

### Value-Based Security Risk Mitigation in Enterprise Networks that are Decentralized

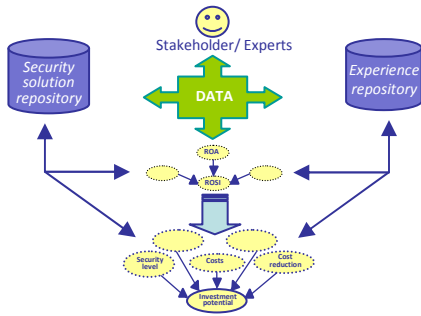
In industrial practice, security engineering is risk management: how to mitigate security risk given a finite budget? Today the IT of a business is connected to that of others in a value web of business partners, suppliers and customers, each of whom has its own confidentiality, integrity and availability requirements. This creates new security challenges, because there is no central decision-making authority in these networks. The problem to be investigated in VRIEND is how to extend current risk management practices with methods and techniques to deal with security risks in decentralized networks.



# VRIEND

<http://vriend.ewi.utwente.nl/>

## Project framework



VRIEND framework consists of three main parts: (1) two repositories, where one contains the alternative security solutions and the other experience data from previous security investments. (2) BBN-based Return On Security Investment module that incorporates ROA. (3) BBN-based security investment trade-off analysis that takes relevant information in the repositories and the resulting ROSI as input and outputs the investment potential of alternative security solutions. This enables us to evaluate alternatives against each other.

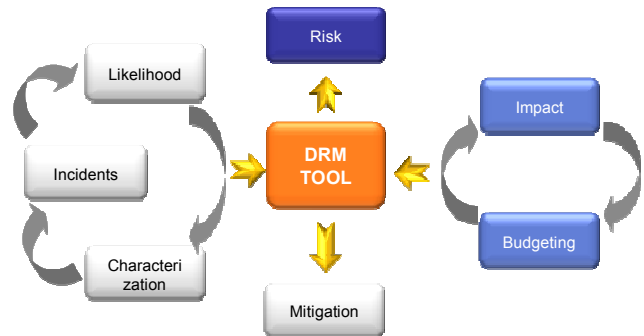
Data are fed into the two repositories from several sources, such as domain experts, public repositories, system stakeholders and the results from previous or relevant investment evaluations. The two repositories both provide input to and receive results from the ROSI and Investment Potential modules in the VRIEND framework.

## Vision

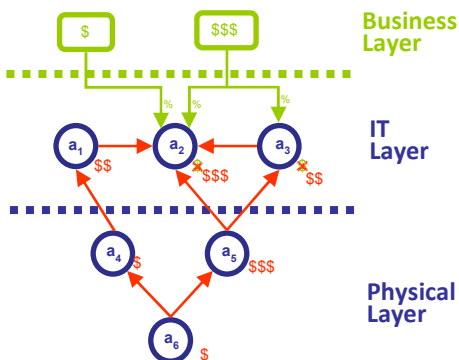
IT systems as well as their environment are subject to dynamic changes. Nowadays, risk management is done to a great extent manually. This yields to risk analyses which are not as accurate as they should be and which can not deal easily with changes in the infrastructure.

VRIEND will support organizations in IT risk related decision processes by delivering models and tools which can deal with a dynamically changing environment. This approach is suitable for rapidly changing organizations where it is important that the level of risk is constantly kept under control.

Technically, we split the classical Risk Management Cycle into two smaller cycles (technical cycle and business cycle) to speed up the decision making process.



## Results



We have developed two models for supporting the dynamic risk management process: (1) Time Dependency Model (TDM) in the field of availability risk management and business continuity, (2) Distributed Risk Assessment Model (DRAM) in the field of confidentiality risk management. The TDM Model has already been implemented as a tool and the DRAM Model is meant to be implemented by Fall 2008. They both assess the risks in a continuously changing environment by considering the impact of propagating incidents in an IT system.

Furthermore, for architecture alignment of business requirements on IT systems we model the relations among the system components using so-called layers. The motivating idea is that, layers enable concentrating on different attributes of assets and studying the mutual relations among them on different abstraction layers, meanwhile remaining expressive.

**Project members:**

- prof.dr. R.J. Roel Wieringa (project leader)
- prof.dr. Pieter Hartel
- prof. dr. Sandro Etalle
- dr. Maya Daneva
- dr. Pascal van Eck
- dr. Siv Hilde Houmb
- Ayse Morali (a.morali@utwente.nl)

**Industrial partners:**

- AkzoNobel
- Corus
- DSM
- Philips Electronics