CONCEPTUAL FRAMEWORK OR INFORMATION SECURITY POLICY

Rahul Mohare*

Dr. U A Lanjewar**

Background

To protect overall security, it's important to formulate a clear policy that states what rights the employee has and how the employee should responsibly handle company resources. That policy should be signed by each employee when he or she is first hired. In some instances, having an employee who works with sensitive or proprietary information sign a nondisclosure or confidentiality agreement is also a wise precaution.

A good security policy is comprehensive and flexible; often, it's not a single document but a group of documents, each with its own specific emphasis. The next section discusses general best practices for security policies. Then, you examine major factors that result in an effective set of rules and procedures: the consideration of cyber risk insurance coverage; the need to base a policy on a thorough risk assessment; the need to teach employees about acceptable use of network resources; the need to specify what an employee's expected privacy rights are when on company property and equipment; the need to enable management to set priorities; the need to help administrators do their jobs; and the need to see a security policy as making subsequent risk analyses possible.

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

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

Formation of New Information Security Policy

An information security policy addresses many issues such as the following: disclosure, integrity, and availability concerns; who may access what information in what manner; basis on which the access decision is made (for example, user characteristic such as nationality or group affinity, or some external condition such as time or status); maximized sharing versus least privilege; separation of duties; who controls and who owns the information; and authority issues. In the proposed information security policy we had constituted it in six different phases, where each phase has to perform its own significant tasks and need to contribute to build a strong information security policy.

The Information Security Policy is based on the ISO 27002:2005 standard for information security management. This standard provides a structured approach to identifying the broad spectrum of information security activities in the life-cycle of information systems. The Information Security Policy manual provides the framework for government organizations to establish local policies and procedures necessary for the protection of government information and technology assets. Implementation of a structured Information Security Program will provide more consistent protection of government information and technology resources.

The policies incorporate a risk assessment approach to security using Security Threat and Risk Assessments to consider:

- Business process and government service delivery implications;
- Technological implications; and,
- Communications strategies including changes to personnel information security awareness programs.
- The risk assessment approach enables:
- Compliance with legislative and policy objectives;
- Cost-effective allocation of resources based on a risk assessment;
- Responsible governance of the Province's information assets; and,
- Secure provision of government e-services.

The Information Security Policy contains operational policies, standards, guidelines and metrics intended to establish minimum requirements for the secure delivery of government services. Secure service delivery requires the assurance of confidentiality, integrity, availability and privacy of government information assets through:

- Management and business processes that include and enable security processes;
- Ongoing personnel awareness of security issues;
- Physical security requirements for information systems;
- Governance processes for information technology;
- Reporting information security events and weaknesses;
- Creating and maintaining business continuity plans; and,
- Monitoring for compliance.

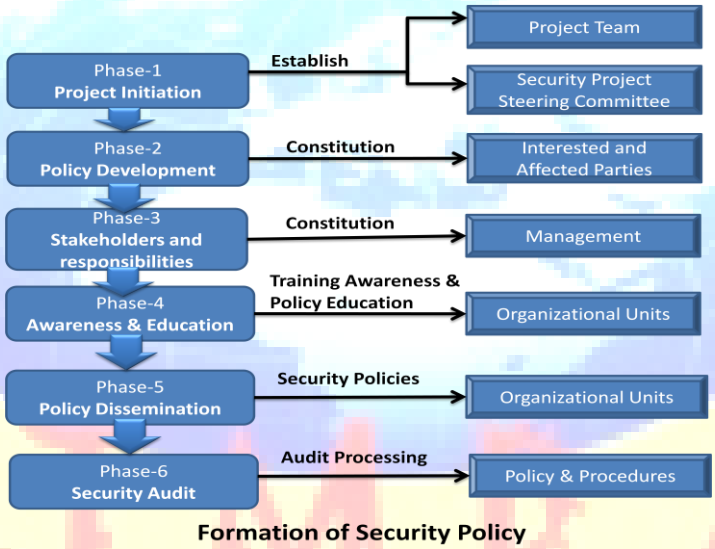

Figure 1: Conceptual Framework for Information Security Policy

Phase-1: Project Initiation

The purpose of Project Initiation is to begin to define the overall parameters of a project and establish the appropriate project management and quality environment required to complete the project. Development of the Project Charter is a pivotal starting point for the project, establishing the project definition that will serve as the foundation for all future efforts. As part of Project Initiation, an initial Project Plan is developed, which comprises the Project Charter, These

documents, once approved, ensure a consistent understanding of the project, help to set expectations, and identify resources necessary to move the project to the next level of detailed planning. Potential problems are identified so that they can be addressed early in the project. Also during Project Initiation, a high-level Project Schedule is developed as the roadmap to more detailed Project Planning and Project Execution and Control. This high-level schedule will be refined over time, and will serve as the primary source of information regarding project status and progress. An accurate, realistic, and complete schedule, rigorously maintained, is essential to the success of a project.

In this phase after extensive research and literature review researcher had concludes that it is important to determine who is going to be involved in the actual development phase of policy at an early stage. The group who develops the policy should ideally also be the group who will own and enforce the policy in the long-term; this is likely to be the information security department. The overall composition of the policy development team will vary according to the policy document being developed and deployed.

Phase 2: Policy Development (Information Security)

In this phase researcher had focused on the basic information security framework parameters some of them are

- An information security risk management methodology
- A comprehensive security strategy explicitly linked with business and IT objectives
- An effective security organisational structure
- A security strategy that talks about the value of information protected—and delivered
- Security policies that address each aspect of strategy, control and regulation
- A complete set of security standards for each policy to ensure that procedures and guidelines comply with policy
- Institutionalised monitoring processes to ensure compliance and provide feedback on effectiveness and mitigation of risk
- A process to ensure continued evaluation and update of security policies, standards, procedures and risks

Researcher further studied, which governance model will be best for governing the proposed information security policy in terms of mission/business needs, risk tolerance and its overall effectiveness. Here researcher had studied three different approaches; centralized, decentralized and hybrid. Next researcher had studied the various trust model to describe ways in which organizations can obtain the levels of trust needed to form partnerships, collaborate with other organizations, share information, or receive information system/security services.

Down the line in same chapter researcher had introduced the information security framework which relies mainly on eight parameters they are: Ensuring data integrity, Processes to respond identity fraud, clear accountability and deterrence mechanism, Legal framework for the policy, clear response and navigation mechanism for data breaches, ensuring internal content security and control, ensure secure enrollment and authentication and finally encrypted information.

Next important task was to determine the process of information security, here researcher had presented the model for information security process, which is given below

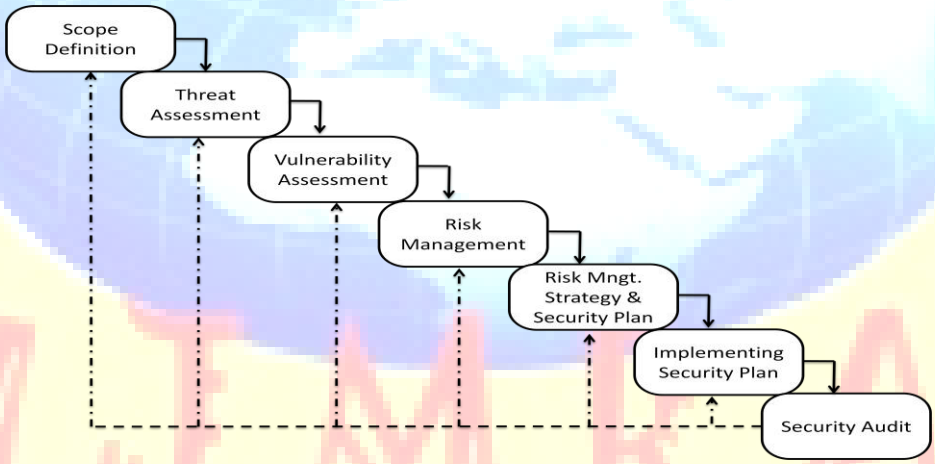

Figure 2: Information Security Process

And finally the development of information security policy is combined with the security tools, standards and protocols to be followed. And the last thing which is discussed is the firewalls to be followed and adapted for the information security policy.

Phase 3: Stakeholders and responsibilities

The third phase of the information security policy is to consider the participating stakeholders and their roles and responsibilities, what kind of strategic and regulatory framework these stakeholders have to follow to build a strong information security policy is discussed, followed by this researcher had discussed the benefits that can be availed by using this approach. How total system security can be achieved? What permissions are sought to be obtained to which file? Many things like this are discussed in this phase. Then comes the program management of stakeholders their composition and roles and responsibilities as well

Phase 4: Awareness and Education

Once the policy is developed and ready to deploy, its time to educate the people how to use the policy? how to handle and troubleshoot the errors? How to report the errors? This can be done by explaining the user the value of and needs for the information security. Four major components are discussed Awareness, Training, Education and Certification. A training and awareness module is developed to cater the needs of the training. This is judged by the program success indicator. Researcher had drawn these references by going through various information security awareness standards of the ISO 17799:2005 wherein security awareness is very much an integral part of an ISO 17799-compliant information security management system. A recurring theme throughout the standard is that people in an organization must be made aware of the security policies, procedures and control requirements that they are expected to uphold. Next is the same phase it is being discussed how to implement the awareness and training program? How to communicate the plan? How awareness material is delivered? How training material is delivered? What is to be done post implementation? What is the feedback mechanism? Etc.

Phase 5: Policy Dissemination

Now since, the policy is developed and training and awareness program is conducted its time to deploy the policy, because this is the perfect time to deploy the policy. Researcher had insisted on the web base approach for policy deployment. Next the researcher had discussed the policy evaluation and maintenance techniques

Phase 6: Information Security Audit

This is the last phase of our security model, which in culprits the review to meet the stated objectives of information security policy. it begins with major developments in information security that have to be keep in track in terms or information security audit. Then researcher had stated the strategic plan for information security audit starting from defining mission and objectives, linking the objectives to supporting activities and finally using web base security approach

Advantages of the proposed policy

1. Automates routine tasks-workflow/ Business rules/ Processes
2. Work/ Task prioritization
3. Standardization of the common processes
4. Reduced cycle time and dependencies
5. Improved opportunities for value addition
6. Enabling environment for efficient administration
7. Assists in decision making-decision support analysis
8. Easy and efficient referencing – search engines
9. Creation of knowledge base by integrating various departments to form a single repository
10. Traceability and accountability of actions - Audit trail
11. Remainders and notification to officers

Conclusions

The primary focus of this study was to determine what issues security professionals perceived as being the most problematic with regard to security in organizations. Here we tried to explore the process of building and implementing successful Information Security Policy in detail.

The security within any organisation starts with building a Security Policy, a centralized, evolving document defining what is allowed and what is not. The implementation process requires constant monitoring of Internet Threats, along with the measurement of staff knowledge and awareness levels to ensure that there is a continuous improvement in their level of knowledge and security awareness.

The dearth of quantitative methods for measuring, forecasting, and improving information security has left those of us who depend on information systems in a precarious state.

Because quantitative metrics have not been available, our security decisions have instead relied upon the opinions of those believed to be experts, anecdotal evidence, and other heuristics.

While security will never be an exact science, we have shown in this paper it is possible to answer questions of security with quantitative metrics that provide answers in meaningful terms. These techniques lay groundwork that can be used for quantitative and economic studies of security. Researcher argued that models of information security is the measure of these other deterrents, which include the cost of time and resources to carry out a threat scenario.

Security strength is important to the security of encrypted messages because eavesdropping can often be achieved with low risk. In order to accomplish this, it was first necessary to redefine security strength in the context of software systems and determine how it could be measured. Researcher introduced an economic measure of software security strength, with respect to a threat scenario. The key observation was that security strength depended most on whether the adversary knew of the existence of an exploitable vulnerability in the system.

References

- M. Suduc, M. Bizoi and F. G. Filip, "Ethical Aspects on Software Piracy and Information and Communication Technologies Misuse," *Preprints of IFAC SWIIS Conference*, Bucharest, 2009.
- Anil k Kaushik, Chandan Mazumdar, Jaya Bhattacharjee, Shilpi Saha. "Model Driven Security Analysis of Egovernance Systems" in eIndia 2008, November edition.
- http://www.egovonline.net/Resource/eindia08-full-paper-for-abstract-173.pdf
- Charles p. Pfleeger, Shari Lawrence Pfleeger., *Security in computing*, Third Edition, Prentice Hall, 2003
- Dorothy E. Denning., *Information Warfare and Security*, Addison Wesley, 2001
- Eric Maiwald., *Network Security A Beginner's Guide*, Osborne McGraw-Hill, 2001
- M. Apata, *The Essence of Information System Security and Audit.* Retrieved January 2010, from Jidaw.com, Available at: http://www.jidaw.com/security1.html