Respond to this post ( rebecca's Gaidich )

 In order to answer the question posed, one must first go back to the original definition of risk and the importance of our critical infrastructure. Last week, critical infrastructure was defined as both physical and cyber-based components which are prime targets for potential terrorist attacks due to the fact that they are integral to the functionality of our society (“Homeland Security Presidential Directive 7”, 2015). This means that without them, society will crumble and the damage will be catastrophic. The implication is that they must be protected at all costs and the priority for that is extremely high.

In the first week, Kaplan and Garrick (1981) was referenced as stating that not only is there a difference between “probability” and “frequency” but the concept behind “probability” is intrinsically intertwined and connected to the idea of risk (Kaplan & Garrick, 1981, p. 11). In addition, when one attempts to define risk, one must understand that risk encompasses a multitude of components such as uncertainty and/or loss; the possibility of loss and/or injury; as well as the knowledge that risk is “relative to the observer” (Kaplan & Garrick, 1981 p. 11-12). This implies that risk is a combination of “what you do”, in collaboration with “what you know”, as well as “what you do not know” (Kaplan & Garrick, 1981, p. 12).

With the above in mind, acceptable risk is simply deciding what risk factors are acceptable in comparison to others. It is a concept based upon a logical progression of decisions where risk is further defined under the idea of “simplifying assumptions” (Fischhoff, Watson, & Hope, 1984, p. 137). This is important because risk factors will vary as well as the perception associated with them. A great example of this was given by Fischhoff, Watson, and Hope (1984) who breaks down their example by assigning weight with the following five tradeoffs, if you will, of five risk attributes: public deaths, occupational deaths, morbidity, unknown risk, and dread risks (Fischhoff, Watson, & Hope, 1984, p. 134). In doing so, they utilize a logical framework where each component is assigned a value and/or weight. This now allows for a logical progression when making a decision.

The importance of this concept is tied back to what Kaplan and Garrick (1981) state about how risk is relative to the observer (Kaplan & Garrick, 1981, p. 12). In other words, their perception of value and/or their personal point of view can dictate the value assigned to a risk factor. This means that when considering a risk management plan in relation to critical infrastructure, one of the most difficult things to determine will be the value associated with each risk and ultimately, the weight associated with it. This means that the level of acceptable risk can drastically vary from stakeholder to stakeholder based upon the value they assign to a risk factor. The ability to come to an agreement on the various risk factors and a mutual agree on the value of each factor, will be critical to making decisions moving forward. In any type of critical infrastructure, the goal is to make decisions utilizing logic, not emotion.

References

Fischhoff, B., Watson, S. R., & Hope, C. (1984). Defining risk. Policy sciences, 17(2), 123-139.

Kaplan, S., & Garrick, B. J. (1981). On the quantitative definition of risk. Risk analysis, 1(1), 11-27.

Homeland Security Presidential Directive 7. (2015, September 22). Retrieved April 10, 2019, from https://www.dhs.gov/homeland-security-presidential-directive-7