Quantifying IT Security – Risk Management Metrics

COST ECON@Tel Public Workshop
Stockholm, June 16 - 17, 2009

Denis Trček

Laboratory of E-media

Faculty of computer and information science

University of Ljubljana

denis.trcek@fri.uni-lj.si

Introduction

- Security is among top priorities in IS for more than a decade.
- This area still lacks appropriate metrics:
  - It took some time to recognize that IS risk management is “just another” decision making process under uncertainty.
  - But existing risk management methods are of a limited use in information systems, because information technology is so rapidly changing that decades old aggregates of data are not existing.

The outline of this presentation

- Risk management basics (RM).
- Presentation of a generic risk management model that supports computerized implementation, covering reactive, active, and pro active treatment.
- Overview of the latest approaches in this field that are suitable for RM.
- Evaluation of these approaches for deployment in IS risk management.

IT Risk Management Basics

- The main standards in this area:
  - Int. standards organization, Information security risk management, ISO 27005, Geneva, 2008.
  - NIST, Managing Risk from Information Systems, NIST SP 800-39 Draft, US Dept. of Commerce, Washington D.C., 2007.
  - US Department of Health, Basics of Risk Analysis and Risk Management, US Dept. of Health & Human Services, Washington D.C., 2008.

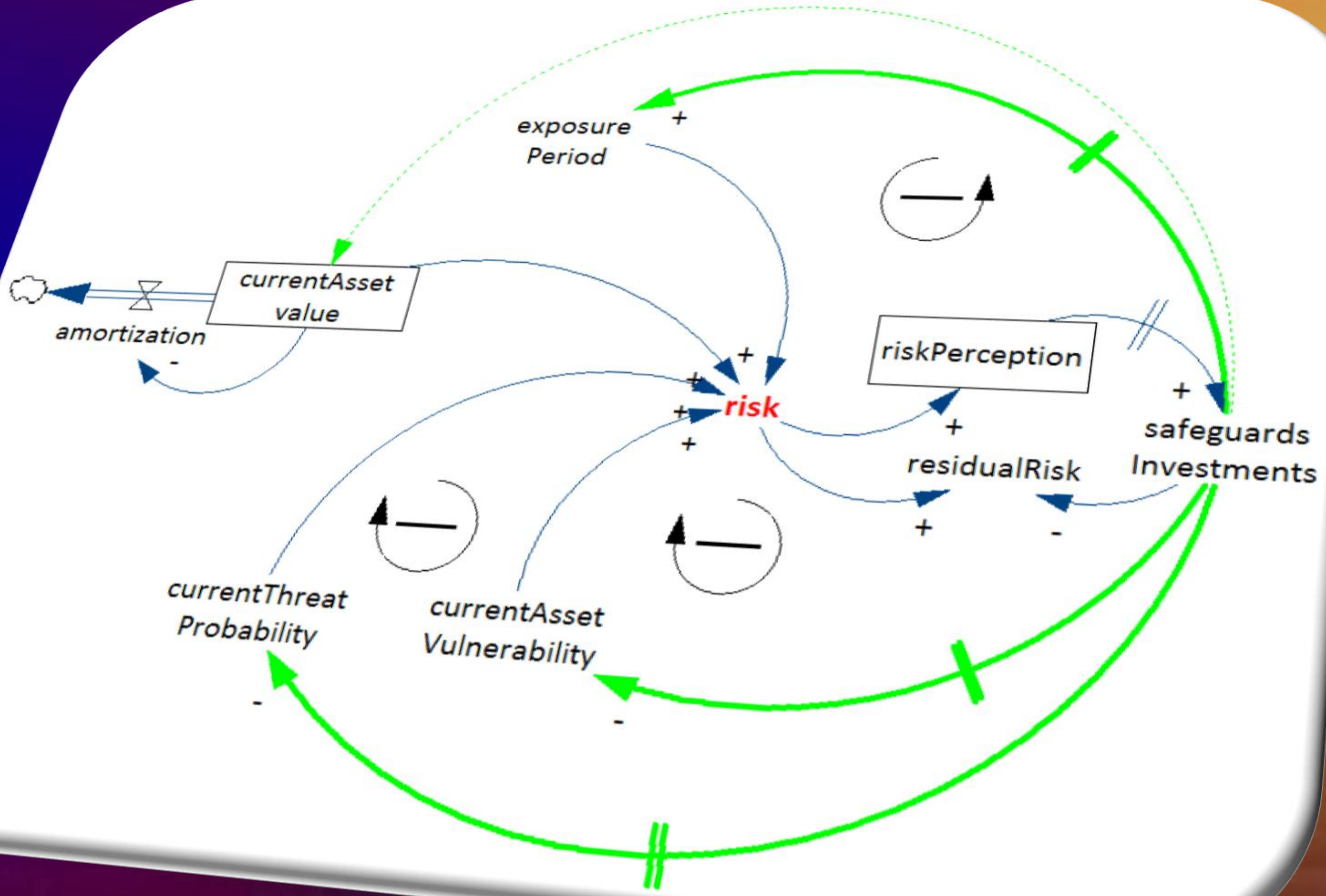
IT Risk Management Basics

- According to these standards the following basic RM elements are defined:
  - asset(s) with its (their) value and vulnerability (vulnerabilities),
  - threat(s),
  - risk as a consequence of assets' vulnerability and interaction with threats,
  - safeguards and risk minimization,
  - security policy.

Generic IT Risk Management Model

- Generic IT RM model [Trček].
  - It is based on system dynamics:
    - System dynamics is intended for modeling complex systems.
    - It supports coverage of socio-technical systems.
    - It operates on the aggregates level.
  - Our problem area
    - has to address human factor and technology as a whole;
    - it has to operate at the aggregates level and provide computerized support.

Generic IT Risk Management Model

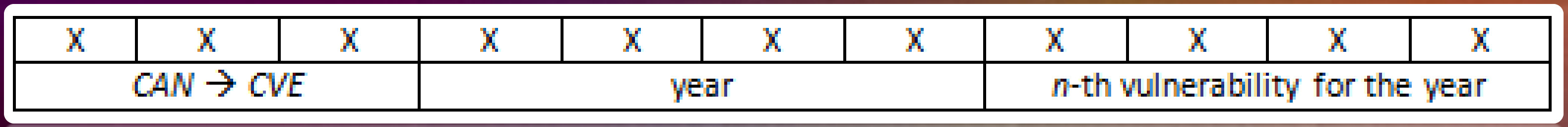


Risk management in IS - applicable initiatives

- IS risk management metrics as a "side-effect" of two main (related) initiatives:
  - MITRE Corporation Common Vulnerabilities and Exposures and
  - US National Vulnerability Database.
- In addition, a complementary effort that is focused on web applications security flaws is Open Web Application Security Project, or OWASP.

Risk management in IS - applicable initiatives

- MITRE Corporation Common Vulnerabilities & Exposures Database.
  - Vulnerabilities can be in one of two states:
    - publicly known, with no patch available from the vendor, or
    - publicly known, with a patch available from the vendor.
- All vulnerabilities have an ID which is an eleven digit unique number with its syntax as given in the table below:



X	X	X	X	X	X	X	X	X	X	X
CAN → CVE			year				*n*-th vulnerability for the year			

Risk management in IS - applicable initiatives

- Using this database as a foundation, Jones suggests metric called DVE (daily vulnerability exposure) [Jones]:
  - – DVE is a sum of num. of publicly known vulnerabilities for a system *s* without corresponding patch on each day of the year:

$$DVE_s(date) = \sum_{vuln\ s} (date_{known} < date) \wedge (date_{patched} > date)$$

  - – DVE expresses for any given day the exposure (number of exposures) of a system to those vulnerabilities that were publicly disclosed prior to that day, but patches were not available until after that day.

Risk management in IS - applicable initiatives

- Harriri et al. suggest vulnerability index (VI) [Harriri]:
  - This index is based on qualitative (categorical) assessment of a state of a system (be it a router, a server or a client), which can be normal, uncertain and vulnerable.
  - Each of the above devices has an auditing agent that measure the impact factors in real-time (they calculate the ratio between the changes of a normal and abnormal state). The vulnerability analysis engine statistically correlates the agent generated events to system impact metrics.

Risk management in IS - applicable initiatives

- Harriri et al. suggest to use vulnerability index (VI) [Hariri]:
  - For each kind of a system a component impact factor (CIF) is calculated for a given fault scenario (FS).
  - CIF is the ratio between two differences – the first is the difference between the normal and faulty operation parameter value, and the second is the difference between the normal and acceptable threshold value of this operation parameter.

Risk management in IS - applicable initiatives

- Vulnerability index (VI) [Hariri]:

$$CIF(client, FS_k) = \frac{\left|TR_{norm} - TR_{fault}\right|}{\left|TR_{norm} - TR_{min}\right|}$$

$$CIF(router, FS_k) = \frac{\left|BU_{norm} - BU_{fault}\right|}{\left|BU_{norm} - BU_{max}\right|}$$

$$CIF(server, FS_k) = \frac{\left|CQ_{norm} - CQ_{fault}\right|}{\left|CQ_{norm} - CQ_{max}\right|}$$

  - Now the system impact factor (SIF) can be obtained that identifies how a fault affects the whole (sub)network.

Risk management in IS - applicable initiatives

- Vulnerability index (VI) [Harriri]:
  - For a given fault a SIF is obtained by evaluating the weighted IFs of all network components. This means the percentage of components in vulnerable states (i.e. where CIF exceeds normal op. thresholds *d*) in relation to the total num. of components:

$$SIF_{client}(FS_k) = \frac{\sum_{\forall j, CIF_j > d} COS_j}{total\ num\ clients}$$

$$SIF_{router}(FS_k) = \frac{\sum_{\forall j, CIF_j > d} COS_j}{total\ num\ routers}$$

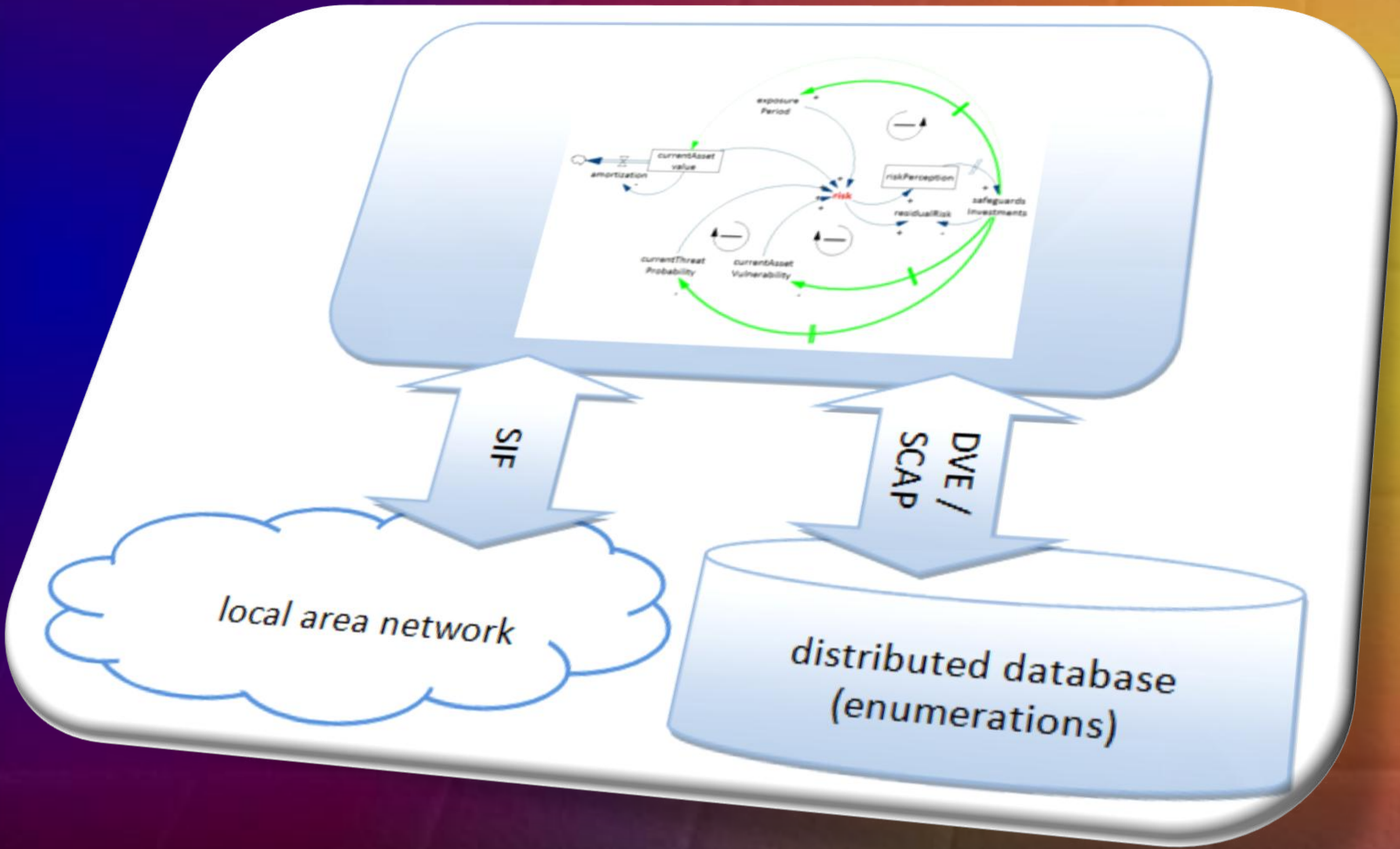
$$SIF_{server}(FS_k) = \frac{\sum_{\forall j, CIF_j > d} COS_j}{total\ num\ servers}$$

  - Component oper. state (COS) equals to 1 when the component operates in an abnormal state (that is, $CIF_i > d$), and 0 when it operates in a normal state ($CIF_i < d$).

Risk management in IS - applicable initiatives

- Other metrics approaches in the literat.:
  - The first one is survivability analysis, where a fault is injected in systems specification and consequences are visualized by scenario graphs. → not really providing metric.
  - Graph-based network vulnerability analysis, where a database of common attacks is used and applied to a particular network configuration to identify the most probable attack paths).
  - Attack trees, which are similar to former technique, but of a more general nature.

Computer supported IT risk management



Computer supported IT risk management

- Automation of metrics assessment:
  - For DVEs, a SCAP protocol has been developed and is available.
  - For SIFs, we are studying two options:
    - deployment of SNMP or
    - deployment of slim agents, e.g. CORBA.
  - In both cases an “engine” code is needed to calculate aggregates expected values and apply forecasting methods.

Conclusions

- Thanks to some US initiatives for CIP there exists now a basis for quantitative risk management of IT / IS.
- We have developed a generic, system dynamics based RM model that links techno-elements and human factor.
- Currently, we are working on reactive and active RM, while pro-active RM is still a matter of research.

References

- [Jones] Jones J.R., Estimating Software Vulnerabilities, IEEE Security & Privacy, July and August, IEEE, 2007, pp. 28-32.
- [Hariri] Hariri S., Qu G., Dharmagadda T., Ramkishore M., Cauligi S., Raghavendra A. , Impact Analysis Of Faults And Attacks In Large-Scale Networks, IEEE Security & Privacy, September/October, IEEE, 2003, 49-54.

References

- [Jaquith] Jaquith A., Security Metrics: Replacing Fear, Uncertainty and Doubt, AW, Upper Saddle River, 2007.
- [Trček] Trček D., System Dynamics Based Risk Management for Distributed Information Systems, Proceedings of ICONS 09, IARIA / IEEE, Gosier, 2009.
- [Trček] Springer book chapter (?), SCI journal paper (?)…