systems Security,
- Distributed Systems Security and
- Dependable Systems.

Mandatory courses were

- Principles of information security, dependability and safety,
- Introduction to cryptography,
- Information systems security management and
- Computer systems security.

The course description for Information systems security management was:

"Management of information systems, models, frameworks and trends. The security manager within the organization: Roles and responsibilities. Implementing principles of management. Managing security policies. Fit of business with security strategy. Methodologies for the management of risks and for contingency management. Software for risk analysis reviews. Auditing for IS security. Management of physical security. Global model for information security management: Proactive and reactive approaches, predictable and unpredictable threats and opportunities. Disaster recovery. Business continuity planning. Awareness and incident reporting. Personnel management: selection, training, assessment. Developing and reviewing a security programme/policy of an organsation." (Katsikas and Gritzalis 1995, p17)

It was also identified that most information security professionals in those days were 'ex' something. In evaluations of the practical and academic backgrounds of students in the first Swedish academic bachelor program in Security Informatics 1985-88 7% had previous law studies, 47% previous studies in computer science and 33% previous studies in economics and management. In the same group previous experiences were from police and armed forces 16%, security 47%, IT industry 60% and various working experiences 11%. Amongst positions held by the same group (n=71 where 57 had distinct positions prior to the program) four years after the academic program were Corporate security and IT security manager and general management (14), IT security consultant and security coordinator (18), Project manager and programmer/system analyst (16), IT auditor (5), and teacher (4). (Yngström L 1996, table 4.1A p 105 and table 4-7 p 111). In the same survey it was evident that increasingly the academic backgrounds

include law, economics and management, and computer science with a bias to computer science. And the percentage of students' practical backgrounds is decreasing as the average age of university students in the program is lowered; today most university students take the academic program prior to their career in IS/IT security.

Teemupekka Virtanen (2003) makes an interesting remark in a similar survey of Finnish academic and vocational IS/IT security education 1990-94. After various educational programs in IS/IT security people stay on in the same or a higher position within IS/IT security. The same phenomenon was also seen but not underlined in the Swedish study (Yngström 1996): of the 58 persons completing the Security Informatics program 1985-87 four years later 42 were professionally employed within the security/risk area in trade and industry, 22 returned to their former companies and positions while 20 changed positions leading to higher status and, to many of them, greatly raised salaries; however they all (but one) stayed in the IS/IT security area. Virtanen also found explicitly that the IS/IT security managers in 1994 expressed different educational needs than in 2002; even if they stayed in their old positions after the education, they had no longer need for deep specialization knowledge but rather for knowledge on business processes and managerial activities. IS/IT security management has become a managerial position - and a position difficult to be promoted from.

3. REFLECTIONS

In the IS/IT security area generally R&D has been more targeted towards theoretical than empirical issues (Bjorck 2005). This has many reasons, for instance: within the security area as such information about fabrics and details of the trade are usually viewed as sensitive, to collect and analyze such research material of relevance takes long time and large efforts, analyses need to be context and time dependant resulting in difficulties to generalize findings, etc. But it needs to be done, as Ross Anderson already 1993 underlined in "Why Cryptosystems Fail" (Anderson 1993), empirical research will facilitate the area with continuous learning mechanisms useful for adjusting or changing. For IS/IT security management obviously new knowledge and skills are needed to perform as expected – which are they and how can they be facilitated, learnt, planned? Currently two issues seem urgent, if not new: communicate the relevance of IS/IT security to business needs and formulate observable consequences useful to corporate management. One way to express this is to cite one of the Four Grand Research Challenges for IT security in the next decade as expressed by

(Grand Challenges 2003) "Develop quantitative information-systems risk management to be at least as good as quantitative financial risk management within the next decade." I hesitate to rename 'Information Security' 'Business Security', but maybe it will be part of the communication needed. Let's research that issue.

References

1. A Call to Action for Corporate Governance, IIA, AICPA, ISACA, NACD, <www.theiia.org/eSAC/pdf/BLG0331.pdf (March 2000)
2. Anderson, Ross: Why Cryptosystems Fail, 1st Conf.-Computer and Comm. Security '93 – 11/93 – VA, USA (1993)
3. Basel II at www.bis.org/publ/bcbsca.html
4. Bjorck, Frdrik J. Discovering Information Security Management, upcoming PhD thesis, Department of Computer and Systems Sciences, Stockholm University (2005)
5. Burg, William D., Singleton, Tommie W: Assessing the Value of IT: Understanding and measuring the link between IT and strategy. Information Systems Control Journal 3 (2005) 40-44
6. Carr, Nicholas G.: IT Doesn't Matter. Harvard Business Review. (May 2003)
7. Eriksson, Kjell: Electronic Highways in Sweden – Experiences from public sector. Safe EDI in the city of Gothenburg. In Yngström, L., (ed): Addendum to Proceedings of the IFIP TC11 eleventh international conference on information security, IFIP/Sec'95, South Africa, 9-12 May (1995) 6-10
8. Grand Challenges 2003 at http://www.cra.org/Activities/grand.challenges/security/home.html
9. Katsikas, S.,Gritzalis D. (eds): A Proposal for a postgraduate curriculum in Information Security, Dependability and Safety, European Commission, Erasmus ICP-94(&95)-G-4016/11, Report IS-CD-4a, Athens, (September 1995)
10. Magnusson, Christer: Hedging Shareholder Value in an IT dependent Business Society – the Framework BRITS. PhD thesis, Department of Computer and Systems Sciences, Stockholm University report No 99-015 (1999)
11. Näckros, Kjell: Visualising Security through Computer Games. Investigating Game-Based Instruction in ICT Security: an Experimental Approach. PhD thesis, Department of Computer and Systems Sciences, Stockholm University report No 05-014 (2005)
12. Porter, M.E., What is strategy? Harvard Business Review. 74 (1996) 61-78
13. Sarbanes-Oxley Act at www.sec.gov/spotlight/sarbanes-oxley.htm
14. Sarup Deepak. IT Does Not Matter ---Or, Does IT? Has IT moved from a strategic to a purely tactical function? Information Systems Control Journal 3 (2005) 28 – 31
15. Schultz, E. Eugene: Sabanes-Oxley – a huge boon to information security in the US, Computers & Security. 23 (2004) 353-354
16. Virtanen, Teemupekka: Changes in the profile of security managers. In Irvine, Cynthia, Armstrong, Helen (eds): Security Education and Critical Infrastructure, IFIP TC11/WG11.8 Third Annual World Conference on Information Security Education (WISE3), June 26-28, Monterey, California, USA, Kluwer Academic Publ, (2003) 41 - 49

17. Von Solms, Basie, von Solms, Rossow: From information security to ….business security? Computers & Security 24 (2005) 271 – 273
18. Yngström L A Systemic-Holistic Approach to Academic Programmes in IT Security, PhD thesis, Department of Computer and Systems Sciences, Stockholm University report 96-021(1996)