Physical security clients assessmants

Physical Security Clients AssessmentUniversity of PhoenixCJA/585IntroductionThis paper discusses the physical security that always has been basic to protecting facilities, people, and physical assets. Next the paper discusses the importance of building security and all the fundamental components of architectural and construction concerns that make buildings safe places for living and working. Perimeter and grounds security is still a matter of restricting physical access to secure areas.

The physical structure of the building should be designed in the most appropriate manner that provides the highest levels of security measures for its inhabitants. Ground security can be viewed as ways in which we protect areas around airports. Following September 11, 2001, airports have implemented various adjustments to ensure that passengers are safe, all equipment, and bags are safe before they leave the ground to enter the airplane. Access control system can be as simple as possessing a security guard to stop people from entering a certain area. Access control systems are highly used at most businesses to keep unauthorized individuals out of places where they does not belong. Perimeter Security can be described as a boundary that separates an area from the rest of the universal. The reason for perimeter security is to detect, deny, deter, and delay unauthorized access to a perimeter without the owner??™s consent to avoid theft, vandalism, or other criminal acts. Information Systems and Technology Security, information security means protecting information from unauthorized use, access, disclosure, modification, disruption, inspection, perusal, destruction, or recording.

Many organizations and homes have intrusion detection systems on their computers. Intrusion detection systems allow companies to monitor unwanted attempts to gain access to their systems. Physical SecurityPhysical security is the protection of hardware, personnel, networks, programs, and data from physical circumstances and events that could cause serious losses or damage to a business, organizations, or association. This includes protection from natural disasters, fire, theft, burglary, vandalism, and terrorism. Physical security is the wide phenomena taken for the prevention or determent of attackers from a possible access of a resource, information stored within physical media and facilities. Physical security is viewed under three fundamental aspects.

These are responding adequately to the measures of security that would repeal or catch the possible attackers in the event of detection. Using gadgets, and implements that are forthwith important in the control of secure atmosphere. This could include cameras, security lighting, and use of alarms, patrols by security guards that provide easy noticing of attacks. Facilitation of obstacles that are aimed at frustrating any possible attackers and delaying the serious security cases. A proper set of security designs has the complement of all these structures that work cohesively with one another. A good physical security design is a complement of four important factors, which are intrusion detection, electronic, and mechanical access controls environmental design and video monitoring. Physical security is based on various principles that are applied to solve various security concerns at varied depths. Building securityBuildings are the source of residence for human beings.

However, their structural planning and establishments is compromised by various security threat factors that make the lives of those living in them unsafe. Building security therefore implies all the fundamental components of architectural and construction concerns that make buildings safe places for living and working. It is the compound of all structures that provide authenticity in the physical structures that provides the safest levels for the habitation (Nadel, n. d). The guarantee for this security is well afforded during the designing phase of the building the aspect of this security is inclusive of both the internal and the external environments that are occupied by the building. The physical structure of the building should be designed in the most appropriate manner that provides the highest levels of security measures for its inhabitants. It should include a coordinated design in the roofs, walls outlet, such as doors, windows, and locks (Nadel, n.

d.). Unfortunately, some of the best methods for implementing building security at the level of initial access necessarily create so-called “ soft target” opportunities wherever large numbers of individuals must assemble to present their access credentials. Whether large numbers of individuals seeking access to secure facilities assemble immediately in front of the building, or in any area not immediately adjacent to the facility, the regular and predictable presence of large crowds will always present a potential target for terrorists without the need to ever enter the facility (DeGrazio & Copper, 2005). However, that risk can be mitigated with behavioral observation specialists trained to spot suspicious activity and other resources, such as explosive detection canines.

Otherwise, the principal methods of protecting buildings from unauthorized access are a combination of directed flow of individuals to specific entrances based on their level of authority and the coordinated use of technological tools, such as identification cards implanted with digital authentication chips for automatic recognition by automated doors. However, neither of those techniques is reliable without simultaneous use of security personnel to ensure that access protocols are not deliberately circumvented in the entrance zone (DeGrazio & Copper, 2005). Ground securityGround security can view as ways in which land around the airports are protect.

Following September 11, 2001, airports have implemented various adjustments to ensure that passengers are safe, all equipment, and bags are safe before the leave the ground to enter the airplane (Berrick, 2004). Before that tragic event, there were no major security measures in place except screenings but people could just come and go as they please. Because of the hijackings, security was beefed up tremendously. Passengers are screened more closely. People are not allowed to carry liquids into the airport and not like before only passengers with boarding passes may enter the terminal.

This protective aspect is to airports and its surrounding environment. It includes all aspects to the physical structure of an airport that makes it a safe place for the various activities that goes on within their contemporaries. It incorporates adequate placement of the structures, such as runways, surveillance services, communication systems, and all aspects endowed within the structures of an airport.

Because of the delicacy of the airport operations, high importance should be in the highest levels of security for the activities and processes of the airport (Parker, 2007). Access control systemsAccess control systems are highly used at most businesses to keep unauthorized individuals out of places where he or she does not belong. Access control systems also can be as simple as possessing a security guard to stop people from entering a certain area. There are levels of access controls that allow systems to respond to a pin or a card number, there is an intelligent system that controls access to doors locks and has the capability to store information. Access cards have been proven to have some vulnerability.

Hackers are very intelligent and have found ways to copy the cards information (Benantar, 2005). Hackers have become so accomplished that they have created portable readers that can capture the card number. No security method can ever be listed as 100% effective.

Perimeter securityPerimeter control is also very important for external building structures. Examples of perimeter control are fences, gates, walls, landscape, lighting, and locks. Fences include gates, turnstiles, and mantraps. Fences provide crowd control, and help to deter trespassers.

Programmable locks can be either electronic or mechanical. These types of locks are often dial combination locks similar to those used in high school lockers, however; electronic locks require a digital number to be entered into a key pad in order for them to unlock. Examples of landscape control is hedge bushes, tall trees, or mountains that may surround the area deterring people from entering because of a lack of vision or an unwillingness to attack

(Groom, 2007). Information systems and technology securityInformation security means protecting information from unauthorized use, access, disclosure, modification, disruption, inspection, perusal, destruction, or recording.

Many organizations and homes have intrusion detection systems on their computers. Intrusion detection systems allow companies to monitor unwanted attempts to gain access to their systems. The primary technological advances in physical facility, building, grounds, and perimeter security relate to computerization of relevant security information and its complete integration (Spears & Barki, 2010). Typical emerging technologies that increase physical security include automatic license plate readers to identify potentially dangerous vehicles before they traverse the perimeter, system-wide integration software capable of automatically cross-referencing multiple sources of security-related information (or agency-specific databases).

Personnel identification systems, such as finger print readers and iris scanners to minimize the vulnerability of identification card scanners systems to situations where individuals other than those to whom identification cards and other electronically read credentials are issued come to possess those (Spears & Barki, 2010). ClosingEveryone in the world is concern with safety in his or her home or workplace. The main purpose of physical security is to make sure that the organizations are protected and everyone that works there is safe and protected. The physical structure of the building should be designed in the most appropriate manner that provides the highest levels of security measures for its inhabitants. Access

control systems are highly used at most businesses to keep unauthorized individuals out of places where he or she does not belong.

When trying to determine what, it is that needs to be in protection a person needs to ask these questions. Information security means protecting information from unauthorized use, access, disclosure, modification, disruption, inspection, perusal, destruction, or recording. What assets need protection, what threats are there to those assets, what vulnerabilities are there to the assets and the priorities Once those can be answered, there is a good chance in developing a good physical security system in place.

ReferencesBenantar, M. (2005). Access Control Systems: Security, Identity Management and Trust ModelsBerrick, C.

(2004). Aviation Security: Further Steps Needed to Strengthen the Security of Commercial Airport Perimeters and Access Controls: GAO-04-728. GAO ReportsDeGrazio, R.

, & Cooper, W. (2005). Building Security: An Architects Guide.

Retrieved April 14, 2012, from http://cryptome. org/archsec. htmGroom, R. (2007). Protecting the Perimeter of Your Building. Retrieved April 14, 2012, from http://bizsecurity. about.

com/od/buildingsecurity/a/protectperm. htmNadel, B. (n. d). Building Security: Handbook for Architectural Planning and Design. Published by McGraw-Hill Parker, P. (2007).

Airport Security and Ground Handling Equipment in Jordan. A Strategic ReferenceSpears, J. & Barki, H. (2010). User Participation in Information??™s Systems Security Risk Management.

MIS Quarterly, 34(3), 503-A5