RISK ASSESSMENT

On IT Infrastructure

Mr Pradhan P L & Prof P K Meher

Objective:

To develop risk assessment method to safeguard or protect of Information System assets of an organization.

Element that identify and analyze the risk forced by an organization and ways these risks can be managed

The IS auditor or IS security administrator is responsible for developing risk assessment method.

Risk assessment is the process of identifying vulnerabilities and threats to an organization's information resources or IT infrastructures in achieving business objectives and deciding what counter measures, if any, to take in reducing the level of countermeasures and deciding which, if any, to take in reducing risk to an appropriate acceptable level, based on the value of the information resource to the organization. A summary of this concept is shown in the equation as follows:

Mathematical Equation:

Total Risk = Threats x Vulnerability x Asset Value

Generally, risk can be transferred, reject, reduced or accepted at high, medium and low level risk, but risk never eliminated.

An example of risk can be transfer, when a company buy insurance. An organization can be choose to reject risk by ignoring it, which can be dangerous. Risk can be reduced by implementing or improving security controls (Firewall, Intrusion detection system, Network monitoring tools/NMS/HP Open View) and procedure (countermeasures). At the time of implementing control, an organization may be consider costs & benefits of implementing it. If the cost of controls exceeds the benefits, an organization may choose to accept the risk rather than incurring additional costs securing its system.

Existing Risk Assessment:

Developing a Risk Assessment Program:

To develop a risk management and assessment program in the following ways:

A: Establish the purpose and objective of the risk assessment program.

The first step is to determine the organization's purpose for creating a risk management program. The program's purpose may be to reduce the cost of insurance or to reduce the number of program-related injuries. By determining its intention before initiating risk management planning, the organization can evaluate the results to determine its effectiveness. Typically, the executive director a non-profit, with the board of directors, sets the tone for the risk management program

B: Assign responsibilities for the risk assessment plan.

The second step is to designate an individual or team responsible for developing and implementing the organization's risk management program. While the team primarily is responsible for the risk management plan, a successful program requires the integration of risk management within all levels of the organization. Operations staff and board members should assist the risk management committee in identifying and developing suitable loss control and intervention strategies.

Risk Assessment process (Assets Identification & Classification)

The first step in the process is the identification and classification of information resources or assets, which need protection because they are vulnerabilities to threats. The purpose of the classification may be either to prioritize (High/Medium/Low) further investigation and identify appropriate protection (simple classification based on the asset value), or to enable a standard model of protection to be applied (classification in term of criticality, sensitivity and risk). Example of typical assets associated with information and IT includes:

.

- Information & data
- Hardware
- Software
- Services
- Documents
- Personnel

Other more traditional business assets for consideration are building, stock of goods(inventory/spare parts : like hard disk , Ram, Motherboards, backup drives & tapes)
Cash and less tangible assets, such as goodwill or image/reputation.

The next step in the process threats and vulnerabilities associated with the information resource and likelihood of their occurrence. In this context, threats are any circumstances or events with the potential to cause harm on an information resource, such as destruction, disclosure, modification of data and/or denial of service.

Common Class of threats are as follows:

- Errors
- Malicious damage/attack
- Fraud
- Theft
- Equipment/Software failure

Threats occur because of vulnerabilities associated with use of information resources. Vulnerabilities are characteristics of information resources that can be exploited by a threats to cause harm. Example of vulnerabilities are:

- Lack of user knowledge
- Lack of security functionality
- Poor choice of passwords
- Untested technology
- Transmission over unprotected communications.

The result of any of these events occurring is called an impact, and can result in a loss of one sort or another. In commercial organizations, threats usually result in a direct financial loss in the short term or an ultimate (indirect) financial loss in long term. Examples of such losses include the following:

- Direct loss of money (cash or credit)
- Breach of legislation
- Loss of reputation/goodwill
- Endangering of staff or customers
- Breach of confidence
- Loss of Business opportunity
- Reduction in operational efficiency/performance
- Interruption of business activity

Once the elements of risk have been established, they are combined to form an overall view of risk. A common method of combining the elements is to calculate Impact X's vulnerability (probability of occurrence related to a particular information resource) for each threat to give a measure of overall risk. The risk is proportional to the value of loss/damage and to the estimated frequency of the threat.

Once risk have been identified, existing control can be evaluated or new control designed to reduce the vulnerabilities to an acceptable level of risk. These control are referred to as countermeasures. They could be actions, devices, procedures or techniques. The strength of a control can be measures in terms of its inherent or design strength include whether the controls are preventative or detective, manual or programmed, and formal (documented in procedure manuals and evidence of their operation is maintained) or ad hoc.

The remaining level of risk, once controls have been applied, is called residual risks. Residual risk can be used by management to identify those areas in which more control is required to further risk. A target of an acceptable level of risk can be established by management. Risk in excess of this level should by the implementation of more stringent control. Risks below this level should be evaluated to determine if excessive level of control is being applied and if cost saving can be removing these excessive controls. Final acceptance of residual risks takes into account:

- Organizational policy
- Risk identification & Measurement
- Uncertainty incorporated in the risk assessment approach itself
- Cost & effectiveness of implementation

STEP AS FOLLOWS:

The first step in the process is the identification and classification of information resources or assets, which need protection because they are vulnerabilities to threats. The purpose of the classification may be either to prioritize (High/Medium/Low) further investigation and identify appropriate protection (simple classification based on the asset value), or to enable a standard model of protection to be applied (classification in term of criticality, sensitivity and risk). Example of typical assets associated with information and IT includes:

.

- Information & data
- Hardware
- Software
- Services
- Documents
- Personnel

Other more traditional business assets for consideration are building, stock of goods(inventory/spare parts : like hard disk , Ram, Motherboards, backup drives & tapes)
Cash and less tangible assets, such as goodwill or image/reputation.

The next step in the process threats and vulnerabilities associated with the information resource and likelihood of their occurrence. In this context, threats are any circumstances or events with the potential to cause harm on an information resource, such as destruction, disclosure, modification of data and/or denial of service.

Common Class of threats are as follows:

- Errors
- Malicious damage/attack
- Fraud
- Theft
- Equipment/Software failure

Threats occur because of vulnerabilities associated with use of information resources. Vulnerabilities are characteristics of information resources that can be exploited by a threats to cause harm. Example of vulnerabilities are:

- Lack of user knowledge
- Lack of security functionality
- Poor choice of passwords
- Untested technology
- Transmission over unprotected communications.

RESULT:

The result of any of these events occurring is called an impact, and can result in a loss of one sort or another. In commercial organizations, threats usually result in a direct financial loss in the short term or an ultimate (indirect) financial loss in long term. Examples of such losses include the following:

- Direct loss of money (cash or credit)
- Breach of legislation
- Loss of reputation/goodwill
- Endangering of staff or customers
- Breach of confidence
- Loss of Business opportunity
- Reduction in operational efficiency/performance
- Interruption of business activity

Once the elements of risk have been established, they are combined to form an overall view of risk. A common method of combining the elements is to calculate Impact X’s vulnerability (probability of occurrence related to a particular information resource) for each threat to give a measure of overall risk. The risk is proportional to the value of loss/damage and to the estimated frequency of the threat.

Once risk have been identified, existing control can be evaluated or new control designed to reduce the vulnerabilities to an acceptable level of risk. These control are referred to as countermeasures. They could be actions, devices, procedures or techniques. The strength of a control can be measures in terms of its inherent or design strength include whether the controls are preventative or detective, manual or programmed, and formal (documented in procedure manuals and evidence of their operation is maintained) or ad hoc.

The remaining level of risk, once controls have been applied, is called residual risks. Residual risk can be used by management to identify those areas in which more control is required to further risk. A target of an acceptable level of risk can be established by management. Risk in excess of this level should by the implementation of more stringent control. Risks below this level should be evaluated to determine if excessive level of control is being applied and if cost saving can be removing these excessive controls. Final acceptance of residual risks takes into account:

- Organizational policy
- Risk identification & Measurement
- Uncertainty incorporated in the risk assessment approach itself
- Cost & effectiveness of implementation

Proposed Risk Assessment Method:

As per recent scenarios of the IS security system, we can propose and implement the most essential points as following ways:

A) Management Level Policy Planning for Assessment:

The top management develop the policies, procedures & guidelines as per their business objective to safeguards the IT infrastructure for their long term assignment**.**

To reduce the expected losses from hacker, intruder and viruses, security administrator can implement the following types of controls.

The top management develop the policies, procedures & guidelines as per their business objective to safeguards the IT infrastructure for their long term assignment**.**

To reduce the expected losses from hacker, intruder and viruses, security administrator can implement the following types of controls.

- **Preventive control:**

Use only " clean " certified copies of software files/data, that contain macros.
Implement read-only access over software.
Check new software that with anti virus before it is installed.
Educate the users about the dangerous virus that mean of preventing infection.

- **Detective control:**

Regularly run anti virus software to detect infections.
Implement & regulate date/time stamps of updation , modification and user access to the OS, Server, Network, Internet, Data & files etc.

- **Corrective control:**

Ensure clean backup is maintained.
Proper documentation plan for backup & recovery.
Run Anti Virus Software to remove infection on the system.

Current Risk Assessment Tools:

The risk assessment tools market is relatively small and is comprised approximately a dozen companies, of which seven most important tools appear to garner the majority of the market share. These tools range in cost from a little as a few hundred US dollar to more than US $25,000. The total number of risk assessment tools in active use today is less than 12,000 worldwide.

Risk Analysis Tools

Product	Company	Focus
CRAMM	Insight Consulting Ltd. www.insight.co.uk/cramm/	Government, Public Sector
CORA	International Security Technology Inc.	Telecom, Logistics Government, IT
COBRA	C & A Systems Security Ltd. www.security-risk-analysis.com	Enterprise
Risk Check	Norman Security Solutions www.norman.com	Enterprise
RiskPAC	CSCI Inc. www.csciweb.com	Business Continuity
RiskWatch	Risk Watch, Inc www.riskwatch.com	HIPAA, DITSCAP, NIACAP
The Buddy System	Alion Science & technology Inc. www.buddysystem.net	IT

These products & tools are more widely accepted at Europe. However, as a result of the US Health Insurance Portability and Accountability Act (HIPAA) and the event of 11 September 2001, they are growing in acceptance throught the US.

B) System level assessment:

- **Disaster Recovery Plan (DRP):**

Comprehensive disaster recovery plan comprise four parts as follows:
Emergency Plan:
Backup Plan
Recovery Plan
Test Plan

The Plan lay down the proper policies, procedure and guidelines for all personnel who have responsibilities for the information system functions to follows.

> Emergency Plan:
> Backup Plan
> Recovery Plan
> Test Plan

The Plan lay down the proper policies, procedure and guidelines for all personnel who have responsibilities for the information system functions to follows.

- Emergency Plan:

Organization should be undertake a comprehensive security review program regularly.

- **Backup Plan:**

The following resources must be considered: personnel, Hardware, Software, Facility, Document and Information.

To develop Hot Site, Cold Site, Worm Site of IS infrastructure as per business objective of the organization.

Reciprocal agreement with other related organization, vendor and contractor.

- **Recovery Plan:**

Under take the regulate backup & recovery should be maintained centralize & decentralize and remotely. (On-site & off-site, hot backup & cold backup)

- **Test Plan**:

Periodically, test plan must be invoked first the disaster recovery: desk checking and Inspection.

.

- **Others:**

- **Insurance:**

Insurance sometime can be used to mitigate losses that arises when disaster eventuate. Policies usually can be obtained to cover the following resources-: Hardware, Software, Data and Network.

- **BCP:**

Implement business continuity plan as per following steps:

Keep Sufficient Contingency fund for future requirement.

- Implement the latest tool & technique such as Firewall, Intrusion detection system and HP Open View as per requirement.

- Periodically, scanning the OS, Server, Network related protocols (IP address).
- Periodically, verify and review the various system logs and take in time corrective action and implement new patches as per requirement of policies, procedure and guidelines of the organization.
- Separation of & rotation of duty.
- Access control list must be implement (Read, Write, Execute level of data & program for owner, group or others)
- Regularly, follow up vulnerabilities assessment.
- Implement incident handling procedure, analysis and investigation .
- Implement release management & version control.
- Help desk & technical support.
- Internal system auditor must be periodically audit the system logs, policies, procedure, documentation as per advice of external system or IS auditor. (as per NSA, BS7799, ISO17799 standard).

Benefits:

Minimize the risk factor at minimum level.

Therefore, we can able to safeguard or protect the IS infrastructure/assets (Data, Hardware, Software, Network), from intruder, hacker and external vendor or contractor.

The risk management & assessment method to ensure and achieve protection, data integrity, effectiveness and efficiencies must be designed implement as per requirement of business objective of an organization

Conclusion:

In summary, the risk assessment process is about making decisions. The impact of a successful attack and the level of acceptable risk for any given situation is a fundamental policy decision. Likewise, vulnerabilities are design issues and must be addressed during the design, development & implementation of information resources. A fundamental problem of risk management then is to achieve a costeffective balance between design characteristics and the related countermeasures to threats and impact

References:

1). Information System audit & control by Ron Weber PHI (Chap 7 P- 243-285)
2) CISSP Exam study guide by Shon Harrish DRP/BCP (Chap 9 P 591-603)
3). CISSP Exam study guide by Shon Harrish Security Mgmt Practices (Chap 4 P 57-92)
4) Mcl.ean, Kevin & Lenwatts (1996) Risk Analysis Methodology " IS audit & contron Journal III 32-36

5). Essentail of System Administration O' Reilly (Chap 10, P467- 485) & Chap 6 (p201-243)
6). CISSP Exam cram by Coriolis (Chap 4 p 61-77)
7) Software Engg by Pressman Chap 6 (P 145- 162)
8) ISACA Monthly Journal Vol 2, 2003

Author:

Supervisor: Prof P K Meher NTU, Singapore, pkmeher@yahoo.com

P L Pradhan, M. Sc (Phys), DCA, PG DBA, Sun Solaris Certified (UNIX)
plpradhan@rediffmail.com

At present doing Ph D program on System Security Under Sambalpur University, Orissa, India

Working Area: (18 Yr exp in System/IT) System Security, Risk Mgmt, Unix System Administration, Backend Solution (Unix Oracle Database), ERP, Datacomm & Networking, Internet Technology, MIS & System Analysis and Design.