Fraizer

Discuss what is meant by "acceptable risk" in determining a risk management plan relating to critical infrastructure, and how the level of acceptable risk may differ among stakeholders.

There is risk associated in every action taken; reference can be made to the Sir Isaac Newton's third law of motion the "Law of Reciprocal Actions." Which pronounces that "for every action, there is an equal but opposite reaction." The observation could be presented that for every action, there can be different outcomes associated with the actions taken. These results will have different levels of risk and the consequences assigned to them. Even if the significant threats and vulnerabilities are identified, examined, and have criteria in place to subdue specific hazards; there will yet be the opportunity for residual risks to remain. Some of these residual risks will also require to be compared amidst tolerances of an event occurring, and for the safeguarding of personnel, information, and assets while others may be considered an acceptable risk, due to lack of belief of a valid threat.

Risk has always been a problematic word to define because everyone views risks differently due to the risk not having a negative outcome on them; which is the "not my problem since that does not affect me" approach to risk management. In the end, stakeholders are customarily the individuals making the determinations on what risks are deemed high and low value; along with rendering funding plus support concerning the acquisition and implementation of devices and procedures, for assuring the protection from identified risk.

The initial step towards evaluating "risk" should be the development of a customized based on the organization's needs and concerns; this will assist in identifying areas of interest and classifying levels of acceptable and unacceptable consequences that the risk management strategy should address. Because risk outcomes and threat probability depend upon each distinct quandary, unusual circumstances must be stipulated to allow for possible conditions that could occur. The framework utilized in appraising the risks of incidents, the threat likeness, and the analysis of whether the risk is low level and considered being acceptable or the risk should be regarded as a high priority for the safeguarding of critical information, components, or personnel (Fischhoff, Watson, & Hope, 1984).

On July 15 of 1996, President Clinton signed Executive Order 13010, which authorized the "President’s Commission on Critical Infrastructure Protection," gave definitions as to what constitutes critical infrastructure. Identifying that there some components that are operated daily that fashion our way of life that have become so essential that their inability to function normally due to disruption of service, damage, or destruction of components. Any of these events would produce a debilitate result that could undermine the security or financial assurance in areas of the United States or the country as a whole. Some of the crucial areas identified by the executive order were finance, emergency services, energy, water, gas, and oil along with transportation. After 9/11 President Bush signed an order authorizing the Office of Homeland Security and the Homeland Security Council and task the newly formed organizations with the coordination of information between United States government agencies and state agencies to implement measures to protect and safeguard critical infrastructure components. President Bush also signed Executive Order 13231,13 which added more crucial area such as health care, agriculture, and food (Moteff, Copeland, & Fischer, 2003)

Regards,

Nate

References:

Fischhoff, B., Watson, S.R., & Hope, C. (1984). Defining Risk. Retrieved April 17, 2019, from http://sds.hss.cmu.edu/risk/articles/definingrisk.pdf

Moteff, J. D. (n.d.). Critical Infrastructures: Background, Policy, and Implementation. 39.

Moteff, J., Copeland, C., & Fischer, J. (2003). Critical Infrastructures: What Makes an Infrastructure Critical? 20.