Systematic Literature Review: Factor For Physical Security And Access Control In Maximum Security Protection

Article history

Received:
15 May 2021

Received in revised form:
25 May 2021

Accepted:
15 June 2021

Published online:
26 June 2021

*Corresponding author
lindaisyahazizan@gmail.com

Roslinda Mohamed, Hafiza Abas, Noor Hafizah Hassan and Saiful Adli Ismail
Razak Faculty of Technology and Informatic, UTM, Kuala Lumpur, Malaysia
lindaisyahazizan@gmail.com,hafiza.kl@utm.my,noorhafizah.kl@utm.my, saifuladli@utm.my

Abstract

Physical security and access control as one of the installations should be upgraded to confirm the security and readiness of the asset belong to the group to continue safely. As the quick development in technology offers a boundless defence level for physical security and access control in the office, every organization must offer a passable budget pertinent to the transformation of the world today. Through a very humane approach of natural surveillance, access control, maintenance, and reinforcements of territory, this strategy will contribute to the field of physical security as a whole. The purpose of this paper is to recognize the features that regulate taking for perimeter protection and access control in maximum were identified and analysed. The findings have revealed that five categories of features can be used to study the taking for perimeter protection and access control in maximum security protection: physical security; access control; security standard and policy; security awareness program and security training and security protection. A Systematic Literature Review (SLR) was accepted since it uses a more rigorous and well-defined method to swotting the study indication pertinent to the study. Initially, 62 papers were retrieved by a manual search in six databases and 17 primary studies were finally included. Consequently, 5 factors education.

Keywords-*physical security, access control, security awareness, security standard policy, systematic literature review.*

I. INTRODUCTION

Physical security refers to the protection of building sites, equipment, and all information and software contained therein from theft, vandalism, natural disaster, manmade catastrophes, and accidental damage [1] . Physical security is a vibrant fragment of any security design and is vital to all security efforts without it, information security, software security, user access security, and network security are substantially more problematic, if not unbearable to initiate [2]. It remains possible to characterize physical protection as a safety tool conceived to refute unauthorized access to buildings, facilities, and services.

Physical safeguard is identified as well as a system or plan of measure to defend staff and properties from mistreating or injuries, such as spying, stealing, or arsonist assault [3]. The use of several tiers of interrelationship security systems, such as CCTV monitoring, security guards, defensive obstacles, locks, a procedure for access control, and many other plans of action, must include physical security. In safeguard, the organization for every one of the installed systems at the organization has their task.

Access control is a security feature that restricts who or what can access or use resources in a computing environment [4]. It is a basic protection notion that minimizes the danger to the corporation or organization. Electronic access control systems that rely on user passwords, access card readers, auditing, and reporting are used to monitor employee access to restricted business locations and proprietary areas, such as data canter.

To avoid unauthorized access or activities, some of these devices comprise access control panels to limit entry to rooms and buildings, as well as alarms and lockout abilities. Individuals and objects are recognized and verified by access control systems using mandatory login identifications such as passwords, personal identification numbers (PINs), biometric scans, security tokens, and other verification methods. To secure access control systems, multifactor authentication (MFA), requiring multifactor authentication, is also an essential part of tiered security [5]. Access management seeks to decrease the security risk of illegal entree to physical and logical nets to a minimum. Access control is a vital element of security enforcement initiatives to confirm that security technology and access control measures such as user data are in place to keep delicate info.

Once approaching a physical security plan, either for a present property or new-build, it's vital to have a thoughtful of common physical security and access control threats or vulnerabilities. Once identify physical security and access control threats only after that provide an approach to overcome them. Various types of physical security risks may be handled at various stages of the property's design, implementation, and maintenance. It is therefore in the property owner's best interest to have a broad understanding of the risks, their associated vulnerabilities, and available countermeasures.

In practice, anyone who has physical access to a computer can take over your system in seconds. As a result, talk about certain physical security protocols to help reduce the possibility of an intrusion by implementing effective access controls. Each access control system has three levels of development: physical, administrative, and technical. Examples of threats for physical security and access control such as sabotage, vandalism, hardware failure, man-made disaster, and natural disaster.

Physical protection has three main components [6]. First-line defenses can be erected in the direction of potential attackers, and locations can be fortified against accidents and natural disasters. Multiple locks, fences, doors, fireproof safes, and water sprinklers may be used in such steps. Second observation and warning devices such as lighting, heat sensors, smoke detectors, intrusion detectors, alarms, and cameras, may be mounted on the spot. Third to capture attackers and to recover quickly from collisions, fires, or natural disasters, strategies may be introduced.

II. MAXIMUM SECURITY PROTECTION

The high maximum-security level is the highest and most stringent. Such a system is planned to delay, notice, measure, and deactivate all illegal external and internal actions. Example guard duty for up to 24 hours a day and under strict monitoring. However, implementation of maximum security is costly but changes attack from internal or external is low availability. Nuclear installations, jails, bound military bases, government special research centres, and a few international embassies, for example, provide the highest degree of physical security safety [7].

III. PROBLEM BACKGROUND

The physical security and access control providers and installed around the MAF- DOC compound have already met the basic security prerequisite for Malaysian Armed Forces installation during 1995. However, as technology usage becomes advanced the basic physical security and access control technology capacity outdated which then might expose the building to physical security also access control threats.

In this study, the current problems of physical protection and access control systems will be discussed and this will help to describe the problem, propose solutions and recommendations. There is also a need to scrutinize the safety problems and awareness of the new execution as well as other forms of treat and guidance.

Poorly managed physical security and access control possibly result in notable cybersecurity risks. That is why physical security and access control are must be required to gain access to the IT infrastructure. It is important that once physical security and access control are possibly accessed even the most sophisticated cybersecurity devices have credential reset procedures. Intrusion into government buildings also reason to financial losses to that organization and country, harm to the image and reputation of the government, negative input to publicity, and damage to classified information may also be caused. That technology is as powerful as the individuals behind it and the process means three-component must work together. Defined defensible space as a residential area whose physical characteristics, such as building layout and site plan, enable residents to act as key agents in their defense [8].

The following scenarios and problems related to problem physical security, access control, and awareness among employees are discussed based on the results of reference, observation, and experience of the researcher as a Malaysian Military Personnel.

IV. METHODOLOGY

Physical security and access control to the protected areas, services, or materials of an entity containing confidential data and make it simpler for a malicious sneak to relegate an offense. The physical security and access control of an organization therefore as essential as its technical security controls. A

systematic literature review (SLR) method was chosen for this study. SLR is a secondary analysis that reviews the research evidence applicable to the study using a more robust and well-defined described and interpreted or process. SLR is a method for locating, analyzing and interpreting all available research on a specific research issue, subject field, or area of interest. The methodological measures, search methods, and study questions are all defined in detail so in the future authors possibly follow the same procedure. SLR is likely to deliver objective and complete literature reviews. Scheduling review, conducting the review, and documenting the review are the three stages of SLR operations. Based on the five-step procedure described above this research took a systematic or evidence-informed approach [9]. The five procedures used in this analysis are depicted in Figure 1.

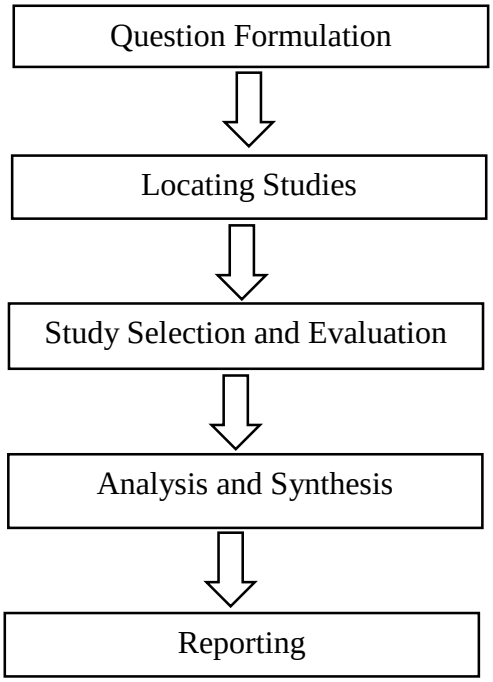

Figure 1. Five steps to conducting a systematic literature review (Denyer and Tranfield, 2009)

These steps are briefly described as follows:

Question formulation – This is a dynamic phase where an appraisal query is articulated. A specific appraisal query is essential for the study's focus and direction. The query must be broken down into lesser, more precise queries that may be addressed by individual studies.

Locating studies – In this phase, resources to be investigated will be notorious. Searching electronic literature databases is the most popular technique to find material for a systematic review.

Study selection and evaluation - Study selection criteria are used to identify which research should be included in the review and which should be eliminated. Time or publication date range, language or national setting, and principal

emphasis of the work are all common inclusion criteria. Selected research will be submitted to a more in-depth quality assessment, which will typically be based on eminence valuation principles.

Analysis and synthesis – The pertinent lessons drive be discovered after the initial screening. The analysis's goal is to cessation particular studies into their component elements and explain how they relate to one another. On the other hand, the purpose of combination is to make connotations amid the parts recognized in individual studies.

Reporting - After the five steps in the SLR have been carefully made then the article search results supporting each factor will be presented. The results will provide more detailed and thorough details for each factor involved in this study.

V. RESULT AND DISCUSSION

This segment will present the outcomes recognized for respectively step in SLR.

i. Question Formulation

A study's main goal is to answer the following question: 'What vulnerabilities factors of physical security and access control in maximum high-security level? In this study, literature search was executed in electronic records with "physical security OR perimeter protection OR access control" AND "military area OR restricted area" AND "maximum high-security level OR maximum high access level" as the search key. This review's literature search technique was purposefully broad, covering a wide range of physical security and access control protection. In the figure below the total string was demonstrated:

("Physical Security" **OR** "Perimeter Protection" **OR** "Access Control") **AND** ("Military Area" **OR** "Restricted Area" **OR** "Maximum High Security Level" **OR** "Maximum High Access Level")

Figure 2. Search for Systematic Literature Review

ii. Locating Studies

This SLR focuses on searching scientific records rather than particular books or technical reports since it is expected that major study results in books and reports are also discussed or referenced in scientific journals. Six electronic databases were recognized as data sources in this study. They are ACM Digital Library, ScienceDirect-Elsevier, Springer Link, IEEE Computer Society Digital Library, and other government collections. The emphasis was put on manually looking for various references relating to primary researches in order to ensure a thorough search.

iii. Study Selection and Evaluation

Specified the vastness and fragmentation of the topic, it was decided not to try to reduce the number of publications even further by optimizing search strings. The variety principles were as follows:

a. The research was conducted observed with a strong emphasis on quantifying characteristics linked to the acceptability of any sort of physical security, perimeter protection, or access control.

b. The article was published entirely in English.

c. The paper was published in a peer-reviewed journal or the proceedings of a conference.

Because this review study concentrated on empirical data addressing physical protection and access control, it eliminated review papers, theoretical and philosophical pieces, editorials and letters. Articles released between January 2010 and January 2021 are included in the reviews.

The browsing procedure takes been completed by concentrating on two different parts of the article constructed on the subsequent categorization: title and abstract, and the main body of the article. Initially, the hunt yielded 60 papers for consideration, which were read for titles and abstracts. After removing redundant documents and those that did not meet the inclusion criterion, 20 articles were held for a more thorough evaluation. Lastly, 17 publications were found to meet the requirements and were included in this report. Figure 3 The Selection Process For Including Articles In Revie**w** depicts the method selecting papers for inclusion in the study.

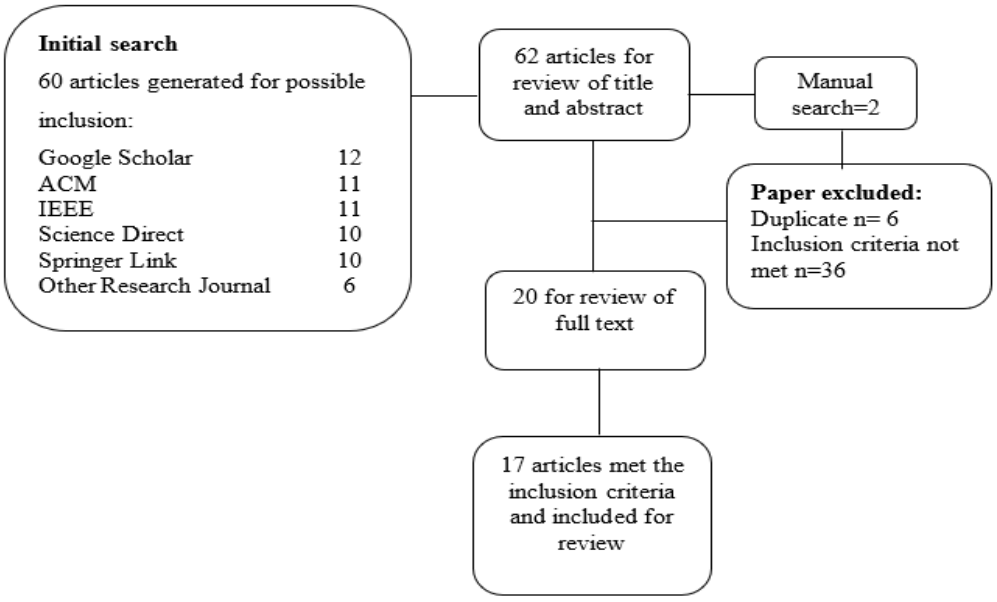

Figure 3. The Selection Process For Including Articles In Review

Table 1. Figure of related articles and their source

Source	Papers Found	After Excluded	Selected
Google Scholar	12	4	5
ACM	11	5	3
IEEE	11	3	4
Science Direct	10	3	2
Springer Link	10	3	2
Other Research Journal	6	2	1
Total	62	20	17

iv. Analysis and Synthesis

We can be confident that most fields in any sector incorporate these two aspects in their sector structure, based on the 17 studies analyzed. Previous research has found that implementing physical security and access control along with program security to employees makes it provide maximum high security to an organization [10]. Physical security and access control to the protected areas, services, or materials of an entity containing confidential data and make it simpler for a malicious sneak to relegate an offense [11].

Access control is the technologies and processes to make sure only authorized people can enter your workplace, or secure spaces within. When a corporation has strong physical security measures in place, it can help limit who has access to its system. This can be done on a variety of levels. Providing very limited access to your office space or implementing authorization levels that only give the appropriate folks access to areas of the network could be used to address the matter. This will significantly improve any network access policies that may already exist. An employee without the appropriate security clearance will be unable to get access to a server room or conduct unlawful transactions from a networked stand-alone computer.

Physical security programs important by knowing the hazards, test the safeguards and engage employees in awareness [12]. The effects of 5 different factors on organizations' application and receiving of Physical Security and Access Control must come with a security awareness program in the 17 studies revised. Table 2 displays the proportion of papers for each factor.

Table 2. Acceptance factors for articles reviewed were identified

Factor	No of Articles
Physical Security	5
Access Control	5
Security Standard and Policy	1

Security Awareness Program	3
Security Training and Education	2

v. Reporting

Each article is evaluated for its descriptive and thematic content, which focuses on classifying the paper by year, factor, and topic of study. Thematic analysis analyses and categorises aspects using conceptual frameworks that are appropriate to the situation. The 17 articles reviewed, aimed at implementing all the factors tested for the physical security and access control model related to physical security, access control, Security Standard and Policy, Security Awareness Program, Security Training, and Education.

This survey shows that the acceptance of physical security-oriented factors such as the maximum use of all technologies in overcoming physical threats is still the dominant factor in the study (29.41%). Factors of access control implementation were also tested (29.41%). Evaluation of the level of security standards and policy in ensuring the level of success of the organization in maintaining the level of physical security and access control through a correct security standard and policy (5.88%). Some researchers also studied the positive and negative effects of the security awareness program on an organization (17.65%). Overall assessment of Security Training and Education on impact organizations (11.8%).

VI. CONCLUSIONS

Constructed on an SLR, this paper has recognized the factors that can assist the researcher in achieving the research goals of this entire research. This study would concentrate on the need to strengthen some of the issues found about the physical security of the building to improve the level of security for perimeter safety and control of access to the high maximum security. It is important to revise the use of technology to increase the protection of physical security and the level of access control so that the degree of security covered remains at the best level.

VII. ACKNOWLEDGMENTS

We would like to thank Universiti Teknologi Malaysia, Ministry of Education and Malaysian Armed Forces

REFERENCES

[1] Dabin Sun, Bowei Wang Research on the Design of the Implementation Plan of Network Security Level Protection of Information Security: 2021 7th International Symposium on Mechatronics and Industrial Informatics (ISMII)

[2] Andrew Martin (December 2006), Information Availability and Security Policy, Americas Conference on Information Systems (AMCIS)
[3] Baker, P. R., & Benny, D. J. (2016). The Complete Guide to Physical Security. CRC Press.
[4] Pietro Colombo, Evaluating the effects of access control policies within NoSQL systems, Science Direct 2021
[5] Nickson M. Karie, Hardening SAML by Integrating SSO and Multi-Factor Authentication (MFA) in the Cloud, 2020, ACM Digital Library
[6] Michael Cobb (2016). Physical Security. Retrieved February 1, 2016, from https://searchsecurity.techtarget.com/definition/physical-security
[7] International Atomic Energy Agency, Nuclear Power, the Environment and Man, Information Booklet, IAEA, Vienna (2018).
[8] Newman, The seminal works on defensible space are Defensible Space: People and Design in the Violent City, Macmillan, 1972
[9] Denyer, D., & Tranfield, D. 2009. Producing a systematic review. In D. A. Buchanan & A. Bryman (Eds.), The SAGE handbook of organizational research methods (pp. 671–689). London: Sage Publications Ltd [10]
[10] MoneerAlshaikhab,Sean B.Maynard,bAtifAhmadb. Applying social marketing to evaluate current security education training and awareness programs in organisations, , January 2021, https://www.sciencedirect.com/
[11] University, S. (2016). HIPAA Security: Facilities Security Policy | University IT. https://uit.stanford.edu/security/hipaa/facilities-security-policy
[12] George K. Campbell (2014). The Manager's Handbook for Business Security (Second Edition). https://www.sciencedirect.com/