Information Security Risk and Management in Organizational Network

Rustono Farady Marta, Achmad Daengs GS, Agus Daniar, Wa Ode Seprina, Alfred Pieter Menayang

Abstract*: Any association that needs to work deliberately with PC systems and data security should receive certain structure for system and data security the board. Suitable administration of PCs (host, servers and work areas), the system foundation interconnecting them and data security is a basic necessity for any association. Associations every day face dangers to their systems and data resources. Most administration procedures are not characteristically verify, and specialized arrangements are just one bit of an all-encompassing way to deal with oversee PC systems and data security. Late years have seen various devices made to robotize this methodology. There are moreover instruments that compass sorts out and discover possible attack circumstances including complex blend of different vulnerabilities. This Paper is worried about issues identifying with the administration of PC system and data security in associations.

Keywords* : Computer Networks; Network Management; Information Security.

I. INTRODUCTION

Setting up data security prerequisites is basic, yet to do as such, associations must comprehend their very own one of a kind risk condition. It is difficult to verify something except if you obviously comprehend what you needs to verify. Danger situations are controlled by the execution of an efficient security chance evaluation. When security dangers are seen, fitting counters might be chosen to moderate these hazard factors. Associations of any size ought to have a grip of the associations' data resources (for example data, databases, application frameworks, records, and so on.) and a lot of archived assets, resources and frameworks utilized for PC systems with their area and any notes on conditions. Instances of things that ought to be considered are servers, workstations, storagesystem, routers, switches, center points, system and Telco links, and some other system components, for example, printers and UPS frameworks.

Every one of these components should have a relative worth allotted in some way as to their significance to the association. For example most PCs will depend on power supply reinforcement frameworks, for example, UPSs which themselves might be a piece of the PC organize in the event that they are overseen. A key issue in system and data security the executives is the manner by which to characterize a formal security arrangement. Managing PC framework and information security is less complex than it may show up, especially if you have security methodology of steady improvement—to keep the various necessities in setting and to decline dismissing portions of security. A decent strategy determination ought to be anything but difficult to get right and moderately steady, even in a progressively evolving system.

The enormous topic of system security is poor somewhere around analyzing the going with:

- History of security in frameworks
- Internet building and vulnerable security parts of the Internet
- Types of web attacks and security methods
- Security for frameworks with web get to
- Current progression in framework security hardware and programming

II. ORGANIZATION OBJECTIVE

Organizational PC network and data security the board tends to the requirement for an administration structure that makes, continues, and deals with the PC coordinate with security. The PC system must be planned, obtained, conveyed, worked and kept up as per great data security standards. Simultaneously security frameworks must be kept up in a way suitable to the prerequisites and equivalent with the estimation of information they contain and grant access to.

To avoid interferences to association exercises and guarantee the right and secure activity of PC organize we require the accompanying errand to be finished by that system:

- Minimizing the danger of frameworks disappointments
- Safeguarding the integrityof the hierarchical programming and information
- Maintaining the respectability and accessibility of data administrations
- Provide continuous administration backing to the PC arrange
- Preventing harm to resources by controlling and physically securing PC arrange
- Develop security goals, techniques, and strategies
- Review security incidentreports and goals
- Formulate risk administration edges and confirmation necessities

Revised Manuscript Received on July 22, 2019.

***** Correspondence Author
Rustono Farady Marta, Universitas Bunda Mulia, Indonesia. E-mail: rmarta@bundamulia.ac.id
Achmad Daengs GS, Universitas 45 Surabaya, Indonesia
Agus Daniar, Universitas Bunda Mulia, Indonesia.
Wa Ode Seprina, Universitas Bunda Mulia, Indonesia
Alfred Pieter Menayang, Universitas Bunda Mulia, Indonesia

The PC frameworks and information security the administrator's structure complement on the possibility of a security game plan, which is a report that involves a ton of rules which depicts how information security should be intended for all systems to make preparations for a once-over of security perils. The security course of action makes amicability among security and usability. The supervisory gathering includes Chief Information Officer, System Administrator, Engineering Manager, Data Center Manager, and the Information System Security Officer ought to find where to check the line between information security concerns and accommodation. Just consider a security course of action as the security rules for relationship nearby methodologies for tireless usage and improvement.

III. DEVELOPING SECURE NETWORK

The engineering of an association PC system incorporates equipment, programming, data connection controls, benchmarks, topologies, and conventions. A convention characterizes how the PCs convey and move data inside a system or outside the system. There must be security controls for every segment inside the engineering to guarantee dependable and right information trades.Generally the respectability of the framework might be undermined. During the time spent advancement the PC arrange, it's important to think about after variables:

The Computer network and information security the officials structure complement on the possibility of a security game plan, which is a report that contains a great deal of rules which depicts how information security should be intended for all systems to make preparations for a once-over of security risks. The security plan makes amicability among security and usability. The supervisory gathering involves Chief Information Officer, System Administrator, Engineering Manager, Data Center Manager, and the Information System Security Officer ought to find where to check the line between information security concerns and comfort. Just consider a security plan as the security rules for relationship close by methodologies for tenacious execution and improvement.

•The data/information ought to be moved inside the system utilizing the most limited cost way, as long as different elements, similar to unwavering quality, are not traded off. The most limited cost way is commonly the briefest channel between two devices with the least transitional segments. The information which have low need information can be moved over generally economical phone lines; and the information which have high need information can be transmitted over costly fast satellite stations.

•Reliability ought to be expanded. By the term dependability expansion we guarantee legitimate receipt all things considered. PC organize unwavering quality incorporates the capacity to convey blunder free information, just as to recoup from mistakes or lost information.

IV. SECURITY RISK ASSESSMENT

The route toward managing the risk is polished by structure up a peril the officials what's more, mitigation framework, whereby assets, risks, and vulnerabilities are recognized and the proportionate danger is assessed. Controls would then have the option to be picked to evade, move, or decrease risk to a tasteful level. Security chance examination is a procedure to extend usage of constrained various leveled assets subject to quantifiable danger and definitive peril opposition. Peril examination steps are according to the accompanying:

- Identify assets inside the security parameter

A favored position can be a huge thing, for example, equipment, or immaterial, for example, a complete database. By definition, a good position has a spurring power to the alliance, subsequently requires security. Resources must be seen, and possession must be created. A relative worth should in like way be set up for each piece of elbowroom so criticalness can be created when risks are evaluated.

- Identify dangers to the advantages

Threat experience or try resource vulnerabilities to make dangers. Dangers to each benefit must be perceived. There can be various dangers for each preferred position. Perceiving confirmation of dangers must be sensible. Just those hazards that have a basic likelihood, or insane devilishness ought to be considered. For instance, a danger to the genuine database might be theft or change.

- Identify vulnerabilities to the assests

Vulnerabilities are seen deficiencies in resources that can be mishandled by dangers to make chance. A favored position may have different vulnerabilities. For instance, the absence of insurance to an association's database might be a poor access control or lacking stronghold.

- Determine realistic probability

Probabilities for each risk/vulnerability mix ought to be settled. Mixes with evidently inconsequential likelihood might be dismissed.

- Calculate harm

Malicious (a bit of the time recommended as effect) might be surveyed numerically to reflect harm from a beneficial encounter. This worth permits the rating on a general size of the validity of a given threat autonomous of its likelihood. Damage isn't identified with likelihood.

- Calculate Risk

Deductively, hazard can be passed on as: Probability x Harm = Risk. This count accomplishes a numeric rating of favored position based danger for a given course of action of dangers and vulnerabilities. This numerical translation awards prioritization of confined peril moderating assets.

V. TYPES OF ATTACKS

System are in danger to attacks from noxious sources. Additionally, with the appearance and expanding utilization of web join is most normally making on developing. The fundamental portrayals of Attacks can be from two requests: "Uninvolved" when a system gatecrasher finds information encountering the structure, and "Dynamic" in which an intruder starts headings to bother the system's standard activity. A framework ought to no doubt farthest point harm and recuperate quickly when attacks happen. There are some more sorts of attack that are in addition fundamental to be considered:

- Passive Attack

A passive attack screen decoded traffic and searches for clear-content passwords and delicate data that can be utilized in different sorts of attacks. The checking and tuning in of the correspondence channel by unapproved assailants are known as uninvolved attack. It wires traffic assessment, seeing of unprotected correspondences, deciphering feebly encoded traffic, and getting endorsement data, for example, passwords. Inactive catch of system activities empowers foes to see impending activities. Passive attacks understand the disclosure of data or information reports to an assailant without the assent or learning of the client.

- Active Attack

In active attack, the attackers tries to maintain a strategic distance from or break into affirmed structures in the going on correspondence. This should be possible through stealth, disease, worms, or Trojan horse. active attacks breaker attempts to go around or break security highlights, to show malicious code, and to take or change data. The unapproved assailants screens, looks at and changes the information stream in the correspondence channel are known as unique attack. These attacks are mounted against a system spine, misuse data in development, electronically attack an enclave, or attack a certified remote client during an endeavor to interface with an enclave. Active attacks accomplish the introduction or spread of information files, DoS, or change of information.

- Distributed Attack

A distributed attack necessitates that the foe present code, for example, a Trojan steed or distorted access program, to a ―trusted‖ part or programming that will later be spread to different affiliations and clients Distribution attacks rotate around the vindictive difference in equipment or programming at the advanced office or during allotment. These attacks present unsafe code, for example, an underhanded access to a thing to assemble unapproved access to data or to a framework work eventually in the near future.

- Insider Attack

As appeared by a Cyber Security Watch review insiders apparently was the reason in 21 percent of security breaks, and a further 21 percent may have been an immediate consequence of the activities of insiders. The majority of respondents to another persistent review said it's sensibly hazardous today to see and avoid insider attacks than it was in 2011, and 53 percent were developing their security spending plans in light of insider dangers. While a fundamental number of splits are accomplished by perilous or disillusioned masters - or past representatives - many are acknowledged by wellmeaning workers who are basically trying to finish their obligation. BYOD adventures and file sharing and joint effort associations like Dropbox propose that it will be more perseveringly than at whatever point in late memory to hold corporate information under corporate control even with these amicable at any rate unscrupulous operators.

- Close-in Attack

A nearby in attack joins somebody endeavoring to get physically close system parts, information, and structures so as to get settled with a structure. Close-in attacks contain standard people accomplishing close physical closeness to structures, frameworks, or working environments to adjust, hoarding, or denying access to data. One without a doubt comprehended sort of close in attack is social structure. In a social arranging attack, the assailant bargains the system or structure through social joint effort with an individual, through an email message or telephone. Different stunts can be utilized by the person to uncovering data about the security of affiliation. The data that the harm individual uncovers to the product designer would unquestionably be utilized in a resulting attack to manufacture unapproved access to a structure or system.

- Spyware attack

An authentic PC security danger, spyware is any program that screens your online exercises or displays programs without your assent for preferred position or to get solitary data. Additionally, this catch data is maliciously utilized as the certified client for that specific sort of work.

- Phishing Attack

In phishing attack the product designer makes a fake site that looks precisely like a remarkable site, for example, the SBI bank or PayPal. The phishing some portion of the attack is that the product engineer by then sends an email message trying to fool the client into clicking an affiliation that prompts the phony site. Right when the client attempts to get together with their record data, the engineer records the username and secret state and after that gives that data a shot the credible site.

- Hijack attack

In a hold attack, a product architect anticipate control over a session among you and another individual and detaches the other individual from the correspondence. Regardless you recognize that you are talking with the essential party and may send private data to the designer by accidently.

- Spoofing attack

InT theT caricaturizingT attack,T theT designerT changesT theT sourceT addressT ofT theT packsT theT individualT beingT alludedT toT isT sendingT withT theT targetT thatT theyT radiateT anT impressionT ofT beingT beginningT fromT anotherT person.T ThisT mightT beT anT endeavorT toT maintainT aT strategicT distanceT fromT yourT firewallT rules.T

- Secret articulation attack

An assailant attempts to part the passwords set away in a structure account database or a secret articulation ensured record. There are three basic sorts of secret key attacks: a jargon attack, an animal power attack, and a crossbreed attack. A jargon attack utilizes a word once-over file, which is a

quick overview of potential passwords. A beast power attack is the point at which the aggressor attempts every conceivable blend of characters.

• Buffer overflow

A buffer attack is the point at which the attacker sends a greater number of information to an application than is standard. A cushion flood attack for the most part accomplishes the aggressor extending authentic access to the structure toward a way concise or shell.

• Exploit attack

In this kind of attack, the attacker thinks about a security issue inside a working framework or a pinch of programming and use that learning by manhandling the feebleness.

VI. COMPUTER NETWORK AND INFORMATION SECURITY MANAGEMENT

Deciding the right zones to improve data safety efforts, equipping with the correct innovation for PC system and representative preparing is the way to progress for supervisory crews. Numerous issues are brought about by inappropriate exercises on systems. In this way when building up a PC organize, a framework manager must think about the total exercises and the data security of PC systems. Here we are showing a total rundown of undertakings which must be considered by the supervisory group while playing out the administration of PC systems and data security.

• Policy the board

Gives an instinctive, rule-based methodology for all device families being overseen, with a total perspective on principle practices and alternatives and incredible separating capacities.

• Network Traffic Monitoring

Observing of system traffic crosswise over system to check for clients associating with shaky spaces and sites.

• User movement the executives

Insurance from unapproved client and following of utilization implies Which client and device associated with which port and when.

• Network Change and Configuration Management

System setup the board to shield arrange from security dangers, to look after consistence, and maintain a strategic distance from expensive vacation.

• Centralized object the executives

Focal organization of system, administration, attack, antivirus/profound assessment objects from one interface that can be utilized by at least one arrangements.

• Real-time checking

Checking the status of enormous quantities of firewall/VPN and IDP Series devices, groups, and VPN burrows.

• Firewall Security Management

Firewall the executives framework that can help oversee firewall exercises to fortify data security and simultaneously, bolster administrative consistence.

• Log and Event Management

Total and dissect the occasion signs progressively and Correlate the log case with other system occasions.

• Endpoint Vulnerability Management

Far reaching review trail of programming on end-client workstations.

• Data Loss Prevention

Ensure information and application with continuous warning

• Disaster recuperation and high accessibility

Database synchronization between the basic and assistant servers with customized bomb over to auxiliary.

VII. CONCLUSION

Today PC system and data security has to do with shielding our delicate data from the two untouchables and insiders. All we need a security approach that covers all dangers. Security devices, for example, firewalls, antivirus programming, and encryption will assist our association with protecting our data from unapproved clients. Accepting that our association is verified isn't sufficient.

We need to adopt a proactive strategy to deal with our authoritative PC system and data security, ensuring that more current advances are actualized to stay aware of complex programmer devices. A total system and security structure will ensure our ventures for the coming years. The entryway to new innovation appropriation likewise opens up the window for more current security occurrences, or zero-day attacks. Associations are probably going to see a greater amount of private and half and half cloud execution, bring your own device (BYOD), programming characterized server farm combination, IPv6, Big information, HTML5, and the sky is the limit from there. It's an ideal opportunity to get readied.

ACKNOWLEDGEMENT

This article has been written with financial support of RUSA–Phase 2.0 grant sanctioned vide Letter No. F. 24-51/2014-U, Policy (TNMulti-Gen), Dept. of Edn. Govt. of India, Dt. 09.10.2018.

REFERENCES

1. Debra Lynn Banning, ―A Distributed Audit System Using Network Management Protocols‖, Master's Thesis, California State University, Long Beach,1992.
2. Li Gong and MenchamShocham, "Elements of Trusted Multicasting", In Proceedings 1994 International Conference on Network Protocols, p. 23-30, IEEE Computer Society, Los Alamitos, CA, 1994.
3. Lee LaBarre, ISO/CCITT to Internet Management Coexistence (IIMC): ISO/CCITT to Internet Management Security (IIMCSEC), Internet draft, MITRE, Feb1994.
4. S.Lechner,―SAMSON:Managementof Security in Open Systems‖, Computer Communications, Sep 1994.
5. Hall Series in Innovative Technology, Prentice- Hall, Englewood Cliffs, New Jersey, 1991.
6. John Rushby, "Critical System Properties: Survey and Taxonomy", Reliability Engineering and System Safety, 43(2): 189- 219,1994.
7. John Rushby, "Kernels for Safety?", Safe and Secure Computing Systems, pp. 210-220, Blackwell Scientific Publications,1989.

8. William Stallings, SNMP, SNMPv2 and CMIP: the Practical Guide to Network Management Standards, Addison-Wesley, 1993.
9. Gregory B. White, Eric A. Fisch and Udo W. Pooch,―CooperatingSecurityManagers:A Peer- Based Intrusion Detection Systeml, IEEE Network, pp. 20-23, January/February 1996.
10. Ninghui Li, William H. Winsborough, and John C. Mitchell. Beyond proof-of compliance: Safety and availability analysis in trust management. In proceedings of 2003 IEEE Symposium on Security and Privacy, Berkeley, California, May2003.
11. M. Siponen. On the scientific background of information security management standards: a critique and an agenda for further development. In Proceedings of the Second Annual Systems Security Engineering Conference (SSE), Orlando FL, USA, March 2001.
12. ISO. Iso/iec 17799:2000 - information technology - code of practice for information security management. Technical report, International Organization for Standards, Geneva, Switzerland,2000.
13. Ernst & Young. Global information security survey. Technical report, Ernst & Young LLP, Cleveland OH, USA,2004.
14. M. Eloff and S. von Solms. Information security management: An approach to combine process certification and product evaluation. Journal of Computers and Security, 19(8):698–709,2000.
15. Chienwattanasook, K., Wattanapongphasuk, W., Prianto, A., & Jermsittiparsert, K. 2019. "Corporate Entrepreneurship and Business Performance of Logistic Companies in Indonesia." Industrial Engineering & Management Systems 18 (3): 538-547.
16. Dawabsheh, M., Hussein, A., & Jermsittiparsert, K. 2019. "The Triangular Relationship between TQM, Organizational Excellence and Organizational Performance: A Case of Arab American University Palestine." Management Science Letters 9 (6): 921-932.
17. Jermsittiparsert, K., Siam, M., Issa, M., Ahmed, U., & Pahi, M. 2019. "Do Consumers Expect Companies to Be Socially Responsible? The Impact of Corporate Social Responsibility on Buying Behavior." Uncertain Supply Chain Management 7 (4): 741-752.
18. Syazali, M., Putra, F., Rinaldi, A., Utami, L., Widayanti, Umam, R., & Jermsittiparsert, K. 2019. "Partial Correlation Analysis Using Multiple Linear Regression: Impact on Business Environment of Digital Marketing Interest in the Era of Industrial Revolution 4.0." Management Science Letters 9 (11): 1875-1886.
19. Sae-Lim, P. & Jermsittiparsert, K. 2019. "Is the Fourth Industrial Revolution a Panacea? Risks toward the Fourth Industrial Revolution: Evidence in the Thai Economy." International Journal of Innovation, Creativity and Change 5 (2): 732-752.
20. Chatchawanchanchanakij, P., Arpornpisal, C., & Jermsittiparsert, K. 2019. "The Role of Corporate Governance in Creating a Capable Supply Chain: A Case of Indonesian Tin Industry." International Journal of Supply Chain Management 8 (3): 854-864.
21. Hartinah, S., Suharso, P., Umam, R., Syazali, M., Lestari, B., Roslina, R., & Jermsittiparsert, K. 2020. "Teacher's Performance Management: The Role of Principal's Leadership, Work Environment and Motivation in Tegal City, Indonesia." Management Science Letters 10 (1): 235-246.
22. Haseeb, M., Hussain, H., Slusarczyk, B., & Jermsittiparsert, K. 2019. "Industry 4.0: A Solution towards Technology Challenges of Sustainable Business Performance." Social Sciences 8 (5): 184.
23. Haseeb, M., Hussain, H., Kot, S., Androniceanu, A., & Jermsittiparsert, K. 2019. "Role of Social and Technological Challenges in Achieving a Sustainable Competitive Advantage and Sustainable Business Performance." Sustainability 11 (14): 3811.
24. Haseeb, M., Kot, S., Hussain, H., & Jermsittiparsert, K. 2019. "Impact of Economic Growth, Environmental Pollution, and Energy Consumption on Health Expenditure and R and D Expenditure of ASEAN Countries." Energies 12 (19): 3598.
25. Huda, S., Tsani, I., Syazali, M., Umam, R., & Jermsittiparsert, K. 2020. "The Management of Educational System Using Three Law Auguste Comte: A Case of Islamic Schools." Management Science Letters 10 (3) (In press), DOI: 10.5267/j.msl.2019.9.018.
26. Usak, M., Kubiatko, M., Shabbir, M., Dudnik, O., Jermsittiparsert, K., & Rajabion, L. 2019. "Health Care Service Delivery Based on the Internet of Things: A Systematic and Comprehensive Study." International Journal of Communication Systems 32 (14): e4179.
27. Jermsittiparsert, K., Ambarita, D., Mihardjo, L., & Ghani, E. 2019. "Risk-Return through Financial Ratios as Determinants of Stock Price: A Study from ASEAN Region." Journal of Security and Sustainability Issues 9 (1): 199-210.
28. Maseleno, A., Hardaker, G., Sabani, N., & Suhaili, N. (2016). Data on multicultural education and diagnostic information profiling: Culture, learning styles and creativity. *Data in brief*, *9*, 1048.
29. Maseleno, A., Huda, M., Jasmi, K. A., Basiron, B., Mustari, I., Don, A. G., & bin Ahmad, R. (2019). Hau-Kashyap approach for student's level of expertise. *Egyptian Informatics Journal*, *20*(1), 27-32.
30. Maseleno, A., Huda, M., Siregar, M., Ahmad, R., Hehsan, A., Haron, Z., ... & Jasmi, K. A. (2017). Combining the previous measure of evidence to educational entrance examination. *Journal of Artificial Intelligence*, *10*(3), 85-90.
31. Thabhiranrak, T. & Jermsittiparsert, K. 2019. "Towards Sustainable Functioning of Organization: Women Empowernment and Corporate Management Culture." Journal of Security and Sustainability Issues 9 (1): 321-332.
32. Chienwattanasook, K. & Jermsittiparsert, K. 2019. "Impact of Entrepreneur Education on Entrepreneurial Self-Employment: A Case Study from Thailand." Polish Journal of Management Studies 19 (1): 106-116.
33. Jermsittiparsert, K., Sutduean, J., Sriyakul, T., & Khumboon, R. 2019. "The Role of Customer Responsiveness in Improving the External Performance of an Agile Supply Chain." Polish Journal of Management Studies 19 (2): 206-217.
34. Jermsittiparsert, K., Sutduean, J., & Sriyakul, T. 2019. "Effect of Service Innovation and Market Intelligence on Supply Chain Performance in Indonesian Fishing Industry." Industrial Engineering & Management Systems 18 (3): 408-417.
35. Jermsittiparsert, K., Namdej, P., & Somjai, S. 2019. "Green Supply Chain Practices and Sustainable Performance: Moderating Role of Total Quality Management Practices in Electronic Industry of Thailand." International Journal of Supply Chain Management 8 (3): 33-46.
36. Somjai, S. & Jermsittiparsert, K. 2019. "The Trade-off between Cost and Environmental Performance in the Presence of Sustainable Supply Chain." International Journal of Supply Chain Management 8 (4): 237-247.
37. Jermsittiparsert, K. & Sawasdee, A. 2012. "Formal Education for Non-Thai or Undocumented Person in Thailand amidst the Challenge of Nationalism and Transnationalism: A Case Study of Wat Sirimongkhol School, Samut Sakhon Province." Kasetsart Journal - Social Sciences 33 (2): 203-213.
38. Wright, Joe; Jim Harmening (2009) "15" Computer and Information Security Handbook Morgan Kaufmann Publications Elsevier Inc p. 257
39. Dr. G. Padmavathi, Mrs. D. Shanmugapriya, ―A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks‖, (IJCSIS) International Journal of Computer Science and Information Security,Vol. 4, No. 1 & 2, 2009.
40. Adeyinka, O., "Internet Attack Methods and Internet Security Technology," Modeling & Simulation, 2008. AICMS 08. Second Asia International Conference on, vol., no., pp.77-82, 13-15 May 2008.