Abstract

Information is a key asset for organizations, and reducing the risk of information compromise is a high priority. There are a lot of risk analysis methods available today, some of which are qualitative while others are more quantitative in nature. They all have the same fundamental target to estimate the overall value of risk, but most attempts to hit the target from very different approaches. Some approaches can be applied to all types of risk, while others are specific to particular risks. This work addresses some of the methodologies used currently to analyze information security risks. The main task for an organization is to determine which one to use. Since the organization will spend money on whichever method they choose, it is vital that the
chosen methodology meet the requirements. The purpose of the study is to compare and clarify the different activities, inputs, and outputs required by each model of information security risk assessment and the analysis that effectively addresses the risks of information security.

References

- Casualty Actuarial Society CAS, Overview of Enterprise Risk Management.
- S. Hariri, Q. Guangzhi, T. Dharmagadda, M. Ramkishore, and C. Raghavendra, "Impact analysis of faults and attacks in large-scale networks," IEEE Security and
A Comparative Study on Information Security Risk Analysis Practices

- International Security Technology Inc (IST Inc), "A brief history of CORA,"

Index Terms

Computer Science

Security
Keywords
Component  Information Security  Risk Analysis  Risk Assessment  Risk Analysis
Models  Analysis Method

Risk Analysis Comparison

Information Security Risk Analysis Methods