International Journal of Electrical Electronics & Computer Science Engineering
Special Issue - NCSCT-2018 | E-ISSN : 2348-2273 | P-ISSN : 2454-1222
March, 2018 | Available Online at www.ijeecse.com

Security and Risk: Information Risk Management

Ayush Bhaskar[1], Mona Supriya[2]
[1, 2]UG Scholar, Department of CSE, Poornima Institute of Engineering & Technology, Jaipur, Rajasthan, India

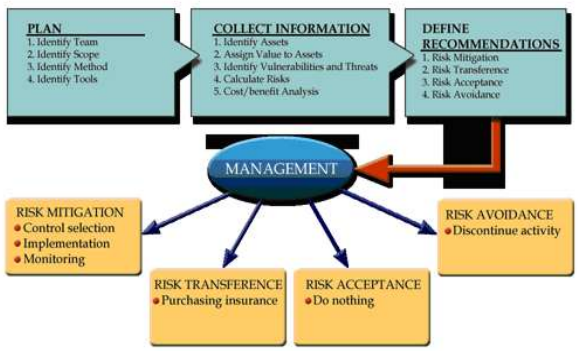
Abstract: ***In today's world, we people have very subtle information about frequency of occurrence of adverse events and about the seriousness of their consequences. And if that adverse event comprises of risk over a valuable information asset then it belongs to information risk management. Threats (risk) to sensitive and private information come in many different forms. Hence, information security processes and policies typically involve physical and digital security measures to protect data from unauthorized access, use, replication or destruction. So if someone wants to be secured with its privacy must deal effectively with the problem of information security.***
This paper presents a theory of information risk management that dominates most academic discussions of the subject.

Keywords: Component; Formatting; Style; Styling; Insert.

I. INTRODUCTION

Information Risk Management (IRM) solution offers a holistic approach to identify, aanalyze, report and remediate information risks. It leverages the Risk Insight platform to automate assessment activities and reduce cycle time. The solution consists of a comprehensive catalog of controls for specific information domains to address compliance and information risk management needs of organizations.

This brief will cover the various exposures that companies now face as they increasingly rely on twenty-first century technology. It will cover information in all forms and the new perils that put this information at risk. Classification of data into categories will determine the type and degree of risk. The types of processes and controls that firms can implement to minimize these risks will be examined. Within each section, targeted references and tips are provided for further insight. Finally, the paper will address the steps needed to react, respond, and remediate in the event of an untoward event. As a postscript, the paper will also cover the forms of insurance available to help alleviate the financial pain often associated with these types of events.



1) Information:

The facts provided and learned about something or someone is basically information. The value of information comes from characteristics it posses. When the characteristics of information change the value of information either increases or more commonly decreases.

Each critical characteristic of information that is, the expanded C.I.A. triangle is defined in the sections below.

Availability: This enables authorized users persons or computer systems to access information without interference or obstruction and to receive it in the required format.

Accuracy: Information has accuracy when it is free from mistakes or errors and it has the value that the end user expects. If information has been intentionally or unintentionally modified, it is no longer accurate.

Authenticity: Authenticity of information is the quality or state of being genuine or original, rather than a reproduction or fabrication. Information is authentic when it is in the same state in which it was created, placed, stored, or transferred.

Confidentiality: Information has confidentiality when it is protected from disclosure or exposure to unauthorized individuals or systems. It also ensures that only those with the rights and privileges to access information are able to do so. When unauthorized individuals or systems can view information, confidentiality is breached.

Integrity: Information has integrity when it is whole, complete, and uncorrupted. The integrity of information is threatened when the information is exposed to corruption damage, destruction, or other disruption of its authentic state. Corruption can occur while information is being stored or transmitted.

A key method for detecting a virus is to look for changes in file integrity as shown by the size of the file. Another key method of assuring information integrity is file hashing, in which a file is read by a special algorithm that uses the value of the bits in the file to compute a single large number called a hash value. The hash value for any combination of bits is unique.

Risk: The probability that something unwanted or undesired will happen to information.

Security: Anything that is secured or out of danger or being secured from adverse effect either intentionally or otherwise.

II. IDENTIFICATION YOUR RISK

The first step to mitigating risks is identifying what these could be. The top three supply chain risks for any global organisation are:

Inventory Risk:

This is one of the biggest risks, and is often the result of a mismatch in projections and actual market demand. Maintaining excess inventory can become a liability and put a strain on one's finances. An inventory risk can also come from failing to predict a high probability of internal or external triggers of disruption in the supply chain.

*Procurement Risk**:***

Factors in this category include unpredictable natural events, which can create shortages and increase the cost of acquiring raw materials, and fluctuating exchange rates or supplier price hikes, which can dramatically raise costs.

*Financial Risk**:***

Having your working capital tied up in languishing inventory and slow moving receivables can increase the cost of your supply chain. The ProfitPoint, Supply Chain Survey Report 2012 found that globally only 70 percent of SCM experts are able to estimate their supply chain costs accurately.

Advantages or Benefits of Risk Management Process:

- Risk management process is considered as an important discipline that the business has in its recent times.
- Many organizations tend to realize the benefits of risk management strategy. Following are few advantages of risk management policy.

Following are the few advantages of risk management policy

Identification of Possible Threats: This identification provides compensatory mundane activities that aim at motivating the employees to gather information about the consequent changes. It spends time on the research and development of the execution of maintenance strategies. It accustoms the employees within the persuaded timing.

Identification of Risks: Risk management system helps in identifying the risks that have precise network to determine the optimal management of risks. It has the maximized opportunity of the risks that are relevant in implementing the guidance provided. It has holistic support from the entire organization when the risks are identified. It will become streamlined and efficient within the complex elements.

Reduces Impact and Loss: Risk management has more defined proceedings when there is pre-planned schedule or loss of the object. It contributes a part to stress and worry. The complexity matters when they are gathered. Here it endures the organization with all possible outcomes of the independent and objective assessments that are analyzed on taking challenges.

Minimization of Risks: The risks that are handled within the given assessments plans are foreseen within the business functions. It enables one to speed up the data to change policies and contingencies that are made successful within the mapped business functions. Here the cost beneficial analysis is to be revised within the ownership of risks. It focuses on change of policies within the detailed structural behaviour.

Awareness About the Risks: Here the terms that are noticed will create awareness among the scheduled terms of risks that are a successful analysis and evaluation of exercising the modules of risks. It enables one to concentrate on the risk treatments within the lessons learnt and are scheduled into lack of preparation. It has subsequent phases regarding each module within the identified data.

Disadvantages of Risk Management Process:

Managing the risks provides the waste of time to compensate the projects. It persuades the projects that reciprocate to improve the funds in the company. It is spent on the research and development of the allocated issues that holds to ensure project management.

Complex Calculations: Risk management involves complex calculations in terms of managing risks. Without the automatic tool each and every calculation regarding risks becomes difficult. It involves the ideal data that contributes to the employees standards. This process is really difficult to predict.

Unmanaged Losses: If the organization is meddled with loss, then that pay will be delivered to the pay loss of the firm. Here, the organization is responsible for the loss that happened due to improper schedule about the risk management.

Ambiguity: Even if the ambiguity is out of loss then people has to cover it within the planned scale of losses of the discounts and even the consideration into unnecessary insurance discounts.

Depends on External Entities: Managing risks depends on the external entities that are modulated within the organization, usually depends on the external data. It includes all the dependent information about the risks regarding other valid resources. The transferable resources depend on the external entities that are tend to have data.

Mitigation: Usually mitigation guarantees losses of the concealed impairment of money which may cause improper management of risks. This leads to unsafe acceptance of data within rare company losses.

Factors Analysis of Information Risk (FAIR):

- Founded in 2005 by Risk Management Insight LLC – Jack Jones
- The basis of the creation of FAIR is "result of information security being practiced as an art rather than a science."
- It can help organizations understand, analyze, and measure information risk according to Whitman & Mattord (2013).
- FAIR is not another methodology to deal with risk management, but it complements existing methodologies.
- FAIR is not in direct competition with the other risk assessment frameworks, but actually is complementary to many of them.

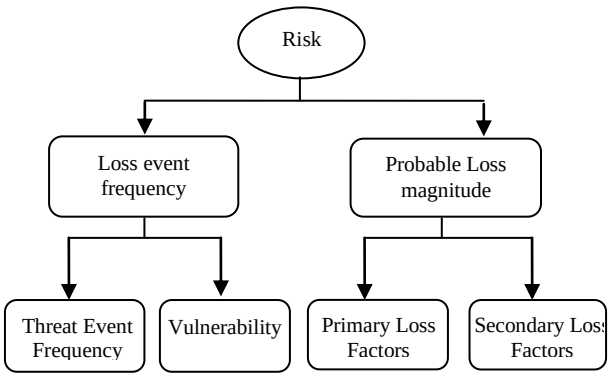
FAIR defines value /liability as:

a) Criticality

b) Cost

c) Sensitivity

Fig. 1. FAIR (Factors Analysis of Information Risk)



III. SECURITY AS SCIENCE

Technology developed by computer scientists and engineers - which is designed for rigorous performance levels - makes information security a science as well as an art. Most scientists agree that specific conditions cause virtually all actions in computer systems. Almost every fault, security hole, and systems malfunction is a result of the interaction of specific hardware and software. If the developers had sufficient time, they could resolve and eliminate these faults. The faults that remain are usually the result of technology malfunctioning for any one of a thousand possible reasons. There are many sources of recognized and approved security methods and techniques that provide sound technical security advice. Best practices, standards of due care, and other tried-and-true methods can minimize the level of guesswork necessary to secure an organization's information and systems.

IV. EMERGING SECURITY TECHNOLOGIES

Surveys of security technologies indicate that most organizations use security technologies such as firewalls, anti-virus software, some kind of physical security to protect their computer and information assets or some measures of access control (Richardson, 2003).Technologies such as virtual private networks (Zeng & Ansari, 2003) and biometrics using a fingerprint are predicted to grow very fast, and others are still emerging. The newest version of an intrusion detection system based on open-source Snort 2.0 supports a high-performance multi-pattern search engine with an anti-denial of service strategy (Norton & Roelker, 2003). However, detecting distributed denial-of-service (DDoS) is still emerging due to the complexity of technical problems not known to build defenses against this type of attack. Current technologies are not efficient for large-scale attacks, and comprehensive solutions should include attack prevention and preemption, attack detection and filtering, and attack source trace back and identification (Chang, 2002).

In addition, new protocols are defined and old protocols are enhanced. One example is IP security protocol (IPSec) defined by IETF. IPSec protocol is implemented for new IPv6 services in the very high-broadband-speed networks for new-generation Internet applications (Adam, Fillinger, Astic, Lahmadi & Brigant, 2004). In the near future, the network environment is expected to include hosts that support IPv4 and IPv6 protocols (Tatipamula, Grosette & Esaki, 2004), and new tools are needed for network administrators.

Other trends include integration of information security with physical security (Hamilton, 2003), self-securing devices and sensor networks. Self-securing devices offer new capabilities for dealing with intrusions, such as preventing undetectable tampering and deletion. If the detection mechanism discovers a change, an alert is sent to the network administrator for action (Cummings, 2002). Sensor networks are essential to the creation of smart spaces, which embed information technology in

everyday home and work environments (Marculescu, Marculescu, Sungmee & Jayraman, 2003; Ashok & Agrawal, 2003). The privacy and security issues posed by sensor networks and sensor detectors represent a rich field of research problems (Chan & Perrig, 2003).

Within the past years, a new security market has emerged, known as Security Event Management (SEM), which is part of Security Incident Management. SEM includes the processes that an organization uses to ensure the collection, security and analysis of security events as well as notification and response to security events. Although limited on capabilities, new products based on solutions for SEM are emerging slowly. The new products lack the prevention capability and still rely on human expertise to make decisions, or require substantial manual configurations up front. Data mining and other techniques for extracting coherent patterns of information from a call are near the top of the research agenda. For example, focusing on telephone calls from a particular installation, searching for specific words and phrases in e-mails, or using voice recognition techniques all are deployed. Cell and satellite phones can also reveal a caller's location (Wallich, 2003). The following section discusses issues and solutions for information security management.

V. CONCLUSION

Security event management solutions are needed to integrate threat data from various security and network products to discard false alarms, correlate events from multiple sources and identify significant events to reduce unmanaged risks and improve operational security efficiency. There is a need for increased use of automated tools to predict the occurrence of security attacks. Auditing and intelligent reporting mechanisms must support security assessment and threat management at a larger scale and in correlation with the past, current and future events.

VI. REFERENCES

[1] http://encyclopedia.jrank.org/articles/pages/6625/Information-Security-Management.html.

[2] http://www.fairinstitute.org.

[3] Information Security is Information Risk Management, By- Bob Blakley Tivoli Systems, Inc. Blakley @ us, ibm.com, Ellen McDermott J. P. Morgan Chase, Dan Geer @ Stake.

[4] SANS Institute InfoSec Reading Room, John Wurzler, john.wurzler@gmail.com, Advisor: Rick Wanne Accepted April 23, 2013.

[5] Risk Management Guide for Information Technology Systems , Gary Stoneburner, Alice Goguen1, and Alexis Feringa1 , July, 2012.