Cohesive Approach to Integrate Goals of Information Security Management Function with Corporate Goals of Enterprise

Ashish Ukidve M.E, CISA(USA)

Abstract **-** The activities of information security management function are most of the times based on imprudent knee-jerk reactions such as remediation of operational vulnerabilities rather than enhancing the corporate strategy. This disengagement between information security operations and strategic corporate objectives results in pressure to control security spending while risks, incidents and losses continue escalating to unsustainable levels. Hence it is necessary to have cohesive approach in the corporate objectives of an enterprise and the activities of information security management function. This can provide an intentional and powerful tool and source for competitive edge, creating support for additional expenditures for this function. This develops a business oriented approach while managing information security in the context of framework such as Control Objectives for Information and related Technology (COBIT). It utilizes integrated systems thinking to clarify complex relationships within the enterprise, and thus to more effectively manage the information security function.

Keywords--Cohesive Approach, Integrated Information Security, Corporate Goals

I. INTRODUCTION

ORGANIZATIONS are spending and hiring information security practitioners on record numbers and legislation and regulations are ever increasing.

Despite this effort, nearly every statistical measure of performance, from the number of incidents and vulnerabilities to the cost and impact of a breach, demonstrates that the problems are getting worse. It has been an interesting observation that more investments in terms of money and technology has not been able to reverse this trend. Further, the extent of enterprise adoption of information security management function and related practices vary widely across countries and industries. There are several factors that may be attributed for this, such as availability of skilled and experienced practitioners, uncertain outcomes of efforts in other organizations and, perhaps the most telling, actual value realized from information security management function. Although the information security management function is more than 20 years old, Generally it has not been given the due recognition it deserves for being able to bridge business and IT strategies effectively.

Ashish Ukidve is working as the Principal with Vidyalankar Polytechnic, Mumbai,India (Mobile No- 91-22-9821075538 Email Id- ashish.ukidve@vpt.edu.in)

There is wide acceptance of the need for strategic IT planning and information security management architecture (COBIT processes PO1and PO2 respectively). The information security profession suffers from several problems that lead to disconnect between the business and the information security program. One of the major reasons is the focus on technology. Many practitioners in the information security field are information technology (IT) engineers and technicians who just "happen to be in the field of Information security" Their training and background is technical, so they overlook the elements that technology depends on organization, people, processes and systems. Efficient and effective information security requires a balance among these elements. This lopsided technical focus can isolate the information security function from the other stakeholders in an organization and can create a gap between information security and the business units. Another reason is that the organizational leaders are concerned with other risks, such as physical security, legal financial and safety, in addition to information and technology. It is observed that both the sides continue to think in silos and fail to understand how all of these risks are interrelated. Under this situation, the investments in such unbalanced security programs cannot deliver the "value", while the organizations continue to demand a greater return on their information security investments.

II. THE INTEGRATED SYSTEMS APPROACH

From the above discussion it is clear that the security functions are short of holistic approach and are ad hoc, reactive and tactically focused. Presented below is a holistic system approach, towards information security management, focused on business, not only technology. This approach blends technology with the strategic direction and needs of the organization. In coming together, they form a holistic and dynamic approach to information security that is both predictive and proactive as it adapts to changes, considers the organizational work culture and delivers value to the business.

This approach requires that the organization is sensitized towards adopting information security in its culture. This sensitization process has following important components:

Risk Analysis -- Information security practitioners must understand the business, its objective, operating and regulative environment, potential threats, risk impacts, operational flexibility. Only then can appropriate control be selected to mitigate risk effectively. Information security controls often are implemented with little or no assessment of

the actual risks and threats to an organization, which results in failure to protect valuable assets or wasteful overprotection.

Concurrency of Corporate objective and information security -- The Information Security program should align with the organization from the boardroom to end users, and information security controls should be practical and provide real measurable risk reduction.

Equilibrium between organization, people, systems, process and technology -- effective risk management requires organizational support competent people, effective systems, standardized processes and the selection of appropriate technology. Each element impacts and supports the other elements, in complex ways, so it is crucial to achieve the balance among these elements.

Convergence of security strategies -- To maximize return on investment, all security functions (Data or Information security, environmental security etc.) should be properly integrated. Nonaligned security functions are wasteful and hinder the identification and mitigation of cross- functional risk.

As can be seen the approach is independent of any particular technology or technical changes overtime and is therefore applicable across wide range of industries, geographies and regulatory and legal systems. Also it should be seen as a long-term exercise that will ultimately aid the enterprise in achieving business goals. In fact, it may help to think of it as a key to organizational maturity. The maturity of the information security program is often related to the maturity of the enterprise, which is linked to the degree to which systemic thinking is used in the organization.

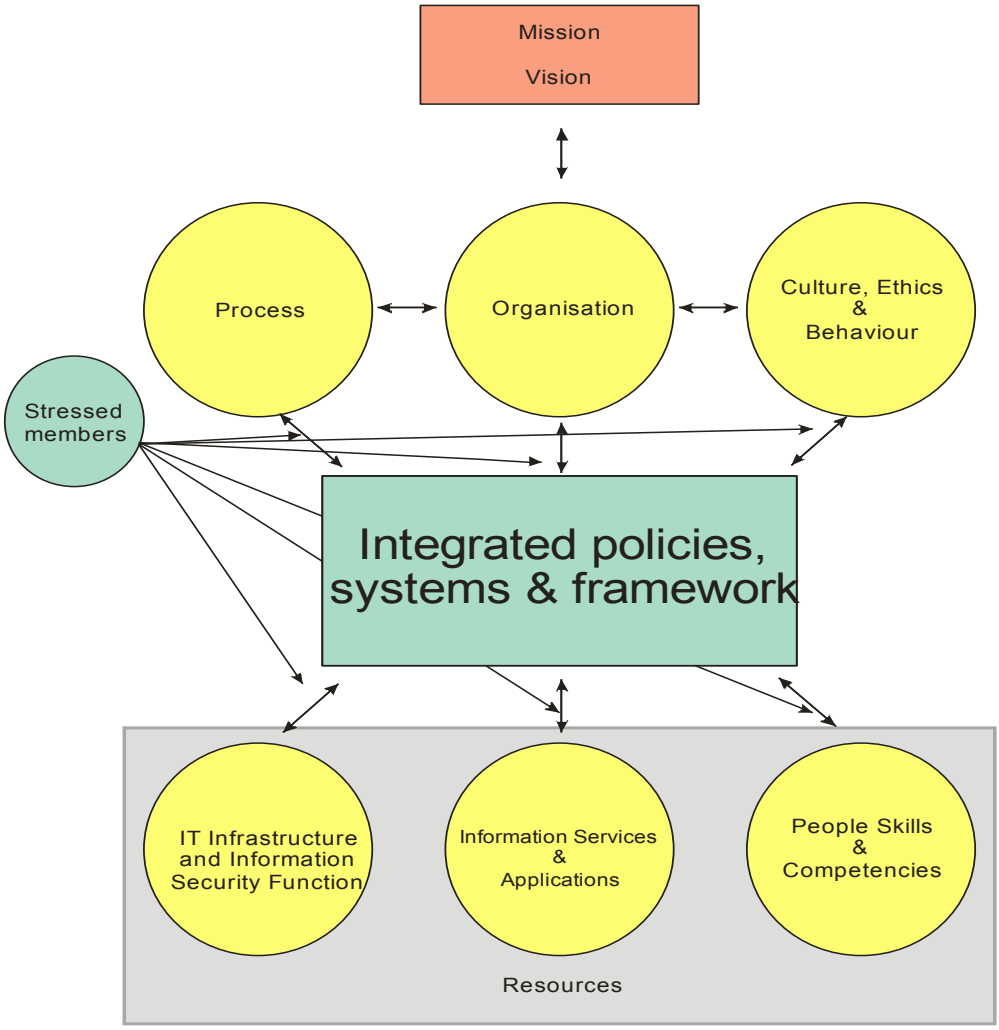

Fig. 1. Framework Depicting Integration of IT Security & Corporate Objectives

The figure (1) depicts this integrated system approach. It includes the traditional elements of a people, systems/process and technology and adds organization- design and strategy.

From an information security practitioner's perspective the interplay and dependency among these entities, the stress-members, create the opportunity to integrate the information security program with the business by focusing on the issues that too often are overlooked. The stress-members are logical linkages between organization, culture, processes, IT-infrastructure & security function management, information services, people skill and communication; connected to integrated policies, systems and framework.

These stress-members interact with each other and the entities in complex dynamic and sometimes competing ways. The role of information security function is not to eliminate the tensions among these stress members but to recognize and understand their interactions to create a more comprehensive information security program by addressing the whole organization. Some of the benefits gained by this approach are;

Recognizing new and unidentified risks and evaluating them cross- functionally.

Linking different information security value chains within the context of the extended enterprise. Facilitating the analysis of risks and control implementation on the whole organization.

Fig 2 shows the 5-stages process flow indicating how the above mentioned integrated framework can put into practice. As can be seen, the integrated framework development stage encompasses Business vision and IT & Info security function. A critical component of this new approach is that the technology element is not restricted to a particular vendor, architecture, protocol or standard and more important, focus is not on the technology, but rather the interaction of the technology with the rest of the organization. This framework, for Information Security enables security professionals to examine security from integrated systems point of view, creating an environment where actual risks can be effectively addressed.

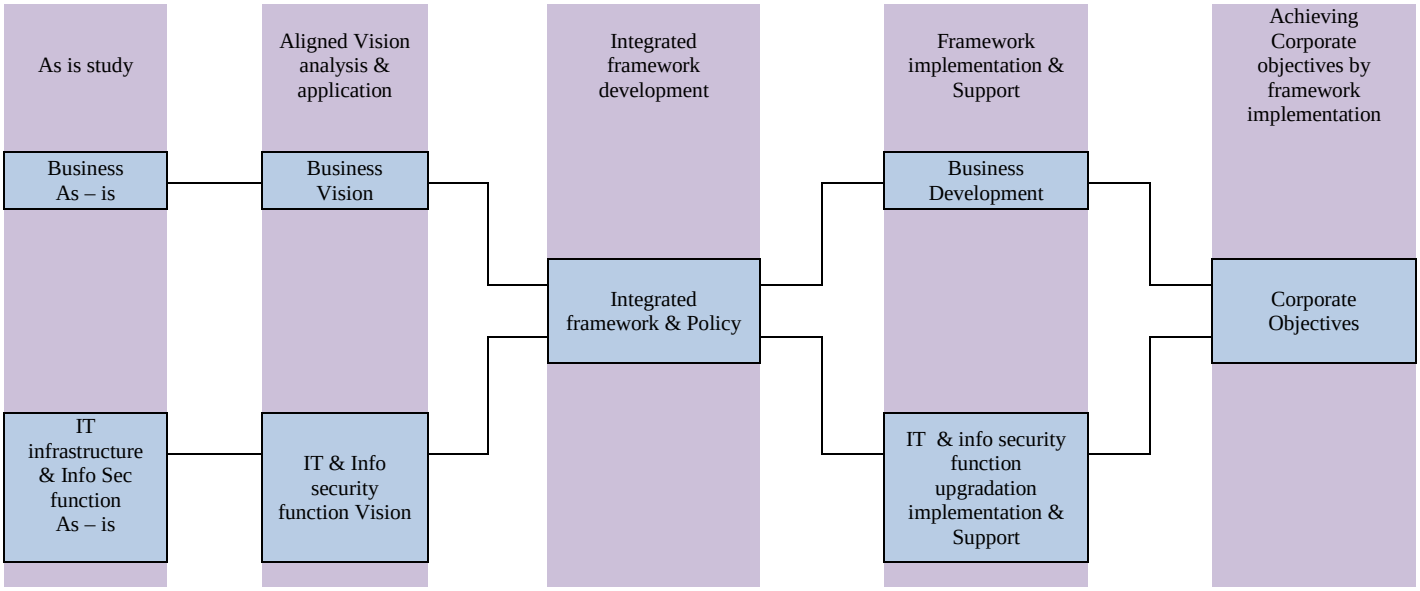

Fig 2. Process Flow for Integrating IT, Info Security and Corporate Objectives

REFERENCES

[1] Deliottte & Touche LLP and Ponemon Institute " Enterprise @ Risk: Insights into the Emerging privacy and Data Protection Function." 2007

[2] Anderson, K.E.; " Convergence: A Holistic Approach to Risk management," Network Security, vol.2007 Issue-5, May,2007

[3] Kiely, l.; T. Benzel; Systemic Security Management: A New Conceptual Framework for understanding the Issues, Inviting Dialogue and Debate, and Identifying Future Research needs." Institute for critical information.

[4] URL- www.fao.org/docrep/w5830e/w5830e0f.htm

[5] URL http://public.dhe.ibm.com/common/ssi/ecm/en/til14080usen/TIL14080USEN.PDF