International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 5 Issue 1, November-December 2020 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Risk Management

Dr. C. Umarani[1], Shriniketh D[2]

[1]Associate Professor, [2]Student,
[1,2]Masters in Computer Applications, Jain (Deemed-to-be) University, Bangalore, Karnataka, India

ABSTRACT

Risk management is one of the main concepts that have been used by most of the organisations to protect their assets and data.

One such example would be INSURANCE. Most of the insurance like Life, Health, and Auto etc have been formulated to help people protect their assets against losses.

Risk management has also extended its roots to physical devices, such as locks and doors to protect homes and automobiles, password protected vaults to protect money and jewels, police, fire, security to protect against other physical risks.

Keywords: *RISK MANAGEMENT, CYBER FORENSICS*

How to cite this paper: Dr. C. Umarani | Shriniketh D "Risk Management" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-5 | Issue-1, December 2020, pp.361-363, URL: www.ijtsrd.com/papers/ijtsrd37916.pdf

IJTSRD37916

What is cyber security risk management?

When it comes to real world doors, locks and vaults are used whereas IT departments depend on a combination of strategies, policies and procedures.

Employees are educated about the technologies and vulnerabilities in order to protect the organisation against cyber security attacks that can compromise systems.

There is a linear growth in cyber attacks as well as cyber security risk management systems.

Organisations hire employees well versed in the field of information security and form a team cyber security incident response management team.

The idea of cyber security risk management comes from real world risk management which is then applied in cyber world.

Identifying risks and vulnerabilities, applying administrative actions and comprehensive solutions are all involved in cyber security risk management system.

Implementation of Risk Management System:

Prior to the setting up of the cyber security risk management system, the organisation needs to list the assets it needs to protect and prioritise it.

The technology, infrastructures and the potential risks differ from organization to organisation.

Most financial services firms and healthcare organizations have regulatory concerns along with the business concerns in parallel that need to be addressed in a cyber security risk management system.

It is important to follow a layered structure when it comes to cyber security with additional security for other important assets like customer data and corporate data.

It is important to keep the organisation clean and maintain the reputation as reputational harm from a breach can cause more damage than the breach itself.

Citrix recommends that organizations have fully documented and implemented procedures for all activities which create cyber security risks.

Risk Management Process:

Before we go on with risk management process, it is important to understand the severity of risk and then determine the solution.

No system is 100% secure if anybody wants to make their system 100% secure then it has to be inaccessible by a means, which is practically impossible. If at all the system is locked down, it becomes harder for authorised personnel to conduct business. If authorised people cannot find the data and information that they require to conduct their business, they may look for alternatives which may compromise systems.

There are a few recommendations by Deloitte which the risk management process follows the Capability Maturity Model. This approach has 5 steps in it:

- Initial
- Repeatable
- Defined
- Managed
- Optimizing

If network systems are connected in a way that intrusion into an unimportant area can provide an unauthorized entry into more important systems and more sensitive data, then even a small risk can be the reason for huge losses.

RISK MITIGATION:

The following points should be kept in mind in order to mitigate the risk:

- The devices with internet access should be limited.
- Network Access Control should be installed properly.
- The number of people with administrator credentials and access control rights for each admin should be restricted.
- Operating systems should be automatically patched.

Older operating systems should be restricted or limited as they do not have security patches that are up-to-date.

- Firewalls should be installed.
- Security patches should be up-to-date and antivirus programs should be installed.
- Two-factor authentication should be setup in order to gain access to certain confidential files and systems.
- Current IT governance structure should be evaluated in order to ensure the checks and balances throughout the organisation and system.

Apart from the above recommendations, there are a few more recommendations for enhanced risk management.

Advanced Encryption:

Encryption has been a very old feature in databases, but in the present world and IT scenarios. It is important to implement encryption in a more strategic and systematic way to protect data from data breach.Granular role-based access, standards-based cryptography, advanced key management etc. are all included in advanced encryption. These methods and algorithms decrease exposure of data to a great extent. Encryption is helpful in protecting against outside breaches but it doesn't help in internal data theft. If the employees within an organisation have access to sensitive data then they will definitely have the credentials to decrypt it. Hence the access to sensitive data should be limited to very few and authorised personnel.

Element-level security:

It is important for companies to implement custom as well as out-of-the-box rules as security at every level and in each and every element is very necessary and important.

INCIDENT RESPONSE:

The approach to addressing and managing the after effects of the security breach or an IT incident is known as incident response. Its main goal is to manage the situation in such a way that the damage is limited and the recovery time and costs is reduced. All the activities and actions of the incident response management is performed by an organisation's computer security incident response team.

INCIDENT RESPONSE PLAN:

This is the methodology used by an organization to respond and resolve a cyber attack.

an attack to the organisation can affect its customers, company time and its resources and its reputation and brand value.

PHASES OF AN IRP:

- Preparation: This is the first phase of an IRP is preparation where the policies and procedures are developed to follow in the course of a cyber breach.
- Identification: This is the phase where the breach is detected and the response is quick and focused.
- Containment: This step involves in analysing the damage and stopping the attack from further penetration.
- Eradication: The threat is neutralized and internal systems are restored.
- Recovery: The affected systems should be validated and should be returned to working condition.
- Lessons learned: The future possible threats are analysed and preventive measures are taken.

Incident Prevention:

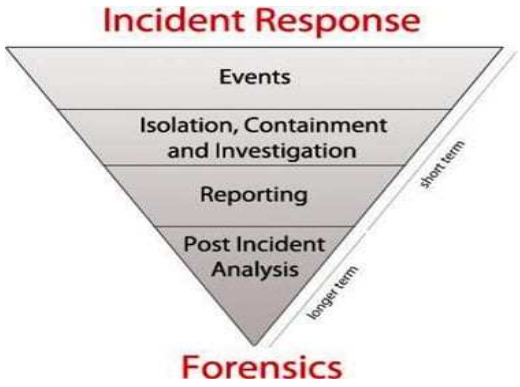
- Educate employees in cyber security principles.
- Physical access to computers and network components should be controlled.
- Change passwords regularly.
- Firewall should be setup.
- Keep the security software up-to-date.

CYBER FORENSICS

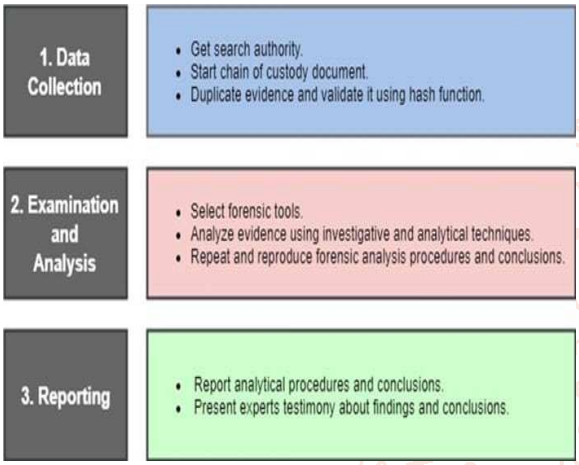
- Cyber/Computer forensics is the method or technique of analysing ways to gather and preserve evidences and later present it to the court of law.
- Most of the cyber forensics' specialists/analysists make use oftheir knowledge in computer science and forensic skills in order to retrieve information from the computer or storage devices that have been ceased in the particular case during investigation.
- One of the major and the most important steps for forensic investigation is the FORENSIC IMAGING where in the investigator takes an exact copy of the original evidence before moving on with the investigation and extraction of data from the evidence or media.

ROLE OF CYBER FORENSICS IN RISK MANAGEMENT:

- In the occurrence of an incident like a breach or a natural disaster, the Incident Response Team acts based on a predefined set of rules.
- Here, the application of computer forensics plays an important role in permitting in-depth analysis of all the evidence gathered by the incident response team.
- Most of the times forensic analysis occurs in the later stages of the operations headed by the IRT and hence is a vital part of the Post Incident Analysis.



- Digital forensics is mainly focused in understanding the end result of a digital incident and hence represents the tip of the pyramid which is the life cycle of a security incident.
- Within the Post Incident Analysis phase a few standard process techniques have made an important place:



CONCLUSION:

Department of Energy project directors, program managers, and senior managers have the responsibility to assess and manage risks on their projects and project portfolios. Project risks can be managed to successful conclusions through the following basic actions:

- Establish and maintain management commitment to performing risk management on all capital projects.
- Start the risk management process early in the project life cycle—prior to approval of mission need.
- Include key stakeholders in the process, with the DOE project director as the lead and the integrated project team (IPT) intimately involved in the process.
- Evaluate project risks and risk responses periodically during the project life cycle through approval of the start of operations.
- Develop risk mitigation plans and update them as the project progresses.
- Follow through with mitigation actions until risks are acceptable.
- Tie a project's level of risk to cost and schedule estimates and contingencies.
- Effectively communicate to all key stakeholders the progress and changes to project risks and mitigation plans.

An example of a risk assessment tool that uses some of the risk assessment methods discussed in this report is the Construction Industry.

REFERENCES:

[1] **Risk management system for ERP software project**
2013 Science and Information Conference
Year: 2013 | Conference Paper

[2] **Management of Complex Project Risks Based on Qualitative Assessments**
International Conference "Management of large-scale system development" (MLSD
Year: 2018 | Conference Paper

[3] **A Study of Software Development Project Risk Management**
International Seminar on Future Information Technology and Management Engineering
Year: 2008 | Conference Paper

[4] **Optimal Risk Response plan of project risk management**
IEEE International Conference on Industrial Engineering and Engineering Management
Year: 2011 | Conference Paper