Today's Risk Might Be Problematic for Tomorrow's

Shivi Singhal[#1], Shalvi Rastogi[#2], Tarachand Verma[#3]

[#1, #3]Computer Science and Engineering Department, [#2] Electronics & Communication Engineering Department
Gautam Buddh Technical University
Raj Kumar Goel Institute of Technology for Women
Ghaziabad (U.P), India

[#1]shvsinghal20@gmail.com, [#2]shalvi411@rediffmail.com,[#3] cs.vermatara@gmail.com

***Abstract*— In E-society IT risk management has become both prudent practice and, in many cases, a legal necessity to protect the organization and its ability to perform their mission, not just its IT assets with respect to the cost. In this paper we will provide information on the selection of cost-effective security controls used to mitigate risk for the better protection of mission-critical information and the IT systems that process, store, and carry this information. The issue is raised to know how much security is enough? We will analyze the term risk as well as the importance of executing proper risk management planning by means of a risk management plan in terms of Risk Management overview, Risk Assessment, Risk Mitigation and Evaluation and Assessment and the factors that will lead to a successful risk management program. We observed that present risk might be problematic for future. We emphasized enhanced ethical and professional roles. Our paper explores the impact on E-society with practical approach of preventing tomorrow's probable problem by managing today's risk efficiently.**

***Keywords*—Risk, Cost,Security,Time, Information Technology(IT)**

I. INTRODUCTION

In the digital era, where automated IT systems are widely used, there always lies the probability of occurrence of the uncertain events resulting in adverse effects. No one has the exact answer of the question "HOW MUCH SECURITY IS ENOUGH?" for IT –Risks. Risk management is the total systematic process to identify, control, and manage the impact of uncertain harmful events, commensurate with the value of the protected assets. It aid managers to strike an economic balance between the costs associated with the risks and the costs of protective measures to lessen those risks. A practical approach to Risk management will accommodate flexibility and adaptability to diverse software projects by stressing early prototyping, frequent functional builds, and a set of metrics to provide management insight during software development.
The objective of performing risk management is to enable the organization to accomplish its mission(s)

a) By better securing the IT systems that store, process, or transmit organizational information;
b) By enabling management to make well-informed risk management decisions to justify the expenditures that are part of an IT budget; and
c) By assisting management in authorizing (or accrediting) the IT systems on the basis of the supporting documentation resulting from the performance of risk management.

Need of IT Risk management—

a) Higher education's network infrastructure is both a direct target and a source of hijacked bandwidth IT security efforts are required at all network levels which is difficult to manage
b) More sophisticated and dangerous exploits and attacks are released daily
c) Potential for terrorist attacks or natural disasters
d) Risk management as an opportunity not just to protect the firm, but to drive improvements in IT management and business outcomes
e) IT executives can use risk to justify important investments that might not have a clear financial return.
f) IT managers can improve alignment and understanding, both in IT and the business, by discussing IT risk considerations in terms of four key enterprise risks: -

- Availability
- Access
- Accuracy
- Agility

Role of IT Risk Management is to Meet the goals under the presence of risk. Risk management is the process that allows IT managers to balance the operational and economic costs of protective measures and achieve gains in mission capability by protecting the IT systems and data that support their organizations' missions. A well-structured risk management methodology, when used effectively, can help management identify appropriate controls for providing the mission-essential security capabilities.

Organizations build effective IT risk management capability through three disciplines:

a) *Foundation:* A base of infrastructure, applications and supporting personnel which is well-structured, well-managed, and no more complex than absolutely necessary.
b) *Risk governance process:* Procedures and policies that provide an enterprise-level view of all IT risks, so that managers can prioritize risks and invest appropriately.

c) *Risk aware culture:* A culture in which everyone has appropriate knowledge of risk, and in which open, non-threatening discussions of risk are the norm.

Table 1 shows various threats with their source and actions which highlight the need of effective security measures.

Table 1: Threats

Threat-Source	Motivation	Threat Actions
Hacker, cracker	Challenge Ego Rebellion	• Hacking • Social engineering • System intrusion, break-ins • Unauthorized system access
Computer criminal	Destruction of information Illegal information disclosure Monetary gain Unauthorized data alteration	• Computer crime (e.g., cyber stalking) • Fraudulent act (e.g., replay, impersonation, interception) • Information bribery • Spoofing • System intrusion
Terrorist	Blackmail Destruction Exploitation Revenge	• Bomb/Terrorism • Information warfare • System attack (e.g., distributed denial of service) • System penetration • System tampering
Industrial espionage (companies, foreign governments, other government interests)	Competitive advantage Economic espionage	• Economic exploitation • Information theft • Intrusion on personal privacy • Social engineering • System penetration • Unauthorized system access (access to classified, proprietary, and/or technology-related information)
Insiders (poorly trained, disgruntled, malicious, negligent, dishonest, or terminated employees)	Curiosity Ego Intelligence Monetary gain Revenge Unintentional errors and omissions (e.g., data entry error, programming error)	• Assault on an employee • Blackmail • Browsing of proprietary information • Computer abuse • Fraud and theft • Information bribery • Input of falsified, corrupted data • Interception • Malicious code (e.g., virus, logic bomb, Trojan horse) • Sale of personal information • System bugs • System intrusion • System sabotage • Unauthorized system access

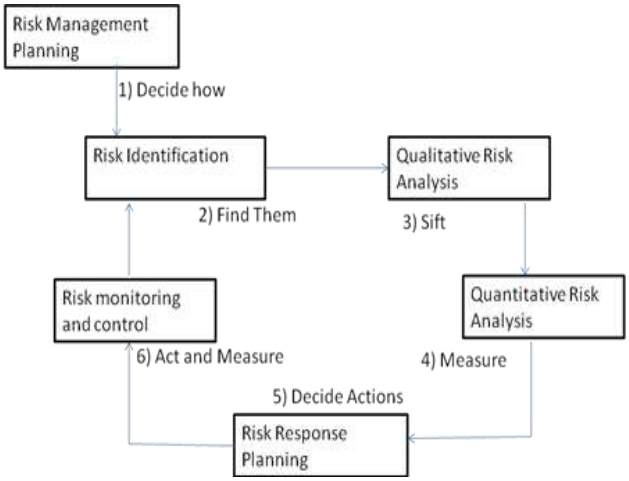

Figure 1: Risk Handling

II. Risk Management Overview

Here we will describe the risk management methodology, how it fits into each phase of the SDLC(Software development lifecycle), and how the risk management process is tied to the process of system authorization.

Figure 2: Key Words for IT risk management

Risk management encompasses three processes: risk assessment, risk mitigation, and evaluation and assessment. The risk assessment process includes identification and evaluation of risks and risk impacts, and recommendation of risk-reducing measures. The risk mitigation refers to prioritizing, implementing, and maintaining the appropriate risk-reducing measures recommended from the risk assessment process. The continual evaluation process and keys for implementing a successful risk management program, comprises the final step.

III. Integration Of Risk Management Into SDLC

Minimizing negative impact on an organization and need for sound basis in decision making are the fundamental reasons organizations implement a risk management process for their IT systems. Effective risk management must be totally integrated into the SDLC. An IT system SDLC has five phase: initiation, development or acquisition, implementation, operation or maintenance, and disposal. The risk management methodology is the same regardless of the SDLC phase for which the assessment is being conducted. Risk management is an iterative process during each major phase of the SDLC.

A. Risk Assessment

Risk assessment is the first process in the risk management methodology. Organizations use risk assessment to determine the extent of the potential threat and the risk associated with an IT system throughout its SDLC. The output of this process helps to identify appropriate controls for reducing or eliminating risk during the risk mitigation process. *Risk* is a function of the *likelihood* of a given *threat-source's* exercising a particular potential *vulnerability*, and the resulting *impact* of that adverse event on the organization.

To determine the likelihood of a future adverse event, threats to an IT system must be analysed in conjunction with the potential vulnerabilities and the controls in place for the IT system. Impact refers to the magnitude of harm that could be caused by a threat's exercise of vulnerability. The level of impact is governed by the potential mission impacts and in turn produces a relative value for the IT assets and resources affected. The risk assessment methodology encompasses nine primary steps: System Characterization, Threat Identification, Vulnerability Identification, Control Analysis, Likelihood Determination, Impact Analysis, Risk Determination, Control Recommendations, and Results Documentation.

B. Risk Mitigation

Risk mitigation, involves prioritizing, evaluating, and implementing the appropriate risk-reducing controls recommended from the risk assessment process. Because the elimination of all risk is usually impractical or close to impossible, it is the responsibility of senior management and functional and business managers to use the *least-cost approach* and implement the *most appropriate controls* to decrease mission risk to an acceptable level, with *minimal adverse impact* on the organization's resources and mission.

1) Risk Mitigation Options

Risk mitigation is a systematic methodology used by senior management to reduce mission risk. Risk mitigation can be achieved through any of the following risk mitigation options:

- Risk Assumption. To accept the potential risk and continue operating the IT system or to implement controls to lower the risk to an acceptable level.
- Risk Avoidance. To avoid the risk by eliminating the risk cause and/or consequence (e.g., forgo certain functions of the system or shut down the system when risks are identified).
- Risk Limitation. To limit the risk by implementing controls that minimize the adverse impact of a threat's exercising vulnerability (e.g., use of supporting, preventive, detective controls).
- Risk Planning. To manage risk by developing a risk mitigation plan that prioritizes, implements, and maintains controls.
- Research and Acknowledgment. To lower the risk of loss by acknowledging the vulnerability or flaw and researching controls to correct the vulnerability.
- Risk Transference. To transfer the risk by using other options to compensate for the loss, such as purchasing insurance.

Priority should be given to the threat and vulnerability pairs that have the potential to cause significant mission impact or harm.

2) Risk Mitigation Strategy

The following rules of thumb, which provide guidance on actions to mitigate risks from intentional human threats:

- When vulnerability (or flaw, weakness) exists: implement assurance techniques to reduce the likelihood of vulnerability's being exercised.
- When vulnerability can be exercised: apply layered protections, architectural designs, and administrative controls to minimize the risk of or prevent this occurrence.
- When the attacker's cost is less than the potential gain: apply protections to decrease an attacker's motivation by increasing the attacker's cost (e.g., use of system controls such as limiting what a system user can access and do can significantly reduce an attacker's gain).
- When loss is too great: apply design principles, architectural designs, and technical and nontechnical protections to limit the extent of the attack, thereby reducing the potential for loss.

3) Approaches For Control Implementation

When control actions must be taken, the following rule applies: *Address the greatest risks and strive for sufficient risk mitigation at the lowest cost, with minimal impact on other mission capabilities.*

The following risk mitigation methodology describes the approach to control implementation:

Step 1: Prioritize Actions
Output -Actions ranking from High to Low

Step 2: Evaluate Recommended Control Options
Output -List of feasible controls

Step 3: Conduct Cost-Benefit Analysis
Output-Cost-benefit analysis describing the cost and benefits of implementing or not implementing the controls

Step 4: Select Control
Output -Selected control(s)

Step 5: Assign Responsibility
Output -List of responsible persons

Step 6: Develop a Safeguard Implementation Plan
Output -Safeguard implementation plan

Step 7: Implement Selected Control(s)
Output -Residual risk

4) Control Categories

In implementing recommended controls to mitigate risk, an organization should consider technical, management, and operational security controls, or a combination of such controls, to maximize the effectiveness of controls for their IT systems and organization. Security controls, when used appropriately, can prevent, limit, or deter threat-source damage to an organization's mission.

The control recommendation process will involve choosing among a combination of technical, management, and operational controls for improving the organization's security

posture. The trade-offs that an organization will have to consider are illustrated by viewing the decisions involved in enforcing use of complex user passwords to minimize password guessing and cracking. In this case, a technical control requiring add-on security software may be more complex and expensive than a procedural control, but the technical control is likely to be more effective because the enforcement is automated by the system. On the other hand, a procedural control might be implemented simply by means of a memorandum to all concerned individuals and an amendment to the security guidelines for the organization, but ensuring that users consistently follow the memorandum and guideline will be difficult and will require security awareness training and user acceptance.

5) Cost-Benefit Analysis

To allocate resources and implement cost-effective controls, organizations, after identifying all possible controls and evaluating their feasibility and effectiveness, should conduct a cost-benefit analysis for each proposed control to determine which controls are required and appropriate for their circumstances.

The cost-benefit analysis can be qualitative or quantitative. Its purpose is to demonstrate that the costs of implementing the controls can be justified by the reduction in the level of risk. For example, the organization may not want to spend $1,000 on a control to reduce a $200 risk. A cost-benefit analysis for proposed new controls or enhanced controls encompasses the following:

a) Determining the impact of implementing the new or enhanced controls.
b) Determining the impact of *not* implementing the new or enhanced controls.
c) Estimating the costs of the implementation. These may include, but are not limited to, the following:
   - Hardware and software purchases.
   - Reduced operational effectiveness if system performance or functionality is reduced for increased security.
   - Cost of implementing additional policies and procedures.
   - Cost of hiring additional personnel to implement proposed policies, procedures, or services.
   - Training costs.
   - Maintenance costs.

d) Assessing the implementation costs and benefits against system and data criticality to determine the importance to the organization of implementing the new controls, given their costs and relative impact.

The organization will need to assess the benefits of the controls in terms of maintaining an acceptable mission posture for the organization. Just as there is a cost for implementing a needed control, there is a cost for not implementing it. By relating the result of not implementing the control to the mission, organizations can determine whether it is feasible to forgo its implementation.

6) Residual Risk

Organizations can analyse the extent of the risk reduction generated by the new or enhanced controls in terms of the reduced threat likelihood or impact, the two parameters that define the mitigated level of risk to the organizational mission. Implementation of enhanced controls can mitigate risk by-

- Eliminating some of the system's vulnerabilities (flaws and weakness), thereby reducing the number of possible threat-source/vulnerability pairs.
- Adding a targeted control to reduce the capacity and motivation of a threat-source. For example, a department determines that the cost for installing and maintaining add-on security software for the stand-alone PC that stores its sensitive files is not justifiable, but that administrative and physical controls should be implemented to make physical access to that PC more difficult (e.g., store the PC in a locked room, with the key kept by the manager).
- Reducing the magnitude of the adverse impact (e.g., limiting the extent of vulnerability or modifying the nature of the relationship between the IT system and the organization's mission).

C. Evaluation An Assessment

In most organizations, the network itself will continually be expanded and updated, its components changed, and its software applications replaced or updated with newer versions. In addition, personnel changes will occur and security policies are likely to change over time. These changes mean that new risks will surface and risks previously mitigated may again become a concern. Thus, the risk management process is ongoing and evolving. This section emphasizes the good practice and need for an ongoing risk evaluation and assessment and the factors that will lead to a successful risk management program.

The risk assessment process is usually repeated at least every 3 years for federal agencies, as mandated by OMB Circular A-130. However, risk management should be conducted and integrated in the SDLC for IT systems, not because it is required by law or regulation, but because it is a good practice and supports the organization's business objectives or mission. There should be a specific schedule for assessing and mitigating mission risks, but the periodically performed process should also be flexible enough to allow changes where warranted, such as major changes to the IT system and processing environment due to changes resulting from policies and new technologies.

Figure 3: Risk Management Techniques

D. IT Risk Management Best Practices Tools

Six types of RM tools and processes today:

- Rapid Application Development (RAD)
- Quality assurance (QA)
- Automated test tools

- Version control
- Disaster recovery
- Business continuity planning

1) Rapid Application Development (RAD) Tools

They are rule-based licensed software that once learned allow the tool user to have thousands of lines of code developed automatically – almost instantly. Mainly, time to market business risk they help to avoid. Imagine if development time would normally take six-nine months to complete and you can do that in one-third the time. The earlier the service is provided to the business user, the less risk there is of losing market share.

2) Quality Assurance (QA)

It assures that the likelihood of failure of any new application put into production is extremely low because it has been so methodologically tested and retested. It is a very strict regimen – and almost as importantly an insurance policy for the CTO/CIO. Many kinds of business risk it helps to avoid- the risk of starting up and failing because the system doesn't perform as advertised- the risk of losing disappointed users, the risk of losing the business, the risk of the CTO/CIO getting fired.

3) Automated Test Tools (Arrows In The QA Quiver)

They speed significantly all kinds of testing – functionality, stress and failover. They allow one to simulate and test and understand bandwidth requirements. They can be licensed from multiple sources and take some time to learn how to use properly – but well worth investigating. They help to avoid many business risks including speedier testing of new and revised software (time to market) and ensuring no system failure when running at maximum capacity. But they are not limited to these.

4) Version Control

Version Control (Change Management) keeps track of where (in which computers) each version of application and system software is running. Its methodology ensures that all preliminary steps required verifying the readiness of a new software version to go into production has been accomplished. They mainly avoid those mission critical applications that don't go down when new versions of application and system software are upgraded. It ensures that old versions of existing software will work as expected with the application version being upgraded, and that new features and bug fixes are actually implemented in new releases.

5) Disaster Recovery (D/R)

D/R is a capability to keep computer systems running at a back-up data center – with minor hitches – when a catastrophe occurs at a primary data center. D/R is not the same as failover. It helps control those business risks that have loss of data processing capability.

6) Business Continuity Planning (BCP)

It's different than D/R, but clearly includes D/R. It's a strategy and plan to keep the business running by assuring that the people needed to run the business have required facilities and information provided to them quickly. A BCP is very inclusive and detailed and is a dynamic document with multiple accesses for instant availability.

IV. Good Security Practice

The risk assessment process is usually repeated at least every 3 years for federal agencies, as mandated by OMB Circular A-130. However, risk management should be conducted and integrated in the SDLC for IT systems, not because it is required by law or regulation, but because it is a good practice and supports the organization's business objectives or mission. There should be a specific schedule for assessing and mitigating mission risks, but the periodically performed process should also be flexible enough to allow changes where warranted, such as major changes to the IT system and processing environment due to changes resulting from policies and new technologies.

V. Keys For Success

A successful risk management program will rely on

a) Senior management's commitment.
b) The full support and participation of the IT team.
c) The competence of the risk assessment team, which must have the expertise to apply the risk assessment methodology to a specific site and system, identify mission risks, and provide cost-effective safeguards that meet the needs of the organization.
d) The awareness and cooperation of members of the user community, who must follow procedures and comply with the implemented controls to safeguard the mission of their organization.
e) An ongoing evaluation and assessment of the IT-related mission risks.

VI. Conclusion

Technology drives the consolidation of industries, globalization of markets, and invention and reinvention of organizations worldwide. Technology supports collaboration and innovation at rates never seen before. But technology failures can bring entire segments of the economy to a halt, corrupt records or leave them inaccessible, and compromise employees' productivity. Managing risks introduced by IT is a business imperative. In this report, we have observed that:

- IT failures in your organization ripple through customers, suppliers and partners.
- IT risks come from multiple sources, change constantly, and require a continuous program of discovery, monitoring, and management.
- IT risks are managed by the combination of people, process, and technology, balancing risks against business objectives.
- IT Risk Management is a business process that adapts to organizational requirements, guided by best practices.

As you launch or expand your IT Risk Management program, keep in mind that managing IT Risk rarely means eliminating it. Instead, IT Risk Management disciplines and practices help keep IT services flexible, adaptive, and aligned to organizational goals in a constantly changing business climate. In addition, IT Risk Management can provide the insight that allows you to take calculated risks with confidence and use IT to drive competitive advantage.

VII. Future Work

We will continue our research into IT Risk Management to discover additional practical Recommendations and best practices to help organizations develop and implement their

own programs. Future research will assess the state of deployment and maturity of IT Risk Management programs, including the prevalence of IT Risk Management initiatives and the use of programs-based best practices. Symantec will continue to explore the how the management of IT Risk contributes to business productivity, competitive advantage, and the spirit of innovation."IT Risk Management is more than using technology to solve security problems. With proper planning and broad support, it can give an organization the confidence to innovate, using IT to outdistance competitors."

ACKNOWLEDGEMENT

The authors would like to thank Department of Computer Science and Engineering and Department of Electronics and Communication for their special support in Raj Kumar Goel Institute of Technology For Women (RKGITW), Ghaziabad (U.P) under which this work has been done.

REFERENCES

[1] Computer Systems Laboratory Bulletin. *Threats to Computer Systems: An Overview*. March 1994.

[2] NIST Interagency Reports 4749. *Sample Statements of Work for Federal Computer Security Services: For Use In-House or Contracting Out.* December 1991.

[3] NIST Special Publication 800-12. *An Introduction to Computer Security: The NIST Handbook*. October 1995.

[4] NIST Special Publication 800-14. *Generally Accepted Principles and Practices for Securing Information Technology Systems*. September 1996. Co-authored with Barbara Guttmann.

[5] NIST Special Publication 800-18. *Guide for Developing Security Plans for Information Technology Systems*. December 1998. Co-authored with Federal Computer Security Managers' Forum Working Group.

[6] NIST Special Publication 800-26, *Security Self-Assessment Guide for Information Technology Systems*. August 2001.

[7] NIST Special Publication 800-27. *Engineering Principles for IT Security*. June 2001.

[8] OMB Circular A-130. *Management of Federal Information Resources.* Appendix III. November 2000.