Ian Waweru

Hamza, Demirel

Cyber risk management

11/4/2023

Planning Risk Mitigation Throughout an Organization

Chapter 10 of the reading focuses on the critical topic of “Planning Risk Mitigation Throughout an Organization”. This chapter underscores the significance of integrating risk mitigation strategies into an organization’s core processes and decision-making, rather than treating risk management as a standalone function. It highlights that risk mitigation planning should be initiated after identifying organizational assets, threats, and vulnerabilities. Not all risks are equal in their potential impact and likelihood. Organizations must identify which asset is considered the most to least important. Many organizations tend to label their assets with either high, medium, or low. This evaluation helps in understanding, which risks require immediate attention and resource allocation. Every organization should have a risk management team. The risk management team for an organization is multifaceted, encompassing various aspects of identifying, assessing, mitigating, and monitoring risks. The management team's main objective is to achieve specific objectives and safeguard the organization’s interests. One of the many things they do is implement controls and strategies that can effectively mitigate risks throughout the entire organization. Identifying risks and assessing them is a foundational step, but it’s in the implementation of mitigation strategies that planning risk mitigation is translated into action. Once the risks are understood, organizations need to develop and execute strategies to mitigate or manage them effectively. Effective communication about risks and risk mitigation strategies is vital. It ensures that employees are aware of potential risks and understand their role in mitigating them. I can relate to a lot of things this chapter discussed. I am currently an intern for a company called Telos. I am on the content management team and my team specializes in risk mitigation. I've handled a couple of government regulations, and they are all unique in their way. The following regulations I've worked with are The National Institute of Standards and Technology (NIST), Information Security Manual, (ISM), Cybersecurity Framework (CSF), and Committee on National Security Systems (CNSS). Each of these regulations has a multitude of controls and supplemental guidance. I got to work on a couple of these regulations, and I got familiar with the groupings of each control. For example, access control (AC) is a control group that talks about what personnel have access to within an organization. Based on that control you know it has high importance and understanding roles within the organization can help mitigate potential risks. Another project I worked on had to do with the CSF, the CSF is a document that contains a group of controls that understand cyber risks and improve defenses. I extracted the controls and their guidelines and put them in an Excel sheet. A new regulation came out a few months later and it was called the CSF 2.0. Updates are going to happen because technology is consistently rising, and hackers are getting clever by the day. I was tasked to compare each document to see whether new controls were added, what controls changed, what got deleted, etc. Updates like this will mitigate risks and it could help the organization stay ahead. I telework and there is a mitigation strategy for that as well. We have a private WIFI that I can connect to and it’s much safer than my home WIFI. In Chapter 10 it is stated as one of the seven domains, and it is called the “remote access domain.”. In conclusion, Chapter 10 provides valuable insights into the need for organizations to proactively incorporate risk mitigation into their DNA. By doing so, organizations can better protect their objectives and foster a culture of adaptability, ultimately increasing their chances of long-term success.