Information Security: The Enemy from Within

Seev Neuman, Moshe Zviran and Jacob Mendel

The rapid growth of information technologies and networks has led organizations to consider the issue of systems and data security, where the main objectives are secrecy, integrity and availability of the systems and the information. The cornerstone of information security in organizations is defining and applying appropriate procedures and mechanisms for systems and information security, without compromising organizational needs. While many protection structures deal with detecting and preventing the access of external threats to the organizational systems, only little attention has been paid to the "insider threat" - authorized users within the organization who can damage systems security either maliciously or unintentionally. This paper focuses on describing the threats and risk factors internal to the organization, discusses the risks emanating from them and suggests ways to reduce threats and protect against them.

Classification in Behavioral Big Data: Machine, Human, or Both?

Inbal Yahav and David Schwartz

Data classification is a common task in many real-world applications: retail companies, for example, use classification models to predict customer churn, while banks and financial companies use them to detect fraud, and healthcare providers apply them to disease diagnosis. Classification problems are more challenging when applied to data on human and social behavior, and especially when these data are textual. Examples are the classification of opinion articles, the classification of tweets, and the classification of interviews. This article deals with the classification of textual behavioral content using an innovative human-machine integration framework. The research presented is interdisciplinary, borrowing from concept theory, machine learning, and qualitative research.