Risk Assessment

By Devarsh Parmar

Records

There is a lot of inconsistency in the records which are on paper and on the cloud. This is such an information hazard which can lead to lose of millions which damage.

Let’s talk about the CIA Triad and how its linked to the above problem:

- C stands for Confidentiality means that only authorized individuals/systems can view sensitive or classified information. The data being sent over the network should not be accessed by unauthorized individuals. The attacker may try to capture the data using different tools available on the Internet and gain access to your information. A primary way to avoid this is to use encryption techniques to safeguard your data so that even if the attacker gains access to your data, he/she will not be able to decrypt it.
- Integrity means that data has not been modified. Corruption of data is a failure to maintain data integrity. To check if our data has been modified or not, we make use of a hash function such as SHA (Secure Hash Algorithm) and MD5 (Message Direct 5).
- Availability means that the network should be readily available to its users. This applies to systems and to data. To ensure availability, the network administrator should maintain hardware, make regular upgrades, have a plan for failover, and prevent bottlenecks in a network.

Seeing these definitions, we conclude that information security is maintained by all of these but the case of inconsistency is taken care under Integrity of data. Also there is no control on who can access the company files, this violated the Confidentiality aspect of the triad which every company should abide to.

Root Cause Analysis

Root cause analysis looks to find what the underlying vulnerability or mechanism of failure is that leads to the incident. By contrast, proximate cause analysis asks, “What was the last thing that happened that caused the risk to occur?”

So firstly we will look into Quantitative and Qualitative Analysis to gauge where we lie with our existing problems.

Qualitative vs Quantitative Analysis

1. Subjectivity: Qualitative analysis is subjective and scenario-based, while quantitative analysis assigns numeric values to risk components
2. Cost and Time: Qualitative analysis is cheaper and faster to implement, but quantitative analysis can enhance cybersecurity planning efforts
3. Measurement: Qualitative analysis uses ordinal or relative scales to rate risks based on expert opinion, while quantitative analysis shows risk in dollar terms based on a standard model and produces consistent results
4. Data Collection: Qualitative analysis relies on data that is difficult to quantify, such as expert opinions, while quantitative analysis uses measurable data
5. Risk Assessment: Qualitative analysis is scenario-based and subjective, while quantitative analysis is based on a standard model and produces consistent results
6. Risk Prioritization: Qualitative analysis prioritizes risks based on expert opinion, while quantitative analysis prioritizes risks based on their financial impact

What should we adopt?

We should definitely need to adopt quantitative analysis.

Quantitative method could be more adapted for information security risk assessments.

Quantitative Analysis uses measurable data and prioritizes risk based on their financial impact.