CHAPTER 6 - CONCLUSION AND RECOMMENDATIONS

This chapter concludes the discussion in the pervious chapters. It further recommends some facts for the business organisations in dealing with the Information Security needs which are developed based on the research outcomes. Some useful recommendations to the future researches are also included in this chapter.

6.1 Conclusion

Process based businesses demands massive use of information and information technologies. This trend will even cultivate in the time to come. Computers are getting faster, smaller, cheaper, and easier to use day by day. Developments of device independent computing – ubiquitous computing – and the growing demand of accessing information where and when it is needed has made businesses dependent in information systems at a major. This is well supported by the growing cyber space; every year tripling in size and would definitely obsolete the business models we practise today very soon.

With the development of information technology and the dynamic changes in business environment achieving perfect Information Security is a nightmare. Even if a business tries to achieve this, it will end up with an immense scope of work which is practically hard and difficult to justify in financial terms. In contrast person who tries to misuse information only has to master one particular area and identify a weakness in the system to start attacking. Therefore avoiding the week areas of a system and maintaining the security measures implemented is a vital move as a start. To understand and develop such weaknesses pertaining to Information Security a solid business integrated balanced approach will help. Integration should consider a proper balance in the following areas as detailed in the discussion in chapter 05.

- Functional Balance
- Managerial Balance
- Technical Balance

- Investment balance

The integration balance in each of above area is to be decided as a collective approach by the business. Information security managers and the business managers have to look at the concept as a holistic business solution.

Information Security is not only to do with IT. It is a business risk as analogues to all the other kinds of risks, which has to be treated in the same way. Identified business risk should be the base to decide the extent to which Information Security measures are needed. This is to be followed as collective effort in the organisation in every functional area as applicable. Model to develop a new Information Security framework is discussed in the chapter 5. Review process includes considerations and analysis of the legal framework, international standards, risk and impact and other policies of the business organisation. Purpose of Information Security strategies is to support business goals of the organisation. Framework for successful implementation of Information Security strategy is discussed in the chapter 5 However protecting information systems from hackers, crackers, attackers, viruses, spyware, spam and other threats that exist because of connectivity is a complex work. It involves individual users, organisational IT departments and policy makers. By putting good security practises into use, a business not only will protect its own systems; but also will contribute to the overall security of the global networks.

Awareness and the gaps in the two different knowledge areas is a major barrier for integration as identified. To fill this gap and to make informed decisions Information Security and Business Managers are to work hand in hand and educate each other. Building organisation wide awareness about Information Security and expected behaviour with regard to the same is a high priority. This should be a constant repeated approach followed by the reviews for the Information Security policy and framework for the business organisation.

Information Security is a fuzzy concept as discussed in literature survey and hence need to be continuously monitored and reviewed for betterment. This is non-avoidable with the development and 'development rate' of information systems. The time and resources need to keep the systems up to date is huge. Hence the organisations must consider the development of Information Security as an integrated balanced approach. All the areas concerned not demanding resources equality. The proper balance of the resources is to be determined by the business and Information Security managers as a combined effort. Top management should facilitate purposeful interactions and discussions between these two parties to develop a holistic framework for Information Security needs.

6.2 Recommendations

Business organisations should deploy organisation wide Information Security measures to secure the extensive information transaction needs of today and tomorrow. Integrated approach with business management is required to make sure the proper balance and stability of Information Security dispatch is achieved. Information Security risk and impact analysis should be the basis for Information Security deployments. Organisation should start building awareness of all the categories of employees and educating them about the expected behaviour with regard to Information Security measures taken. It will make sure the employees will do the right things when facing an incident. Awareness will keep the employees alert with regard to Information Security. Once the organisation wide commitment for Information Security is established, it has to be maintained; business managers should resource the new way of operation.

An organisation can start quantifying the Information Security braches and prepare the consequences in terms of financial figures. That will give accurate data to take decisions in future with regard to Information Security. This will help to non-technical managers to figure out the matter pertaining, specially the business requirements from Information Security. That will lay the foundation for information security requirement awareness and acceptance.

Business managers and Information systems and security managers have to devote their time to study about each other to make informed decisions in Information Security. Organisations have to make arrangements to share experience and knowledge with regard to business and Information Security areas to each other. International Standard Organisation (ISO) has developed several Information Security and related standards which is discussed in the literature survey. The standards are continuously developed for about a decade; the current versions have comprehensive details which will be useful. Having heard about the legal developments will do nothing much, the managers have to read and understand the Information Security related legal documents. For this matter combined effort by Business and Information Security managers is recommended.

Information Security manager or any other interested person for that matter can refer the Information Security breaches surveys done by various organisations. In the Internet Search of Chapter 3 those details are discussed. Findings and the recommendations of these surveys will help an organisation to understand about the global trends in Information Security and subsequently to develop the Information Security measures.

6.3 Suggestions for Future researches

Combined knowledge of Information Security and business management is rare in business organisations. The thesis tried to build awareness among the managers with regard to the same. If a business organisation decides to make use of the outcomes of the thesis, facts presented can be tested as a case study. The proposed models can be further studied and reviewed in practical settings.

With the technical developments and the organisational environmental changes the threats for information systems can not be mistreated. Hence developing the information systems to be secured in the presence of attacks and vulnerabilities is also a good researched area.

References

[1] Juhani Anttila, Jorma Kajava, Rauno Varonen, Balanced Integration of Information Security into Business Management, Proceedings of 30th EUROMICRO Conference, Rennes – France, 1- 3 September 2004

[2] Jayalath L Jeewani, “Organizational IT Security for Sri Lanka Organizations,” MBA dissertation, University Moratuwa, Moratuwa, Sri Lanka, 2004

[3] United Kingdom, Department of Trade and Industry, Information Security Breaches Survey 2006, 2006. [Online], Available: http://www.dti.gov.uk [Accessed: July 19, 2006

[4] Jacquelin Bisson and René Saint-Germain, The BS 7799 / ISO 17799 Standard For a better approach to Information Security: White Papre, Callio Technologies, 2004. [Online], Available: http://www.callio.com [Accessed: July 14, 2006]

[5] Eric Jackson, “Cost of Losing Information: A Framework for Information Management Planning,” xosoft.com, January 2005. [Online]. Available: http://www.xosoft.com/whitepapers/ [Accessed Sep 03, 2006]

[6] David Simchi-Levi, Philip Kaminsky, and Edith Simchi-Levi, Designing and Managing the Supply Chain - Concepts, Strategies and Case studies: Second edition, Tata McGraw-Hill, New Delhi, 2004

[7] “Information Sensitivity,” in the WikiPedia [Online], Available: http://en.wikipedia.org/wiki/ Information Sensitivity [Accessed: Oct 03, 2006]

[8] Shantha Fernando, “IT security”, MBA-IT Lecture notes, University of Moratuwa, Moratuwa, Sri Lanka, 2005.

[9] Denver De Zylva, Combating ICT Crime & Terrorism – Are we ready?, Proceedings of the 23rd National IT Conference, Colombo, Sri Lanka, 2004

[10] Microsoft Corporation, Information Security workers hand book, 2004

[11] Joy Peppard, Rob Lambert and Chris Edwards, "Whose Job is it anyway?: Organizational Information Competencies for Value Creation," Information Systems Journal, p.291-322, 2000. [Online] Available: http://www.blackwellpublishing.com [Accessed July 18, 2006]

[12] National Academy of Sciences, Cybersecurity Today and Tomorrow: Pay Now or Pay Later, National Research Council, 2002. [Online] Available: http://www.nap.edu/catalog/10274.html [Accessed Sep 03, 2006]

[13] CIO Magazine, Insiders Pose the Biggest Threat to Data Security, CIO Magazine, October 15, 2005. {Online] Available: http://www.cio.com/sponsors/100105_vontu.pdf [Accessed Sep 03, 2006]

[14] Kanishka Sugathadasa and Lionel Jayasinghe, *The Human Element of Security – Circumventing Technological Protection - Survey of the Literature, 23rd National IT Conference, Colombo, Sri Lanka*

[15] Juhani Anttila, "Business Management and Quality Aspect for Information Security Management," Venture Knowledgist Quality Integration, 2004, Available [Online] Available: http://www.qualityintegration.biz/ [Accessed Aug 15, 2006]

[16] Iivari J & Kerola P, *A Sociocybernetic Framework for the Feature Analysis of Information Systems Design Methodologies. In: Olle TW, Sol HG & Tully CJ (eds) Information Systems Design Methodologies: A Feature Analysis*, Elsevier Science Publishers, North-Holland, Amsterdam, 87-139, [21-0.1]83

[17] Petri Puhakainen, "A design theory for Information Security awareness," Ph.D. dissertation, University Ouluensis, Oulu, Finland, 2006

[18] Sans Institute, [Online] Available: http://www.sans.org/top20 [Accessed: Sep 28, 2006]

[19] Matthew K. Burnburg, "Proposed framework for business Information Security based on the concept of defense-in-depth," Masters Thesis, University of Illinois at Springfield, Springfield, Illinois, 2003

[20] Dr. Rolf Reinema, Malta Lecture, Malta, January 29th/30th 2004, Security Management – Part 4: Standards, Regulations, and Legal Issues, Fraunhofer Institute SIT, Germany, 2004

[21] Hansche S, Designing a Security Awareness Program: Part I, Information system security, Page 15-16, 2001.

[22] International Organization for Standardization, [Online] Available: http:// http://www.iso.org [Accessed: Sep 28, 2006]

[23] British Standards Institute, [Online] Available: http://www.bsi-global.com/index.xalter [Accessed: Sep 28, 2006]

[24] Ted Humphreyson, "IBM State-of-the-art Information Security management systems with ISO/IEC 27001:2005", ISO Management Syustems, 2006. Available [Online] www.iso.org/ims [Accessed Sep 22, 2006]

[25] Howard F. Lipson & David A. Fisher, "Survivability — A New Technical and Business Perspective on Security," 1999 New security Paradigm Workshop, 2000.

[26] Shantha Fernando, Computer Forensics – an Introduction, International Conference on Information Systems Audit, Control and Governance, April 1-2, 2005.

[27] Juhani Anttila, “Managing and assuring Information Security in integration with the business management of a company,” Venture Knowledgist Quality Integration, 1998, Available [Online] Available: http://www.qualityintegration.biz/ [Accessed Aug 15, 2006]

[28] Student of the Australian Computer Society, “Information Technology and business Alignment”, Masters Thesis, Australian Computer Society, Australia, 2001

[29] Curtin T E, ‘IT Alignment: New Ideas for an Old concept’, IBM Advanced Business Institute, [Online] Available: http:// itebg.bus.oregonstate.edu/ProgramFiles/Curtin1.pdf [Accessed Sep 06, 2006]

[30] Philip Kotler, Marketing Management, Eleventh Edition, New Delhi, Prentice-Hall of India Private limited, 2004, pp 666.

[31] United State of America, U.S. Small Business Administration, Curtailing crime-inside and out, U.S. Small Business Administration, 2004.

[32] Eben Otuteye, Framework for E-Business Information Security Management, University of New Brunswick, Fredericton, Canada, 2001.

[33] Joan Hash, Nadya Bartol, Holly Rollins, Will Robinson, John Abeles, and Steve Batdorff, “Integrating IT Security into the Capital Planning and Investment Control Process,” National Institute of Standards and Technology, US Department of Commerce, USA, 2005.

[34] Richard A. Caralli, William R. Wilso, The Challenges of Security Management, Software Engineering Institute, 2004

[35] IT Governance Institute, Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition, 2006. [Online] Available: www.itgi.org [Accessed Sep16, 2006]

[36] Lawrence A. Gordon, Martin P. Loeb, "The economics of Information Security investment," ACM Transactions on Information and System Security (TISSEC) archive Volume 5 , Issue 4, P438 – 457, 2002. [Abstract] [Online] Available http://portal.acm.org [Accessed Oct 05 18, 2006]

[37] Amitava Dutta, Kevin McCrohan, "Management's Role in Information Security in a Cyber Economy," Harvard Business Review, Oct, 01 2002.

[38] Kjell Näckros, "Empowering Users to become Effective Information Security and Privacy Managers in the Digital world through Computer Games: Positioning computer games as means to increase information and communication security awareness," Stockholm University and Royal Institute of Technology, Sweden, 2002

[39] Computer emergency and response team, [Online] Available: http://www.cert.org/stats/ [Accessed Oct 05 18, 2006]

[40] CSI/FBI Computer Crime And Security Survey, 2006, [Online] Available: http://www.gocsi.com [Accessed Oct 05 18, 2006]

[41] Global Information Security Survey 2005, [Online] Available: http:// www.ey.com [Accessed Oct 05 18, 2006]

Appendix