Physical security in federal reserve essay sample

Law, Security

Federal Reserve is an agency that has various branches in the USA, which forms a system. The physical security system of Federal Reserve is very complex and sophisticated, since this agency deals with money and control of various banks. The processes involved include control of finances, communication protocols to all branches and control of personnel in different points of work requires a complex system (Philpott, Shuki, 2006). The continuity of operations is a challenging task to maintain, this calls for a complex that can be able to tackle all the operations simultaneously and provide timely response.

Another significant tool is the backup plan in systems such as that of Federal Reserve. Back up is as important as the protection to the system itself. This is because disasters are unpredictable and in such cases losses inevitable. Lack of having a backup plan on the Federal Reserve is very detrimental and precarious to the crucial and critical materials and data stored in the system. A total catastrophe can cause a total loss of all materials and data such as computers and data servers. Critical information when lost due to a catastrophe is hard to recover. Since it is the headquarters, it contains critical and sensitive data about all banks in the USA, and therefore; loss of massive and sensitive data makes the situation undesirable to the running of the system. Information accumulated over several years cannot be recreated in a few months for the operations to resume and this forces stalling of operations (Norman, 2007). Sometimes, the organization has to start as if it is a new company. The presence of back up facilitates assist in the continuity of operations even after a total catastrophe.

2) What are some other possible scenarios that could completely shut down the Federal Reserve's headquarters building located in Washington DC? Other than back-up plan, other scenarios that can cause the Federal Reserve Headquarters in Washington DC to shut down include fire, bomb explosion, total damage to the network infrastructure and adverse natural disasters such as tsunami, Katrina and strong earthquakes. Fires are known to cause large quantity of damage to the point that even a single material cannot be recovered. In case of an outbreak of fire, the physical security should be able to detect it and try to counter it (Norman, 2007). If the fire is big and cannot be put off, then materials in the building such as the working personnel in the premises need to be evacuated to avoid total loss. As started earlier, fires that cannot be put off have much loss and can lead to shut down of the headquarters in Washington DC.

On the other hand, the United States commonly experience high magnitude of Katrina, earth quakes and Tsunamis. These disasters are unpredictable and even cannot be counteracted by the protection mechanism of the system. They can cause the collapse of many buildings especially the skyscrapers on which the Federal Reserve System is positioned. Whenever they occur, a significant amount of damage is caused and can lead to the shutdown of the headquarters (Philpott, Shuki, 2006). In addition, bomb explosion is another cause that can make the closure of Washington DC Headquarters. Despite, the high security mechanisms in the Federal Reserve System, there are still high threats of bomb explosion in the American soil. There are still unsuspected enemies who can pass through the security system and place a bomb inside the premises of the Reserve. Either suicide

bomber or even a truck fitted with explosives that can blow up the entire premises can implement the action (Benny, Baker, 2013). In this case, the whole premises is brought down and forces the headquarters in the Washington DC to shut down.

3) How could the Federal Reserve System prepare itself for such a huge disaster as a massive truck bombing? Should it act proactively to mitigate the hazard even though it has never happened or there may be no intelligence indicating it might happen in the near future? In relation to the disasters, the Federal Reserve System should be always ready for any kind of disaster. The security system with its complexity should be able to detect and advise suitable measures to be taken in case of any disaster. Consequently, preparations are necessary to stay alert of any disaster; each party involved is enlightened on actions to follow to achieve the set-aside protocols. The security sensors such as the security cameras, sniffer dogs and bomb detectors should always be on high alert to detect any kind of explosive in the premises (Benny, Baker, 2013). The security detail should not rest or take it for granted on any threat that can cause risk to the premise. Actually, mitigations should always be there for any risk to the premises. These mitigations should always be in place even if there is or no intelligence that any disaster can happen in the near future (Norman, 2007).

4) What would a good plan of operation be if the Federal Reserve System headquarters was completely put out of commission? Where could all of the employees be relocated? What location could act as a temporary headquarters while the main building was repaired or replaced? Should

parking accommodations already be planned for such a contingency? Should transportation be provided? Might there be a problem of overcrowding at the new location if it is much smaller than the existing headquarters? Could the employees simply be shifted to other Federal Reserve Bank locations? In case the Federal Reserve Headquarters is put out of commission, a good plan of operation is that the most important employees should be relocated to a different premise to ensure continuity of operations.

Some employees can also be moved to other Federal Reserve branches to ensure the information as well as communication to the headquarters is continuous, and nothing will affect the operations of the Federal Reserve System. The building for relocation should be suitable to sustain continuous flow of operations, probably not very far from the main premises (Norman, 2007). On the other hand, transport can be provided to carry machines and equipment, which can be required in the temporary location. In case of overcrowding, job expansion can be done to some employees and others given leaves and resume when the main premises are in good condition. In addition, the employees cannot simply be moved to other bank locations because it creates overcrowding conditions in the branch bank locations.

5) Should the computer data stored at the Federal Reserve System headquarters be constantly backed up at an offsite location? How often should this information be backed up? Could this slow down business operations if all data had to be saved in multiple locations all the time? Why would it be important to have multiple safeguards and redundancies in regards to important computer data? As earlier stated, backup plan should

be installed and given priority equal to the protection strategies. The backup should be located in an offsite location different from the main system.

This ensures the security of the backup in case of any fire, explosion or any catastrophe that can occur in the main premises (Benny, Baker, 2013). There should a plan on the times at which the backup is updated. According on the amount of data received and sent in and out of the Federal Reserve headquarters, backup update should be done daily to ensure no information can be lost in case of any disaster. Simultaneous saving of data does not reduce the speed of operations, since the systems are designed with high speed to support multiple operations to occur at the same time with no delays. It also saves time and increase effectiveness of backup updates (Benny, Baker, 2013). In addition, the system should have multiple safeguards and redundancies to increase the effectiveness of the backup and put more measures to ensure that no data is lost.

Conclusion

Overall, physical security of Federal Reserve should be a complex, complicated and sophisticated system that can detect and provide mitigations to suitable solutions. A large agency such as Federal Reserve System, is very vulnerable to various and different security breaches; and therefore, the security system should always be on alert to detect any risks (Norman, 2007). In addition, due to the evolution of the electronic development, the security threats are unpredictable and this makes the security system to be complex (Norman, 2007). Furthermore, backup plan is a crucial part of the system, and without it, the system is not complete. The

most important part of the backup is the updating and recovery process. The backup should also be placed in an offline location in a different place from the main premises (Philpott, Shuki, 2006). Despite that, the system requires protection and backup, the two requirements are very expensive to install and maintain. However, they are very significant to the well-being of the system.

References

Philpott D. & Shuki E. (2006). The Integrated Physical Security Handbook. Virginia: Homeland Defense Journal.

Benny D. & Baker P. (2013). The Complete Guide to Physical Security. Florida: CRC Press.

Federall Reserve System, Board of Governors (BOG) (1947). Federal Reserve System: Its Purposes and Functions. Washington Dc: Washington.

Norman T. (2007). Integrated Security Systems Design; Concepts, specifications and Implementation. Boston; Elsevier Butterworth-Heinemann.