Title

Development an aggregated risk/security index-definition for estimation of the level of arbitrary IT-security constellations[[1]](#footnote-1)

Abstract

* Problems: The increasing usage of technology has made organizations vulnerable ([https://www.symantec.com/security-center/threat-report)](https://www.symantec.com/security-center/threat-report) to cyber threats like (phishing[[2]](#footnote-2)). The IT-security measures like (antivirus software[[3]](#footnote-3)) put in place are not always adequate to protect against these threats.

* Goals: The main goal of this thesis is to investigate ways Like (develop an aggregated[[4]](#footnote-4) risk/security index) to enhance IT-security measures in organizations to better current methods estimation of the level of arbitrary IT-security constellations and protect against cyber threats.

* Tasks: This will involve conducting a thorough review (What is the frequency and nature of cyber-attacks[[5]](#footnote-5) faced by the organization?) of existing IT-security measures and identifying areas like (development of the aggregated risk/security index) for improvement Development of an aggregated risk/security index-definition for estimation of the level of arbitrary IT-security constellations. The study/documentation and the application will also involve conducting interviews The purpose of conducting interviews[[6]](#footnote-6) with experts is to gather their insights and knowledge on the latest best practices and technologies in the field of IT-security, as well as their perspectives on the current state of IT-security measures in organizations with experts (the number of involved experts and their specific domains would depend on the nature and scope of the study, professionals, IT managers, information security), in the field to gather their insights.

* Targeted groups/customers: This study is aimed at organizations of all sizes, from small businesses to large corporations.

* Utilities: The results of this study will be useful for organizations to improve their ITsecurity measures and better the results of this study will be useful for organizations to

improve their IT-security measures and better protect against cyber threats compared to their current measures protect against cyber threats.

* Characteristics of the solution: The solution proposed in this thesis will be based on the latest best practices like (security controls implementation) and technologies like (AI, machine learning) in the field of IT-security.

* Results: The results of this study will provide organizations with a roadmap (as output of the expert system) for enhancing their IT-security measures and protecting against cyber threats with quasi exact estimation about the reduction of the aggregated risk-index concerning each roadmap-item. Parallel, the costs of each roadmap-item should also be estimated/derived.

* Discussions: The findings of this study + application will be discussed in detail, including the advantages and disadvantages of different approaches (see each potential roadmapitems in the generalized combinatorial space of the potential customers). The thesis will also provide recommendations (see optimized set of roadmap-items) for organizations to improve their IT-security measures (incl. quasi exact estimation of the reduced riskpotential).

Future: The results of this study will have implications implementation of more effective ITsecurity measures in organizations, thus improving their protection against cyber threats for the future of IT-security and provide a foundation for further research like (Developing new technologies and best practices in IT-security.

* ) In this field.

In general: we need an extreme precise (sub)-goal,and appropriate (real and/or generated) data for the first model (c.f. AI and/or machine learning work with data for a very-very precise goal…)

Demo about generated data and about the estimation a kind of risk-potential concerning transactions: <https://miau.my-x.hu/miau/296/risk_index_naive_regression_coco.xlsx>

With other words:

We need data - real ones and/or generalized ones.

We need at first one single micro/sub-goal (c.f. deriving risk potential only for phishing or only antivirus-software-quality or more parallel, but transparent levels/layers).

One single sub-goal (e.g., phishing) can also be modeled in an aggregated form: each phenomenon can be "atomized" and rebuilt from its identified parts. These parts (attributes) in case of events (objects) lead to an OAM = object-attribute-matrix. The positions in an OAM store the data. These data can be existing in a real world (see log-data) and/or these data can be generated: c.f. https://miau.my-x.hu/miau/296/risk\_index\_naive\_regression\_coco.xlsx

1. This is a decision point for the author… [↑](#footnote-ref-1)
2. Do you want to create your first model about phishing?

OR [↑](#footnote-ref-2)
3. Do you want to create your first model about antivirus-software? OR do you want to have a still higher level of aggregations? (phishing+antivirus-software+…+…+…+…) [↑](#footnote-ref-3)
4. What should be aggregated? (see: previous footnotes) [↑](#footnote-ref-4)
5. Do we have a real database about detected and undetected cyber-attacks? [↑](#footnote-ref-5)
6. With whom? When? How? [↑](#footnote-ref-6)