The 2006 International Arab Conference on Information Technology (ACIT'2006)

Process Management for Information Security Assessment

Mohamed Osama Kamel Khozium* and Kashif Riaz**

*Faculty of Information Technology, Osama@khozium.com
**Faculty of Information Technology, miankashif@msn.com

MISR University for Science & Technology, 6th of October City, EGYPT

ABSTRACT

Current IT trends have caused huge changes to its infrastructure as compared to its past. Security along with all associated risks has brought great losses to organizations. This paper addresses not only management issues related with security risk assessment but with all those processes that should be initialization with technical aspects.
We can model the security relevant processes through out any information system. It can help us to develop security policy also allowing management to structure its policy outside the technological arena. This can be used as evolution tool even while analysis & designing of applications.
Despite the true realistic approach for senior management it also shows how to co-op up with security issues while considering resources with all its availability; also highlighting how evolving environments should be assessed with self assessment criteria.

Keywords: Security Risks, Security Process Management, Security Assessment, Security Plans, Security Model, Security Audit

1 . INTRODUCTION

Every movement that comes to us bring new challenges. Where as the rising slogan of IT has brought new horizons to our attention. Today continuous progress & service delivery has changed business imperatives as IT security has become integral part for any infrastructure.
Information technology continuous advancements has open the number of possible security threats, vulnerabilities and security incidents are even rising pace despite efforts done by national or international level.
The current problems faced by organizations are not only rising trends in information technology but there unrealistic approach to coop with evolving environment that has caused the world the loss of billions of US dollars.
Actually Probability of loss is not based upon mathematical certainty; it is consideration of the likelihood that a loss risk event may occur in the future, based upon historical data, the history of like events at similar enterprises, the nature of the neighborhood, immediate vicinity, overall geographical location, political and social conditions, and changes in the economy, as well as other factors that may affect probability.

All solutions still are necessary to manage the risk options includes security measures available to reduce the risk of the event. Equipment or hardware, policies and procedures and management practices, and staffing are the general categories of security related options.

Where as service providers claming to protect with help of sum of tools are providing unreliable results and that has been caused by security programs that are not extending its boundaries to combined approach that is people, process and technologies.
Even inter departmental collaboration to manage effective processes is not up to mark to achieve high level of IT security across any organization.

2 . PROJECTED RISK ASSESSEMNET PROBLEM.

For effective risk management, sound business decisions with continuous monitoring over assets and all issues related to their sensitivity and criticality are needed. Along with there associated assets proper decisions are needed to work up risk management plans that can have impact to departments and organization's environment as well [1] .
Today several standards adopted by national and international are needed with all their classification and to be managed with up to date continuous coordinated directions for service providers. Here not only technical but operational issues are also to be targeted in well established way [2] .
Information management can provide continuity of plans and collaborative IT security where availability of critical services are always ensured to its maximum level. For that organization has to apply self assessment criteria for continuous planning so that measured results can be inferred from resources; with evolving security plans that can recognize and provide remedial actions for the organizations [8] .

Information management plans can lead us towards effective planning that enable us to audit administrative and functional areas of IT in terms of resources and finance concerned along with positive reporting process [6] .

3. PROPOSED STRUCTURE FOR SECURITY ASSESSMENT

The formulation of following steps can enhance information security structure for any organization i.e.

1. Identify Security Deficiency
2. Continuous IT planning for technical & operational tasks
3. Self Assessment mechanism
4. Audit Process planning
5. Incident handling procedures
6. Information recovery methodology
7. Back up of Data & Configuration
8. Incident Impacts
9. Future Security Visions
10. Quality measures for security

Where as for any effective plan, senior management should always be involved in implementation process that bound ness can bring true strategy of management.

Current infrastructure providing physical security measures hasn't proved to be adequate enough because of potentially large scale undefined problems can not be limited to few work stations. Security safeguards needed to be improved via identification & authentication where low risk environment prevails. While considering security procedures access privileges need to be monitored and controlled for every level of access [3] .

Organizations have to apply departmental zones with reference to security control and access mechanism. As one key mechanism that is often neglected by many organizations is continuous monitoring of network traffic with all its available resources.

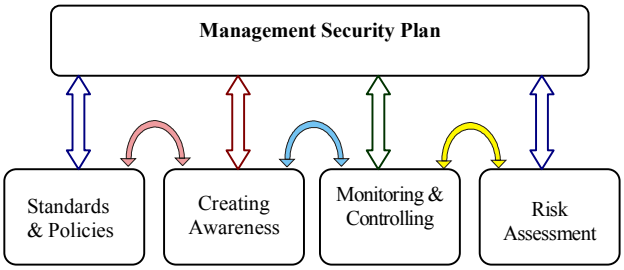

Figure-1 : Information hierarchy for Security Implementation

As shown in figure1, along with proper security standards controlling is also ensured to identify security breaches, suspected or known security threats.

Organizational security plan can be adopted with proper control mechanism that are

1. Physical access controls
2. Device & media controls
3. Procedural controls

With all its departments, organizations should evaluate risk assessment plans often after certain period of time as tools associated with security are not at halt. Where as organizations have to share their experiences for better control as tools provided by venders some time are not focused regional issues [5] .

All technical and operational environments should log the event in case any incident occur .Management plan should qualify to access potential impact and proper identification of the system so to tackle this issue, system control should be configured with best practices[6].

All operational records associated with human's operations and service delivery should always include risk related to IT system with reference to their priority as mentioned or described by security advisors as described in figure 2.

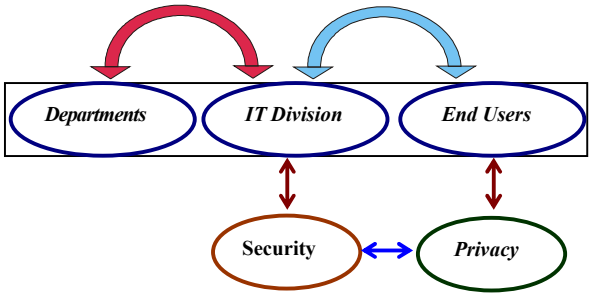

Figure-2 : Securing User's Privacy

4 . RISK ASSESSMENT PROCEDURE

Risk assessment should take into account the potential adverse impact on the organization reputation, operations and assets. Risk assessment should be conducted by teams composed of appropriate managers, administrators and all other personnel associated with those activities. [5]

Organizations need to adopt local notification procedures which include reporting mechanism where as for disaster recovery plan should also specify emergency procedures plan including system documentation required for performing recovery.

In many of organizations where proper systems hasn't been deployed still missing corrective measures or never considered in their security consideration need to apply recovery plans along with all possible strategic planning and that should not be limited to all management decisions but communications and actions should be properly recorded.

5 . CONCLUSION

Information security issues can better be targeted if effective risk management plans come into existence as proposed in this paper that continuous planning along with standards can bring IT infrastructure where processes are not only managed but effective control along with audit can create awareness among humans that can readily initiate action plans for best security configuration. [4]
We strongly address that beside physical security measures following steps are needed for security advancements both in management and technical areas.

1. Promote a culture of security
2. Raise awareness about the risk of Information systems
3. Enhance confidence level among all participants in information system
4. Adopt the culture of cooperation and information sharing
5. Conduct full risk assessment in accordance with international accredited standards
6. Coordination with departments for regular monitoring of all servers.
7. Develop action plans and milestone for information security

REFERENCES

[1] Committee on Energy & Commerce US House of Representatives, "Cyber security & Consumer Data: whats at risk for the consumers?" Pg.6 NOV 19, 2003.

[2] Glaessner.Thomas, "Electronic Security: Risk Mitigation in Financial IT Transactions"- The World Bank. June 2002

[3] Higgins, John C, "Proceedings of the 12th National Computer Security Conference", Nov. 1989.

[4] ISO 17799- "Information Technology Code of Practice for Information Security Management."http://www.iso.org/iso/en/catalogueDetailPage.

[5] NIST 800-30, " Risk Management Guide for Information Technology Systems. http://cbrc.nist.gov/publications.

[6] Pfleeger, charles P., Security in Computing, Prentice Hall,1989.

[7] Sound Practices for Management & Supervision of Operational Risk. http://www.bi.org/publ/bcbs96.pdf.

[8] US Federal financial Institutions Examination Council, "Audit IT Examination Handbook" And "FFIEC Audit Examination Procedures". HB 49, Proc.27.

[9] US President's Information Technology Advisory Committee," Cyber Security Report", Feb.2005.