Towards the Definition of a Dynamic/Systemic Assessment for Cyber Security Risks Through a Systems Thinking approach

Stefano Armenia
Università degli Studi di Roma "La Sapienza"
armenia@dis.uniroma1.it

Eduardo Ferreira Franco
Escola Politécnica of University of São Paulo
eduardo.franco@usp.br

Fabio Nonino
Università degli Studi di Roma "La Sapienza"
fabio.nonino@uniroma1.it

Emanuele Spagnoli
PricewaterhouseCoopers
ema.spagno@gmail.com

Context

Nowadays our society is increasingly becoming economic and social dependent on the cyberspace, which comprehends the set of networks and information systems that are used by government agencies, enterprises, critical infrastructure providers and public administration to provide several essential services.

However, the cyberspace and its core components are exposed to numerous risks, and since these complex systems are rapidly evolving, there is a constant threat of exploitable vulnerabilities. One or several of these vulnerabilities can be exploited by attackers to hack into the computer systems of an organization, thus allowing them to read, steal, disclose or delete critical information up to take full control of physical assets. These numerous vulnerabilities, coupled with the fact that awareness of this situation is not yet well established at all levels of society, meaning that the cyber threats can become an extremely important issue for organizations, which could lead to financial and reputational impacts.

The current work adopts the Italian National Cyber Security Framework for assessing cyber security risks, which has interoperability with industry standards, guidelines, and practices, it inherits its capacity of communication that permits to broaden the discussion of cyber security matters across the organization, from the executive level to the implementation/operations level. Secondly, by joining the risks categories into a causal mapping of a general process-structure of a medium-large private organization, which is also described in causal terms, this work proposes a common ground for discussions concerning the corporate adoption of a systemic perspective as a good practice in cyber security.

Due to its compatibility with NIST's security profiles, the Italian National Cyber Security Framework can favor the communication of its security levels to known standards (for example the ISO standards), but in a cheaper way. The Italian Framework provides a full coverage of the information and system security life cycle (from its conception, development, operation, and maintenance), by maintaining an abstraction degree that ensures companies the freedom in the implementation and *contextualization of controls.*

Objective/Purpose

Using the principles of the Systems Thinking paradigm, the purpose of this paper is to address the following research question:

How the self-assessment risk categories enlisted in the Italian National Cyber Security Framework can be put into causal relationship terms, by associating each category to the various aspect of a theoretical organization structure, hence deriving a systemic causal-effect relationship map capable of evidencing how a change into one or more categories is driving change also into other ones?

The rationale underlying this research question is that when an organization makes an assessment considering those categories, they are defining a risk profile against a desired cyber security level. To achieve this level, the organization must invest on different potential levers connected to those categories (that is, management leverages that allows undertaking actions to improve in one or more categories). They try to move towards a different and better overall risk profile, and one might want to infer whether changing such level of risk means acting on every category in the framework or whether there are some of them that are sensitive leverages points on which it is possible to intervene first to do the most. Moreover, the causal-effect relationship mapping could uncover how acting on these leverages categories (higher polarity and loop dominance), indirectly (systemically) impacts other categories (intensity and direction).

Design/methodology/approach

This exploratory study aims to uncover the causal relationship among cyber security risks categories and investigate how they correlate to an organization's general structure (composed of business areas, processes, functions, and roles). For developing the dual causal mapping, a qualitative approach based on the Systems Thinking paradigm was used, which followed the steps described below:

1. Contextualization: the first step was to characterize the unit of analysis of this work in order to be able to understand and describe general organization structure in causal terms. For this purpose, a general theoretical medium-large private company was created.
2. Causal mapping: after defining the theoretical organization and its inner elements (business areas, process, functions, and roles), two departments were selected for further analysis using the System Thinking paradigm. The "Management, Planning & Control" and "IT & Security" departments were then described in simplified causal terms, but making sure that all their relevant parts and variables to the Italian National Cyber Security Framework were included.
3. Dual mapping: lastly, using the causal loop diagram created in the prior step, each of the Italian National Cyber Security Framework categories was positioned on the related spot of reference and in the relevant businesses' process.

The management of cyber security in a corporate environment can be seen as a complex system since it is characterized by feedbacks, non-linear relationships, cause and effect distant in time and space. These

characteristics make difficult to predict and control the outcomes of the cyber security management and investments. However, using the system thinking paradigm, it is possible to understand the connections between the system's elements and endogenously explaining the relationship among events and behaviors, making possible to identify "structures" that underlie complex situations, and for discerning high from low leverage change.

This work used one of the most basic tools, but central, to systems thinking: the causal loop diagram (CLD). As feedback is one of the core concepts for understanding systems, CLDs are a valuable tool for representing the feedback structures of a system. These diagrams consist of variable connected by links representing causal influence among them, which is assigned a polarity indicating how they influence each other. A feedback loop is a closed chain of link connections, through a set of decisions, rules or actions that are dependent on the state of the system. The most complex behaviors usually arise from the interaction of two basic types of feedback loops: balancing (B) and reinforcing (R), which are shown in Figure .

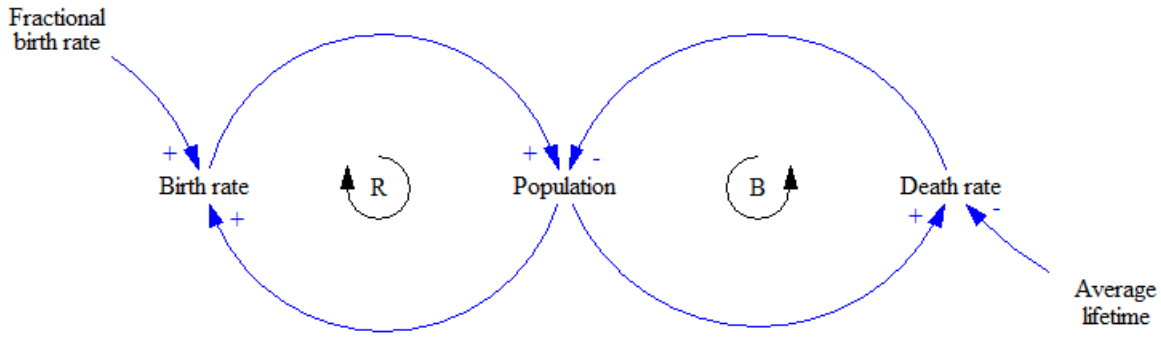

Figure 1. Causal loop diagram example, adapted from (Sterman, 2000).

Results/Findings

To contextualize the National Cyber Security Framework and place the various subcategories within the business organizational processes, it is necessary to identify an organizational structure that is adaptable to the majority of companies. Organizational structure is a system used to define a hierarchy within an organization. It identifies each job, its function and where it reports to within the organization. This structure is developed to establish how an organization operates and assists an organization in obtaining its goals to allow for future growth.

Usually, the existing organizational structure is seen as something static that cannot be modified. However, the organizational structure is like the tactical planning of a football team: everything is built on its foundations but it can take various forms, depending on the type of business and its primary success factors.

In the hypothetical organization structure used for the contextualization of the National Cyber Security Framework, the causal loop diagrams mostly developed will be those departments where subcategories are located but, at the same time, will be highlighted the interdependencies and the linkages with all business functional areas. This hypothetical general organization structure is depicted in **Error! Reference source not found.**.

At a macro level of the causal model, the "Bubble Diagram" (Armendariz, Armenia, & Atzori, 2015) highlights the business areas and their interdependencies (Figure). The diagram gives prominence to what is the systemic approach adopted in this work: the systems thinking, which allows seeing both the parts (functional areas), and the system (the whole company), and is able to operate the best of both.

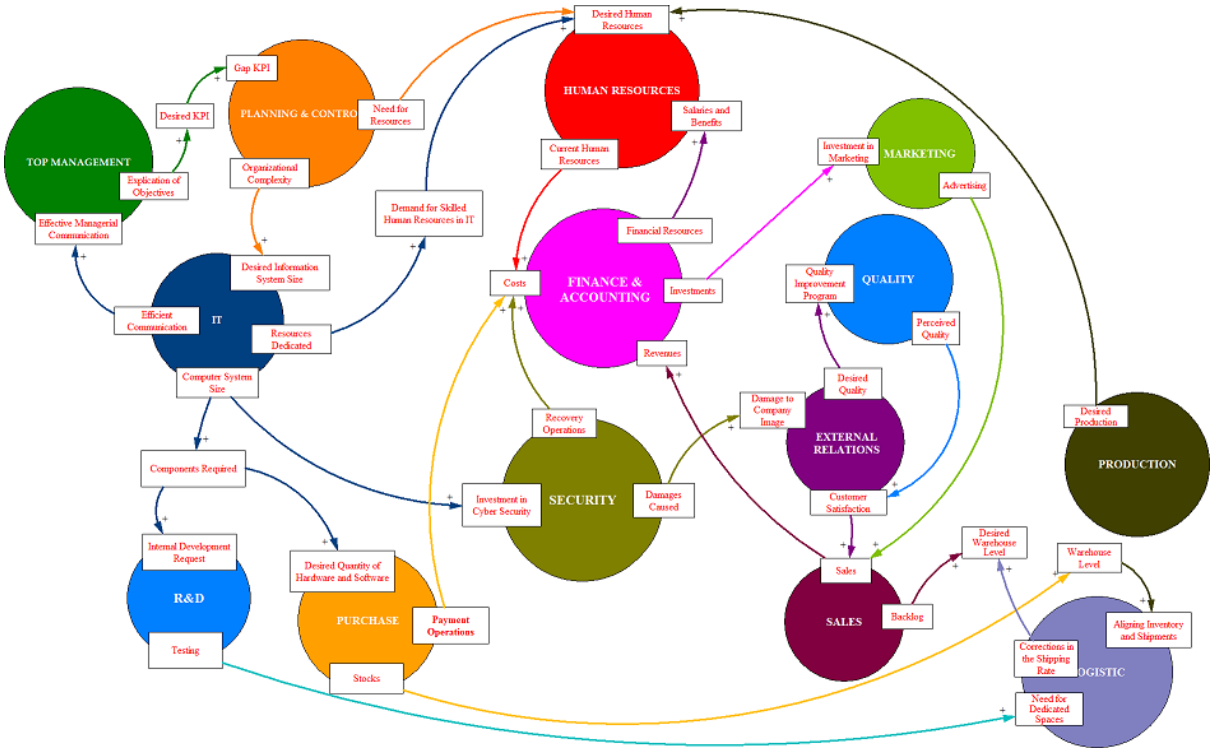

Figure 2. Bubble diagram.

Research limitations/implications

Inevitably, this work has limitations, some originating from the research design and other intrinsic to the qualitative analysis approach that was adopted. Also, the proposed theoretical organization may not be the optimal one, and this obviously imposes restrictions to the generalization of the discussion presented; however, it can be used as a starting point for the development of other, more robust, organizational settings. Also, future studies should be conducted in order to confront and to empirically validate the causal relationship diagrams that we have presented in this paper.

Conclusion

This work presented a causal mapping of cybersecurity risk-categories, based on the definitions laid down into the Italian National Cyber Security Framework, and applied to an organizational structure described by its business areas, processes, functions, and roles. For achieving this objective, a theoretical organization was firstly defined, and its structure described in causal terms. Presenting the whole study in this paper would not have been possible due to lack of space, so three departments were selected for performing the dual mapping, in other words positioning each of the cyber risk categories in the appropriate business area.

The dual causal loop diagrams described in this work can be used to qualitatively support an organization to evaluate how an investment committed to addressing threats related to one or more categories can also "propagate" systemically to other ones.

Furthermore, the results obtained in this paper can be used as a blueprint for developing a complete simulation model that could also bring quantitative data to the evaluation of future return on security investments, thus ultimately supporting organizations in deciding the optimal portfolio investment strategies among the categories used to define their cyber risks.

Keywords — National Cyber Security Framework; Cyber-security Risks; System thinking.

Acknowledgements

We thank the Research Center of Cyber Intelligence and Information Security (CIS) of Sapienza University of Rome, with particular reference to Prof. Roberto Baldoni, and Dr. Eng. Luca Montanari for their support.

References

Armendariz, V., Armenia, S., & Atzori, A. (2015). System Dynamics Updates of FAO Methodological Guide to Understand the Food Supply and Distribution Systems (FSDS). In *Proceedings of the 33rd International Conference of the System Dynamics Society*. Cambridge, Massachusetts, USA.

Sterman, J. (2000). *Business Dynamics: Systems Thinking and Modeling for a Complex World*. McGraw-Hill/Irwin.