iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 8 **Issue:** V **Month of publication:** May 2020

DOI: http://doi.org/10.22214/ijraset.2020.5468

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue V May 2020- Available at www.ijraset.com

Information Security

Saurav Kaushik[1], Mansukh Singh[2], Amit Chugh[3]
[1, 2, 3]*Manav Rachna University, India*

Abstract: Information is a valuable asset. Information includes both in electronic and physical forms such as paper, video or knowledge .With the development of the network and information technology, information security has become the key of information technology in 21st century. Today we are living in "Information world" because information is present everywhere and it's so important for us. If we are in education world or business world then we all want the required information is it's "security". If we want to handling and doing any work we always want to updated according to current scenario. So first of all we have to check that the information is wrong or not and the information is totally secure
Keywords: Information, security, Information security, Information protection, Information safety, CIA traid

I. INTRODUCTION

Information is a valuable asset. A number and practices have attempted to define security in various ways. Security based on computer system perspective is a branch of technology known as information security as applied to computers and networks. Thus Information Security spans so many research areas like Cryptography, Online Social Media etc.
Security is "The quality or state of being secure that is to be free from danger." It means to be protected organization should have following layers of security-:

1) *Physical Security:* To protect the physical items or areas of an organisation from unauthorised
2) *Personal Security:* To protect the individual or group of individuals who are authorised to access it's operations
3) *Operations Security:* To protect the details of a particular operations
4) *Communication Security:* To protect an organisation's communications media and content
5) *Network Security:* To protect networking components and content
6) *Information Security:* To protect of information and it's critical element, including hardware

II. DEFINITION OF INFORMATION SECURITY

According to Merriam Webster Dictionary, security in general is the quality or state of being secure. According to Oxford Students Dictionary Advanced, in a more operational sense. According to Whitman and Mattord, information security is the protection of information and its critical elements, including the systems
The information security performs four important functions for an organisation which enables the safe operation of application implement. The information security also enables the safe operation of application implemented on the organisation will apply or install the appropriate software that will secure the data such as antivirus and other protected app.
Information Security programs are built around 3 objectives, commonly known as CIA – *Confidentiality, Integrity, Availability.*

Every objective has their threat sources and counter measures.

A. *Confidentiality*

Confidentiality means dislocation of information to unauthorized individuals, entities and process. The level of secrecy should prevail while data resides on systems.

1) *Threat Sources*
a) Shoulder Surfing
b) Stealing password files
c) Network monitoring
2) *Counter Measures*
a) Use of network padding
b) Training personnel on proper procedures.
c) Encrypting data

B. Integrity

means maintaining accuracy and completeness of data. Integrity of data is protected when the accuracy and reliability of information is provided.

1) Threat Sources

a) Viruses

b) Logic bombs

2) Counter Measures

a) Hashing

b) Intrusion detection

c) Strict Access Control

C. Availability

Availability means availability of information when there is need of it. It ensures reliability and timely access to data and resources to the person who is authorized.

1) Threat Sources

a) Devices or software failure.

b) Denial of services attacks.

2) Counter Measures

a) Maintains backups for replacing the failed system.

b) Using certain firewall and router configuration.

III. CRYPTOGRAPHY

It also plays an important role in protecting data which is also called "Art of Secret writing" and the efforts done by hackers to break Cryptography is known as cryptanalysis.

Two methods of Cryptography are:

1) *Encryption:* Encryption is defined as the conversion of some data to symbol or code so that its content cannot be understood that is plain text to cipher text
2) *Description:* The conversion of encrypted data into its original form is called decryption. Generally it refers to the reverse process of encryption

A. Objective of Cryptography

1) To provide integrity

2) To provide confidentiality

3) To provide authentication

4) To provide authorization

5) To provide non reputation

IV. INFORMATION SECURITY AWARENESS:

Security awareness refers to which employees are able to prevent and access information security incidents. In addition, the sense of responsibility that employees have information security is necessary. Other terms for consciousness', cyber awareness and information awareness.

Information security happenings which are caused by humans are more than 60%. People lose their USB flash drive, click on phishing links or share information with unknown or unauthorized people. By escalating security awareness and raising desired behaviour, employees will become the strongest link and function as a human firewall. These incidents can make your organisation unsafe to cyber threats and security occurrences.

A clear policy and kosher technology are nor adequate. Employees have to become aware of their authority with regard to information security and – more notably- act accordingly. Employees can make big difference when it comes to the information security of your organization. Producing awareness is not a one-off effort. It requires Organizational attempt. It is advisable to give continuous attention to security awareness as over the time, the awareness of employee will weaken.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.429
Volume 8 Issue V May 2020- Available at www.ijraset.com

V. INFORMATION SECURITY MANAGEMENT

Security management recommendation participates an integrate role in governing organizational information security. An Information security management is a set of approaches and procedures for systematically supervising an organization's susceptible data. The objective of an ISM is to reduce risk and verify business progression by pro-actively minimising the effect of security breach. ISO 27001 is identification for creating ISMS. It does not warrant specific actions, but includes insinuation for documentations, internal audits, continual development and corrective action.

Information security management typically marks employee actions and operates date and technology. It can be instrumented in a comprehensive way that become part of the organisation's culture and targeted towards a specific type of data such as customer data.

VI. INFORMATION SECURITY GOVERNANCE

Many companies at present have many of the parts to a security programs (firewalls, security teams etc.) but the management is not fully involved and security has not perfused throughout the organisation.

If security was only the technology issue, then this security team could suitably install, configure and maintain the products and the organization would get a gold rated and progress the required audits with flying colours. Alternatively, the parts are the responsibility of a minor security team that is imposed to ensure that security happens properly throughout the entire company-which is near to impossible. As a security personal, you should understand that security must be applicable throughout the company and having various points of answerability is critical.

Information security governance is a logical system of merged security programmes and policies that exist to make sure that the company survives and hopefully bloom. ISG is same in nature to corporate and IT governance because there is lap-jointed functionality and aim between the three. All three work within an company and have the same objective which makes sure that organization will survive and thrive.

VII. INFORMATION SECURITY POLICY:

ISP is a set of rules by an organisation to ensure that all the employees or users of this organisation should follow all the prescriptions regarding the security. It should cover all software, hardware, information/data , access control, etc… with its scope . It should reflect risk connected with any organisation that it is looking for.. The goal while we are writing information security policy is to provide direction and value to the employees within an organization. There are many elements of great Security policy like:

A. Reflection of reality on the ground
B. Should be simple to understand. Security policies should be in this way that anyone can understand it
C. Should be measured
D. Less consequences should be there

A security policy is a type of document that contains the confidential data for the company or organisation. The main purpose of Security is to keep you , your family , your data , your organization , your properties safe from burglaries, theft and many other crime. Many organizations feels that the employees, who have the had link in information security, can also be great employees in the effort to reduce information security . Since employees who obey with the security rules and regulations of the organization are the key to strengthen the information security.

There are some good Security questions produces and answers that are:

1) Safe? Which cannot be answered, guessed or researched
2) Stable? This doesn't change with time
3) Memorial? Can be remembered
4) Simple? It is precise and simple
5) Many? Can has many possibilities

VIII. INFORMATION SECURITY RISK MANAGEMENT :

ISRM is the process of managing risks connected with one organization with use of information technology. It can involve identifying and how to tackle any risk associated with the organisation. It is type of technique which focuses Security efforts on some system and along with that risk analysis makes it possible to analyse any type of risk that can be in the form of treat to any organization we are connected too. There are some steps of ISRM(Information security risk management):

1) Step 1. Identifying the risk
2) Step 2. Analyse that risk
3) Step 3. Rank the risk associated with the organisation
4) Step 4. How to treat a risk
5) Step 5. Review the risk

Risk is defined as loss or damage when some threat exploits vulnerability. For example- financial loss, loss of password, privacy, hack any system, etc. Four more steps are there to monitor project risks:

1) There are some response plans for each risks
2) Track identification risks
3) Identifying and analysing new risks
4) Evaluate the risks

In the world of permanent cyber-attacks, risk management is becoming a very important and crucial task for minimization of risks . The possibility of using the approach for an external insurance based on the quantified risk analyses is also provided.

IX. INFORMATION SECURITY CHALLENGES

There are some challenges in our daily changing environment that makes it difficult to secure the data and thus security challenges and breaches increasing time by time. Lacking in information security accepting makes the employees in an organisation not protect the information. This may put the confidential information in risk. Many companies either haven't enforced their policies in past. This makes many group writes the information policies but does not applied it. Information security is not just a simple of having usernames and passwords. Actually Information security becomes a very important part for the organization‟ s assets. The hazard of this action is, the information may be can access by other person from other organisation, such as information security breaches survey. One of the challenges faced in an organisation is the lack of understanding of information security. When employees is lack of information security knowledge in term of keeping organization's information than it is so easy to target and being attacked by hackers.

X. CONCLUSION

As a conclusion, Information security is importance to the development of an organisation that keep the data of an organisation about their customers or company. The development of modern organisations depends upon the availability, confidentiality and integrity to ensure the security. Other than that, the extensive use of information technology had improves the efficiency if the business, but the exposes the organisation to additional risks and challenges such as failure to understand about information technology, mobile workforce or wireless computing, shortage of information security staff and information security attacks. The implementation of the information security is a process that is by far more complex than the implementation of the other management due to the large number of factors that may affect its effectiveness. To ensure information security, the organisation should understand that information security is not solely a technological issue. The organisation should also consider the non-technical aspect of information security while developing the information security. Besides, it should be noted that, well implemented information security in organisation has the ability to reduce the risks of crisis in the organisation.

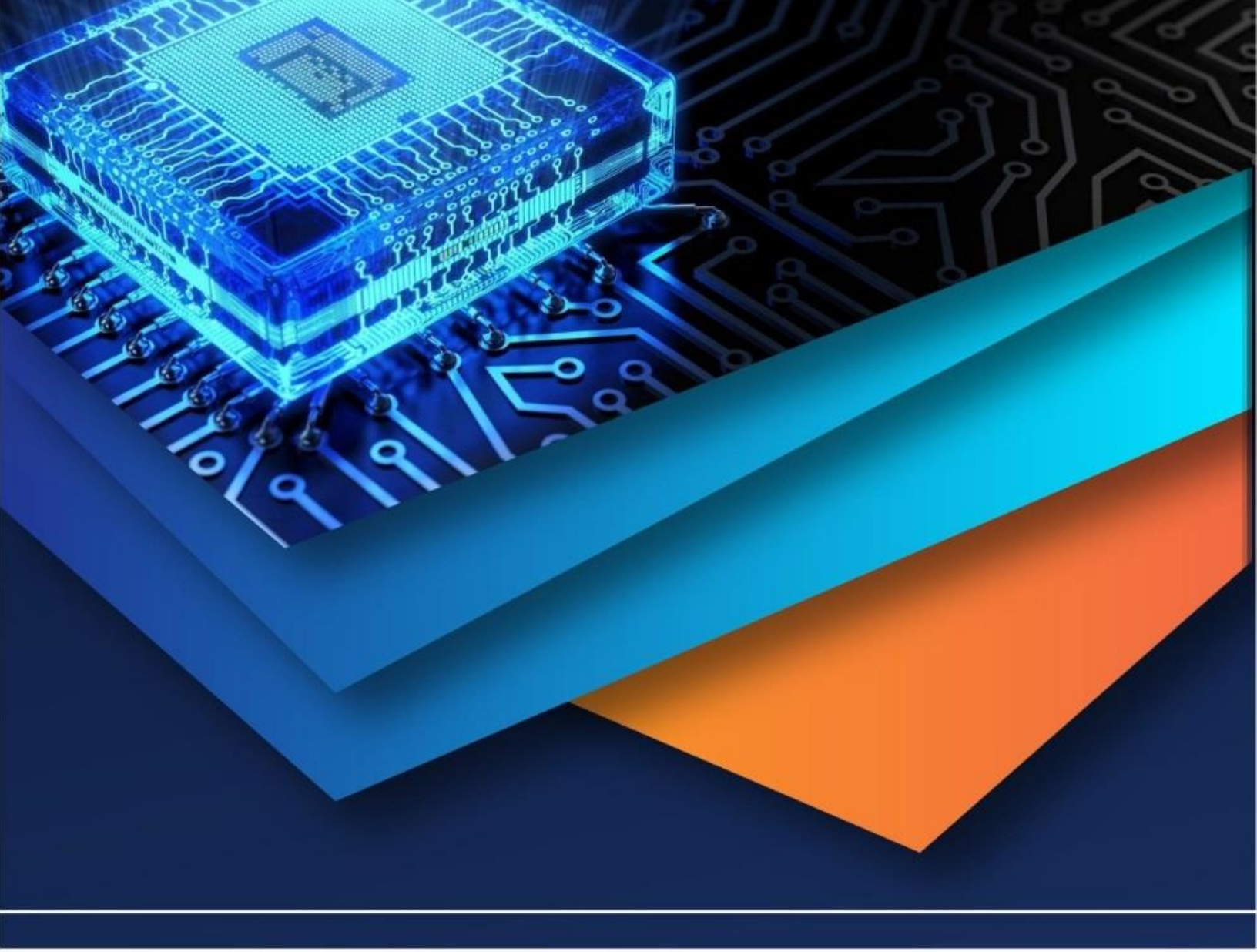
Other than that, information security management committee play an integral part in the successful of information security implementation in organisation. Organization should emphasize the formation of this committee to ensure that the implementation of information security in the organisations achieve the organisation's goals.

Besides, the written policies about information security are also essential to as secure organisation. Everyone in a company needs to understand the importance of the role they play in maintaining security. The way to accomplish the importance of information security in an organisation is also has made a great effort in implementing the information security in an organisation. Information security in an organization.

REFERENCES

[1] https://safecomputing.umich.edu/protect-the-u/protect-your-unit/information-security-risk-management
[2] https://dcvizcayno.wordpress.com/2012/02/16/what-is-information-security-governance/
[3] https://whatis.techtarget.com/definition/information-security-management-system-ISMS
[4] https://www.nexttech.nl/en/security-awareness/
[5] https://www.essaysauce.com/information-technology-essays/essay-importance-of-information-security-in-an-organisation/
[6] https://www.paloaltonetworks.com/cyberpedia/what-is-an-it-security-policy

[7] .Choobineh, Joobin; Dhillon, Gurpreet; Grimaila, Michael R.; and Rees, Jackie (2007) "Management of Information Security: Challenges and Research Directions," Communications of the Association for Information Systems: Vol. 20 , Article 57. DOI: 10.17705/1CAIS.02057 Available at: https://aisel.aisnet.org/cais/vol20/iss1/57
[8] Consumer Affairs. (2005). "Latest Security Breach Exposes 40 Million Credit Card Accounts to Potential Fraud," ConsumerAffairs.com, http://www.consumeraffairs.com/news04/2005/cardsystems.html
[9] Baskerville, R. (1988). Designing Information Systems Security. New York: John Wiley & Sons.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY