Information Security Risk Assessment

Subjects: Mathematical & Computational Biology

Contributor: Ievgeniia Kuzminykh , Bogdan Ghita , Volodymyr Sokolov , Taimur Bakhshi

Information security risk assessment is an important part of enterprises' management practices that helps to identify, quantify, and prioritize risks against criteria for risk acceptance and objectives relevant to the organization. Risk management refers to a process that consists of identification, management, and elimination or reduction of the likelihood of events that can negatively affect the resources of the information system to reduce security risks that potentially have the ability to affect the information system, subject to an acceptable cost of protection means that contain a risk analysis, analysis of the "cost-effectiveness" parameter, and selection, construction, and testing of the security subsystem, as well as the study of all aspects of security.

information risk management | security risk assessment | risk classification | OCTAVE | CRAMM | RiskWatch | fuzzy logic

---

Over time, the complexity of information systems is increasing, and, therefore, the issues of information security are becoming increasingly important for any organization. In this context, particular attention is paid to the analysis and assessment of information security risks as a necessary component of an integrated approach to information security.

Typical analysis (and the associated assessment) of information security risks is performed during the information security audit of a system or the design stage. The main task of an information security audit is to assess the ability and effectiveness of control mechanisms applied to the information technology components, as well as the architecture of information systems in general. An information security audit includes many tasks, such as assessing the effectiveness of the information processing system, assessing the security of the technologies used, the processing process, and management of the automated system. The overall purpose of an information security audit is to ensure the confidentiality, integrity, and availability of an organizationâs assets. Information security risk assessment is also an integral part of an information security audit.

Depending on the result of their evaluation, methodologies for assessing information security risks can be either quantitative or qualitative. The output of the algorithm of a quantitative methodology is the numerical value of risk. The input data for evaluation are usually used to collect information about adverse or unexpected events in the information security system, which may jeopardize the protection of information (information security incidents). However, the frequent lack of sufficient statistics leads to a decrease in the accuracy and relevance of the results.

Qualitative techniques are more common, as they use overly simplistic scales, which usually contain three levels of risk assessment (low, medium, high). The assessment is carried out by interviewing experts, and intelligent methods are still insufficiently used.

It is apparent that both of the above options have a number of inherent shortcomings. In order to overcome them, recent research focused on identifying alternative techniques that would be both more accurate and more adaptive, as the constant emergence of new sources of threats often renders existing methodologies inaccurate and ineffective. Among the promising methods, there are models based on solving uncertainty problems such as fuzzy logic models and artificial neural

networks.

Existing textbooks and studies provide a substantial amount of information, describing either the theoretical concept, a novel approach, or a specific case study implementation. While relevant for specific audiences, such studies are either too extensive or too specific, hence not providing a summary for potential researchers and adopters in the area of information security risk assessment. This entry provides an analysis and comparison of existing methods of information security risk assessment, highlighting their common features, benefits, and shortcomings. The structure of the entry follows closely the concept of information security risk. Section 2 provides a definition, followed in Section 3 by a comparative review of the two main categories of risk analysis (qualitative and quantitative). After the necessary theoretical context is provided, Section 4 provides an extensive analysis of proposed information security risk assessment approaches, including CRAMM, FRAP, OCTAVE, and RiskWatch. Section 5 reviews the limitations shared by the existing techniques and provides possible solutions to overcome them, and then Section 6 concludes the entry.
