11th International Conference on Critical Information Infrastructures Security

10-12 October 2016
UIC HQ Paris

CRITIS
2016

Using incentives to foster security information sharing and cooperation: A general theory and application to critical infrastructure protection

Alain Mermoud[ab], Solange Ghernaouti[b], Marcus Matthias Keupp[a], and Dimitri Percia David[ab]

[a] Military Academy at ETH Zurich

[b] Swiss Cybersecurity Advisory and Research Group, University of Lausanne

Introduction and context

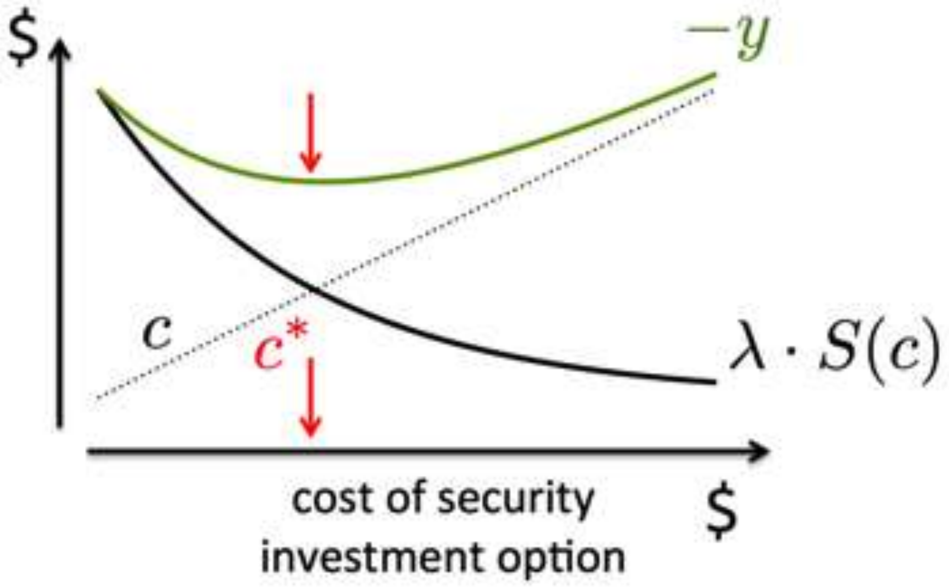
- A holistic and multidisciplinary approach to cybersecurity
- The economics of cybersecurity
- Security Information Sharing (SIS) is a key activity
- Critical Infrastructures (CIs) are vital assets which are essential for the functioning of a society and an economy, and therefore also relevant for national security

- *Topic 2 - Procedures and organisational aspects in C(I)IP: Policies, best practices and lessons learned*

Theoretical basis

- Cybersecurity investment models have theoretically demonstrated the potential of SIS for Critical Infrastructure Protection (CIP)
- E.g. the Gordon-Loeb Model
- The free rider problem remains a major pitfall
- The literature on the incentives for SIS is fairly limited and largely theoretical

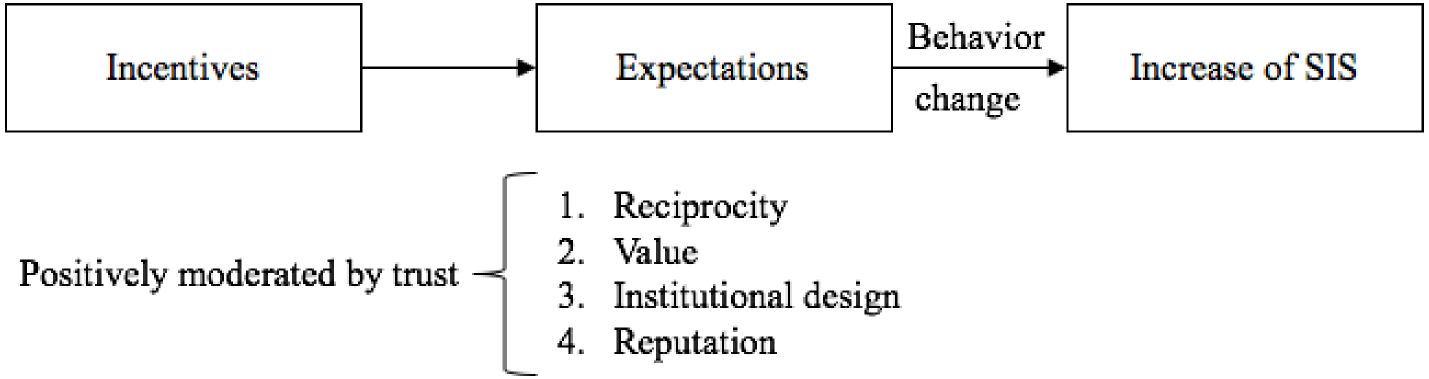
Optimal information security investment



Methodology

- Literature review, research gap identification : the free rider problem
- Theoretical framework linking incentives and voluntary SIS
- Identification of the four main incentives (effects) : reciprocity, value, institutional design, reputation (ENISA, 2010)
- The relationship between each of these effects and SIS is positively influenced by the degree of trust between individual agents (the moderating role of trust)
- Measure of frequency (number of shared transactions between participants) and intensity (depth of SIS in one single transaction)
- Design of the propositions and a two-stage SIS model to analyse the incentive mechanisms that most effectively support SIS for CIP
- Application of the proposed model to Critical Infrastructure Protection

Design of a two-stage SIS model



Incentives → Expectations → Behavior change → Increase of SIS

Positively moderated by trust

1. Reciprocity
2. Value
3. Institutional design
4. Reputation

Design of two-stage SIS model describing how incentives change expectations, modifying the behavior of actors to improve voluntary SIS

Propositions

- Proposition #. The increase in the frequency of SIS will depend on the extent to which investors expect an act of sharing to be reciprocated.
- Proposition #. The increase in the intensity of SIS will depend on the extent to which investors expect an act of sharing to be reciprocated.
- …

- Proposition #. The relationship between the expectation of reciprocity and SIS will positively reflect the degree of trust between the sharing agents.
- …

Contributions to theory and practice

- We close an important research gap by providing a theoretical framework linking incentives and voluntary SIS
- Our study differs from previous research in this domain by being grounded in empirical observations from an ISAC
- Our findings will constitute an evidence base and an important contribution to the new fast growing field of the “economics of cybersecurity”
- As a result, we deliver multiple contributions for
- academia: incentive-based security SIS model (incentive mechanisms)
- the industry: ISACs/ISAOs design, fusion centers, Big Data analytics, etc.
- policy makers: voluntary based SIS or regulation ?

Case study from a Swiss CI

- Illustration of the theoretical framework
- Humans are the weakest link
- Security information sharing is key to produce Cyber Threat Intelligence (CTI)
- Collaboration with the Swiss Reporting and Analysis Centre for Information Assurance (MELANI)
- Importance of public-private partnerships (PPPs)

Next steps

Research milestones	Status
Literature review	🟩
Research gap and research question	🟩
Novelty and relevance	🟩
Design of a SIS model	🟩
Theory development (paper 1)	🟩
Empirical results and propositions testing (paper 2)	🟨
Policy recommendations (paper 3)	🟥

Questions and discussions

- Thank you for your attention !

- alain.mermoud@unil.ch
- https://swiss-intelligence.info/