# Risk management table

Technology, Information Technology

Risk Management The team applied a significant set of risk management considerations in the process of ranking the probability and impact of the different types of information security threats to an organization (Wheeler, 2011).

It is vital to note that, in the final ranking, major emphasis was laid on the impact of a threat to an organization followed by its probability to happen. This is because; it is the impact that defines how a particular threat can affect the confidentiality, integrity and day-to-day availability of the organization resources (Wheeler, 2011).

In simple terms, probability was considered as the second requirement in the ranking process. This is due to the fact that, probability mainly defined the expected number of times that a particular impact can happen. Therefore, if the impact is high and the probability is also high, then the team ranked this as a top threat. Contrastingly, if both are low then that particular threat was ranked at the lowest level (Wheeler, 2011).

The reasoning behind the mitigation steps for different types of threats is as stipulated below. If a threat affects the operations of a network device, then the mitigation steps shed light on protecting its data storage locations along with its network access layer. Secondly, if the threat is due to poor user practices, the mitigation steps focused on coming up with the proper policies on the use of organization resources. Lastly but certainly not the least, if a particular threat affected a whole system, then focus was laid on configuring the interconnection devices such as routers and switches (Wheeler, 2011).

References

Wheeler, E. (2011). Security risk management: Building an information

security risk management program from the ground up. Waltham, MA: Syngress.