IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Comprehensive Analysis Of Factors Influencing The Security Of Information And Technology*

Mr.Aniket Chandurkar[1]
MTech in Computer Science Engineering
G H Raisoni University,
Amravati, India

Prof.Vijay Gadicha[2]
Assist. Professor,Department of Computer Science Engineering
G H Raisoni University,
Amravati, India

Abstract**—** *Computer network Information System Security is critical to all modern computer users (individuals and organizations). To insure that information remain secure, many organizations implemented various security structure to protect IS security from malicious incidents by establishing security procedures, processes, policies and information system security organization structures. However, despite of all the measures, information security is still a catastrophe.With the continuous progress of computer network technology, computer network has been closely related to people's daily life. Internet with a great convenience, can help people get more information, on the basis of which, numerous shopping platform, chat platform and game platform constantly grew up in dealing with people. It can be said that the existence of the computer network is an important part of modern society, at the same time ,the computer network to bring convenience to people there being some hazards that the main is the issue of information security. Due to the openness of the Internet, the user's personal information is easy to leak out which becomes a means of criminals to reap benefits, threatening the normal life of the people. This article analyzes the influence factors of computer network information security, and gives some preventive measures to promote the healthy development of Internet security, and protect the privacy of users..*

Keywords—Computer network; Management of information security; Influence factors and comprehensive measures;

I. INTRODUCTION

Computer network plays an important role in all walks of life, and is also one of the important manifestations of globalization, through which we can achieve long-distance communication and business operations, at the same time relying on the development of computer networks, the various platforms affecting people's normal life. Network information security has been a problem in the development of computer network, because of the characteristics of the network itself and the popularity of the computer network, the importance of network information security being enhanced constantly, For individuals, network information containing a lot of personal factors, for the enterprise, containing important information of the enterprise, and for the country, containing a significant state secrets. So network information security is a problem that must be paid great attention to in the process of computer network development.

Analyzing from a narrow point of view, the so-called computer network security is to protect that the resources of network information system data information are not illegal to be obtained, change, leakage, to ensure information security so to maintain the stability of the computer system. Computer network information is an important part of the network, information security threatened, it means that the entire network system has been destroyed, affecting the normal and stable operation of the entire network.

Analyzing from a general point of view, computer network information security includes many features, reliability, authenticity and integrity, availability and confidentiality, which can be used as a part of computer network security, below for specific analysis Reliability. Reliability refers to the reliability of the entire computer network, to ensure users can use normally and can be assured of transmission the individual or enterprise information to the network which is the basis of computer network to be able to run stably, to make clear the lack of user trust and reliance on the computer network whose application value will be greatly affected, thus affecting the normal development trend

Authenticity and Integrity. The authenticity and integrity of the network information refers to the information that exists in the network is not modified and deleted by others illegally, which effectively ensure the security of user information, to prevent the problem of user information in the process, resulting in serious losses

Availability. Availability means that when users access information through legal channels, computer network can give a timely response, to help users to search and query information and ensure that users can get the information you want which is an important guarantee for user to rely on internet to search information

Confidentiality. Confidentiality refers to the user's information under normal circumstances is absolutely safe and confidential, only through normal channels and methods

to be able to access, so that users can fully guarantee the security of personal information, for individuals, businesses, the country which is essential.

II. LITRATURE SERVEY

Information Security is the state of being protected against unauthorised use of information, electronic data, software applications and hardware (Lundgren & Möller, 2017). The main goal of information security is to achieve information confidentiality, integrity and availability (Lundgren & Möller, 2017). In a case where the security of Information Systems is compromised, the organisation faces risks such as breaches, data loss, cyber security attacks and loss of business (Thorwat, 2018; Al-Omari, El-Gayar, & Deokar, 2012; Arbanas & Hrustek, 2019). It is estimated that the loss of resources due to poor information security will cost the world 10.5 trillion US$ by 2025 (Sausalito, 2020). This loss is equivalent to a quota of the budget of a country like Tanzania (with above 55 million people) as reported by its government in the 2020/2021 financial budget (URT, 2020). It is unarguable that resources, which could be used to enrich the standard of living of people is wasted through criminal schemes because of inadequate electronic protection.

Literature and international reports present vast data on Information Security across the world. Helpnetsecurity has recently reported about 445million attacks detected in 2020 (Helpnetsecurity, 2020).The study by ITU (2020) reports that 50% of internet users acknowledge being victims of security breach, LIFARS (incidence response and digital forensics firm) estimates that 29% of organisations that experience Information Security breaches end up losing revenue because of impact of criminal activities (LIFARS, 2020). Collectively, it is evident that cyber-attacks are ever increasing; therefore, the knowledge of factors affecting the Security of Information System remains to be significant among the stakeholders.

Literature provides various studies by different researchers about factors that affect IS security (Alhogail, Mirza, & Bakry, 2015; Alhogail, Areej; Mirza, A., 2014; Allam, Flowerday, & Flowerday, 2014; Arbanas & Hrustek, 2019). Al-Omari, El-Gayar and Deokar (2012) analyses factors that affect IS security by focusing on users complience to ICT policies. AlHogail (2015,) focuses on security culture as a factor toward the protection of organizatio IS security, while Alhogail, Mirza and Bakry (2015) developed a framework to only deal with human factor in protection of IS security. Arbanas and Hrustek (2019) almost tolks about all the factors that affect IS security of organizations with disregard to human factor which is very important when talking about IS security to modern ICT users. Hence, the key objective of this paper is to dteremine common factors that affect IS security to all modern computer users in African context (individuals and organizations (public/Private)), through literature synthesis.

Organization data protection process is a tedious and expensive job, organization faces many challenges in case of data breach. Data breach in organization is estimated to cost 3.92 million US$ with an average data breach of 25,575 records per year as reported in IBM Cost of Data Breach Report (2020) as well as ITU, Global Cybersecurity Index (GCI), (2017).). Also, it may deteriorate trust and lead to investors and customers refraining from doing business with the affected organizations (Gordon, Loeb, & Zhou, 2011). Organizations needs to have the right IS security controls in place to guard against cyberattacks and insider threats while providing document security and insure data availability at all times. It is important to understand IS security attributes so as to evaluate what need to be protected in organization's IS. The IS security basics/attributes includes Confidentiality, Integrity and Availability (CIA) which are the focus of any organization's Information Security Policy (Dieser, Covella, & Olsina, 2014; Mir, Mohammad, & Quadri, 2016).

III CONCLUSION

In the information society, the Internet having been a part of people's daily life, people enjoy the convenience brought by the Internet but at the same time enjoy the threat of information leakage.Computer Network information security issues having seriously affected the order of the Internet, the state, society, users should pay more attention to information security, clear the impact of information security factors from all aspects to take measures to protect and prevent the network information, and promote the healthy development of the internet.

IV REFERENCES

[1] AlHogail, A. (2015,). Design and validation of information security culture framework. Computers in Human Behavior, 49, 567-575.

[2] Alhogail, A., Mirza, A., & Bakry, S. H. (2015). A comprehensive human factor framework for information security in organizations. Journal of Theoretical and Applied Information Technology, 78(2), 201-211.

[3] Alhogail, Areej; Mirza, A. (2014). A framework of information security culture change. Journal of Theoretical and Applied Information Technology, 64(2), 540-549.

[4] Allam, S., Flowerday, S., & Flowerday, E. (2014). Smartphone information security awareness: A victim of operational pressures. Computers & Security, 42, 56-65.

[5] Al-Omari, A., El-Gayar, O., & Deokar, A. (2012). Security Policy Compliance: User Acceptance Perspective. IEEE, 45(12), 1-10.

[6] Arbanas, K., & Hrustek, N. Ž. (2019). Key Success Factors of Information Systems Security. Journal of Information and Organizational Sciences, 43(3), 131-144.

[7] Arian, T., Kusedghi, A., Raahemi, B., & Akbari, A. (2017). A Collaborative Load Balancer for Network Intrusion Detection in Cloud Environments. Journal of Computers, 12(1), 28-47.

[8] Astakhova, L. V. (2016). The ontological status of trust in information security. Scientific and Technical Information Processing, 43(1), 58-65.

[9] Boehmer, J., Larose, R., Rifon, N. J., Cotten, S. R., & Alhabash, S. (2015). Determinants of online safety behaviour: Towards an intervention strategy for college students. Behaviour and Information Technology, 34(10), 1-14.

[10] Li Siwei. Discussion about the influence factors and preventive measures of computer network security [J]. Science and technology innovation and application, 2013, 05:62.

[11] Wang Ren. Research on computer network information technology security and preventive measures [J]. Computer CD software and application, 2013, 10:92-93.

[12] Liu Haifeng, Yin Lei. Influence factors and prevention analysis of computer network information security [J]. Information security and technology, 2013, 08:41-43+67.

[13] Yan Guoxiang. Influence factors and preventive measures of computer network information security [J]. Information and computer (THEORY EDITION), 2016, 04:178-179.

[14] Yang Yongming. Discussion about the influence factors and preventive measures of computer network security [J]. Electronic technology and software engineering, 2015, 12:218.

[15] Diao Jian. Research on security of computer network information technology and preventive measures [J]. Heilongjiang science and technology information, 2015, 22:161.