Risk assessment scenario

Law

Risk Assessment Scenario Samson Akhigbe CJA/520 July 13, Being the director of security for a computer software company, one has to detect any forms of intrusion and determine the risks of any illegal physical or internet intrusion into the database. Intrusion detection is the process of identifying activities that would attack and destroy the company’s confidentiality of data, resources and information. Illegal physical intrusion is where a person who isn’t authorized to access the company’s system breaks in physically to the system where resources, information or data is kept (Haas, 2011). Once the intrusion is successfully completed the intruder then can have the company’s administration’s privileges and use it to attack the company that would cost them thousand’s of dollars because once the physical intrusion is made, the company’s operation will then be interrupted and disturbed because there is a very high probability that their resources, information and data will be corrupted which will lead to the ineffectiveness and inefficiency of the company’s operation. It would also cause the company to have a bad reputation because once the public will know that the company’s confidential information was intruded it will give them a negative image that they do not have a tight security system, allowing investors and clients to feel unsafe under the company’s supervision which would also lead to sales depreciation. As the director of security I have to implement the Perimeter Intrusion Detection System (PIDS) to prevent these consequences from happening. PIDS is a system used in maximum – security areas such as airports, detention centers, nuclear facilities and more to prevent the intrusion of unauthorized personnel. There are four basic elements in PIDS and these are: Sensors, Video Detection Equipment, Threat Assessment and Alarm Correlation/Management System and Data Communication Systems.

Barrier, Volumetric and Fence Mounted sensors are types of sensors that would detect intruder’s motion in a secured area that would create a physical barrier for the intruder in a form of a wire system and would detect vibrations caused by climbing or cutting of objects in secured areas. Video detection equipment such as cameras is necessary in PIDS because it would detect and capture possible threats such as intruders, vehicles and packages. Once threat is detected by the video operator they will automatically sound the alarm so that immediate action would be taken. The video footage will also serve as reference to any threat analysis in the future. Threat Assessment and Alarm Correlation/Management System will alert and alarm the operators once intrusion or unauthorized change of state has occurred. The alarm will activate once the secured area and the perimeter is breached so that immediate action can be done. The Data Communication System is the most critical infrastructure of PIDS because this provides conjunction between the sensors, video detection equipment and the alarm management system. The Data Communication System must be 99. 999% reliable because once this infrastructure fails; all the other instruments such as sensors, video detection equipment and alarm management system will be useless because these instruments are linked to the data communication system which is the command center of these instruments (“ Perimeter Intrusion,” n. d.). Internet intrusion is where an attacker or an intruder gains access to the company’s confidential resources, information and data through the use of the internet or through the network of the company. Large and small companies operate a website for faster and efficient transactions. These websites allows companies to attract investors, clients and develop a wider market. These websites will also allow the company to market and advertise their products worldwide in a less expensive manner. And in order to advertise their products and transact with their clients the company has to provide their information to the public, such as email addresses, bank account numbers and other necessary information. Clients on the other hand will also have to provide their information in order to complete the transactions such as credit card numbers, email addresses, cell phone numbers and etc. And giving out this kind of confidential information on the internet will attract attackers and intruders to get hold of this information to gain access in people's personal and business accounts to use in their advantage. Once this intrusion is successfully completed it will create interruption to the company because it can destroy the system, there will be interception because there was an unauthorized access to the system and it will compromise the data and transactions made because the system can be modified by the attacker once the system has been intruded. As stated above this will also cost the company and its clients thousand's of dollars and the company's reputation would be at stake if this happens. In order to prevent this intrusion, as the director of security, I have to implement the Agent – based Monitoring, Intrusion Detection and Response System (AMIDAR). The AMIDAR system provides security services that will prevent internet or network - based intrusion. The AMIDAR system will monitor the IP packets traveling; it will monitor the server's log entries online, it will monitor the log generated by the firewalls and it will monitor the behavior of the router. Monitoring the IP packets traveling in the network will allow AMIDAR to detect and respond to network – based attack. Monitoring the servers log entries online will allow AMIDAR to detect and respond to host – based attacks. Monitoring the log generated by the firewall will allow AMIDAR to look for suspicious activities in the network. And monitoring the behavior of the router will allow AMIDAR to detect and respond to attacks targeted at it (Ting, Hwee, Tai, Yong, n. d.). As the director of security I have to implement the PIDS and AMIDAR system in order to prevent illegal physical and internet or network – based intrusion from happening. PIDS is the system used by maximum – security areas to protect and secure the perimeter of high - risk establishments. And AMIDAR is the best system to be used in preventing internet or network – based intrusion because of its complex and diverse methods of detecting and identifying activities that would attack and destroy the company’s database. Once this intrusion is prevented it will allow the company to have a safe and efficient operation allowing the company to generate profit and sales. Reference Page Ting, C., Hwee, O., Tai, T., Yong, N. (n. d.). Intrusion Detection, Internet Law Enforcement and Insurance Coverage to Accelerate the Proliferation of Internet Business Retrieved from http://www. raid-symposium. org/raid99/PAPERS/Ting. pdf Anderson, A. (2011). Illegal Physical and Internet Intrusion to the Database. Retrieved from http://www. angelanderson. com/illegal-physical-and-internet-intrusion-to-the-database/ FUJITSU. (n. d.). Perimeter Intrusion Detection System (PIDS). Retrieved from http://www. fujitsu. com/downloads/TEL/fnc/whitepapers/Atrica_PIDS. pdf Haas, J. (2011) Intrusion. Retrieved from http://linux. about. com/cs/linux101/g/intrusion. htm