Amenaza
TECHNOLOGIES LIMITED

Aerospace Risk Assessment Methodology

Title: ***An Allied Government Requires Objective Way of Evaluating and Comparing Risk***

Executive Summary

The government of a major NATO member frequently awards projects to defense contractors. Deciding who should be awarded contracts presents a challenge. Equally important to cost is the need to ensure that bids represent products of similar functionality, quality and security. The fulfilment of cybersecurity requirements is particularly important. Historically, each contractor had their own processes for evaluating cyber risk. This made apple-to-apple comparisons difficult.

A major aerospace contractor developed a risk assessment methodology for a very major project. Unfortunately, several of the methodology steps were cumbersome or infeasible to perform manually. The contractor required a partner with an approach, a software technology and a training program compatible with their in-house solution. After evaluating various options, the contractor selected Amenaza Technologies as their partner. Amenaza provided tools, training and contributed to the overall success of the project.

The government backer was impressed by the quality of analysis and assurance that was performed. With the cooperation of the defense contractor, the pioneering risk assessment approach became a standard for all similar projects. This led to the widespread adoption of Amenaza's approach across many aerospace contractors. Today seven of the world's top ten defense contractors have adopted Amenaza's approach and use the SecurITree® threat modeling software to ensure the integrity of their products. It is now the industry standard in this field.

Amenaza's Approach

Many industries have their own hostile risk assessment methodologies. In fact, a U.S. research group found over one hundred threat-risk methodologies in existence. However, they noted that virtually all of these methodologies shared fundamental principles. They all need to evaluate both the likelihoods and projected impacts of possible attacks. And, almost without exception, the methodologies provide no guidance as to how attack likelihood should be determined.

In the world of hostile risk statistics either don't exist or are only applicable in a very limited situations. They lack general applicability. Most organizations fall back on qualitative estimates based on the intuition of subject matter experts. Even if these estimates are valid, they fail to capture the reasoning process used to generate them. This leaves the assumptions open to criticism.

Amenaza's threat assessment process understands that attacks are primarily driven by human behavior. The methodology uses attack tree models to assess the feasibility and desirability of thousands of potential attacks from potential adversaries. This identifies high risk scenarios and the most effective mitigation strategies – the effectiveness of which can be validated in the models.

Amenaza
TECHNOLOGIES LIMITED

The process captures and documents the decisions that were made. This provides strong evidence of due diligence should an incident still occur.

Why It Mattered

Amenaza's advisory work, training and technology allowed standard threat-risk assessment processes to become widely prevalent in the aerospace industry. Government sponsors can now make rational decisions as to which defense contractor is best able to create the best deliverables for a project.