Factors Affecting Organizational Information Security in Today's Technological World

Dr. Sarang R. Javkhedkar
Assistant Professor
D.A.I.M.S.R.
Nagpur

Dr. Anjali Shrungarkar
Assistant Professor
City Premier College
Nagpur

Abstract

Information Security plays major role in almost every field and it is challenging day-by-day as the advancement in technologies. Insufficient security can result in downtime, or even worse, reduce credibility with customers and partners. Many organizations 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 Organization / business information.

Keywords – Firewall, Information Security, Networking Monitoring Software

1. **Introduction –** Information security is the major concern for every organization and the challenges are increases day—by-day as the change in technologies and advancement in technology. 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 and people that use computers can describe their needs for information security and trust in systems in terms of three major requirements:- (a) Confidentiality: controlling who gets to read information; (b) Integrity: assuring that information and programs are changed only in a specified and authorized manner; and (c) Availability: assuring that authorized users have continued access to information and resources. These three requirements may be emphasized differently in various applications. For a national defense system, the chief concern may be ensuring the confidentiality of classified information, whereas a funds transfer system may require strong integrity controls. The requirements for applications that are connected to external systems will differ from those for applications without such interconnection. Thus the specific requirements and controls for information security can vary.

The framework within which an organization strives to meet its needs for information security is codified as security policy. A security policy is a concise statement, by those responsible for a system (e.g., senior management), of information values, protection responsibilities, and organizational commitment. One can implement that policy by taking specific actions guided by management control principles and utilizing specific security standards, procedures, and mechanisms. Conversely, the selection of standards, procedures, and mechanisms should be guided by policy to be most effective.

2.1. Policies & Principles: A security policy must not only state the security need, but also address the range of circumstances under which that need must be met and the associated operating standards. 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. Management Perspective: Management controls are the mechanisms and techniques—administrative, procedural, and technical—that is instituted to implement a security policy. An effective program of management controls is needed to cover all aspects of information security, including physical security, classification of information, the means of recovering from breaches of security, and above all training to instill awareness and acceptance by people.

2.3. Flow of Information: The High-level – to Low-Level i.e. 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 Analysis and Management: Risk analysis and 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. Awareness: The weight given to each of the three major requirements describing needs for information security—confidentiality, integrity, and availability—depends strongly on circumstances. To achieve the desired results of the security program, an organization must communicate security aspects to their employees briefly.

2.6. Recovery: A system that must be restored within an hour after disruption represents, and requires, a more demanding set of policies and controls than does a similar system that need not be restored for two to three days. Likewise, the risk of loss of confidentiality with respect to a major product announcement will change with time**.** Early disclosure may jeopardize competitive advantage, but disclosure just before the intended announcement may be insignificant. In this case the information remains the same, while the timing of its release significantly affects the risk of loss.

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

3. **Confidentiality –** Confidentiality is a requirement whose purpose is to keep sensitive information from being disclosed to unauthorized recipients. The secrets might be important for reasons of national security, law enforcement, competitive advantage, or personal privacy. 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. We have observed four main objectives with respect to an organization 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.

Planning	The major role is to have a tactical arrangement which helps to provide qualitative and quantitative measure whenever available.
Risk	It helps to develop the strategies and plans and used methods, tools and techniques to guide the management.
Resources	Utilization of resources is a key function of management it help to maintain the life-cycle of information.
Performance	Evaluation of all the process from planning to performance is the continuous process helps to ensure mutual understanding.

3.1. Planning

A – Top level management plans the specific information security activities in accordance with specific business plan.

B – Response to define business requirements which maps to the organizations information security objectives is the duty of the middle level management.

C - The transformations of the organizational and information security objectives in to business activities, which are defined and clearly understood by all involved in information security and related assurance activities is performed by the lower level management.

3.2. Risk

A. Defining the 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) done by top management.

B. The middle level of management review an overall information security strategy and program for achieving acceptable levels of risk by designing the risk management process and disaster recovery objectives.

C. Continuous assessment of breaches, attacks and risks in disaster recovery is performed by the lower level of management.

3.3.Resources

A- Identification and incorporation of the information security related resources for standardizing the use of resources in effective and efficient manner is the major function of the Top level of Management.

B- Standardization of the process of utilizing the resources and defines responsibilities and roles of an individual for effective use of information security resources managed by the middle level of management

C- The lower level of management gets an authorization code for access to implement information security functions at organization level.

3.4.Performance

A- 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

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

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

Conclusion

From the above study we concluded 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 organization. We proposed a preliminary framework for setting information security objectives in this paper. As Information security is the continuous 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 proper guidance and efficient training, assessment, protection, monitoring & detection, incident response & repair, documentation, and review are the key factors of never ending process of information security.

Abbreviations

ICT - Information and Communication Technology

CIA - Confidentiality, Integrity and Availability

DRP - Disaster Recovery Plan

RTO - Recovery Time Objectives

References

1. Galloway, D.J. "Control models in perspective," The Internal Auditor (51:6) 1994, pp 46-52.
2. 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.
3. Whitman, M. "Enemy at the Gate: Threats to Information Security," Communications of the ACM (46:8) 2003, pp 91-95.
4. 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.
5. Budhiraja, R. Electronic Governance – A Key Issue in the 21st Century, Concept Paper http://www.mit.gov.in/eg/article2.htm.
6. Dhillon, G., and Torkzadeh, G. "Value-focused Assessment of information systems security in organizations," Information Systems Journal (16:3) 2006, pp 293-314.