World Academics Journal of Management **Review Paper**
Vol.7, Issue.1, pp.12-17, October (2019) **E-ISSN:** 2321-905X

Information Assurance and IT Management: *The Key Issues, Solutions in Indian Scenario based on International Trends*

P. K. Paul[1*], P. S. Aithal[2]

[1]Executive Director, MCIS, Department of CIS, Raiganj University (RGU), West Bengal, India
[2]Vice Chancellor, Srinivas University, Karnataka, India

**Corresponding Author: pkpaul.infotech@gmail.com*

Available online at: www.isroset.org

Received: 20/Oct/2019, Accepted: 27/Oct/ 2019, Online: 31/Oct/2019

Abstract- Information Technology as a field of study is growing due to its importance and applications in diverse fields, areas, and sectors. Initially, IT treated as a small domain but gradually different areas have been added into it and this includesweb technology, network technology, database technology, etc. Hence all kind of domains and fields of IT is employing everywhere. The wider applications of IT subfields for different purposes lead the concern of security and that includes in its all the sub fields. Gradually security fields became started with various nomenclature with different names and objective viz. Computer Security, IT Security, Information Security, Cyber Security and most recent Information Assurance. Importantly, Information Assurance is most wider incorporating all the areas, most interdisciplinary, skill based, management and socially touched. Though it is important to note that, human resources and skilled manpower is still limited in developing countries in this field. This paper talks about the traditional areas of Information Assurance including educational opportunities, challenges, issues, etc. Moreover, the field is concerned with the technologies related to security. Hence this paper showcases the emergence of security as a technical and HR context.

Keywords-IT Security, Information Assurance, IT Management, Academics, Development, India, Universities, Interdisciplinary

I. INTRODUCTION

It is known thatInformation Assurance or IA is not only about the practicing Information Technology Security but also it talks about the managerial issues pertaining to security and additionally it also covers the social areas of security and privacy and legal areas of security and privacy. Importantly, Information Assurance talks about the issues which are purely technology based and indirect to the technology [1], [7], [18]. Moreover, it talks about the manual affairs of security and technology. As Information Assurance is the only discipline that officially deals with the aspects of manual content's security is its area is truly broads (containing manual and technological security) and interdisciplinary (containing areas of social sciences, management and legal studies, etc). Thus, Information Assurance is doing and covering the bellow mentioned areas from a different perspective—

- Computer Security & Cryptography
- Information Technology Security
- Information Security etc.

The field Information Assurance though has tremendous and wider areas for complete IT Management but it holds various issues [3], [4], [15]. The details of issues and concern of Information Assurance with their probable solutions have been described as follows—

II. OBJECTIVE

The core aim of this theoretical and techno-managerial paper includes but not limited to the following—

- To learn about the basics of IT Security including its nature and components in the basic sense.
- To learn about the overview of different Security related areas including their role and objective.
- To know about Network Security including the reason and protecting tools and measurement.
- To know about the Web Security and the way with reference to the defending methods in the basic sense.
- To learn about Database Security, Operating System Security and the need, way of protecting.
- To know about the emerging security areas viz. Mobile Security, Cloud Security, IoT Security, etc.

- To learn about the foundation, philosophy of Information Assurance including techno-managerial affairs.
- To learn about the current Human resource related issues and concern of the Information Assurance including the availability of the degrees internationally etc.
- To know about the potentialities to introduce Information Assurance based degrees in India including the challenges and issues briefly.

III. INFORMATION TECHNOLOGY SECURITY

Information Technology Security is a big concern and deals with various sub field's security such as Web Security, Network Security, Database Security and also other emerging areas and these are including as follows—

Network Security: Issues and Concern

Network Security is an important concern within IT Security andwidely become known and responsible for the handling different network related securities viz. technologies that prevent or defend network privacy and security related issues [5], [10], [18]. Initially,there was no such concept of Network Security except the concept of Computer Security but gradually other areas have emerged and within this Network Security is important and most valuable. A network can be affected in various waysand among these most important are as follows—

By *Malware*, this is a program responsible for damaging entire computer systems viz. computer, server, network or database systems.

By *Spyware*,this is kind of malware as well needed to collect the information/ content from the computing device/s and this happens without acknowledging the client/ users.

Computer Virus or Virus is also a malware and there are various ways to get or infected viz. by email attachment, infected files, executable files, etc. Among the infection vectors, few important are include—

- Software Bugs
- Poor security practices in Social Media and Engineering places [6], [11], [22].
- Weak Operating Systems etc

*Worms*basically do not change or delete the contents; it is generally responsible to replicate files or objects. This type of worms doesn't require any host.

*Backdoor*can be managed by the system administrator by installing a backdoor program and this ultimately enablesthe threat to gain command-and-control. Additionally, it moves laterally across the targeted *network.*

Denial of Service (DoS) is a kind of attack where the whole network resources may be unavailable temporarily from the host systems or network.

Phishing is a kind of IT attack and here email plays a big role; here attackers normally send the malicious virus by email with the attachment.

Eavesdropping is associated with the telecommunication systems and it is a kind of technique and procedure dedicated to the listing private content but normally conversation of communication without the consent of the users.

Advanced Persistent Threat is a systematic and robust cyber attack to collect data as well as information from the individual computer but normally it happens from the group of computers. Additionally, APT can be possible from the same or different network [12], [19].

Network Security: Solutions and Requirement

There are different ways to protect the Network Systems and among this important are mentioned as follows—

Computer and network surveillancemanaged by the network manager to monitor computer activity. This may include monitoring of the database or storage devices or hard disk or monitoring of data transformation of the inner and outer network.

Computer Access Controldedicated to the identification, authorization, authentication, access control of a complete computer system as well as networks. Allowing operations viz. Read, Write, and Execute are the core of CAC or Access [8], [12], [19].

Application Security is another onededicated to finding, fixing as well as preventing vulnerabilities in a machine or group of machines or complete systems. There are different techniques may be used for this viz. Whitebox Security Review, Blackbox Security Audit, Design Review, Tooling etc.

Antivirus software and ***Anti malware*** are needed for robust security system establishment and few products are able in securing the systems including threat management from the infected items or objects viz. URLs, Spam, Online banking attacks, etc [7], [13].

Secure codingprovides emphasis on designing and programming with security and dealing with the following—

- Insecure Defects
- Insecure Bugs
- Insecure logic flaws etc.

Secure software developmentis very close to Secure Coding and it is the core attention of mainstream development; additionally, this may contain the concept of Domain driven designing [8], [14].

Web Security: Issues and Concern

Web Security mainly concerns within IT Security and this is mainly dealing with the Websites. As now days commercial organizations, institutions use the web systems to manage the data and contents so that proper security should be provided into the systems. Here cross site scripting, SQL

Injections, Arbitrary Code Execution, Remote File Inclusion, Path Discloser, etc. are the core way of threat.

Web Security: Solutions and Requirement

Different strategies and techniques may be adopted to keep healthy and secured websites and systems and among them, few important are include—

- Black Box testing tools
- Web Application Scanner
- WAF—Web Application Firewall
- White Box testing tools
- Fuzzing tools
- Password Cracking etc [9], [16].

Broken authentication, insecure direct object references, un-validated redirects and forwards,security misconfiguration, missing function level access controlare also treated as an important concern for lack of web security.

Database Security: Issues and Concern

Database security is simply dedicated to protecting the database from the intentional and accidental threats; which is required for hardware, software. Additionally, database security defendshuman resources and data safety directly and indirectly. Usually, the security of the DBMS can be as follows—

- Access authorization and access.
- Backup and recovery of data.
- Integrity of Data
- Encryption of data.
- Technology related to the RAID [10], [15], [23]

It is worthy to note that among the various types of threats on the computer many are technical and few are from physical as well.

Database Security: Solutions and Requirement

There are different kinds of ways and tools for the Database Security and among these,some are as follows—

- Database Management System (DBMS) should have the recovery facilities of the concerned database and there should be a provision as well for the backup copies regularly in the systems concerned or in the best location as well.
- Unauthorized access of the database needs to be ensured by the administratorstrongly; additionally,multifactor access including the data management controls
- Load balancing like capacity testing is also valuable in database systems and it should ensure it is not crashing a DDoS attack for the safety of the database.
- Physical security of the systemswith servers and almost types of backup facilities viz.tools, devices, equipment needs to be provided from the safety concern.
- Monitoring, evaluating database is highly prescribed from the vulnerability management as well.

OS Security: Issues and Concern

As far as Information Technology Security is concerned, Operating Systems security is desirable for the secured operating systems. And for these different tools, techniques and mechanisms are highly required. It is responsible for the ensuring OS for the benefits viz. better integrity, confidentiality as well as availability deeply. In generally OS Security is required due to following arrangement like—

- Securing OS from the Threats as well as Virus
- Securing OS from the worms as well as malware
- Securing OS from the remote hacker intrusion

OS Security: Solutions and Requirement

The computer systems are everywhere be it small organizations or large or even individual computers. And due to its importance worldwide companies are engaged in designing and developing of trusted operating systems with a different aim and objectives viz.—

- For the general OS patch updates
- Installing and updating antivirus engines for the OS
- Scrutinizing various types of incoming as well as outgoing network traffic and for this firewall support highly required.
- Creation of the user account with proper user management needed for a sophisticated OS Management [16], [19], [28].

Emerging Technologies: Issues and Concern

The Information Technology Security is a vast field and apart from the traditional areas viz. Web Security, Database Security, Network Security it holds and deals with other emerging areas viz. Cloud Security, Mobile Security, IoT Security, etc.

Cloud Security

Cloud Computing Security or Cloud Security is a kind of technique, way, and procedure for protecting data/ contents from the online systems and maybe a solution regarding leakage, deletion of the data, etc. There are various popular methods regarding cloud systems securityviz.—

- Use of firewall systems
- Penetration testing of the systems.
- Use VPN if required.
- Tokenization as well as voiding public internet systems etc

Mobile Security

Mobile Security is about securing mobile services including mobile devices from vulnerability or weakness. Today most organizations are engaged with various tools, technologies; mostly these are mobile based and there are various attacking systems for mobile security including-

- Attack by the SMS or MMS
- Attack by the networks viz. GSM network/ WIFI based network

- Web browser based attack
- By the in secured operating system
- Hardware based vulnerabilities etc.
- Vulnerability in software and programs etc.

IoT Security

IoT means doing computational activities with the help of the Internet. IoT is emerging and future technologies that are applicable in almost all types of sectors and fields. The growing applications of IoT in various industries and even individual's life lead the proliferation. IoT is based on the Internet so its security is highly required. Normally by the virus, worms, malware, DoS Internet of Things can be affected [17], [19], [24].

Emerging Technologies: Solutions and Requirement

There are various ways to protect computer systems by emerging computational and Information Technology. The following are a few details in this regard—

Cloud Computing

Cloud Computing for its safety measures needs various things and controlling measures and among these few important are—

- Deterrent Control
- Preventive Control
- Detective Control
- Corrective Control

Some of the encryption model and algorithms areAttribute-based encryption (ABE), Key-policy ABE (KP-ABE),Ciphertext-policy ABE (CP-ABE),Fully homomorphic encryption (FHE), Searchable encryption (SE), etc. Additionally, for a healthy Cloud Systems management, few important concerns include—Identity Management, Physical Management, Personal Security Privacy Security, etc.

Mobile Security

Mobile Security is possible to manage by keeping securities in the wide range of security areas viz. Operating Systems, Product Development and Manufacturing, User Awareness, Centralized Storage Systems, Security Software, Resource Monitoring in Devices, Network Related Issues,etc.

IoT Security

IoT Security can be managed by various means and ways and among these important are providing importance in the following—

- Inclusion of the security in designing phase
- PKI and Digital Certificates
- API Security
- Identity Management
- Hardware and Network Security Ensuring
- Patch Management etc [8], [20], [26].

IV. INFORMATION ASSURANCE AND HUMAN RESOURCES

Information Assurance is a broad field and as deals with different attributes kind of areas of security viz. managerial, social and legal so that the field is gaining popularity internationally. Worldwide different universities have started educational programs on Information Assurance leading to Bachelors, Masters and Doctoral Degree. Many of such universities either offered the program by the individual unit or allied department like Computer Science, IT, etc. Information Assurance is holding the liabilities of both computational and manual documents as well and thus it has been increased rapidly. It is worthy to note that many universities have offered the field merging with other nomenclature viz.

- Information Assurance and Security
- Information Security and Assurance
- Information Assurance and Security Management
- Cyber Security and Information Assurance etc.

The field is also offered as a full-fledged program or also as a Major or Specialization in allied programs. It is interesting to note that many universities have a Doctoral program that inbuilt with core and specialized courses in Information Assurance. Hence candidates coming from the allied branches can learn and get skilled in Information Assurance by the Ph.D. degree itself without Masters in the field. Additionally, many universities have good and strategic industrial tie-ups for different purposes.

Information Assurance and Human Resources: Indian Context with Potentialities

India is a large nation and thus country holdsa huge number of educational institutes and many of such are Higher Educational Institutes and within this category colleges, universities (including private, state, central, deemed), institutes of national importance fall under. Many of such universities offer Computing related degrees in different nomenclature viz. Computer Science, Computer Applications, Computer Engineering, Information Technology, Information Science, etc [18], [19].

There are different subfields that fall under these subjects and among these important are Network, Web Technology, Database, Software Technologies etc. As far as Security is concerned it is also started to offer by very few universities at Masters level but most of these are with the nomenclature of the following—

- Cryptography
- Computer Security
- Network Security and Management
- Information Security
- Cyber Security and Cyber Forensic etc

It is difficult to find out a university with degrees in the field of Information Assurance; though there are huge

potentialities of the nomenclature due to its role, areas, skill sets etc. It is important to note that Information Assurance or merged nomenclature may be started at Bachelors, Masters, Doctoral Degrees in different Computing related faculties. Moreover, it can be started as an individual or full-fledged program itself. However due to many challenges including lack of interest in the HEIs, concerned department, Government Departments, Concerned Ministries regarding the Information Assurance field it has not yet up to the level. Moreover, financial obligations, lack of planning and policies regarding introducing the program is another challenge of Information Assurance and IT Management in India. Though the field has huge and wider potentialities compare to the exiting/ mentioned departments. It is worthy to note that unawareness regarding the way to introduce the program into the IT faculty is another reason for its non-promotion as a field of study.

Moreover,the unwillingness of existing systems is another issue. It is important to note that, Information Assurance needs proper affiliation/collaboration among the allied or related departments and also auxiliary departments viz. management, social science, legal studies, etc but there is an issue of lack of interest to join hand with the computing related department for the Information Assurance or allied programs or lack of skills i.e. social, managerial, legal knowledge in security and allied field as well.

Information Assurance and IT Management: Social-Legal-Managerial Issues & Concern

Information Assurance not only deals with the security in Computing and IT products but it provides huge importance in managerial affairs and among these, concern policy is an important one.

For a healthy Information Assurancepractice policy should be planned and implemented nicely. Information Protection Policy is dedicated to the trusting and protecting from different modification andthe following areas may be covered for its betterment—

- Policies in Network Security
- Policies in Computer Security
- Policies in Information Security
- Policies in User account within the different forms and means
- Policies in Remote access (i.e. tools and systems with guidelines)
- Internet security policies
- Policies in Data Privacy etc [12], [21], [25].

Information is the driving force of almost all kinds of organizations, institutions for different affairs like collection, selection, organization, processing, management, dissemination of information. Information and Data Security, Content Privacyare important and valuable; and here policy is an important mechanism. The management is an important component here and here policy is applicable in different IT in different activities likePolicies in Network designing to Management, Policies in Web Development to Management, Policies in Database Development to Administration, etc. Moreover,IT professionals need to handle variousprocedures as well as a way to develop good IT policies and that needs to be healthy, authentic as well as appropriate in a different context.

Because of Information Technology is a large field and consisting of various dimensions and subfields so it is important that all such fields should be nicely managed. As a whole this concept internationally recognized as IT and Management [16], [27], [28].

V. CONCLUSION

The world is becoming technology centric and depending gradually. Today it is difficult to find out an area and sector which are not associated with Information Technologies. It is worthy to note that various organizations and institutions are also engaging proper technologies to keep and maintain security. As far as human resources are concerned, the availability of real and skilled manpower really an important challenge and this is especially true an important in respect of developing countries like India. As Information Assurance is a broad and interdisciplinary areas so that for its true academic development support from academics is required for the sectors viz. concerned IT or allied department/s, Management department for handling and additional input on policies, Social Science and Legal Studies Departments to deal the Information Assurance truly interdisciplinary and in real sense. Academic institutions and organizations thus need to attend various aspects for true, sustainable and healthy information systems which are secured in various context and forms.

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.

