Cyber security and ubiquity. An approach human-centric.

ABSTRACT

Antonio Colella
Ph.D. in Informatics and Information Engineering XV N.S.
Tutor: *Alfredo De Santis*

Recent security breaches showed that every attack begins with the involvement of users and continues with the exploitation of technology bugs.
In almost all cases, without human collaboration, conscious and unconscious, it would be really difficult to reach the criminal goal. Our approach has mainly three characteristics:

- Centrality of the human factor;
- The ability to mold the scenario to be protected;
- Dynamic adaptation to external and internal threats.

The First step is to deal with the identification of a set of attributes to be used for the construction of a security system fitting to a given context, going beyond the strategy of the pre-established paradigms (CIA and similar). More precisely, in this thesis we focus on the idea that members of Society need to gain sufficient knowledge and experience to avoid the consequences of the limitations of technical solutions. This has lead us toward an integrated model based on a cultural approach in which the trust and co-partnership of the security system are the main focal point. This model implies that technology solutions separated from the surrounding environment are completely inadequate. Social, organizational, and psychological factors have to be considered when implementing security within an organization. The conjunctions among social factors, technological factors, trust, co-partnership, culture, motivation, and organizational models will be better harmonized in a single system. We analyzed Trust in a Security Environment setting up on a rational component, based on information built on experience and on an irrational element, a so-called leap of faith made out of pure instinct, without any logic. We found that Trust and Risk are two inseparable concepts whose bond is supported by rational and irrational character of

confidence. We then focus on a correct approach to risk management that, by considering the holistic character of the problem, would at same time adequately support the internal working relationships as well as the relationships between organizations. Moreover, we clarify why technology solutions alone are completely inadequate to ensure security. Social, organizational and psychological factors must be considered when implementing security within an organization. Indeed, we need to consider how people build communities and must take into account how communication patterns affect interactions. The above considerations guided us towards a model that includes the cultural approach where both trust and co- partnership of a security system have a very important role. Security behaviors fostered by information organizations must be achieved by pursuing the motivation and desire as cultural factors. The model considers the societal elements as the most important part of the security system. Trust and co-partnership help create a strong security culture that serves as a framework to the information security system. At the end of the thesis, we will apply trust and co-partnership to introduce a predictive cyber security risk assessment model based on Bayesian Networks and hybrid methodology (as defined by Francois-Xavier Aguessy). The motivations underlying this thesis are mainly based on two observations. The first observation is that trust and co-partnership imply a full involvement of the whole of management style. In order to gain co-partnership, the human factor needs to be the pivot of the security model.

The second observation is that an hybrid risk assessment model can help provide a strong foundation for dynamic security modeling. The accuracy of such a model would be related to the number of available scenarios and to the use of the ability of the Bayesian networks to learn parameters from data.

The organization of the rest of this thesis is as follows:

- *Chapter 2*: In this chapter we proposed an approach beyond CIS paradigm that has mainly three characteristics: the centrality of the human factor; the ability to mold the scenario to be protected; the dynamic adaptation to external and internal threats.
- *Chapter 3*: In this chapter we analyze the hypothesis of an adaptable model based on consumerization. The basic idea that the members of Society need to gain knowledge and experience sufficient to avoid the consequences of the limitations of technical solutions. This idea has lead us toward an integrated model based on a cultural approach in which the trust and co-partnership of the security system are the main focal points. Our model implies that technology solutions separated from the surrounding environment are completely inadequate.
- *Chapter 4:* In this chapter we deal with integrated Societal Digital Security Culture.

- *Chapter 5:* In this last chapter we propose to improve cyber security through human System integration and propose a hybrid risk assessment model.
- *Chapter 6:* Finally, in this chapter, we conclude the thesis by providing discussions and some final remarks.