Physical Security

Student’s Name

Institutional Affiliation

 Protective barriers are defined as the installation and the business activities within a given area or location. In different organizations, several barriers may be affecting the daily programs in the company. Protective barriers are the obstacles that are used to physically define the area, the post, or the activities in a particular region. The security personnel also use these barriers in capturing the intruders; the boundaries are also used in the gates to show the direct entries of the vehicles entering and leaving the premises. Protective barriers are categorized in different categories depending on their functions.

Barriers also provide essential benefits for the state of physical safety. They create a psychological deterrent for anyone who wants to enter without permission may delay or even block them. Constraints have a direct impact on the number of security positions required and the frequency of use of each post. The categories of protective barriers are natural and structural. The physical obstacles are the barriers that affect the unlawful entries; they include the natural terrain features such as the mountains, water, mashes, and the desert. Structural barriers are the installed devices to detect unwanted entries (FEffective Physical Security Fourth Edition Lawrence J. Fennellyennelly & L 2016). They may include the gates, fence, and walls.

 Avoidance is the best procedure for successful mitigation. According to Zhou et al. (2017) it is confirmed that the best thing to do for preventing the barrier is to exit the companies that seem to be dangerous to someone’s life. Establishing the procedures and the policies are the other approach that helps different organizations in foreseeing and avoiding the risks that may affect the activities of the business. Acceptance is the other procedure that can be used for successful mitigation. There are some of the business activities that may affect the transaction either positively or negatively. The company should avoid the activities that may affect the events in the business. Therefore the industry should check on the activities that they got involved in for the sake of the company’s security purposes.

 According to Fennelly & L. (2016) it is found that every product produced can fail in the hands of your customers. If the risk is at an acceptable level and the estimated on-site failure rate is low enough, the product can accept any opportunity. If the only decision to take the risk is based in part on an estimate or forecast, the information may erroneously predict the future. Therefore, it may be advisable to monitor field performance or to set up an early warning system in the event of a field failure.

There are several hardening methods of entry control. One of the hardening methods includes the use of the service park. The entire computer Apps should be kept on to date and should always be updated to new the new version whenever the system requires the update.

They are determining which groups can access these rules or not. Sometimes only a user error leads to a successful cyber-attack. Set up or update user policies and make sure that all users understand and follow these processes. For example, each user should implement strong passwords, protect their credentials, and modify them regularly (Fennelly & L 2016). Another method is the security templates. This happens when the policies of the group are applied in the required environment. Any group policy that can be passed in a group should be used in a required business environment. Removing unneeded programs from the computer program is another potential entry point for tracking hackers. Cleaning these computer programs limits the way they are typed.

If these computer programs are not in the company review and locked, the application should not be allowed to access the computer data. When trying to break the network, the hacker or the attacker will look for backdoors of the computer and also the security holes. Minimize the chances they pass. When the entire group policies are applied in only the required business environment, the business is said is fully secured since no business policy would help leek outside the business environment (Ghai et al. 2015). Also, the factors that can make the group maintain the rules of the group.

 The unnecessary programs in the computer should be removed from the system potential entry point for a hacker. The company should clean their systems by flushing the system and removing the unnecessary programs from the system to avoid and limit the chances of the hackers accessing the company’s data. Once this is done, the company document is considered to be safe and free from hackers and theft. The baseline is the mode of changes within the network, the software, and the hardware of the computer.

 Creation of baseline needs a selection of what you want to research and continue to step over time. Establish benchmarks and weigh them according to an acceptable schedule for your standards to ensure safety and meet customer needs. In computer programs should be updated to make sure that the hackers do not hack the company data in the system, (Ghai et al. 2015). The device securities should be updated to make sure that the data is not accessed with any third party who is not part of the company.

References

Fennelly, L., (2016). Effective physical security. Butterworth-Heinemann.

Ghai, V., Sharma, S., & Jain, A. (2015). *U.S. Patent No. 9,111,088*. Washington, DC: U.S. Patent and Trademark Office.

Zhou, X., Song, L., & Zhang, Y. (2016). *Physical layer security in wireless communications.* CRC Press.