Global Journal of Enterprise Information System

# Information System Security and Risk Management: Issues and Impact on Organizations

Shikha Gupta[1], Anil K Saini[2*]

[1] School of Computer Applications, Ansal University, Gurgaon, India; shikhagupta@ansaluniversity.edu.in

[2*]University School of Management Studies, GGS Indraprasth University, India; aksaini1960@gmail.com

**Abstract**

Information Technology (IT) based information systems have become the backbone of not only success but of survival of organizations in this highly competitive world. Considering that IT is an important asset it must be managed efficiently to minimize the risks associated with it and the systems it supports. The paper is based on literature review of existing work on information security and risk management. It attempts to describe the theoretical perspective of information system security. It also discusses and analyses the various information security methodologies in practice.

**Keyword:** information security implementation, IT risk, information security methodologies

## 1. Introduction

Information Systems (IS) are set of interrelated components that retrieve, process, store and distribute information to support decision making and control in organizations. IS basically consists of data hardware, software, procedures and people which are usually developed to support business function (Godbole, 2009). In the present scenario information systems have become an essential aspect and an integral part of any business have graduated from being just a tool and information provider to facilitator in effective decision making to help in improving efficiency. Growing dependence of most organizations on their information systems has provided problems such as theft of data, attacks using malicious code, denial of service etc. New opportunities for IT related issues coupled with risks have made IT Governance an increasingly critical facet of overall governance. Information security is not just a technology problem, it is a business issue, it was seen as a negative factor creating value through nonoccurrence. Organizations that make extensive use of information technology can be more efficient and productive. However, this ever-growing dependence on IT also leads to a dramatic increase in expensive information security incidents and failures (BSI, 2004).

As organizations become increasingly dependent on information systems (IS) for strategic advantage and operations, the issue of IS security also becomes increasingly important (Kankanhalli, Teo, Tan, & Wei, 2003). The information must be protected from harm caused due to threats leading to loss, non-availability, alteration and wrongful disclosure. Threats include errors and omissions, fraud, accidents and intentional changes (Saleh, Alfantookh, 2011). The main goal of information security is to protect the interest of stakeholders by ensuring confidentiality (disclosure of information to the righteous persons), availability (information systems are available and usable) and integrity (information is protected against unauthorized changes). Thus, Information Security is a key aspect of information technology governance.

Information security industry in itself encompasses diverse set of products, services, processes and policies ranging from encryption algorithm to human resource management. The success of information security implementation can be determined through technological, operational and managerial controls. The lack of a fully inclusive guideline document to assist the functioning of sufficient Information Security Governance is common in the business environment.

* Address for correspondence:

Anil K Saini

University School of Management Studies, GGS Indraprasth University, India.

aksaini1960@gmail.com

## 2. Impact of IT Implementation on Organizations

There has been an exponential growth in IT in years which can be exploited by corporation to meet the challenges of rapidly changing economy (Morton, 1991). The relationship between IT and business in recent years has changed from strategic level to supporting operational processes in business (eg. Workflow systems, document management, case management, etc) (Radianti & Gonzalez, 2007). 'Modern societies, organizations & business depend on reliable information system (Hallberg, Hallberg & Hunstad, 2007).

One can not deny the role of IT in success of a business. In fact, IT services have proven to be directly affecting business process performance & organization success (Hosseini, 2005).

As per the companies, IT services have resulted in companies performance enhancement in terms of higher return on sales and even the market share is directly impacted by efficient use of IT (Kempis, & Ringback, 1999) and researchers indicated this linkage of IT to enterprise very strongly. Studies suggest that this linkage can significantly affect the efficiency of the business and hence give it a competitive edge above others (Hosseini, 2005). It majorly improves customer service; integrate supplier and customer operations (Luftman, Lewis, & Oldach, 1993). In a way financial and non-financial, both business functions are impacted by adoption, implementation and expansion of an information system in organizations (Chatzoglou, & Diamantidis, 2009). Researchers even advocated the positive impact of investments in IT on firms' production process (Shao, & tin, 2001). Some are of the view that though IT impact performance, but the improvement in productivity is not as per expectation (Ko, & Bryson, 2002).

## 3. IT Implementation: Not a Risk Free Affair

Though several researchers have advocated the positive role of It in improving organization's performance and providing a competitive edge to it (Morton,1991; Radianti & Gonzalez, 2007; Hosseini, 2005; Kempis, & Ringback, 1999; Luftman, Lewis, & Oldach, 1993), the dependence of organizations on IT has made them vulnerable to issues like IT frauds, diverse set of security risks ranging from virus attacks to intentional or unintentional damage to the organization by employees resulting in failures of critical processes, due to problems in infrastructures like servers, data centers (Luftman, Lewis, & Oldach, 1993; Hosseini, 2005). 75% of organizations have confirmed being attacked (Bagchi, & Udo, 2003). Studies have revealed six categories of IT security issues have emerged which are as follows:

- System development
- System operation
- Risk management
- Communication and management of security
- Competence regarding security
- Attainment and preservation of trust (Hosseini, 2005).

Financial and non financial business functions are impacted by IT implementation risks (Chatzoglou, & Diamantidis, 2009). Use of IT encapsulates both systematic and unsystematic risks (Hallikainen, Kivjarvi, & Nurmimaki, 2002). Some studies have revealed that IT risk levels can not be fully eliminated or even lowered by advances in IT (Chatzoglou, & Diamantidis, 2009). As per Netherlands National Bank manual, IT risk is the predictable or possible risk that comes up because of the insufficient processing of existing information system (Chatzoglou, & Diamantidis, 2009). The manual also suggests a descriptive definition of IT risk in terms of following indicators

- Exclusivity - level of inappropriate authorization and unauthorized access
- Integrity -volume of incorrect and irregularly used and processed data
- Controllability-loosely controlled IS procedures
- User operations-inadequate IT support lack of skill and experience applied to IS
- Continuity-non availability of high level data and high volumes of system failures and disruptions
- Manageability-low degree of IS flexibility and maintainability leading to risks (De Nederlandsche Bank, 2001).

This categorization is supported by many researchers (National Institute of Standards and Technology, 2002; O'Donnell, 2005). As per the study 8 types of IT risks impact the performance of an organization which are:

- Operator error-by computer operator
- Hardware malfunctions-errors due to faulty hardware design
- Software errors or bugs-flaw in programs
- Data errors-invalid data
- User's carelessness-leading to accidental disclosure of information
- Protection error-inadequate protection against failure of system components leading to damage to physical infrastructure
- Performance error-failing to meeting the desired expectation
- Liability-system's level of responsibility (Steven, 2002)

Several authors have suggested IT implementation risk to be divided into 5 broad categories

- Application complexity-refers to number of links to other systems
- Application size-refers to number of users needed in development of IS and usage
- Organizational environment-refers to association between users and creators
- Team expertise
- Technology novelty (Hallikainen, Kivjarvi, & Nurmimaki, 2002)

As per the researchers, coordination and partially information ability are the most impacted non-financial factors and IT risk levels can not be fully eliminated or even lowered by just implementing or improving IT (Chatzoglou, & Diamantidis, 2009).

## 4. Risk Management: Basic Principle of Risk Analysis

Companies Can Estimate Possible Damages if a Threat Event Were to Arise (Godbole, 2008)

There has been tremendous study on handling the information security issue in IT based organizations. Different traditional information security methods have been developed with time. Some researchers have categorized infosec methods into 3 (Baskerville, 1988) generations and some into 5 (Baskerville, 1993) RM among the most commonly used early generation (first or second) infosec method (Siponen, 2005) called traditional method. They are widely used in practice (Baskerville, 1992; Fitzgerald, 1995; Solms, 1996; von Solms, & van de Haar, 2001) these are as follows:

- Checklist-AFIPD, SAFE, Moultan-Moultan, Wood et al
- ISS Standards-BS ISO/IEC17999 , GASSP, Sanders et al
- ISS Maturity Criteria-SSE-CMM, Software Security metrics, The Information Security Maturity Grid
- Risk Management- The generic RM approach, Hallidat et al. X-ifying RM, LRAM, communication approach
- Formal methods-Anderson, Barnes (Siponen, 2005)

Most of these methods are not integrated into ISD which results in conflict between normal functionality of Information Systems and Security functionality. These problems range from increased costs, user resistance in implementing the system to malfunctioning of the system which leads to various types of losses.

Of all methods stated above the most common methods are the Infosec management standards which are widely used and advocated. But these standards have limitations that the focus of these standards is on existence of processes rather than its content and effectiveness (Siponen, 2006). The underlying principle of these standards is mere existence of security activities not the extant or quality of their existence and hence they are just guidelines without advising how desired results are to be achieved just the use of a particular security process or activity does not ensure the security of the organization as per the objective. It is the content and quality that really matters (Siponen, 2006).

Studies show that Risk Management is the only traditional method which is useful in practice and the key to success of information security system is the alignment of RM to organizations' business strategies. (Siponen, 2005). Risk analysis is the science of observation, knowledge and evaluation-that is, keen eyesight, anticipation, etc. Risk management is the keystone to an effective performance as well as for targeted, proactive solutions to potential threats and incidents [an incidents is any event that is not a part of the standard operation of a service and that causes, or may cause, an interruption to, or a reduction in, the quality of that service]. Risk management is the ongoing process of identifying risks and implementing plans to address them. Risk evaluation is a process that generates an organization-wide view of information security risks. Risk management is the skill of handling the identified risk in the best possible manner for the interests of the organization.

Asset, threat and vulnerability combined are called triple in risk management domain where asset is defined as a resource, process, product, computing infrastructure etc. that an organization considers important to be protected, threat is the presence of any potential event initiated by humans or natural that could cause an adverse impact on the organization and vulnerability is the absence or weakness of safeguard.
Risk is described by the following mathematical formula.

Risk=threat* vulnerability* asset value.

Some researchers advocate the definition of risk to be changed from 'the chance of something happening that will have an impact on objectives' to 'the effect of uncertainty on objectives' (AS/NZS, 2009)

AS/NZS ISO 31000:2009 risk management-principles and guidelines has earmarked 11 principles for risk management and 5 attributes to enhance risk management (AS/NZS, 2009) Which are as follows:

- Good risk management contributes to the achievement of an agency's objectives through the continuous review of its processes and systems.
- Risk management needs to be integrated with an agency's governance framework and become a part of its planning processes, at both the operational and strategic level.
- The process of risk management assists decision makers to make informed choices, identify priorities and select the most appropriate action.
- By identifying potential risks, agencies can implement controls and treatments to maximize the chance of gain while minimizing the chance of loss.
- The process of risk management should be consistent across an agency to ensure efficiency, consistency and the reliability of results.
- To effectively manage risk it is important to understand and consider all available information relevant to an activity and to be aware that there may be limitations on that information. It is then important to understand how all this information informs the risk management process.
- An agency's risk management framework needs to include its risk profile, as well as take into consideration its internal and external operating environment.
- Risk management needs to recognize the contribution that people and culture have on achieving an agency's objectives.
- Engaging stakeholders, both internal and external,
- Throughout the risk management process recognizes that communication and consultation is key to identifying, analyzing and monitoring risk.
- The process of managing risk needs to be flexible. The challenging environment we operate in requires agencies to consider the context for managing risk as well as continuing to identify new risks that emerge, and make allowances for those risks that no longer exist.

Agencies with a mature risk management culture are those that have invested resources over time and are able to demonstrate the continual achievement of their objectives. (AS/NZS, 2009)

Five Attributes to enhance risk management range from organizations accepting the accountability for their risks to develop comprehensive controls and treatment strategies to continuous improvement in risk management through setting and review of performance goals, systems, resources and capability/ skills to ensure continuous improvement, to making individuals accountable for risk management, to inclusion of risk management considerations in decision making and last but not least frequent reporting of the entire risk scenario to all stakeholders (AS/NZS, 2009).

## 5. Approaches and Considerations in Information Security Risk Analysis

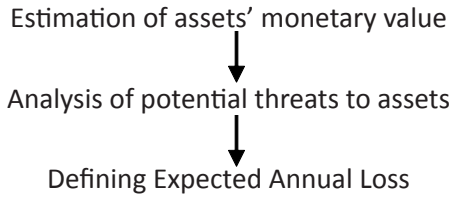
There are various approaches for analyzing risk which are as follows

- Quantitative risk analysis,
- Qualitative risk analysis,
- Valuation of IT/ information system assets,
- Selection of safeguards (Godbole, 2008)

Quantitative risk analysis deals with assigning independently the objective numeric values in monetary terms to the components of the risk assessment and to the assessment of potential losses. Qualitative risk analysis addresses intangible values, of a data/ information loss and its focus is on other issues, rather than on the pure hard costs.

Risk analysis process is considered fully quantitative when all the elements of the risk analysis (asset value, impact, threat frequency, effectiveness, costs of safeguards/countermeasures, etc.) are measured, rated and values are assigned to them.

Qualitative risk analysis process involves the following steps:




Qualitative risk assessment is based on assessing and ranking the seriousness of threats and the relative sensitivity of the assets, or a qualitative grading is provided to them, by using a scenario approach and creating an exposure rating scale for each scenario (Godbole, 2008).

## 6. Conclusion

It has been identified that information system security includes many concepts, facts and techniques. Various researchers and practitioners have defined and formulated the information security and IT risk policies in different ways to accomplish the objectives of securing the information assets in various kinds of organizations. There are a number of methods for information security but risk management should be given the highest priority due to its integration with Information System development. There is a need to address the way risk-based decision making

is applied in places that it may not improve the outcomes of the problems being addressed.

## References


AS/NZS ISO 31000: *2009 Risk Management Principles and Guidelines August 2010*.

Bagchi, K. & Udo, G. (2003). An Analysis of the Growth of Computer and Internet Security Breaches. *Communications of the Association for Information Systems*, *12*, 684–700.

Baskerville, R. L. (1988). *Designing Information Systems Security*. J. Wiley.

Baskerville, R. L. (1992). The Developmental Duality of Information Systems Security, *Journal of Management Systems*, *4*(1), 1–12.

Baskerville, R. (1993). Information systems security design methods: implications for information systems development. *ACM Computing Surveys (CSUR), 25*(4), 375–414. doi=10.1145/162124.162127. Retrieved from http://doi.acm.org/10.1145/162124.162127

BSI, (2004). *IT Grundschutz Manual*, http://www.bsi.de/english/gshb/manual/download/index.html

Chatzoglou, P. D., & Diamantidis, A. D. (2009). IT/IS implementation risks and their impact on firm performance. *The International Journal of Information Management*, *29*(2) 119–128.

doi=10.1016/j.ijinfomgt.2008.04.008, Retrieved from http://dx.doi.org/10.1016/j.ijinfomgt.2008.04.008

De Nederlandsche Bank. (2001 ). fiisk o nalysismanuol (407 11-407 l9).

Fitzgerald, K. J. (1995). Information security baselines. *Information Management & Computer Security, 3* (2), *8*–12.

Godbole, N. (2009). *Information Systems Security*. John Wiley & Sons

Hallikainen, P., Kivjarvi, H., & Nurmimaki, K. (2002). Evaluating strategic IT Investment: An assessment of investment alternatives for a Web content management system. *Proceedings of the 35th Hawii International conference on system sciences.*

Hallberg, N., Hallberg, J., & Hunstad, A. (2007). Rationale for and Capabilities of IT Security Assessment. *Proceedings of the 2007 IEEE Workshop on Information Assurance United States Military Academy, West Point*.

Hosseini, R. (2005). A Practical Approach for Measuring IT-Support of Business Processes. *Proceedings of the 2005, The Fifth International Conference on Computer and Information Technology (CIT'05) IEEE.*

Kankanhalli, A., Teo, H. H., Tan, B. C. Y., & Wei, K. K. (2003). An integrative study of information systems security effectiveness. *International Journal of Information Management*, *23*(2), 139–154.

Kempis, R. D., & Ringback, J. (1999). *Do IT Smart:Seven Rules for Superior Information Technology Performance.* New York: The Free Press, a Division of Simon & Schuster, Inc.

Ko. M., & Bryson, K. M. (2002). A regression tree based exploration of the impact of infomation technology investments on the firm level productivity. *ECIS 2002 Proceedings.*

Luftman, J. N., Lewis, P. R., & Oldach, S. H. (1993). Transforming the enterprise: The alignment of business and information technology strategies. *IBM Systems Journal, 32*(1), 198–221.

Morton, M.S. (1991). *The Corporation of the 1990s: Information Technology and Organizational Transformation.* Oxford University Press.

National lnstitute of Standards and Technology, (2002). *Risk management for information technology systems.* Technology Administration, US Department of Commerce, Special publication 800 30.

O'Donnell. E. (2005). Enterprise risk management: A systems-thinking framework for the event identification phase. *International journal of Accounting information Systems, 6*, 177–195.

Radianti, J., & Gonzalez, J. J. (2007). Understanding Hidden Information Security Threats: The Vulnerability Black Market. *Proceedings of the 40th Annual Hawaii International Conference on System Sciences (HICSS'07) IEEE.*

Saleh, M. S., & Alfantookh, A. (2011).A new comprehensive framework for enterprise information security risk management, *Applied Computing and Informatics*, *9*(2), 107–118.

Shao, B.B.M., & Lin, W.T. (2001). Measuring the value of information technology in technical efficiency with stochastic production frontiers. *Information and Software Technology, 43*(7) 447–456.

Siponen, M. T. (2005). An analysis of the traditional IS security approaches: implications for research and practice. *European Journal of Information Systems, 14(*3), 303–315. doi=10.1057/palgrave.ejis.3000537. Retrieved from http://dx.doi.org/10.1057/palgrave.ejis.3000537

Siponen, M. (2006). Information security standards focus on the existence of process, not its content. *Communications of the ACM-Music information retrieval CACM, 49*(8), 97–100. doi = 10.1145/1145287.1145316. Retrived from http://doi.acm.org/10.1145/114287.11453165

Siponen M. (2005). Analysis of modern IS security development approaches: towards the next generation of social and adaptable ISS methods. *Information and Organization, 15*(4), 339–375.

Solms, R. (1996), Information security management: The second generation, *Computers and Society, 15*(4), 281–288.

Steven, A. (2002). *Information Systems: Foundation of E-Business*, (4th ed.). Prentice-Hall lnc.

von Solms, R., & van de Haar, H. (2001). Trusted Information Security Controls to a Trusted Information Security Environment. *Sixteenth Annual Working Conference on Information Security*, 29–36, Beijing, China.