Vulnerability in Information Technology and Computing- A Study in Technological Information Assurance

P. K. Paul[1], A. Bhuimali[2], P. S. Aithal[3], & R. Rajesh[4]

[1]Executive Director, MCIS, Department of CIS, Raiganj University (RGU), West Bengal, India
[2]Vice Chancellor, Raiganj University, West Bengal, India
[3]Vice Chancellor, Srinivas University, Karnataka, India
[4]Principal, Rohini College of Engineering and Technology, TN, India
Corresponding Author: pkpaul.infotech@gmail.com

Area/Section: Computer Science.
Type of the Paper: Research Paper.
Type of Review: Peer Reviewed.
Indexed in: OpenAIRE.
DOI: http://doi.org/10.5281/zenodo.3544141.
Google Scholar Citation: IJMTS

How to Cite this Paper:
Paul, P. K., Bhuimali, A., Aithal, P. S., & Rajesh, R. (2019). Vulnerability in Information Technology and Computing- A Study in Technological Information Assurance. *International Journal of Management, Technology, and Social Sciences (IJMTS), 4*(2), 87-94. DOI:http://doi.org/10.5281/zenodo.3544141.

International Journal of Management, Technology, and Social Sciences (IJMTS)
A Refereed International Journal of Srinivas University, India.
IFSIJ Journal Impact Factor for 2018 = 4.764

Vulnerability in Information Technology and Computing- A Study in Technological Information Assurance

P. K. Paul[1], A. Bhuimali[2], P. S. Aithal[3], & R. Rajesh[4]

[1]Executive Director, MCIS, Department of CIS, Raiganj University (RGU), West Bengal, India

[2]Vice Chancellor, Raiganj University, West Bengal, India

[3]Vice Chancellor, Srinivas University, Karnataka, India

[4]Principal, Rohini College of Engineering and Technology, TN, India

Corresponding Author: pkpaul.infotech@gmail.com

ABSTRACT

Information Assurance is the prime name for the security and privacy related affairs. It is responsible for the secure design, development and building of healthy sophisticated information systems. The technologies have become crucial for the development of content and information systems. Information Assurance is a new name in respect of Computing and IT Security; however, it has important significance as the area deals with both traditional and technological security related affairs. The IT Security primarily responsible for the computational secure systems whereas Information Assurance focuses not only on the design and development of secure systems but also policies, framework and regulations leading to secure information systems preparation. Among the technological space few common names are include vulnerabilities, virus, denial of services etc. Moreover, the vulnerabilities include the affairs of hardware, software, network, personal and physical site, organizational security systems etc. This paper talks about the basics of Information Assurance and allied affairs. Moreover, it talks about the vulnerabilities and affairs leading to computer access control, application security, authentication, authorization, aspects of data centric security, encryption, firewall etc. The paper also highlights the basic overview of the technologies and solution as well.

Keywords: IT Systems, Information, Information Assurance, IT Management, Vulnerabilities, Informatics, Secure Policies.

1. INTRODUCTION :

Information is a most vital and critical things now a days; it is required and responsible for almost all the organizations and institutions. Apart from Information, similar facets viz. data also a vital matter for different purposes. Information Technology components and Computers are responsible for storing and proving information to different means. Practically, the weakness is an important issue in Information Systems [1], [7], [18]. Vulnerability simply is the weakness in the Computing and Information Systems. And that may be in any of the components viz. Database, Network, Operating Systems, Communication Systems etc [2], [3], [19]. Vulnerability may be checked or handled by different types of measure and many of them may be physical apart from the logical means and threat management systems and tools. Vulnerability is an important name in different computational systems viz. –

- Computer Security
- Network Security
- Mobile Security
- Automotive Security etc.

There are different ways to identifying, classifying, remediating, and mitigating vulnerabilities and these are called Vulnerability Management. Security hole and security bug are the related and allied term of Vulnerability

(Refer Figure 1). Within technical areas of Information Assurance, Vulnerability is an important and emerging concept.

Fig. 1: Core facets of Vulnerability

2. OBJECTIVE AND AGENDA :

The aim and objective of this paper include but not limited to the following—

- To learn about the basics of Information Assurance with special reference to the features, characteristics.
- To learn about the function of Information Assurance in general and modern-day concept.
- To know about the basics of Vulnerability with reference to features and characteristics in brief.
- To learn about the types and category of vulnerability systems in brief.
- To learn about the Threat and Defenses related to the Vulnerability in brief.

3. INFORMATION ASSURANCE: THE WAY :

Information assurance is a safeguarding mechanism for the security, privacy and integrity of data and importantly these are used by the individuals and organizations. Information Assurance is responsible for managing the data's risks, processing, storing and transferring [4], [5], [18]. Information assurance is applicable in different form viz. digital and physical. According to the NIST, i.e. National Institute of Standards and Technology, IA is dealing *any measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.* Information Assurance is very close with the IT Security and IT Security is close with Cyber Security. The Cyber Security with its fundamentals is depicted in Fig: 2 in brief.

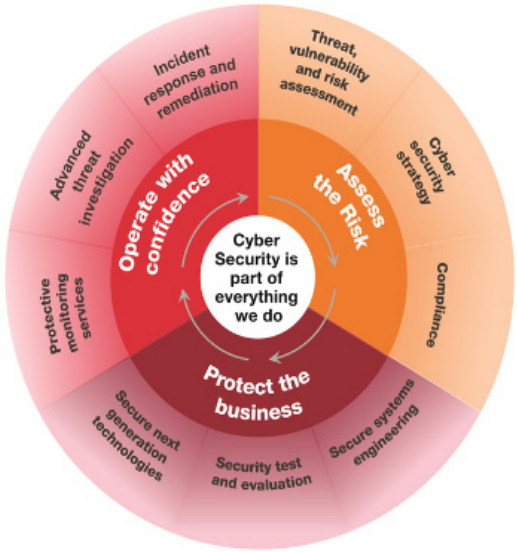

Fig.2: Depicted the Fundamentals of Cyber Security and Allied affairs

Information Assurance is dedicated to the information privacy and security in technological and managerial context [6], [8], [10]. The following are the few characteristics of Information Assurance—

- Information assurance is responsible for the delivery of information to each and every seeker with right form, time and right place [9], [11], [12].
- Information Assurance is dedicated for the data protection and unauthorized and illegal access from different sources [13], [15], [20].
- Technological information security is the component of Information Assurance and

here Information Assurance principles play a leading role.

- Information Assurance helps in reduction in Terrorism, cyber terrorism, cyber war by the use of proper mechanism.
- Information Assurance also helps in reduction and management in Cloud Security, mobile security etc.
- The Design, development, modernization, development of information repositories, database is closely associated with Information Assurance.
- Infrastructure management and Risk management become possible with Information Assurance practice.

4. SECURITY: THE ROOT :

Security is most vital in the Information Assurance Systems as far as technical side is concerned [14], [16], [28]. The security includes the way of saving information and contents from different IT Components viz.

- Secure Operating Systems,
- Secure Network Systems,
- Secure Database Systems,
- Secure Communication Systems etc.

Information Assurance is the broadest branch of security related subject, it includes the other areas viz. Information Security, IT Security (also known as Cyber Security), Computer Security, Cryptography etc [17], [20], [23]. Both the Information Assurance and Information Security deals with two types (computational & manual) of Information Privacy and Control; though Information Assurance is additionally dealing with managerial and legal aspects of security. The figure3 depicted the basic areas in this regard.

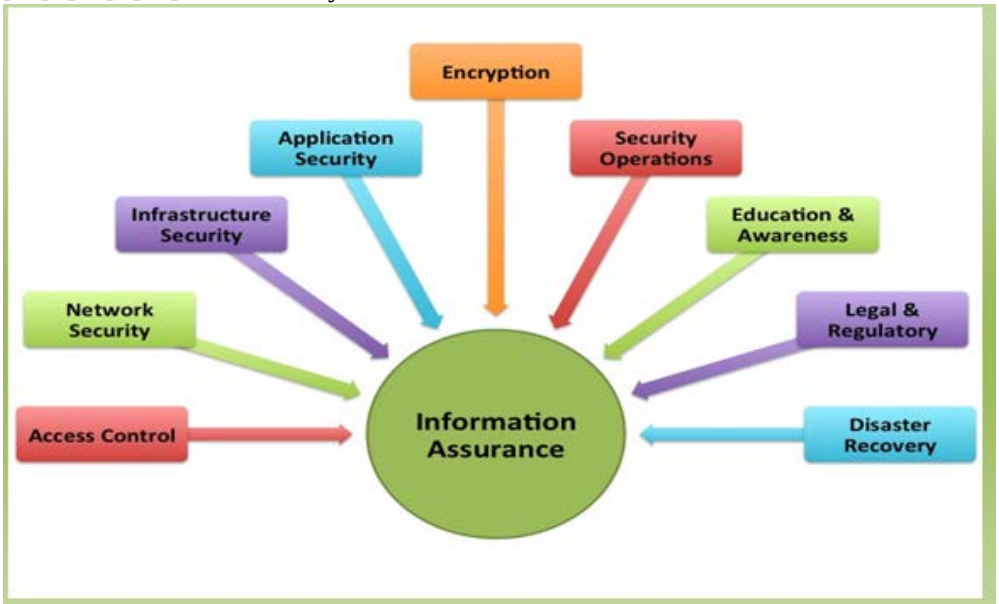

Fig.3: Depicted few areas covered within IA.

5. VULNERABILITY: A STUDY :

Vulnerability is an important concept of cyber-security which is responsible for flaw in a system that can leave it open to attack. Moreover, any type of weakness in a computer system set or in anything that leaves information security exposed to a threat may be called as Vulnerability [18], [21], [22].Definitions and meanings are given by different stakeholders and bodies and among these few important are listed in Table 1. The vulnerability include the following (but not limited to the following)—

- Physical environment
- The HR and personnel management

- Security measures of the institution or organization
- business operation including delivery with security
- hardware as well as software security
- devices related to the communication facilities with security concern [19], [24], [27]

Table 1: Depicted different definitions given by the important bodies on Vulnerability

ENISA	**The existence of a weakness, design, or implementation error that can lead to an unexpected, undesirable event [G.11] compromising the security of the computer system, network, application, or protocol involved.(ITSEC)**
ISACA	A weakness in design, implementation, operation or internal control.
ISO 27005	A weakness of an asset or group of assets that can be exploited by one or more threats where an asset is anything that has value to the organization, its business operations and their continuity, including information resources that support the organization's mission.
NIST	A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy.

6. ISSUES AND MANAGEMENT :

Computer users can protect computer systems from the weakness and vulnerabilities by taking appropriate. Computer and network personnel need to undertake current vulnerabilities to protect the systems of computing and among the threat few important are listed in Table 2.

Table2: Depicted different threat for the Vulnerability

Threat for Vulnerability	
• **Backdoors** • **Logic bombs** • **Payloads** • **Viruses** • **Worms** • **Rootkits** • **Bootkits** • **Keyloggers** • **Eavesdropping**	• Malware • Spyware • Ransomware • Trojans • Screen scrapers • Exploits • Denial of service • Web shells • Phishing

However, these threats can be managed by different kind of tools and defenses and among these few important are include—Application Security Management; which include Antivirus, Secure Coding and Default, Secure Designing, Secure and improved Operating Systems [25], [26]. Authentication is another Threat Management system required for vulnerability management. Authorization is needed for healthy computing systems management as well. Data Centric Security, Encryption are also needed as a suitable agent for Threat Management (i.e. Defenses against vulnerabilities). Apart from these for vulnerability management following are also important viz.—

- Encryption methods
- Systems of the Firewall

- Proper Intrusion Detection System (IDS)
- Runtime Application Self Protection
- Mobile Secure Gateway

The figure4 depicted the comprehensive vulnerability assessment in this regard; which include external assessment, internal assessment, application & development, physical security assessment, wireless assessment and social engineering.

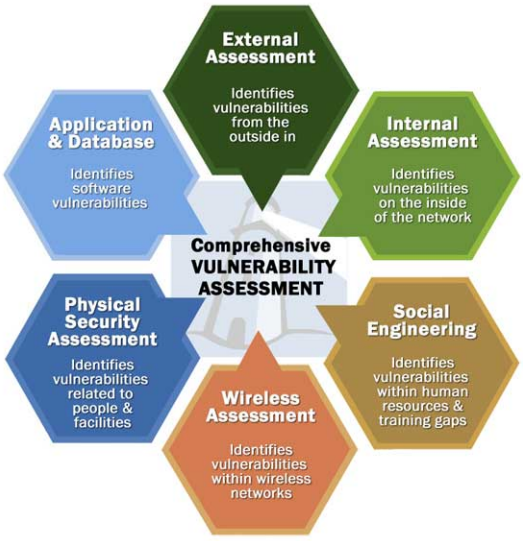

Fig.4: The different areas of Vulnerabilities in brief (info sight)

7. CONCLUSION :

Worldwide security and privacy is an important issue. Different types of organizations and institutions are providing importance to the secure systems designing, development, management, evaluation. Instead of different kind of measurement and initiatives still within privacy and security vulnerabilities is an emerging issue and still growing. Apart from the technological security and vulnerabilities few are emerging from the human resources (which include less security awareness, inadequate manpower); physical site (which include the situation in disaster management, climate, etc.), organizational (viz. lack of audits or may be less audits, it may also lack of continuity plans. Moreover, it may be lack of security as well). The Complexity, Connectivity related causes are increasing in the context of vulnerabilities. In Information Assurance apart from technological means thus managerial are increasing and here every organizations should take proper step.

REFERENCES :

[1] Bacon, T., & Tikekar, R. (2003). Experiences with developing a computer security information assurance curriculum. *Journal of Computing Sciences in Colleges*, *18*(4), 254-267.

[2] Baskerville, R., & Siponen, M. (2002). An information security meta-policy for emergent organizations. *Logistics Information Management*, *15*(5/6), 337-346.

[3] Bonner, W., & Chiasson, M. (2005). If fair information principles are the answer, what was the question? An actor-network theory investigation of the modern constitution of privacy. *Information and Organization*, *15*(4), 267-293.

[4] Borgesius, F. Z., Gray, J., & van Eechoud, M. (2015). Open data, privacy, and fair information principles: Towards a balancing framework. *Berkeley Technology Law Journal*, *30*(3), 2073-2131.

[5] Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS quarterly*, *34*(3), 523-548.

[6] Burkell, J., & Carey, R. (2011). Personal Information and the Public Library: Compliance with Fair Information Practice Principles/Les renseignements personnels dans les bibliothèques publiques: le respect des principes d'équité dans les pratiques de collecte de renseignements. *Canadian Journal of Information and Library Science*, *35*(1), 1-16.

[7] Cannoy, S. D., & Salam, A. F. (2010). A framework for health care information assurance policy and compliance. *Communications of the ACM*, *53*(3), 126-131.

[8] Chakraborty, R., Ramireddy, S., Raghu, T. S., & Rao, H. R. (2010). The information assurance practices of cloud computing vendors. *IT professional*, *12*(4), 29-37.

[9] Chen, Y., Ramamurthy, K., & Wen, K. W. (2012). Organizations' information security policy compliance: Stick or carrot approach?. *Journal of Management Information Systems*, *29*(3), 157-188.

[10] Cherdantseva, Y., & Hilton, J. (2015). Information security and information assurance: discussion about the meaning, scope, and goals. In *Standards and Standardization: Concepts, Methodologies, Tools, and Applications* (pp. 1204-1235).

[11] Cooper, S., Nickell, C., Piotrowski, V., Oldfield, B., Abdallah, A., Bishop, M., ... & Pérez, L. C. (2010). An exploration of the current state of information assurance education. *ACM SIGCSE Bulletin*, *41*(4), 109-125.

[12] Ezingeard, J. N., McFadzean, E., & Birchall, D. (2005). A model of information assurance benefits. *Information Systems Management*, *22*(2), 20-29.

[13] Hamill, J. T., Deckro, R. F., & Kloeber Jr, J. M. (2005). Evaluating information assurance strategies. *Decision Support Systems*, *39*(3), 463-484.

[14] Höne, K., & Eloff, J. H. P. (2002). Information security policy—what do international information security standards say?. *Computers & security*, *21*(5), 402-409.

[15] Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, *31*(1), 83-95.

[16] Knapp, K. J., Morris Jr, R. F., Marshall, T. E., & Byrd, T. A. (2009). Information security policy: An organizational-level process model. *computers & security*, *28*(7), 493-508.

[17] Knapp, K. J., Marshall, T. E., Kelly Rainer, R., & Nelson Ford, F. (2006). Information security: management's effect on culture and policy. *Information Management & Computer Security*, *14*(1), 24-36.

[18] Paul, P.K., Chatterjee, D., Bhuimali,A., Atarthy, A. (2016). Cyber Crime: An Important facet for promoting Digital Humanities—A Short Review in *Saudi Journal of Humanities and Social Science*, 1 (1), 13-16.

[19] Paul, P.K. & Aithal, P. S. (2018). Cyber Crime: Challenges, Issues, Recommendation and Suggestion in Indian Context, International Journal of Advanced Trends in Engineering and Technology,*3*(1), 59-62.

[20] Paul, P.K.and Aithal, P.S. (2018).Cyber Security to Information Assurance: The Changing World of Cyber Sciences in Proceedings of National Conference on Quality in Higher education challenges & opportunities (ISBN: 978-93-5311-082-6), Srinivas University, 11-18.

[21] Pérez, L. C., Cooper, S., Hawthorne, E. K., Wetzel, S., Brynielsson, J., Gökce, A. G., ... & Philips, A. (2011, June). Information assurance education in two-and four-year institutions. In *Proceedings of the 16th annual conference reports on Innovation and technology in computer science education-working group reports* (pp. 39-53).

[22] Proia, A., Simshaw, D., & Hauser, K. (2015). Consumer cloud robotics and the fair information practice principles: Recognizing the challenges and opportunities ahead. *Minn. JL Sci. & Tech.*, *16*, 145.

[23] Rees, J., Bandyopadhyay, S., & Spafford, E. H. (2003). A policy framework for information security. *Communications of the ACM*, *46*(7), 101-106.

[24] Reidenberg, J. R. (1994). Setting standards for fair information practice in the US private sector. *Iowa L. Rev.*, *80*, 497.

[25] Li, Y., Stweart, W., Zhu, J., & Ni, A. (2012). Online privacy policy of the thirty Dow Jones corporations: Compliance with FTC Fair Information Practice Principles and readability assessment. *Communications of the IIMA*, *12*(3), 5.

[26] Safa, N. S., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. *Computers & Security*, *56*, 70-82.

[27] Schou, C. D., & Trimmer, K. J. (2004). Information assurance and security. *Journal of Organizational and End User Computing*, *16*(3), 123-145.

[28] Twitchell, D. P. (2006, September). Social engineering in information assurance curricula. In *Proceedings of the 3rd annual conference on Information security curriculum development* (pp. 191-193). ACM.

****