Ian Waweru

Hamza, Demirel

Cyber Risk management

09/30/2023

Define Risk Assessment Approaches

 Chapter 5 of this week’s reading discusses the importance of risk assessment approaches in the context of risk management. In an organization, cyber-attacks can have a major impact on people and business operations. Hackers will attack an organization to steal company information, employee personal information, financial gain, revenge, etc. It’s important to neutralize all these attacks to protect the employees and the business itself. Attending to all the cyber-attacks that occur can be a difficult task, each attack can affect an organization differently. Cybersecurity is also an expensive field and for an organization to ask if they can neutralize all these threats can be an expensive investment. Managing these attacks is very important and companies can do this by developing a risk assessment. A risk assessment highlights a crucial process for identifying and prioritizing risks, and it plays a central role in effective risk management. Risk assessments also help allocate security funds efficiently, especially in complex regulatory environments. Depending on the company's business operations, this assessment will manage high-priority risks, and accept low-priority ones. The purpose of this assessment is to help in evaluating the effectiveness of controls and aid in determining which risks should be reduced, avoided, shared, mitigated, or accepted. There are two types of risk assessments: Quantitative and Qualitative. Quantitative risk assessment involves using numbers and formulas to quantify and measure risks. This assessment's key comments include Single loss expectancy (SLE), Annual Rate of occurrence (ARO), Annual Loss Expectancy (ALE), and safeguard values. One of the many benefits this assessment brings is a clear, quantitative basis for decision-making and resource allocation. The second type of risk assessment is the quantitative risk assessment. This assessment involves a more subjected approach to evaluating risks. Instead of using numbers like the previous assessment, this one relies on expert judgment and decisions to assess the probability and potential impact of risks. There are two key components, and they are known as probability and impact. Probability will measure the chances a threat will exploit a vulnerability and impact will measure the outcome if a risk occurs. There are a multitude of benefits this assessment provides. For example, it will provide a quick and accessible way to assess and communicate risks. Both assessments are not going to hurt your organization, they will only help improve security. I work as an intern for a company called Telos and our company takes the quantitative assessment approach. I work with the content development team and for one of my projects I had to check this Excel sheet listed with controls and regulations. One thing I had to ensure when I was checking the Excel sheet was that the prioritization section was labeled correctly. The prioritization section was labeled, low medium, and high. It’s very important to ensure this section is labeled correctly because there are things, we do in the organization that require more attention than others. Phishing email attacks is an attack this company ensures to prepare for. This would be considered a medium to high priority for telos. They make sure to enforce training weakly to remind people not to click on links or explain the different types of cyber-attacks. In conclusion, chapter 5 provided valuable insights into the fundamentals of risk assessment and its crucial role in effective risk management. There is always going to be a threat and it can’t all be periodized, it is important to develop a risk assessment to manage threats that occur in these organizations.