Enterprise risk assessment, audit and Cyberlaw

ISSC 498

The enterprise risk assessment for my organization the 899th Communications Squadron (899 CS) will help leadership understand the important risks and how they relate to the operational, tactical and strategic mission. The process for evaluating the information for the 899 CS is critical as any breach or loss of critical information can be consequential. Performing the enterprise risk assessment for the 899 CS will be the Chief IT security manager and his team of IT security professionals and consultants. The gathering of information for the enterprise risk assessment is very important and will be done with surveys due to the amount of personnel in the 899 CS, also interviews will be conducted for the senior leaders in the organization to gain a better understanding of their focus and to discuss any sensitive topics (Williams, 2018). Lastly meetings will be help in small groups with the middle and lower tier of the organization to discuss the top priorities to focus on for the enterprise risk assessment will be thoroughly discussed. While the collecting of information can be a long and tiresome process, the assessment must be detailed and transparent, everyone in the organization’s roles will be clearly identified.

The main goal of conducting the enterprise risk assessment is to evaluate and study all risks and understand the influence they will have on the 899 CS (Williams, 2018). The probability and occurrence of any risks will be examined. In addition, an internal audit of the 899 CS will be conducted, threats will be defined such as the possibility of attacks such as spoofing, phishing, DDos and any malicious internal threats. The current security performance will be tested and assessed, an external organization will visit the 899 CS to evaluate the organization’s security performance and posture, this can lead to adopting best practices to help combat any risks. The final step is cyberlaw will be instituted to protect the 899 CS from any illegal access and theft of its intellectual property. Every member of the 899 CS must understand cyberlaw, which is put in place to help protect all members of the organization from any malicious attacks and keep order and discipline in place. If a member broke a rule the organization has the right to discipline them and provide punishment. Not only can the senior leaders of the 899 CS take action, the hierarchy will be set up that if the punishment is more serious additional action can be taken by the United States government.

Professor Comments:

Thank you for your work in that assignment as a continuation to the work in the overall security plan. During the discussion of that week, we did research over these three areas so it will be good to leverage much of the information there in this assignment. Your document was pretty good in terms of describing how to develop the plan or best approaches in developing the plan or why you need the plan or who will participate in writing the plan,...etc. However, what you need to do is the "plan" itself and I was not able to see that. Ideally, you will give your document to a team and this team will take your document and then run the plan step by step to do the audit or whatever function described in the plan. Hope this makes sense.

References

Williams, C. (2018, April 23). Enterprise Risk Assessment – Transforming Risk Information into Action. Retrieved February 28, 2020, from <https://www.erminsightsbycarol.com/enterprise-risk-assessment/>