DETERMINANTS OF BUSINESS INFORMATION SECURITY

Mr. Rahul Mohare*

Dr. Ujjwal Lanjewar**

Abstract

Insufficient security can result in downtime, or even worse, reduce credibility with customers and partners. Many organisations have preventive security measures in place, such as firewalls, antivirus systems and networking monitoring software. But while prevention can go a long way in safeguarding information assets, having a plan in place for meeting potential threats is critical. Realizing comprehensive security relies upon organizations ability to strategically assess areas of potential weakness, which is where having an assessment of business overall security program comes in and thereafter setting the business objectives for information security, often called security program design and management. The focus of this paper is on the major objectives to be considered for safeguarding the business information.

* Lecturer, Datta Meghe Institute of Management Studies, RTM Nagpur University.

** Professor, VMV-JMT-JJP Sci. College, RTM Nagpur University.

1. Introduction

Information and Communication Technology (ICT) plays a central role throughout the private and public sector and enables us to work in a network, simplifying communication within and between organizations. The development of this new technology, however, has also ushered in the arrival of a new set of problems.

In the 1980s, the emergence of computer viruses was a common concern; today, such viruses are worldwide phenomenon and only one of the many threats to information security. Despite the installation and implementation of various technical and organizational protection measures, the risk of information security breaches has consistently increased over the years. Apparently, security failures cannot be prevented by suitable technical protection alone. It may be done by, how an organization plans the information security procedure by setting the effective and productive objectives which may comprise all levels of management. This paper will explore and analyze the various potential objectives for any organization that could be used to improve information security.

2. Organizations Perspective towards Information Security

Organizations should signal their commitment towards Information Security procedure by stating their clear and rigid objectives and build the task force to assess their performance and report the results to their upper level management. Any dynamic environment organizations will need to implement decentralized decision making to ensure the necessary flexibility and adaptability of their security posture. And, in such an environment of decentralized decision making it becomes extremely important to implement the right security governance structures and practices to ensure that consistently good decisions are being made, hence while implementing any information security policy the objectives should be very much clear at various levels of organization. Any information security policy that is to be implemented must have the following approach which uses the Plan-Do-Check-Act (PDCA) aspect.

2.1. Security Management & Principles: The core components of risk management, information security policy, procedures, standards, guidelines, baselines, classification, education, and security organization serve as the foundation of information security. Security controls are implemented and maintained to address the three interdependent principles present in all information security programs: Confidentiality, Integrity and Availability, also known as the "CIA triad."

2.2. Security Management Responsibilities: This includes the resources, funding, and strategic representation needed to participate in a security program. Management support is one of the most important factors for the success of the security program.

2.3. Top-Down Approach: The top-down approach means that top management provides support and direction, which is cascaded down through middle-level management and then to staff members.

2.4. Risk Management: Risk management is the process of identifying, analyzing, assessing, evaluating, and reducing risk to an acceptable level, and implementing the right defense mechanisms to maintain an acceptable level of risk.

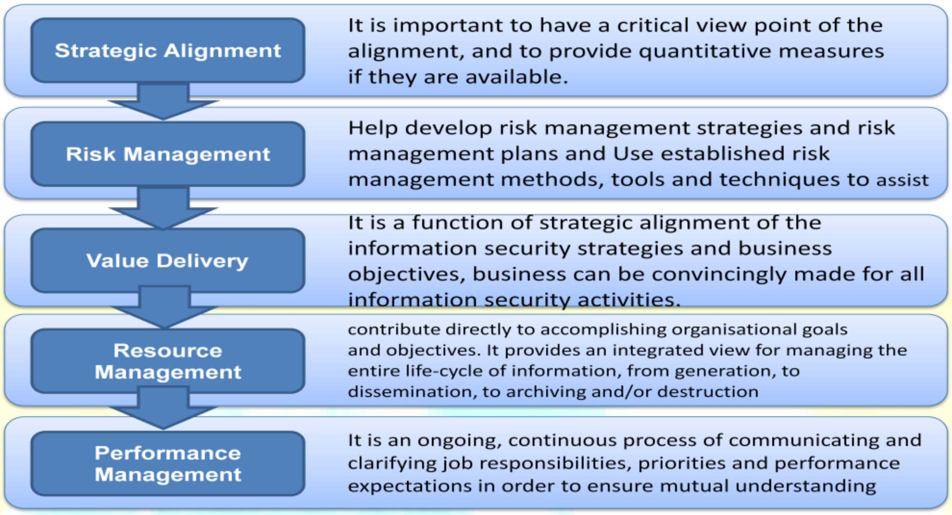
2.5. Security Awareness: To achieve the desired results of the security program, an organization must communicate the "what, how and why" of security to their employees. This awareness should be comprehensive, tailored, and organization-wide.

2.6. Business Continuity and Disaster Management: Ensures continuity, recovery and restoration of the business in case of disaster. In the case of an emergency, it would involve getting critical systems to another environment while repair of the original facilities is taking place.

2.7. Legal Compliance: Includes compliance to various civil, criminal, and administrative (regulatory) laws such as intellectual property laws, trade secrets, copyrights, trademarks, patents, and data protection.

3. Safeguarding the information in Business

It's one thing to establish a security program that meets the needs of an organization. It's quite another to successfully embed the principles of that program into the organization. However, it can be accomplished if we take a multi-faceted approach that incorporates organizational, managerial and operational aspects that are closely associated with the business. The first thing to assess is the culture of an organization. Thus, it's important to know where one stand, from an organizational perspective, before launching an initiative with as potentially high impact as a security program. After all, security is a change agent, and people by nature are not favorable to change. When you work within the boundaries of your organization's culture and align the security program with the cultural reality of your organization, you can gain a key leadership edge. It's essential for the security professional to adapt the look and feel of the local practice. In order to provide value from a security perspective, it's essential to work very closely with the business, understand the business's needs and be able to fully articulate the business value of the security program. Depending on the maturity of the security program in your organization, you may require anything from a few tweaks to a full implementation of substantial controls, implying significant budget considerations. We have observed five main objectives with respect to an organisation that will help to drive the business by protecting their information in most efficient and effective way in different levels of management. The following model is sufficient enough to give the complete view of our study



Strategic Alignment

It is important to have a critical view point of the alignment, and to provide quantitative measures if they are available.

Risk Management

Help develop risk management strategies and risk management plans and Use established risk management methods, tools and techniques to assist

Value Delivery

It is a function of strategic alignment of the information security strategies and business objectives, business can be convincingly made for all information security activities.

Resource Management

contribute directly to accomplishing organisational goals and objectives. It provides an integrated view for managing the entire life-cycle of information, from generation, to dissemination, to archiving and/or destruction

Performance Management

It is an ongoing, continuous process of communicating and clarifying job responsibilities, priorities and performance expectations in order to ensure mutual understanding

Figure 1: Major Objectives of an organization for setting information security policy

3.1 Strategic alignment

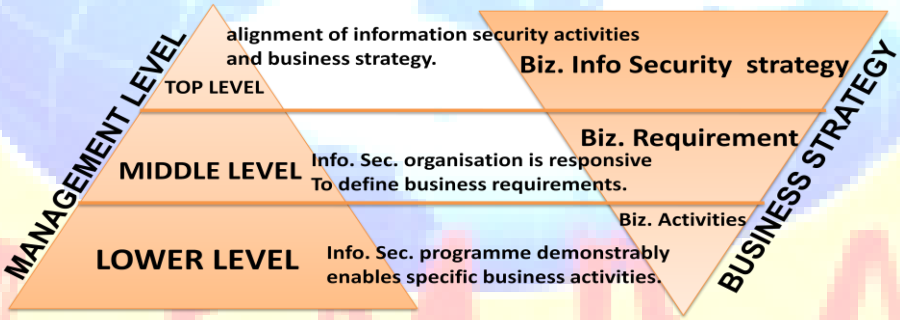

MANAGEMENT LEVEL
TOP LEVEL
alignment of information security activities and business strategy.
Biz. Info Security strategy
MIDDLE LEVEL
Biz. Requirement
Info. Sec. organisation is responsive To define business requirements.
LOWER LEVEL
Biz. Activities
Info. Sec. programme demonstrably enables specific business activities.
BUSINESS STRATEGY

Figure 2: Strategic Alignment

1. The information security programme demonstrably enables specific business activities, the top level of management aligns the specific information security activities in accordance with specific business strategies

2. The middle level management of an organisation is responsive to define business requirements which maps to the organizations information security objectives

3. The Lower level of management transforms the organisational and information security objectives in to business activities, which are defined and clearly understood by all involved in information security and related assurance activities.

3.2 Risk Management

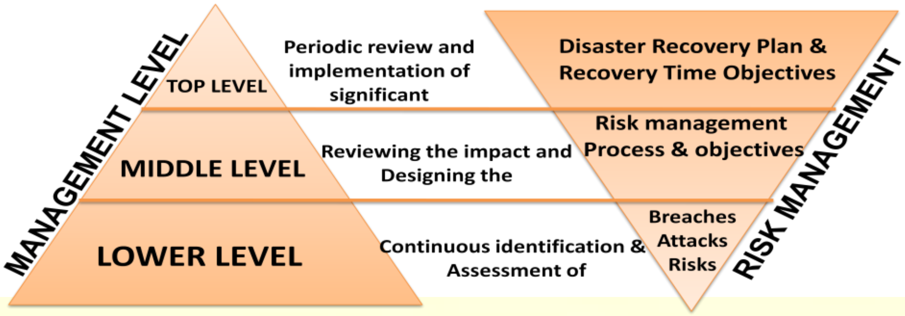

MANAGEMENT LEVEL
TOP LEVEL
MIDDLE LEVEL
LOWER LEVEL
Periodic review and implementation of significant
Reviewing the impact and Designing the
Continuous identification & Assessment of
Disaster Recovery Plan & Recovery Time Objectives
Risk management Process & objectives
Breaches Attacks Risks
RISK MANAGEMENT

Figure 3: Risk Management

1. The top level of management defines risk tolerance in the terms relevant to the organization and performs periodic review and implement significant Disaster Recovery Plan(DRP) and Recovery Time Objectives (RTO)
2. The middle level of management review an overall information security strategy and programme for achieving acceptable levels of risk by designing the risk management process and disaster recovery objectives.
3. The lower level of management performs continuous assessment of breaches, attacks and risks in disaster recovery

3.3 Value Delivery

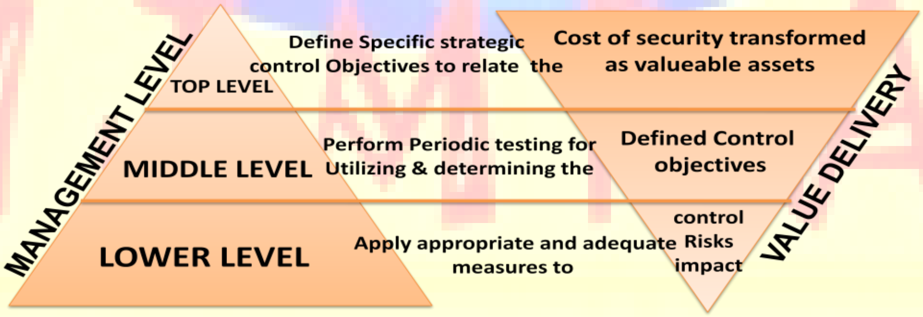

MANAGEMENT LEVEL
TOP LEVEL
MIDDLE LEVEL
LOWER LEVEL
Define Specific strategic control Objectives to relate the
Perform Periodic testing for Utilizing & determining the
Apply appropriate and adequate measures to
Cost of security transformed as valueable assets
Defined Control objectives
control Risks impact
VALUE DELIVERY

Figure 4: Value Delivery

1. Here the top level management defines the specific strategic control objectives to relate the cost of security transformed and the value of the asset
2. The Middle level management performs periodic testing for utilizing and determining the information security controlling risk and potential attacks.

3. The lower level of management applies appropriate and adequate measures defined by the organization to control the risks impact.

3.4 Resource Management

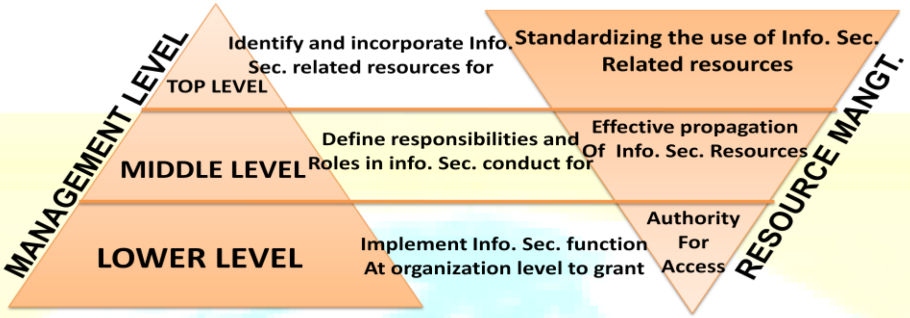

MANAGEMENT LEVEL
TOP LEVEL
MIDDLE LEVEL
LOWER LEVEL
Identify and incorporate Info. Sec. related resources for
Define responsibilities and Roles in info. Sec. conduct for
Implement Info. Sec. function At organization level to grant
Standardizing the use of Info. Sec. Related resources
Effective propagation Of Info. Sec. Resources
Authority For Access
RESOURCE MANGT.

Figure 5: Resource Management

1. The top level of management identifies and incorporates the information security related resources for standardizing the use of resources in effective and efficient manner.
2. The middle level of management standardized the process of using resources and defines responsibilities and roles of an individual for effective use of information security resources.
3. The lower level of management gets an authorization code for access to implement information security functions at organization level.

3.5 Performance Management

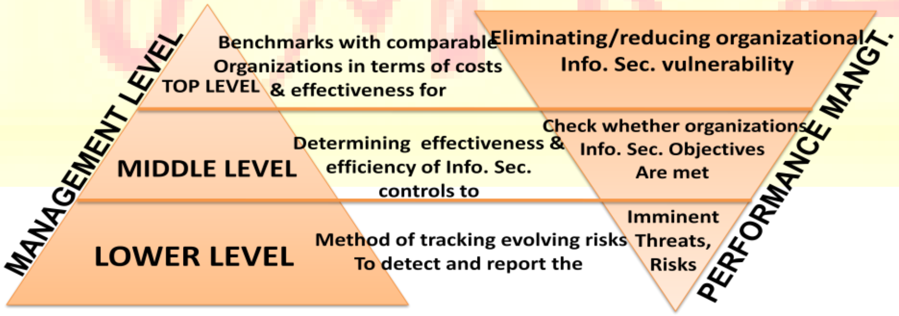

MANAGEMENT LEVEL
TOP LEVEL
MIDDLE LEVEL
LOWER LEVEL
Benchmarks with comparable Organizations in terms of costs & effectiveness for
Determining effectiveness & efficiency of Info. Sec. controls to
Method of tracking evolving risks To detect and report the
Eliminating/reducing organizational Info. Sec. vulnerability
Check whether organizations Info. Sec. Objectives Are met
Imminent Threats, Risks
PERFORMANCE MANGT.

Figure 6: Performance Management

1. The top level of management benchmarks the information security policy comparing it with other available policies in terms of cost and effectiveness by eliminating vulnerabilities

2. Middle level of management determines the effectiveness and efficiency of information security controls to check whether organizational information security objectives are met

3. Lower level management shall deploy method to track the evolving risks to detect the imminent threats and risks.

Conclusion

Our analysis of information security objectives in safeguarding business through organizations point of view found no ready framework or discussion of strategic roles and responsibilities by organisation. In this paper, we have proposed a preliminary framework for setting information security objectives. Information security is the ongoing process of exercising due care and due diligence to protect information, and information systems, from unauthorized access, use, disclosure, destruction, modification, or disruption or distribution. The never ending process of information security involves ongoing training, assessment, protection, monitoring & detection, incident response & repair, documentation, and review.

References

1. Bodin, L.D., Lawrence A. Gordon, and Loeb, M.P. "Evaluating Information Security Investments Using the Analytic Hierarchy Process," Communications of the ACM (48:2) 2005, pp 79-83.
2. Budhiraja, R. Electronic Governance – A Key Issue in the 21st Century, Concept Paper http://www.mit.gov.in/eg/article2.htm.
3. Dhillon, G., and Torkzadeh, G. "Value-focused Assessment of information systems security in organizations," Information Systems Journal (16:3) 2006, pp 293-314.
4. Galloway, D.J. "Control models in perspective," The Internal Auditor (51:6) 1994, pp 46-52.
5. Kirsch, L.J., Sambamurthy, V., Ko, D.-G., and Purvis, R.L. "Controlling Information Systems Development Projects:The View from the Client " Management Science (48:4) 2002, pp 484-498.
6. Siponen, M. "Five Dimensions of Information Security Awareness," Computers and Society:June) 2001, pp 24-29
7. Warkentin, M., and Johnston, A. IT Security Governance and Centralized Security Controls Idea Group Publishing, Hershey, P.A, 2006.
8. Whitman, M. "Enemy at the Gate: Threats to Information Security," Communications of the ACM (46:8) 2003, pp 91-95.