International Journal of Electrical Electronics & Computer Science Engineering
Special Issue - TeLMISR 2015, ISSN : 2348-2273
Available Online at www.ijeecse.com

Dynamic Issues in Managing and Mitigating IT Risks

B. Rajeswari, Nagamani Mutteni
Assistant Professor, Management Education & Research Institute, New Delhi
rajeswarim02@gmail.com, samyukthamutteni@gmail.com

Abstract: With increasing innovations in technologies, there is a plethora of information that flows across the world. Security of information has become a major question mark and the type of environment that people work in involves a lot of risks. IT risk management is all about discovering and measuring risks to information assets in an organization and taking necessary actions to eliminate or mitigate the effects caused by them. Thus information security plays an indispensable part of all the business operations across different domains. This research paper analyzes the details of information security risks that are faced by organizations. It also discusses certain dynamic issues that arise in managing IT related risks and emphasizes the need for risk assessment which can help a business recover from an IT incident. A checklist for IT risk assessment has been proposed which pins down the importance of information security management systems and policies in organizations to help them achieve good information security.

Keywords: Information security, C.I.A. Triad, Risk, Vulnerability, Information Security management system, IT incident response

I. INTRODUCTION

Information technology (IT) plays a critical role in almost all businesses. It is important for a business that makes use of IT to identify risks to its IT systems and data, reduce or manage those risks and develop a response plan in the event of an IT crisis. There are several legal obligations in relation to privacy, electronic transactions, and staff training that influence IT risk management strategies. It also emphasizes the need for risk assessment which can help a business recover from an IT incident. It is now important that we understand IT risks and know about the various ways to prepare for and respond to IT incidents. IT risks include hardware and software failure, human error, spam, viruses and malicious attacks, as well as natural disasters such as fires, cyclones or floods.

II. REVIEW OF LITERATURE

A. What is Information Security?: An organization's efficiency is determined by the information security level implemented in it because information is an asset. Having specific, relevant and correct information can make a massive difference. With the advent of new technologies, it is possible for information to be collected, shared, sold, exchanged and distributed without citation or notice to the owner. Therefore information security should become a natural phase in the daily activities of an organization. *"Information security relates to an array of actions designed to protect information and information systems"* (Gordon & Loeb, 2006). However, information security does not cover only the information itself but also the entire infrastructure that facilitates its use.

Information security in today's enterprise is a *"Well informed sense of assurance that the information risks and controls are in balance".* - Jim Anderson, Inovant (2002).

B. Information Security Attributes: Information Systems are composed in three main portions, hardware, software and communications with the purpose to help identify and apply information security industry standards, as mechanisms of protection and prevention, at three levels or layers: physical, personal and organizational. Essentially, procedures or policies are implemented to tell people (administrators, users and operators) how to use products to ensure information security within the organizations.

The C.I.A. triangle has been considered the industry standard for computer security since the development of the mainframe. It was solely based on three characteristics that described the utility of information: confidentiality, integrity, and availability. The C.I.A. triangle has expanded into a list of critical characteristics of information which include authenticity, accuracy, possession and utility.

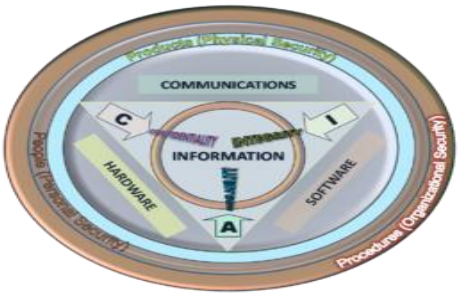

Fig.1 CIA Triad

C. Risk, Vulnerability and Threat: Risk is the likelihood that something bad will happen that causes harm to an informational asset (or the loss of the asset). A vulnerability is a weakness that could be used to endanger or cause harm to an informational asset. A threat is anything (manmade or act of nature) that has the potential to cause harm. Threats can be external (viruses, spam emails, hacking, etc.) or internal (unauthorised access to software, theft of hardware, human mistake, damage by displeased employee, etc.).

NIST (National Institute of Standards and Technology) has defined risk as "*The level of impact on organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring".*

D. IT Related Risk: NIST defines IT related risk as "*The net mission impact considering the probabilities that a particular threat-source will exercise (accidentally trigger or intentionally exploit) a particular information system vulnerability and the resulting impact if this should occur".*

IT related risks arise from legal liability or mission loss due to unauthorized (malicious or accidental) disclosure, modification, or destruction of information, unintentional errors and omissions or IT disruptions due to natural or man-made disasters or failure to exercise due care and diligence in the implementation and operation of the IT system.

ISACA (Information Systems Audit and Control Association) defines IT risk as "*The business risk associated with the use, ownership, operation, involvement, influence and adoption of IT within an enterprise".*

IT risk encompasses not just only the negative impact of operations and service delivery which can bring destruction or reduction of the value of the organization, but also the benefit/value enabling risk associated to missing opportunities to use technology to enhance business.

III. NATURE OF RISKS

A business that relies on information technology (IT) systems such as computers and networks for key business activities needs to be aware of the range and nature of risks to those systems.

A. General IT Threats: General threats to IT systems and data include:

- *Hardware and software failure:* such as power loss or data corruption
- *Malware:* malicious software designed to disrupt computer operation
- *Viruses:* computer code that can copy itself and spread from one computer to another, often disrupting computer operations
- *Spam, scams and phishing:* unsolicited email that seeks to fool people into revealing personal details or buying fraudulent goods
- *Human error:* incorrect data processing, careless data disposal, or accidental opening of infected email attachments.

B. Criminal IT Threats: Specific or targeted criminal threats to IT systems and data include:

- *Hackers*: people who illegally break into computer systems
- *Fraud:* using a computer to alter data for illegal benefit
- *Passwords theft:* often a target for malicious hackers
- *Denial-of-service:* online attacks that prevent website access for authorised users
- *Security breaches:* includes physical break-ins as well as online intrusion
- *Staff dishonesty*: theft of data or sensitive information, such as customer details.

C. Natural disasters and IT systems: Natural disasters such as fire, cyclone and floods also present risks to IT systems, data and infrastructure. Damage to buildings and computer hardware can result in loss or corruption of customer records/transactions.

IV. MANAGING IT RELATED RISKS

The Certified Information Systems Auditor (CISA) Review Manual 2006 provides the following definition of risk management: *"Risk management is the process of identifying vulnerabilities and threats to the information resources used by an organization in achieving business objectives, and deciding what countermeasures, if any, to take in reducing risk to an acceptable level, based on the value of the information resource to the organization".*

A. Risk Management Process: The risk management process consists of:

- *Identification of assets and estimating their value.* Include: people, buildings, hardware, software, data (electronic, print, other), supplies.
- *Conduct a threat assessment* include: Acts of nature, acts of war, accidents, malicious acts originating from inside or outside the organization.
- *Conduct a vulnerability assessment,* and for each vulnerability, calculate the probability that it will be exploited. Evaluate policies, procedures, standards, training, physical security, quality control, technical security.
- *Calculate the impact that each threat would have on each asset.* Use qualitative analysis or quantitative analysis.
- *Identify, select and implement appropriate controls.* Provide a proportional response. Consider productivity, cost effectiveness, and value of the asset.

- *Evaluate the effectiveness of the control measures.* Ensure the controls provide the required cost effective protection without discernible loss of productivity.

For any given risk, management can choose to accept the risk based upon the relative low value of the asset, the relative low frequency of occurrence, and the relative low impact on the business. Or, leadership may choose to mitigate the risk by selecting and implementing appropriate control measures to reduce the risk. In some cases, the risk can be transferred to another business by buying insurance or outsourcing to another business. The reality of some risks may be disputed. In such cases leadership may choose to deny the risk.

B. Legal Requirements: Awareness about the legal and legislative requirements is very important for business owners, such as the *Spam Act 2003*, the *Electronic Transactions (Qld) Act 2001* and privacy laws. Under the Spam Act 2003, it is illegal to send unsolicited commercial electronic messages. Information privacy or data protection laws prohibit the disclosure or misuse of information held on private individuals. Under the Electronic Transactions (Queensland) Act 2001 (ETA) there is a need for prior consent to send contract documentation by electronic means. If a contract is to be exchanged between parties by fax or email then consent must first be obtained from the recipient receiving the contract.

C. Business Continuity Planning: Having identified risks and likely business impacts, the development of a business continuity plan can help a business survive and recover from an IT crisis. A business continuity plan identifies critical business activities, risks, response plans and recovery procedures.

D. IT Risk Management Policies and Procedures: IT policies and procedures explain to staff, contractors and customers the importance of managing IT risks and may form part of your risk management and business continuity plans. Security policies and procedures can assist with staff training on issues such as:

- safe email use
- setting out processes for common tasks
- managing changes to IT systems
- responses to IT incidents

A code of conduct can provide staff and customers with clear direction and define acceptable behaviours in relation to key IT issues, such as protection of privacy and ethical conduct.

E. Information Security Management System: An information security management system (ISMS) is a set of policies concerned with information security management or IT related risks. The governing principle behind an ISM is that an organization should design, implement and maintain a coherent set of policies, processes and systems to manage risks to its information assets, thus ensuring acceptable levels of information security risk.

V. DYNAMIC ISSUES IN IT RELATED RISKS

There are many problems which lead to uncertainty in information security management systems. Some them are listed below:

A. Dynamically Changing Security Requirements of an Organization: Rapid technological development raises new security concerns for organizations. The existing security measures and requirements become obsolete as new vulnerabilities arise with the development in technology. To overcome this issue, the information security management system should organize and manage dynamically changing requirements and keep the system up-to-date.

B. Externalities Caused by a Security System: Externality is an economic concept for the effects borne by the party that is not directly involved in a transaction. Externalities could be positive or negative. The information security management system deployed in an organization may also cause externalities for other interacting systems which are uncertain and cannot be predetermined before it is deployed. The internalization of externalities caused by the information security management system is needed in order to benefit internalizing organizations and interacting partners by protecting them from vulnerable behaviors.

C. Obsolete evaluation of security concerns: The evaluations of security concerns used become obsolete as the technology progresses and new threats and vulnerabilities arise. The need for continuous security evaluation of organizational products, services, methods and technology is essential to maintain an effective information security management system. The evaluated security concerns need to be re-evaluated. A continuous security evaluation mechanism within the organization is a critical need to achieve information security objectives.

D. Awareness about the Technology Used To Support High Risk Business Areas: Understanding business operating environments is critical to understanding and developing strategies to mitigate information risk. This involves understanding whether high risk business areas are using cloud-based service offerings, BYOD (Bring Your Own Device), social media, personal storage networks, etc. Knowing the environments where high risk business is performed will help to plan and

implement strategies to mitigate specific information risks.

VI. Reducing Information Technology Risks

Threats and risks to information technology (IT) systems and data are an everyday reality for most modern businesses. An organization should put in place measures to protect their systems and data against theft and hackers.

A. Practical steps to improve IT security: To help protect IT systems and data, it is important to:

- Secure computers, servers and wireless networks
- Use anti-virus and anti-spyware protection, and firewalls
- Regularly update software to the latest versions
- Use data backups that include off-site or remote storage
- Secure passwords
- Train staff in IT policies and procedures
- Understand legal obligations for online business.

B. Create a Secure Online Presence: If the business has an online presence, then it is essential that the security of the website, email accounts, online banking accounts and social media profiles be assessed.

For example, secure socket layer (SSL) technology is used to encrypt transaction data and to send customer and card details to the acquiring bank for authorization. It should be ensured that any web hosting solution considered is capable of supporting the SSL protocol.

C. Induction and IT Training for Staff: Training new and existing staff in IT policies, procedures and codes of conduct is an important component of IT risk management strategies. Training can cover key business processes and policies, such as:

- Safe handling of infected email
- Protecting the privacy of customer details
- Priority actions in the event of an online security breach.

Providing support and training for new employees is a critical aspect of staff training.

D. Business insurance: It is impossible for a business to prevent or avoid all IT risks and threats. This makes business insurance an essential part of IT risk management and recovery planning. Regular review and update of insurance is mandatory, especially in light of new or emerging IT risks, such as the increasing use of personal mobile devices for workplace activities.

VII. Suggestions for Responding to an Information Technology Incident

Immediate and appropriate response to information technology (IT) incidents determines how well a business recovers, and also influences customers' ideas about reliability.

An IT incident can be confined to the IT components of the business, such as a denial of service attack that targets the business. An IT incident can also be part of a wider business crisis, such as widespread damage to networks due to natural disasters.

A. IT Risk Management Plan: The IT risk management plan and business continuity plan should include:

- IT incident response plans
- Emergency response plans
- Recovery plans

1) *IT Incident Response Plans:* IT incident response plans identify principal IT risks and the steps to be taken to mitigate effects or damage. They may include details of key staff who need to be notified, priority actions, communication plans, contact lists and an event log to record actions taken.

2) *Emergency Response Plans:* IT incidents may be the result of a wider crisis, such as an explosion, bushfire or flood. In any emergency situation the safety of staff and members of the public should be given first priority. An IT incident response plan should integrate with and support emergency response plans.

3) *IT Incident Recovery Plans:* A recovery plan will help to respond effectively if an IT incident or crisis affects the business. A recovery plan can shorten recovery times and minimize losses, and should include:

- Strategies to recover business activities in the quickest possible time
- A description of key resources, equipment and staff required to recover operations
- Recovery time objectives

B. IT Risk Management Checklist: It is important to understand the key steps to be taken to minimise IT risk. This IT risk management checklist helps to determine the basic precautions and steps to take in managing IT risk. Have you:

- Developed and implemented IT risk assessment plans?

- Developed, implemented and tested business continuity plans?
- Assessed IT security at the planning stage of new or changed IT systems?
- Discussed IT risks with system users?
- Conducted desktop or simulated IT incidents to assess the performance of incident planning, emergency response and recovery plans?
- Developed staff training resources with specific IT risk management focus?
- Installed and used firewalls and anti-virus software?
- Assessed the safety of online presence, including social media and security of online transactions?
- Understood and complied with relevant laws, legislation and industry guidelines?
- Kept software up to date?

If the answer is 'No' to any question, then it is necessary to create a list of actions to complete to ensure that the business can manage IT risk.

VIII. CONCLUSION

Providing information security is critical in managing risk in a business and in building and maintaining customer confidence and trust. Knowing the environments where high risk business is performed will help to plan and implement strategies to mitigate specific information risks. So, Information Security should be an integral part of the overall management of the organization related to and reflecting the organization's approach to risk management, the control objectives and controls and the degree of assurance required. It should be based on continuous training and awareness of staff. The risk management would be a never ending process to promote a broad corporate understanding of the high risk/high value information generated and needed by an organization. Change management strategies and training should be deployed to develop an organizational culture which values information management.

IX. REFERENCES

[1] Layton, Timothy P., (2007), Information Security: Design, Implementation, Measurement, and Compliance, Boca Raton, FL: Auerbach.

[2] Mark Stamp, Information Security: Principles and Practice, JohnWiley & Sons, Inc.

[3] McNab, Chris (2004), Network Security Assessment, Sebastopol, CA: O'Reilly

[4] http://en.wikipedia.org/wiki/Information_security

[5] Peltier, Thomas R. (2001). Information Security Risk Analysis, Boca Raton, FL: Auerbach.

[6] Dhillon, Gurpreet (2007). Principles of Information Systems Security: text and cases. NY: John Wiley & Sons.

[7] National Institute of Standards and Technology Special Publication 800-30, Risk Management Guide for Information Technology Systems (July 2002).