International Journal of Engineering and Information Systems (IJEAIS)
ISSN: 2643-640X
Vol. 7 Issue 11, November - 2023, Pages: 27-31

Analysis of Hardware Failure In Elementary Schools

Honni[1], Kevin Christianto[2], Johanes Fernandes Andry[3], Angel Borgenis Fianty[4], Cornelius Benhard[5]

Faculty of Technology and Design, University of Bunda Mulia, Jakarta, Indonesia
Email: l1306@lecturer.ubm.ac.id, l1591@lecturer.ubm.ac.id, jandry@bundamulia.ac.id, s31220024@student.ubm.ac.id, s31220013@student.ubm.ac.id

Abstract—*Currently, computers have become a familiar part of learning media at all levels of education. Even so, it still often happens that schools do not realize the potential quality of learning provided to students / students influenced by the facilities and learning media obtained. As was the case at Elementary Schools in north Jakarta, the evaluated SOPs showed that there was still a lack of security in terms of security and hardware used for a long time and lack of maintenance. In addition, this study aims to identify the hardware needs needed in elementary school computer labs, as well as evaluate the performance of hardware that has been used. This research was conducted using qualitative methods, and the results of this research are expected to be reference material for schools to develop better and effective elementary school computer laboratories. It is known that the most frequently used hardware is a computer, mouse, keyboard, wi-fi and projector. The evaluation results show that there is still less maintenance in terms of hardware used and also still a lack of security personnel in terms of security. Therefore, this research is expected to be a suggestion for schools to repair or replace hardware that is no longer functioning properly and can increase the use of technology in the learning process so that it can provide improved quality of education in elementary schools*.

Keywords—Hardware; Lab; Information Systems; Computer

1. INTRODUCTION

With today's technology, "Computers" are no longer strange in this day and age. In this research, authors analyze hardware problems in schools in North Jakarta. In this research, researchers conducted an analysis of problems related to hardware in the school, especially related to the use of learning media and IT security in the computer laboratory. The aim of this research is to create an expert system that can provide information about hardware to solve information system problems [1], [2].

The use of computers in the world of education, especially formal education, has penetrated all walks of life, and the use of computer programs to deliver lesson material and monitor student learning progress is known as Computer Based Learning. Implementation of this can improve the quality of learning if the learning process runs in a directed, smooth, effective, and efficient manner in accordance with the learning objectives that have been set. There are several factors that influence the learning process, including educators, students, facilities, and the learning media used. The school introduces computers to students to teach them the basics of computer equipment. This school has a special lab for informatics learning, and introduction to computers is carried out through face-to-face learning and SOPs are implemented in the lab [3], [4].

Question research is: how does the Information System at elementary school serve as a learning medium, how to apply for lab information data access at elementary school Elementary School while on guard? ow is IT security at elementary school when guarded? How is the SOP implemented at Elementary School? And what about the Daily Activity that occurs at elementary school?

Scope of problem this research is: The research was only carried out at schools, specifically for elementary, Research only focuses on hardware analysis and IT Security in the lab, The research aims to understand the application of material regarding IS and IT for students at Elementary School and Daily practice of School students in IT Security applications [5] and hardware used in the computer lab room [6].

Objective this research: Maximize and improve hardware usage in the lab, improve management of lab information data access - Implementing IT Security lab, Ensure the school SOP process runs effectively, efficiently, and consistently and ensure daily activities run smoothly and effectively in elementary school [7], [8].

The benefits of this research are increasing efficiency and productivity in the school lab, making it easier to manage and store practicum data while in the lab, increasing student, teacher, and parent confidence in the information system in the school lab, and avoiding data leaks. Minimize the risk of errors, improve service quality, achieve target goals at school, and ensure routine activities are timely and safe for students and teachers at school.

2. LITERATURE STUDY

2.1 Hardware

Hardware is a computer device consisting of electronic components in physical form that have the function of supporting the computerization process. There are several types of hardware that can be seen and touched directly, such as processing equipment

(CPU), input/output devices (keyboard, monitor, disk drive, etc.), and storage devices (main memory). Hardware is also a link between users and systems on a computer [9], allowing users to interact with the computer and carry out certain tasks.

In hardware, the CPU (Central Processing Unit) plays an important role in processing commands and carrying out management through information on the computer system [10]. Apart from that, there are also input/output devices that function to obtain information from outside in physical or non-physical form, such as keyboards, monitors, disk drives, cameras, web, printers, scanners, etc. Lastly, storage devices such as main memory are very important in storing information on a computer system. Thus, hardware is an important part of a computer that has a big role in supporting various computing processes.

2.2 Information Systems Security (ISS)

ISS includes the prevention and detection of fraud in information systems that have no physical meaning. There are three dimensions to measuring information system security, namely knowledge, attitudes, and behavior. Information security must be protected because it is an important company asset, information leaks or system failures can cause financial and productivity losses [11].

ISS dimensions or indicators have 2 sides which are relevant to the knowledge of the environment (relevance) and comply with established bases. In efforts to handle and control Information System Security, there are three important aspects of CIA information security (Confidentiality, Integrity, and Availability). a. Confidentiality. Aspects that ensure that information can only be accessed by authorized people. b. Integrity (Integrity) . The aspect of guaranteeing that there is no change in data without the permission of the authorized party in order to maintain the accuracy and integrity of the information. c. Availability. This aspect provides a guarantee of data availability when the user needs it, whenever and wherever [12].

2.3 Technical Security Control System and Hardware Maintenance

Operating system security is an important part of overall computer system security [13]. Apart from physical security to limit direct access to computer facilities, operating system security is also divided into three main parts: external security, user interface, and internal. External security is concerned with threats from intruders and natural disasters, while user interface security is concerned with identifying users before they are allowed to access stored programs and data. Internal security involves the control of hardware and operating systems in maintaining the integrity of programs and data. Although often used interchangeably, the term security refers to overall security issues, while the term protection mechanism refers to the system mechanisms used to protect information on a computer [14], [15]

Maintenance is an activity of looking after and maintaining facilities or carrying out repairs, adjustments, or replacements so that there is a satisfactory condition of production operations as expected. This maintenance aims to prevent and reduce or avoid further damage to equipment by ensuring the level of reliability and readiness and minimizing maintenance costs. Then also to guarantee the availability and reliability of facilities both economically and technically, so that their use can be optimized as best as possible. Maintenance also extends the life of the facility, guarantees the operational readiness of the facility, and most importantly ensures work safety and security in its use.

Security controls can be categorized based on the type of control and what the control does. The first category includes administrative, technical, and physical controls. The second category includes detective or responsive controls and corrective controls. Examples of these controls include change management processes, antivirus systems, and guardrails for physical controls [16].

3. METHOD

This research activity was realized in collaboration with the school and Bunda Mulia University, Information Systems study program. In the implementation process, there were several stages carried out by the research team as depicted in Figure 1. Stages of Research

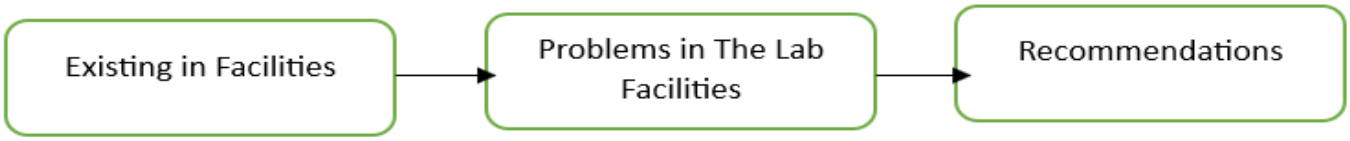

Figure 1. Stages of Research

Pre-Implementation Stage, the research team carried out several things, namely:

1. Existing in Facilities Security Lab, authors receiving problem data, the research team received data in the form of a 10-minute audio recording which contained an explanation of several information security problems experienced by the school.

2. Problems in The Lab Facilities, analysis of problem data, the research team analyzed previously received data with the following line of thinking:

- Current Conditions, discusses how information technology security policies are implemented at this school.
- Problems with Current Conditions, discusses what are the problems with the implementation of the current information technology security policy for the company.

3. Recommendations or Solutions to Problems, Discusses the solutions that the research team can provide to the information technology security problems experienced by the school [17].

Authors Prepare ingredients/materials, The research team prepared material that would later be presented in PowerPoint form to employees who attended this research activity. Some of the things carried out at this stage are as follows: Coordination of the research team to the location, The research team coordinated with accompanying lecturers to gather in the lobby area of Bunda Mulia University, Ancol campus, Implementation of activities, The activity was carried out by making a presentation regarding IT Security Policy on Hardware to the participants.

4. Analysis and Discussion

4.1 Existing in Facilities Security Lab

Security Policies, there is CCTV located in the upper left corner of the computer lab, Wi-Fi passwords can only be accessed by the IT department and some teachers, and students cannot access them. Students can only use it in computer lab facilities during learning activities, and if there is a hacking attempt, the Wi-Fi password will be immediately changed. The computer lab is only accessible to teachers and school staff, and students can only access it during class. There is security at the front door of the computer laboratory. Checking files after use. SOP (Standard Operational Procedure): Students are required to dress neatly and completely inside and outside while the teaching and learning activities are still in progress. No food or drink is allowed in the computer lab. The obligation to maintain the cleanliness of the school environment applies to everyone in the school area. Students must be present and not late as long as the teaching and learning activities continue until they are finished. Hardware cables are neatly arranged and do not interfere with teaching and learning activities. Reorganize and turn off hardware that is only used during teaching and learning activities. Do not damage the hardware in the computer lab room. Daily Activity: During operation, computers will be turned on by IT for students. Re-checking the computer lab CPU to optimize student teaching and learning routines. Students are required to sit in the computer lab based on the absence number determined by school regulations. The door will be locked after the use of the lab room.

4.2 Problems in The Lab Facilities

Security Policies. There are no fire hydrants (fire extinguishers) or alarms if there is an electrical short circuit in the school lab. Lab facilities are too low and vulnerable to damage caused by natural and man-made disasters. Lack of security staff to supervise student activities outside school teaching and learning hours. Computers are not given password access, so students can use them freely. There is no antivirus programming installed on each hardware, making it vulnerable to viruses if students secretly install applications from suspicious and dangerous sites. SOP (Standard Operating Procedure): damaged hardware is not immediately replaced and left as it is. The Windows used for operational teaching is still Windows 7. There is no routine maintenance for any existing hardware other than the CPU. There are no clear and detailed procedures for accessing lab rooms, so anyone can use the lab rooms as long as they are teachers, students, or officials at Elementary School. There are no written rules for prohibitions posted in the lab for students who violate them (for example: sleeping in class, damaging hardware, eating, and drinking in class, and so on). Daily Activities: Hardware components that have been damaged are rarely checked routinely. Use of computer lab facilities outside of teaching and learning activities and subjects determined by students. There is no brief education regarding the use of lab space during teaching and learning activities, so students' ignorance causes the quality of the hardware to decrease. Not doing daily data backups.

4.3 Recommendations for Lab Facilities Security

Security Policies: Add fire hydrants (fire extinguishers) and alarms to prevent electrical short circuits in the school lab. Providing special security staff to maintain lab security, both during teaching and outside. Improve the quality of the lab room by moving the lab room to the 2nd floor of the school to prevent further hardware damage when a disaster occurs. Provide and assign passwords to increase the security of computer lab hardware facilities. Providing additional CCTV indoors and outside to increase the security of the school computer lab. Install an updated antivirus to protect your computer from the entry of undetected viruses. SOP (Standard Operational Procedure): Update damaged hardware at least once every 4-5 years. Upgrading windows to improve the quality of student learning. Provide written regulations and notify every student and school officer who enters the lab to obey orders according to applicable regulations. Carry out weekly or monthly maintenance routines for each existing hardware, not just focusing on the CPU. Record procedures (for example: name, time, and reason for borrowing) for access to borrow lab space for each party who plans to access the lab space. Daily Activity: Carry out a routine of checking hardware components every day to prevent and find information

on components that have been damaged. Providing counseling and warnings to students to maintain proper use of all existing hardware. Carry out strict supervision and give firm warnings to students who violate. Encourage students to remain transparent and active in informing the homeroom teacher or staff if there is hardware that is not working as usual so that it can be repaired immediately and avoid further damage. Perform daily data backups.

5. CONCLUSION AND SUGGESTION

5.1 Conclusion

The research results show that there are several laboratory problems in schools, such as poor room facilities which increase the risk of hardware damage or theft, lab security that is not strict enough, and there has been no replacement of computer facilities in the last 1-year. This has an impact on the performance of hardware that is too old and has not been upgraded for several years, thus affecting the teaching, and learning activities that take place in the laboratory to be less than optimal. Therefore, updating facilities and hardware is very necessary to improve the quality of learning in computer laboratories.

5.2 Suggestion

Based on the results of the analysis to improve the learning experience at the school, there are several actions that can be taken, namely:

- Upgrade hardware and back up data and clean unnecessary data regularly.
- Consider with the school whether to move the computer laboratory room to a better location or to a higher floor to prevent damage due to natural or man-made factors.
- Improving laboratory security and installing special access to monitor the identity of people entering and exiting the computer laboratory to ensure safety from various existing risks, as well as technicians in the school area to prevent scale enlargement.

6. REFERENCES

[1] Hadi, Juandi, D., and Rusdiana, D., (2023). Problem Solving Ability Analysis: Systematic Literature Review. Journal of Mathematics and Mathematics Education, Vol. 13, No. 1, pp. 33-43, doi.org/10.20961/jmme.v13i1.73819

[2] Sudarsono, B, G., Andry, J. F., Ranting, P., and Rahman, A. A., (2020). Redesign The Forwarding Company's Business Processes Using The Zachman Framework. Journal of Theoretical and Applied Information Technology, Vol.98, No 16, pp. 3222-3232.

[3] Abdullah, A, I, N, F., Atrinawati, L. H., and Wiranti, Y. T., (2022). Designing Business Process Model and Standard OperatingProcedures (SOP) of Integrated Laboratory Management At XYZ University. International Journal of Educational Management and Innovation, Vol.3, No.2, pp. 169-182, doi: 10.12928/ijemi.v3i2.5795

[4] Dumas, M., La Rosa, M., Mendling, J., & Reijers, H. A. (2018). Fundamentals of Business ProcessManagement (2nd ed. 2018). Springer Berlin Heidelberg : Imprint: Springer.doi.org/10.1007/978-3-662-56509-4

[5] Andry, J. F., Nurprihatin, F and Liliana, L. (2023). Developing a Decision Support System for Supply Chain Component. Management and Production Engineering Review, Volume 14, Number 2, pp. 124–133, doi: 10.24425/mper.2023.146029

[6] Horn, T., and Lazar, B., (2023). Artificial Intelligence and Information Technology for Clinical Decision Support for Reducing Hospital-Acquired Conditions and Improving Patient Outcomes: A Systematic Literature Review. International Journal of Engineering and Information Systems (IJEAIS) Vol. 7 Issue 8, pp. 12-19.

[7] Navis, M. J., and Kaltsum, H. U., (2021). Learning Efficiency Of Elementary School Students Through E-Learning In The Era Of Disruption. Primary: Jurnal Pendidikan Guru Sekolah Dasar, Vol. 10, No. 2, doi: 10.33578/jpfkip.v10i2.8135.

[8] Al-Fraihat, D., Joy, M., Masa'deh, R., &Sinclair, J. (2020). Evaluating E-learning Computers in Human Behavior, 102, 67–86. https://doi.org/10.1016/j.chb.2019.08.004.

[9] Ugah, J. O., S., C., Agu., and Elugwu, F., (2018). Relationship between Operating System,Computer Hardware, Application Software and Other Software. International Journal of Computer Trends and Technology (IJCTT) – Vol. 64, No.1.pp.12-16.

[10] Simanullang, P. M. (2021). Pengaruh Perangkat Keras Komputer Dalam Sistem Informasi Manajemen, The Effect Of Computer Hardware In Management Information Systems. Doi: 10.31219/osf.io/c43en.

[11] Dirman, A. (2020). Financial Distress: The Impacts Of Profitability, Liquidity, Leverage, Firm Size, And Free Cash Flow. International Journal of Business, Economics and Law, Vol. 22, Issue 1.

[12] Nurul, S., Anggrainy, S., & Aprelyani, S. (2022). Faktor-Faktor Yang Mempengaruhi Keamanan Sistem Informasi: Keamanan Informasi, Teknologi Informasi Dan Network (Literature Review Sim). Ekonomi Manajemen Sistem Informas, Vol. 3, No. 5. doi: org/10.31933/jemsi.v3i5

[13] Chen, C and Hui, Z., (2020). Computer Network System Security Management andMaintenance Strategy. Journal of Physics: Conference Series 1533. IOP Publishing. doi:10.1088/1742-6596/1533/2/022057.

[14] Bernanda, d. Y., Charolina, Y., Azhari, O., Pangrestu, C., and Andry, J. F., (2023). Identification Of Potential And Planning For Disaster Recovery Using The Iso/Iec 24762 Standard At XYZ University. Jurnal Teknoinfo, Vol. 17, No. 1, pp. 140-147.

[15] Johnson, R., & Easttom, C. (2020). Security Policies and Implementation Issues, 3rd Edition by Robert Johnson Chuck Easttom (z-lib.org). https://www.jblearning.com/catalog/productdetails/9781284199840.

[16] Honni, Lee, F. S., Isputrawan, M. F., Limawal, I. I. and Andry, J. F., (2023). Audit Aplikasi Presensi Pada Perusahaan Industri Kosmetik Menggunakan Cobit 5, Infotech: Journal Of Technology Information, Vol. 9, no. 1, pp. 19-30. doi: org/10.37365/jti.v9i1.153

[17] Eason, G., Noble, B., & Sneddon, I. N. (1995). On certain integrals of Lipschitz-Hankel type involving products of Bessel functions, Phil. Trans. Roy. Soc. London, vol. A247, pp. 529-551.