



UNIL | Université de Lausanne

Unicentre

CH-1015 Lausanne

<http://serval.unil.ch>

Year : 2019

THREE ARTICLES ON THE BEHAVIORAL ECONOMICS OF SECURITY INFORMATION SHARING: A THEORETICAL FRAMEWORK, AN EMPIRICAL TEST, AND POLICY RECOMMENDATIONS

Mermoud Alain

Mermoud Alain, 2019, THREE ARTICLES ON THE BEHAVIORAL ECONOMICS OF SECURITY INFORMATION SHARING: A THEORETICAL FRAMEWORK, AN EMPIRICAL TEST, AND POLICY RECOMMENDATIONS

Originally published at : Thesis, University of Lausanne

Posted at the University of Lausanne Open Archive <http://serval.unil.ch>
Document URN : urn:nbn:ch:serval-BIB_5D54879D8F670

Droits d'auteur

L'Université de Lausanne attire expressément l'attention des utilisateurs sur le fait que tous les documents publiés dans l'Archive SERVAL sont protégés par le droit d'auteur, conformément à la loi fédérale sur le droit d'auteur et les droits voisins (LDA). A ce titre, il est indispensable d'obtenir le consentement préalable de l'auteur et/ou de l'éditeur avant toute utilisation d'une oeuvre ou d'une partie d'une oeuvre ne relevant pas d'une utilisation à des fins personnelles au sens de la LDA (art. 19, al. 1 lettre a). A défaut, tout contrevenant s'expose aux sanctions prévues par cette loi. Nous déclinons toute responsabilité en la matière.

Copyright

The University of Lausanne expressly draws the attention of users to the fact that all documents published in the SERVAL Archive are protected by copyright in accordance with federal law on copyright and similar rights (LDA). Accordingly it is indispensable to obtain prior consent from the author and/or publisher before any use of a work or part of a work for purposes other than personal use within the meaning of LDA (art. 19, para. 1 letter a). Failure to do so will expose offenders to the sanctions laid down by this law. We accept no liability in this respect.



UNIL | Université de Lausanne

HEC Lausanne

FACULTÉ DES HAUTES ÉTUDES COMMERCIALES
DÉPARTEMENT DES SYSTÈMES D'INFORMATION

**THREE ARTICLES ON THE BEHAVIORAL ECONOMICS OF
SECURITY INFORMATION SHARING:
A THEORETICAL FRAMEWORK, AN EMPIRICAL TEST
AND POLICY RECOMMENDATIONS**

THÈSE DE DOCTORAT

présentée à la

Faculté des Hautes Études Commerciales
de l'Université de Lausanne

pour l'obtention du grade de
Docteur ès Sciences en systèmes d'information

par

Alain MERMOUD

Directeurs de thèse

Prof. Kévin Huguenin, co-directeur
PD Dr. Marcus Matthias Keupp, co-directeur

Jury

Prof. Rafael Lalive, président
Prof. Mauro Cherubini, expert interne
MER, Dr. Thomas Maillart, expert externe
Prof. Tyler Moore, expert externe

LAUSANNE
2019

IMPRIMATUR

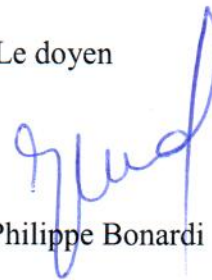
Sans se prononcer sur les opinions de l'auteur, la Faculté des Hautes Etudes Commerciales de l'Université de Lausanne autorise l'impression de la thèse de Monsieur Alain MERMOUD, titulaire d'un Bachelor of Science in Information Science et d'un Master of Science in Business Administration de la HES-SO, en vue de l'obtention du grade de docteur ès Sciences en systèmes d'information.

La thèse est intitulée :

**THREE ARTICLES ON THE BEHAVIORAL ECONOMICS OF
SECURITY INFORMATION SHARING:
A THEORETICAL FRAMEWORK, AN EMPIRICAL TEST,
AND POLICY RECOMMENDATIONS**

Lausanne, le 18 mars 2019

Le doyen



Jean-Philippe Bonardi

Members of the PhD committee

Professor Rafael Lalive

Full Professor at the Faculty of Business and Economics of the University of Lausanne.
President of the Jury.

Professor Kévin Huguenin

Assistant Professor at the Faculty of Business and Economics of the University of Lausanne.
Supervisor.

PD Dr. Marcus Matthias Keupp, Dipl.-Kfm.

Senior Researcher and Head of the Defense Management Department at the Military Academy of the Swiss Federal Institute of Technology Zurich (ETH Zurich).
Co-supervisor.

Professor Mauro Cherubini

Assistant Professor at the Faculty of Business and Economics of the University of Lausanne.
Internal expert.

Professor Tyler Moore

Associate Professor at the Tandy School of Computer Science, University of Tulsa.
External expert.

MER, Dr. Thomas Maillart

Senior Lecturer at the Information Science Institute, Geneva School of Economics and Management, University of Geneva.
External expert.

University of Lausanne
Faculty of Business and Economics

PhD in Information Systems

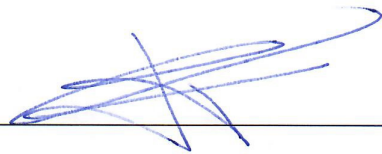
I hereby certify that I have examined the doctoral thesis of

Alain MERMOUD

and have found it to meet the requirements for a doctoral thesis.

All revisions that I or committee members
made during the doctoral colloquium
have been addressed to my entire satisfaction.

Signature: _____



Date: _____

15/03/19

Prof. Kévin HUGUENIN
Thesis supervisor

University of Lausanne
Faculty of Business and Economics

PhD in Information Systems

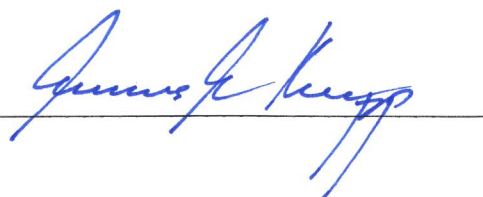
I hereby certify that I have examined the doctoral thesis of

Alain MERMOUD

and have found it to meet the requirements for a doctoral thesis.

All revisions that I or committee members
made during the doctoral colloquium
have been addressed to my entire satisfaction.

Signature:



Date: March 14, 2019

PD Dr. Marcus Matthias KEUPP
Thesis co-supervisor

University of Lausanne
Faculty of Business and Economics

PhD in Information Systems

I hereby certify that I have examined the doctoral thesis of

Alain MERMOUD

and have found it to meet the requirements for a doctoral thesis.

All revisions that I or committee members
made during the doctoral colloquium
have been addressed to my entire satisfaction.

Signature: _____



Date: _____

16/3/2019

Prof. Mauro CHERUBINI
Internal member of the doctoral committee

University of Lausanne
Faculty of Business and Economics

PhD in Information Systems

I hereby certify that I have examined the doctoral thesis of

Alain MERMOUD

and have found it to meet the requirements for a doctoral thesis.

All revisions that I or committee members
made during the doctoral colloquium
have been addressed to my entire satisfaction.

Signature:  _____ Date: 14 Mar 2019

Prof. Tyler MOORE
External member of the doctoral committee

University of Lausanne
Faculty of Business and Economics

PhD in Information Systems

I hereby certify that I have examined the doctoral thesis of

Alain MERMOUD

and have found it to meet the requirements for a doctoral thesis.

All revisions that I or committee members
made during the doctoral colloquium
have been addressed to my entire satisfaction.

Signature:



Date:

14 . 03 . 2019

Dr. Thomas MAILLART
External member of the doctoral committee

To my grandparents

Edith & Hans Waldmann

In recognition of their unconditional love

Abstract

This thesis presents a behavioral economics contribution to the security of information systems. It focuses on security information sharing (SIS) between operators of critical infrastructures, such as systemic banks, power grids, or telecommunications. SIS is an activity by which these operators exchange cybersecurity-relevant information, for instance on vulnerabilities, malwares, data breaches, etc. Such information sharing is a low-cost and efficient way by which the defenders of such infrastructures can enhance cybersecurity. However, despite this advantage, economic (dis)incentives, such as the *free-rider problem*, often reduce the extent to which SIS is actually used in practice.

This thesis responds to this problem with three published articles. The first article sets out a theoretical framework that proposes an association between human behavior and SIS outcomes. The second article further develops and empirically tests this proposed association, using data from a self-developed psychometric survey among all participants of the Swiss Reporting and Analysis Centre for Information Assurance (MELANI). SIS is measured by a dual approach (intensity and frequency), and hypotheses on five salient factors that are likely associated with SIS outcomes (attitude, reciprocity, executional cost, reputation, trust) are tested. In the third article, policy recommendations are presented in order to reduce executional costs, which is found to be significantly and negatively associated with SIS.

In conclusion, this thesis proposes multiple scientific and practical contributions. It extends the scientific literature on the economics of cybersecurity with three contributions on the human factor in SIS. In addition, regulators will find many recommendations, particularly in the area of governance, to support SIS at the legislative level. This thesis also offers many avenues for practitioners to improve the efficiency of SIS, particularly within Information Sharing and Analysis Centers (ISACs) in charge of producing *Cyber Threat Intelligence* in order to anticipate and prevent cyberrisks. Finally, at the societal level, this work contributes to a general equilibrium in perfect competition (Pareto optimum) and thus to achieving the first theorem of welfare economics in the field of cybersecurity, i.e. a complete market with no transaction cost because each actor has perfect information.

Résumé

Cette thèse présente une contribution de l'économie comportementale à la sécurité des systèmes d'information. Elle s'intéresse au mécanisme incitatif permettant de favoriser le partage de l'information utile à la cybersécurité (Security Information Sharing – SIS) entre opérateurs d'infrastructures critiques, telles que les banques systémiques, les réseaux électriques ou les télécommunications. Le SIS est une activité par laquelle ces opérateurs échangent des informations relatives aux cybermenaces, par exemple sur les vulnérabilités, les logiciels malveillants, les violations de données, etc. Ce partage d'informations est un moyen peu coûteux et efficace par lequel les défenseurs de ces infrastructures peuvent renforcer la cybersécurité. Toutefois, malgré ces avantages, les (mauvaises) incitations économiques, telles que le problème du *passager clandestin*, réduisent souvent l'utilité pratique du SIS.

Cette thèse répond à ce problème avec trois articles publiés. Le premier article présente un cadre théorique qui propose une association entre le comportement humain et les résultats du SIS. Le deuxième article développe et teste empiriquement cette proposition d'association à l'aide des données d'une enquête psychométrique développée avec les participants de la *Centrale d'enregistrement et d'analyse pour la sûreté de l'information* (MELANI). Le SIS est mesuré avec une double approche (intensité et fréquence), et des hypothèses sur cinq facteurs importants, probablement associés aux résultats du SIS (attitude, réciprocité, coût d'exécution, réputation, confiance), sont testées. Dans le troisième article, des recommandations politiques sont présentées afin de réduire les coûts d'exécution, qui s'avèrent être associés de manière significative et négative au SIS.

En conclusion, cette thèse propose de multiples contributions scientifiques et pratiques. Ses résultats élargissent la littérature scientifique sur l'économie de la cybersécurité avec trois contributions sur le facteur humain dans le SIS. En outre, les régulateurs trouveront de nombreuses recommandations, en particulier dans le domaine de la gouvernance, pour soutenir le SIS au niveau législatif. Cette thèse offre également de nombreux moyens aux praticiens pour améliorer son efficacité, notamment au sein des *Information Sharing and Analysis Center* (ISACs) chargés de produire du renseignement sur les cybermenaces (Cyber Threat Intelligence) afin d'anticiper et prévenir les cyberrisques. Enfin, sur le plan sociétal, ce travail contribue à un équilibre général en concurrence parfaite (optimum de Pareto) et donc à réaliser le premier théorème du bien-être dans le domaine de la cybersécurité, c'est-à-dire un marché complet sans coût de transaction car chaque acteur dispose d'une information parfaite.

Acknowledgements

First and foremost, I would like to thank my co-supervisor at the Military Academy at ETH Zurich, **PD Dr. Marcus Matthias Keupp**, for guiding me from the beginning and throughout the long journey of writing my thesis. Marcus is a great mentor. He funded my research project, supported me, and offered me the best possible working conditions and the necessary freedom to develop my dissertation. During the last stretch of my PhD research, he gave me the chance to transfer my results as a lecturer at ETH Zurich during the entire fall semester 2018. His expertise in econometrics and strategic management helped me to approach and understand (information) security issues from a new perspective.

Secondly, I would like to thank my co-supervisor at the University of Lausanne, **Professor Kévin Huguenin**, for taking over the supervision of my PhD thesis. He gave me the chance to finalize and defend my dissertation, and in the best possible conditions. His expertise in information security and privacy were a great asset and transformed my PhD work into truly interdisciplinary research, at the intersection of information security and economics. His numerous relevant comments helped me to present my work at the 17th annual *Workshop on the Economics of Information Security* (WEIS) and to revise and resubmit our research in the *Journal of Cybersecurity*.

Besides my two co-supervisors, I am deeply grateful to **Professor Mauro Cherubini**, **Professor Tyler Moore**, and **MER, Dr. Thomas Maillart** for having accepted to sit on my jury. They gave me very interesting and valuable advice in order to improve my manuscript. In addition, I would like to thank **Professor Rafael Lalive** for having accepted to chair my jury, as well as **Professor Jacques Duparc**, **Professor Olivier Cadot** and **Professor Benoît Garbinato** for their support and advice regarding the internal administration processes of the doctoral school.

During my thesis work, I had the pleasure of working with other great scholars, such as **Professor Maximilian Palmié** who supported me with his advanced methodological skills and **Professor Yves Pigneur** who helped me think outside the box by introducing me to *Design Science* and *Design Thinking*. A special thank goes to psychological scientist **Dr. Hubert Annen** who helped me build and test my psychometric questionnaire and to **Holly Cogliati-Bauereis** for her outstanding English editing services, as well as to **Radio Swiss Classic** which accompanied my writing with a relaxing and inspiring playlist.

A word of appreciation also goes to the team of the *Reporting and Analysis Centre for Information Assurance* (MELANI) in Bern, especially **Pascal Lamia**, **Max Klaus**, and **Dr.**

Manuel Suter. They gave me much practical advice and helped me collect my dataset at an extraordinary response rate. Thanks to them, I was able to empirically test my hypotheses, develop a successful system model, and to contribute to the improvement of MELANI.

A sincere thank goes to all my friends who supported me, especially to my best sparring-partner, PhD candidate **Dimitri Percia David**, for his unfailing support during our four years of collaboration. A special thank you goes to my childhood friend, **Dr. Julien Herzen**, who most probably saved my thesis from being a sunk cost, as well as my friends **Dr. Félicien Monnier**, who invited me to finalize my manuscript in the fresh air of the mountains, and **Emérentienne Pasche** for helping me formatting the present manuscript.

This academic work was made possible thanks to the funding of the Military Academy (MILAC) at ETH Zurich. I would like to thank the Director of the MILAC, **Brigadier Peter Candidus Stocker**, as well as all my great colleagues from the Department of Defense Management: **Kilian Cuche**, **Saâd Dhif**, **Sébastien Gillard**, and **Ramon Schöb**.

I am also very grateful to all my colleagues at UNIL who made my journey as an external PhD candidate easier. First, I would like to name all members of the Information Security and Privacy (ISP) Lab: **Dr. Bertil Chapuis**, **Gaël Bernard**, **Benjamin Trubert**, **Noé Zufferey**, **Alexandre Meylan**, and **Didier Dupertuis**. Next, I would like to mention, among others, **Dr. Arielle Moro**, **Dr. Thomas Boillat**, **Dr. Kenny Lienhard**, **Dr. Hazbi Avdiji**, as well as PhD candidates **Dina Elikan** and **Vaibhav Kulkarni**. A special thank goes to **Dr. Mélanie Bosson**, **Benjamin Rudaz**, and **Claire-Marie Schertz** from the Graduate Campus team. They were of great help for achieving my personal goals at UNIL and beyond.

And last but not the least, I would like to express my gratitude to my family for their unconditional support, especially my brother **Yves Mermoud**, currently a PhD candidate himself, who supported me with his advanced LaTeX skills, my mother **Karin Waldmann**, my father **Michel Mermoud**, my godmother **Méry Mermoud**, as well as my uncle ETHZ **Professor Hans Martin Schmid**, for advising me and convincing me to pursue a PhD degree in the first place.

I will be eternally grateful for the support of all the people mentioned above. Without their support and encouragement during my studies, this work would simply not exist.

Table of Contents

INTRODUCTION

1. <i>The Economics of Information Security</i>	15
1.1 The Economics of Security Information Sharing	16
1.2 <i>Homo Economicus</i> vs. <i>Homo Reciprocans</i> in Information Security	19
1.3 Security Information Sharing Definition	20
1.4 Security Information Sharing Best Practice: The RUAG Case	21
2. <i>Related Work and Problem Statement</i>	23
2.1 Mandatory Security Information Sharing	24
2.2 Research Gap in Voluntary Security Information Sharing	25
2.3 Research Questions	27
2.4 Theoretical Foundations	28
2.5 Research Methodology	28
2.6 Fundamental Choice of Research Method	30
2.7 Choices About the Study of Human Behavior	30
2.8 Psychometric Operationalization	31
2.9 Empirical Procedures	32
2.10 Explanation of the Particular Constructs	32
2.11 Research Context	33
3. <i>Thesis Structure and Outline</i>	34
3.1 Part I: Theoretical Framework	35
3.2 Part II: Empirical Analysis	35
3.3 Part III: Policy Recommendations	36
4. <i>Other Scientific Contributions</i>	36
4.1 Conference Paper: CRITIS 2016	36
4.2 Journal Article: Computers in Human Behavior	37
4.3 Bachelor Thesis Supervision	37
5. <i>Research Disseminations</i>	38
5.1 Lecturer at ETH Zurich	38
5.2 Conference on Economic Warfare at ETH Zurich	38
5.3 Massive Open Online Course (MOOC): The Economics of Cybersecurity	39
5.4 Invited Talks	39
5.5 Professional and Trade Magazines, Newspapers and Book Chapters	40
5.6 Consulting Services	41
5.7 Cybersecurity Competitions	41
6. <i>References</i>	42

PART I: Theoretical Framework

Using Incentives to Foster Security Information Sharing and Cooperation: A General Theory and Application to Critical Infrastructure Protection.....	49
1. <i>Introduction</i>	51
2. <i>Theoretical Framework and Propositions</i>	52
2.1 Regulation Alone Cannot Solve the Free-Rider Problem	52
2.2 Linking Incentives to Voluntary SIS.....	53
2.3 A Holistic and Multidisciplinary Approach	53
2.4 A Model Linking Incentives, Behavior, and SIS	55
2.5 Reciprocity Expectation	55
2.6 Value Expectation	56
2.7 Institutional Expectation.....	57
2.8 Reputation Expectation	57
2.9 The Moderating Role of Trust.....	58
3. <i>Application of the Proposed Model to Critical Infrastructure Protection</i>	59
3.1 The Swiss Reporting and Analysis Centre for Information Security	60
3.2 Reciprocity Expectation	60
3.3 Value Expectation	60
3.4 Institutional Expectation.....	61
3.5 Reputation Expectation	61
3.6 Setting the Optimal Size of SIS Circles	61
4. <i>Discussion</i>	62
5. <i>Concluding Comments and Next Steps</i>	63
6. <i>References</i>	64

PART II: Empirical Analysis

To Share or not to Share: A Behavioral Perspective on Human Participation in Security Information Sharing	71
1. <i>Introduction</i>	73
2. <i>Theoretical framework and hypotheses</i>	74
2.1 Attitude.....	76
2.2 Reciprocity	76
2.3 Executional Cost.....	78
2.4 Reputation	78
2.5 Trust.....	79
2.6 Interaction Effects	80
3. <i>Methods</i>	81
3.1 Sampling Context and Population	81
3.2 Measures.....	82
3.3 Implementation.....	83
3.4 Analysis	84
4. <i>Results</i>	85
5. <i>Discussion</i>	88
6. <i>References</i>	92
7. <i>Appendix</i>	99

PART III: Policy Recommendations

Governance Models Preferences for Security Information Sharing: An Institutional Economics Perspective for Critical Infrastructure Protection	109
1. <i>Introduction</i>	111
2. <i>Theoretical Framework and Related Work</i>	112
2.1 An Institutional Economics Perspective of SIS	112
3. <i>Research Artifact and Set of Rules</i>	114
3.1 Institutional Design of an SIS Artifact	114
3.2 Set of Universal Rules for SIS	114
4. <i>Application to Critical Infrastructure Protection</i>	116
4.1 Population and Data Collection.....	116
4.2 Possible Governance Models for SIS.....	117
5. <i>Results</i>	118
5.1 Correlations between Institutional Rules and Governance Model Preferences	118
5.2 Governance Model Preferences by Organization Size.....	120
5.3 Governance Model Preferences by Participation in Trust Building Events.....	120
5.4 Governance Model Preferences by Sector of Activity.....	121
6. <i>Concluding Remarks, Limitations and Future Work</i>	122
7. <i>References</i>	124

CONCLUSION

1. <i>Main Contributions</i>	131
1.1 Results Synthesis Part I: Theoretical Framework	131
1.2 Results Synthesis Part II: Empirical Analysis.....	132
1.3 Results Synthesis Part III: Policy Recommendations	132
2. <i>Limitations and Critical Reflections</i>	132
3. <i>Discussion on Policy Recommendations and ISAC organization</i>	134
4. <i>Outlook</i>	135
4.1 The Influence of Agent Behavior on the Perceived Performance of SIS (submitted)	135
4.2 Setting the Optimal Size of SIS Groups (work-in-progress).....	135
4.3 Empirical Analysis of Mandatory SIS with Authorities (work-in-progress)	137
5. <i>References</i>	139

APPENDIX

1. <i>Resume – Dr. Alain Mermoud</i>	143
2. <i>Online Questionnaire</i>	145
3. <i>Certificate of Achievement Economics of Cybersecurity</i>	155
4. <i>Certificate from the UNIL Graduate Campus</i>	155

List of Figures

INTRODUCTION

Figure 1: An Interdisciplinary and Empirical PhD Thesis	15
Figure 2: The Gordon-Loeb Model: Benefits and Costs of an Investment in Information Security.....	17
Figure 3: The Economics of Security Information Sharing (SIS).....	18
Figure 4: Chronology of the Advanced Persistent Threat against RUAG	22

PART I: Theoretical Framework

Figure 1: Design of a SIS Model.....	55
Figure 2: MELANI Trust-Circles (Adapted from the Onion Model).....	62

PART III: Policy Recommendations

Figure 1: Security Information Sharing Artifact	116
Figure 2: Governance Model Preferences by Organization Size	120
Figure 3: Governance Model Preferences by Sectors	122

CONCLUSION

Figure 1: The Open Source OTX Platform Allows the Creation of ISAC-Like Groups	136
--	-----

List of Tables

INTRODUCTION

Table 1: Literature Review on Security Information Sharing Regulations	25
Table 2: Systematic Literature Review on Voluntary Security Information Sharing	26

PART II: Empirical Analysis

Table 1: Constructs, Items and Scales Used in the Survey	99
Table 2: Final Set of Factor Loadings after Oblique Rotation ^a	101
Table 3: Descriptive Statistics on all Variables.....	102
Table 4: Correlations Among Dependent and Independent Variables ^a	102
Table 5: Final Results of Model Estimations ^{a,b}	103
Table 6: Documentation of Pre-Tests.....	104

PART III: Policy Recommendations

Table 1: Governance Model Preferences for Security Information Sharing.....	119
---	-----

List of Abbreviations

ACM	Association for Computing Machinery
ANOVA	Analysis of Variance
API	Application Programming Interface
APT	Advanced Persistent Threat
BSc	Bachelor of Science
CCS	Conference on Computer and Communication Security
CERT	Computer Emergency Response Team
C&C	Command and Control Server
CI	Critical Infrastructure
CIP	Critical Infrastructure Protection
CISA	Cybersecurity Information Sharing Act
CRITIS	Critical Information Infrastructure Security
CTI	Cyber Threat Intelligence
DDoS	Distributed Denial-of-Service Attack
DSR	Design Science Research
ENISA	European Union Agency for Network and Information Security
ETHZ	Eidgenössische Technische Hochschule Zürich (<i>Swiss Federal Institute of Technology in Zurich</i>)
EU	European Union

EWS	Early Warning System
GDPR	General Data Protection Regulation
HHS	United States Department of Health and Human Services
HIPAA	Health Insurance Portability and Accountability Act
HUMINT	Human Intelligence
HVT	High-Value Target
IBM	International Business Machines Corporation
ID	Institutional Design
IS	Information Systems
ISAC	Information Sharing and Analysis Center
ISAOs	Information Sharing and Analysis Organizations
IT	Information Technology
IOC	Indicator of Compromise
MBA	Master of Business Administration
MELANI	Melde- und Analysestelle Informationssicherung (<i>Reporting and Analysis Centre for Information Assurance</i>)
MISP	Malware Information Sharing Platform
MSc	Master of Science
NCS	National Strategy for Switzerland's Protection against Cyber Risks
NIE	New Institutional Economics
NIS	The UE Directive on Security of Network and Information Systems

OECD	Organization for Economic Co-operation and Development
OS	Operating System
OSINT	Open Source Intelligence
P2P	Peer-to-Peer
PHI	Protected Health Information
PPP	Public-Private-Partnership
PwC	PricewaterhouseCoopers
SCADA	Supervisory Control and Data Acquisition
SEM	Structural Equation Modeling
SIEM	Security Information and Event Management
SIM	Security Information Management
SIS	Security Information Sharing
SOCMINT	Social Media Intelligence
TIP	Threat Intelligence Platform
TLP	Traffic Light Protocol
UK	United Kingdom
VEP	Vulnerabilities Equities Process
WEIS	Workshop on the Economics of Information Security
WISCS	Workshop on Information Sharing and Collaborative Security

INTRODUCTION

“The question to ask when you look at security is not whether this makes us safer, but whether it's worth the trade-off.”

- *Bruce Schneier*

INTRODUCTION

1. The Economics of Information Security

The economics of information security addresses the economic aspects of the privacy and security of information systems. In their seminal article *The Economics of Information Security* (Anderson & Moore, 2006), published in *Science Magazine*, Anderson and Moore explain that many information security systems fail not so much due to technical reasons but because of misaligned incentives. They find that information security is shaped by economic mechanisms, such as bad design that stems from divergent interests, information asymmetry, adverse selection, network externalities, etc. In fact, many unsolved information security problems can be studied through the lens of microeconomic principles.

For instance, the concept of *moral hazard* can explain why information systems fail when the human agents that defend them do not bear the full costs of failure (Moore, Pym, & Ioannidis, 2010). In his article, *Why Information Security is Hard* (Anderson, 2001), Anderson already shows that incentives alignment and economic insights should be integrated into a proper *secure-by-design* approach to security engineering. Other security economics publications also explore the role of incentives, for instance, between defenders and attackers of information systems (Anderson, Moore, Nagaraja, & Ozment, 2007; Moore, 2008; Moore & Clayton, 2009).

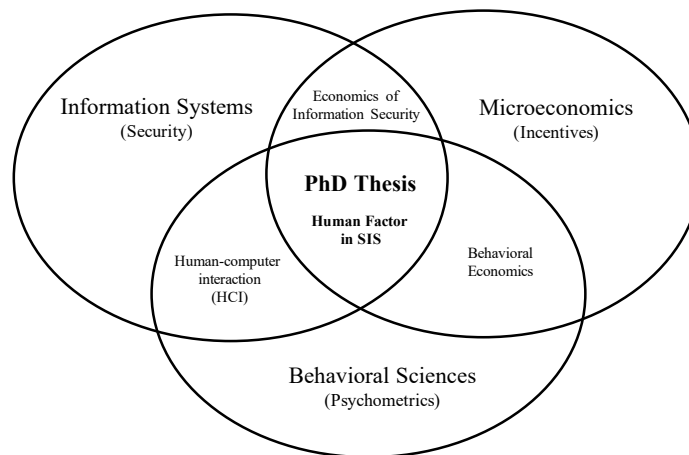


Figure 1: An Interdisciplinary and Empirical PhD Thesis

This figure shows how this PhD thesis expands the scientific literature using a psychometric methodology to investigate the incentives for human agents to share security information.

Since those founding publications, the economics of information security - which was historically a branch of computer science - has blossomed into multiple areas of research

INTRODUCTION

(Anderson & Moore, 2009). It has become a fast-growing research field contributing to the development of a multidisciplinary and holistic approach to information security and information assurance. The field substantially expanded with the first edition of the *Workshop on the Economics of Information Security* (WEIS)¹ held in 2002 in Berkeley, CA. Today, the WEIS typically combines expertise from the fields of economics, social science, business, law, policy, and information systems. Hence, the field age is generally considered to be about 20 years old, which still makes it a relatively young discipline according to academic standards. This dissertation offers a contribution to this fascinating field by growing information security economics out through behavioral economics into psychology.

1.1 The Economics of Security Information Sharing

Neoclassic economics and information security have in common the production of mathematical models (often based on game theory) that assume human agents are strictly rational *homo economicus*, i.e. the assumption that human agents always take rational decisions.

For instance, the Gordon-Loeb model is one of the most well-accepted analytical models in the discipline (Gordon & Loeb, 2002). This economic model analyzes the optimal investment level in information security. The model takes into account the vulnerability of the information to a security breach and the potential loss should such a breach occur. More specifically, the model shows that it is generally not interesting to invest for amounts in information security higher than 37% of the predicted loss.

Example: suppose an estimated data value of 1'000'000 CHF, with an attack probability of 15%, and an 80% chance that an attack would be successful. In this case, the potential loss is given by the product $1'000'000 \text{ CHF} \times 0.15 \times 0.8 = 120'000 \text{ CHF}$. According to Gordon and Loeb, the company's investment in security should not exceed $120'000 \text{ CHF} \times 0.37 = 44'400 \text{ CHF}$.²

¹ <https://econinfosec.org> (retrieved on 28.10.2018)

² https://en.wikipedia.org/wiki/Gordon%E2%80%93Loeb_model (retrieved on 28.10.2018)

INTRODUCTION

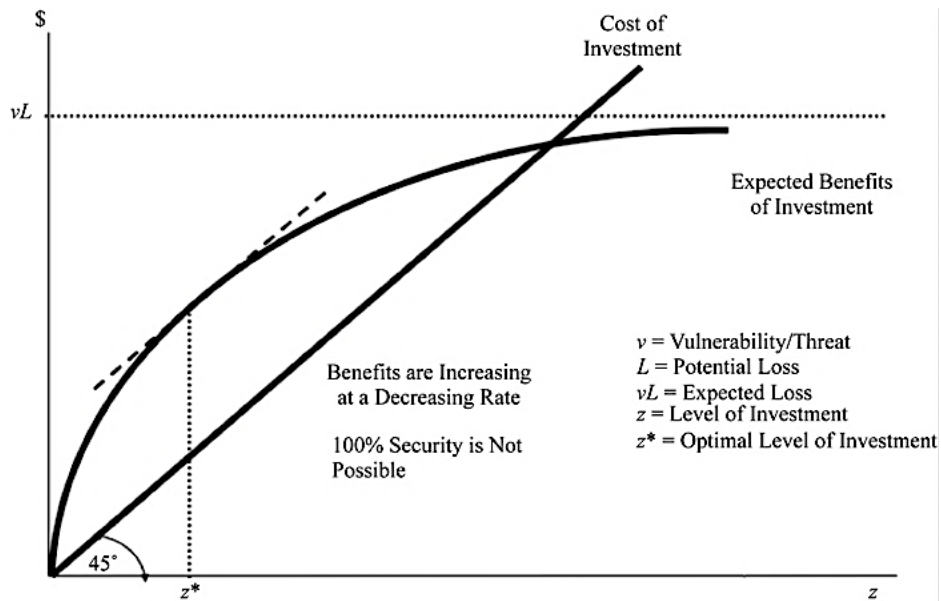


Figure 2: The Gordon-Loeb Model: Benefits and Costs of an Investment in Information Security.

This model seeks the optimal level of investment in information security, given decreasing incremental returns. Figure courtesy of Gordon, Loeb, Zhou, 2016.

Underinvestment in information security causes significant hazards for information systems. Security information sharing (SIS) appears to be a promising way to solve this problem, as theoretical models illustrate that security information sharing lowers the investment cost for any given level of cybersecurity (Gordon, Loeb, Lucyshyn, & Zhou, 2015b).

An extended version of the model shows that SIS can lower the optimal investment into information security (Gordon, Loeb, Lucyshyn, & Zhou, 2015a) and that SIS is social welfare enhancing (Böhme, 2016). Regarding the incentives for voluntary sharing, if each organization is allowed to select its level of information security sharing, the only Nash equilibrium is that nobody shares: $s_i = s_j = 0$ (Böhme, 2016).

INTRODUCTION

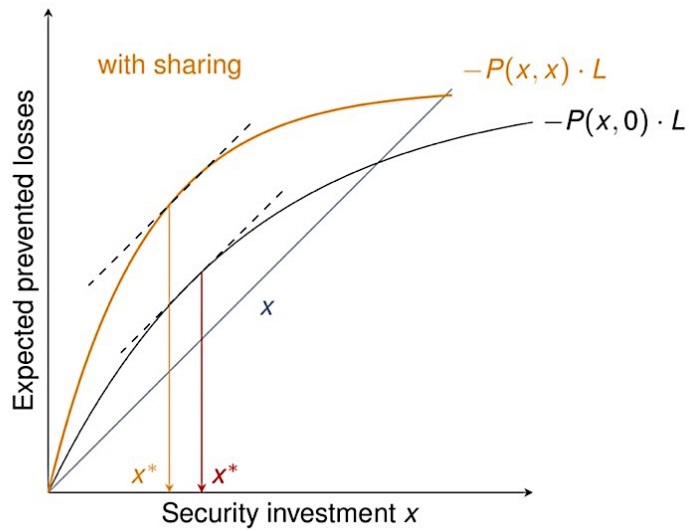


Figure 3: The Economics of Security Information Sharing (SIS)

This figure shows a graphical solution of the Gordon-Loeb model where security investment and security information sharing are strategic complements. Figure courtesy of Rainer Böhme, ACM WISCS (CCS 2016). Source: <https://sites.google.com/site/wiscs2016/>

The core of the Gordon-Loeb model states that in case of no market interaction, organizations minimize the sum of fixed costs of security expected losses from residual insecurity, as presented by Böhme at the 3rd ACM Workshop on Information Sharing and Collaborative Security (WISCS 2016):³

$$x_i^* = \arg \min_{x_i} P(x_i, x_j s_j) \cdot L + x_i$$

P	breach probability function	$(\mathbb{R}^+)^2 \rightarrow [0, 1]$
x^*	optimal security investment	
Choice variable		

³ WISCS 2016 was held in conjunction with the 23rd ACM Conference on Computer and Communication Security (CCS 2016). Two other WISCS took place at CCS 2014 and CCS 2015. The workshop proceedings offer numerous relevant and seminal insights on the economics of SIS:

<https://sites.google.com/site/wiscs2014/> (retrieved on 11.03.19)

<https://sites.google.com/site/wiscs2015/> (retrieved on 11.03.19)

<https://sites.google.com/site/wiscs2016/> (retrieved on 11.03.19)

INTRODUCTION

x	Security investment [€] \approx technology level in Gal-Or & Ghose, 2005.	≥ 0
s	Security information sharing	$\in [0, 1]$
Parameters		
L	loss given breach [€]	> 0

1.2 *Homo Economicus* vs. *Homo Reciprocans* in Information Security

In 2002, Kahneman was awarded the Nobel Prize in Economics for “*having integrated insights from psychological research into economic science, especially concerning human judgment and decision-making under uncertainty*” (Kahneman & Tversky, 1979). Similarly, the economics of information security research has injected the effects of psychological, cognitive, emotional, cultural and social factors into computer science research (Odlyzko, 2003). If computers can be considered rational, the human agents programming and using them are usually not. As a result, human agents often remain the weakest link of the cybersecurity chain (Moore & Anderson, 2011).

Behavioral economics for information security investigates human agents and organizations design in decision making. This approach encompasses models from the traditional rational *homo economicus* concept, as well as more recent model that emphasizes human cooperation. The *homo reciprocans* concept stands in contrast to the idea of *homo economicus*, which states the opposite theory: Human beings are exclusively motivated by self-interest (Gintis, 2000). As a theory on human conduct, it is in contrast to the concepts of behavioral economics that examines cognitive biases and other irrationalities. Behavioral economics and economic psychology emphasize that human agents make many mistakes while using computers and processing information (Anderson & Moore, 2009).

1.3 Security Information Sharing Definition

The *homo reciprocans* concept states that human agents interact with a propensity to cooperate if provided with the right incentives (Fehr & Gächter, 2000). Human agents will compromise in order to achieve a balance between what is best for them and what is best for the environment they are a part of. This dissertation uses concepts of behavioral economics – such as the *homo reciprocans* – in order to understand the incentives mechanism that enable cooperation in the context of SIS.

SIS is an activity consisting in sharing cybersecurity-relevant information between cybersecurity stakeholders. Human agents typically exchange information on vulnerabilities, phishing, malware, and data breaches, as well as threat intelligence, best practices, early warnings, and expert advice and insight (Luijff & Klaver, 2015).

Cyber-risk management can largely be reduced to a race for information between attackers and defenders of information systems (Laube & Böhme, 2017). In his PhD dissertation, Laube describes how defenders can gain advantage in this race by sharing security information with each other in order to reduce the information asymmetry. Unfortunately, defenders often share less information than is socially desirable, as their decisions are guided by selfish reasons and (misaligned) incentives. However, SIS generally operates under Metcalfe's law, i.e. the effect of a SIS network is proportional to the square of the number of users of the system (n^2).

Several game-theoretic models investigate the benefits of SIS for individual agents (Gordon et al., 2015b; Hausken, 2015), as well as mandatory SIS for authorities (Laube & Böhme, 2015). For a firm, SIS is positively associated with its market value (Gordon, Loeb, & Sohail, 2010). For an individual agent, the optimal level of cybersecurity can be attained at a low cost with SIS (Gordon, Loeb, & Lucyshyn, 2003). SIS has also the ability to reduce the uncertainty associated with cyber-risks and to reduce the average time needed to detect a cyber-attack. In principle, SIS could increase the general level of cybersecurity and total welfare (Gal-Or & Ghose, 2005).

INTRODUCTION

SIS is especially relevant in the context of zero-day⁴ vulnerability detection (Hausken, 2007). The Vulnerabilities Equities Process (VEP) is a process used by the U.S. federal government to determine on a case-by-case basis how it should treat zero-day computer security vulnerabilities; whether to disclose them to the public to help improve general computer security, or to keep them secret for offensive use against the government's adversaries.⁵ This example shows the power related to SIS, a key activity to mitigate the impact of zero-day attacks by reducing the time for vulnerability detection.

1.4 Security Information Sharing Best Practice: The RUAG Case

In September 2014, an advanced persistent threat⁶ (APT) started against the strategic government-owned Swiss aerospace and defense group RUAG, a critical infrastructure member of MELANI. The cyberattack was motivated by economic espionage and most probably state-sponsored, even though the perpetrators of the attack were never formally identified. In January 2016, the Swiss intelligence services responded following an information received through SIS with the German intelligence services in December 2015.⁷

⁴ A zero-day vulnerability is a computer-software vulnerability that is unknown to those who would be interested in mitigating it. Until the vulnerability is detected and patched the attackers can exploit it to adversely affect the defender. "Day Zero" is the day on which the interested party learns of the vulnerability.

⁵ <https://www.wired.com/story/vulnerability-equity-process-charter-transparency-concerns/> (retrieved on 15.12.2018)

⁶ An advanced persistent threat (APT) is a stealthy computer network attack (often nation-state sponsored) in which the attacker remains undetected for a long period of time. APTs are typically hard to attribute and are motivated by economic or political interests.

⁷ https://www.swissinfo.ch/eng/politics/ruag_swiss-close-investigation-into-cyber-attack-on-defence-firm/44352550 (retrieved on 15.12.2018)

INTRODUCTION

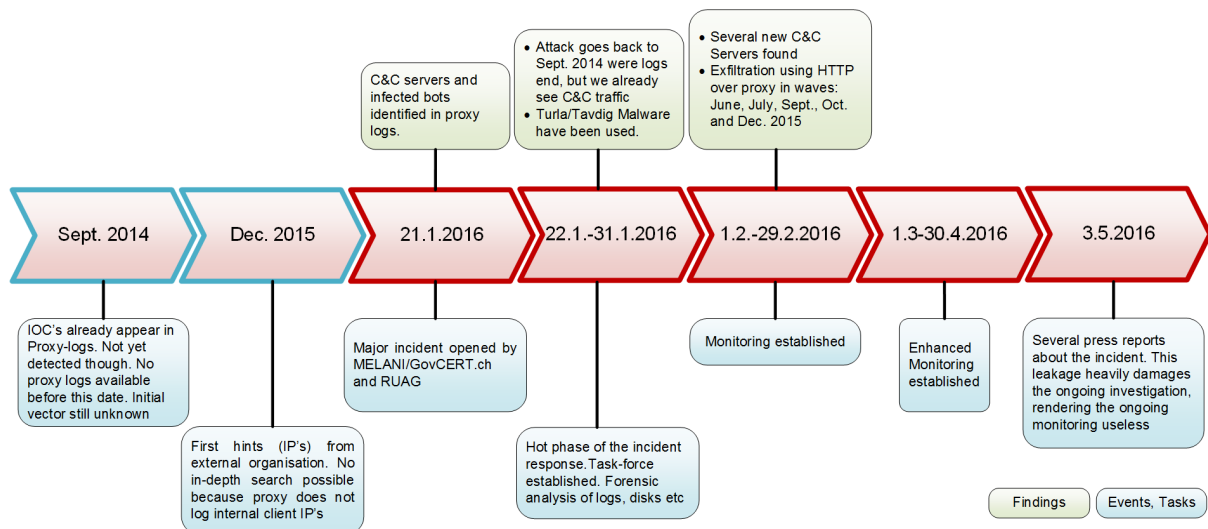


Figure 4: Chronology of the Advanced Persistent Threat against RUAG

This figure shows that the cyberattack against RUAG remained undetected for over one year and was finally discovered in December 2015 following security information sharing between the Swiss and the German intelligence communities. Figure courtesy of: MELANI / GovCERT.

This example shows that SIS is particularly useful against APTs, i.e. stealthy network attacks in which the attacker remains undetected on average for 200 days.⁸ Traditional security technology is typically ineffective in detecting APTs because there are millions of malware variations, increasing the information asymmetry between the attacker and the defender. In the RUAG case, the attackers have been using malware from the *Turla* family, which has been in the wild for several years. The attack has not been discovered through classical network forensics, but thanks to Cyber Threat Intelligence (CTI) exchange, i.e. intelligence based on various sources such as open source intelligence (OSINT), social media intelligence (SOCMINT), or human intelligence (HUMINT). Thus, SIS was an effective and low-cost way to reduce that asymmetry and to discover that the attacker has gained unauthorized access to the network of both the Swiss Confederation administration and the German government information systems.⁹

⁸ <https://www.swisscom.ch/en/business/enterprise/themen/security/advanced-persistent-threats.html> (retrieved on 15.12.18)

⁹ <https://www.bbc.com/news/world-europe-43248201> (retrieved on 15.12.18)

INTRODUCTION

The open-source community have also recognized the importance and usefulness of SIS. For instance, open-source threat intelligence platforms, such as the Malware Information Sharing Platform (MISP)¹⁰ project, develop utilities, tools, and documentation for more effective threat intelligence by sharing indicators of compromise, i.e. an artifact observed on a network or operating system (OS) that indicates a computer intrusion (Jacquet, 2017).

In conclusion, the RUAG case shows that one of the most effective countermeasures from a defender's perspective is the sharing of information about such attacks with other organizations, also crossing national borders. If this is done by any affected party, the price for the attacker raises, as he risks being detected in every network he attacked in different countries. This forces him to either prioritize his targets more, or to use different malware programs. This is precisely what happened in the RUAG case: it was detected based upon mutual sharing of information.¹¹

2. Related Work and Problem Statement

Our networked and interdependent environment generates high externalities, which plays a significant role in the underinvestment in cybersecurity (Gordon et al., 2015a). Investment in cybersecurity is unlikely to reach its theoretical optimum, because negative externalities exist and cannot be completely internalized by the agent. As a result, a *Nash-stable* yet inefficient equilibrium emerges in which each cybersecurity agent attempts to *free ride* on the investments of others, producing a suboptimal global level of cybersecurity in the economy.

Underinvestment in cybersecurity has negative consequences on the stock market and on the economy as a whole (Campbell, Gordon, Loeb, & Zhou, 2003). Although such free-riders are pervasive, especially in privately owned critical infrastructures, hence presenting significant risks to the national economy, the situation is exacerbated when national security is also taken into account (Gordon et al., 2015a). This free-rider problem prevents the full potential of SIS from being realized (ENISA, 2010; Gal-Or & Ghose, 2005), such that SIS is likely to remain at a sub-optimal level unless agents are provided with appropriate incentives (Aviram & Tor, 2003).

¹⁰ <https://github.com/MISP/MISP> (retrieved 03.03.19)

¹¹ Source: GovCERT.ch, *Technical Report about the Espionage Case at RUAG*, May 2016.

INTRODUCTION

2.1 Mandatory Security Information Sharing

Incentives can be provided either positively, by increasing the economic and social benefits gained when agents share security information, or negatively, by punishing agents that fail to share. Despite regulation that has been introduced both in the private and the public sector, imposing legal requirements to share security information, this did not seem to produce the desired effect of increasing SIS.

Reviews conducted in 2015 concluded that such regulatory attempts have been rather unsuccessful (ENISA, 2015), such that despite the introduction of several bills in the USA and in the EU,¹² actual SIS remains at low levels (Gordon et al., 2015b). When forced to share security information, organizations can even choose to share irrelevant or incomplete information, especially with competitors (Moore, 2010; Moran & Moore, 2010). This regulatory failure does not seem to be country specific, as regulatory attempts in other countries have been rather unsuccessful as well (Weiss, 2015).

¹² For example, the USA created the 2002 Sarbanes-Oxley Act and the 2015 Cybersecurity Information-Sharing Act (CISA). In December 2015, the European Parliament and Council agreed on the first EU-wide legislation on cybersecurity, adopting the EU Network and Information Security (NIS) Directive. The EU General Data Protection Regulation (GDPR) aims to harmonize and unify existing EU privacy breach reporting obligations. Like other union breach notification laws, both the GDPR and the NIS Directive impose fines to ensure compliance (Laube & Böhme, 2017).

INTRODUCTION

Region	Law	Obligated	Report	Address	Objective	Effect
EU	Telecoms Package	Firms in the telecoms sector	SB&PB	A or A&I	IP&S or IP&S&R	Sa or Sa&D
EU	Directive 2015/2366	Payment service providers	SB&PB	A or A&I	IP&S or IP&S&R	Sa or Sa&D
EU	Regulation 2016/679	Data controllers and processors	PB	A or A&I	IP&S or IP&S&R	Sa or Sa&D
EU	Directive 2016/1148	Market operators	SB&PB	A	IP&S or IP&S&R	Sa or Sa&D
US	State Laws	Firms controlling personal data	PB	I or A&I	IP&R	D or Sa&D
US	HIPAA & HITECH	Firms in the health care sector	PB	A&I	IP&R	Sa&D
US	GLBA	Firms in the financial sector	PB	I or A&I	IP&R	Sa&D

SB	Security breaches	IP	Incentivize firms to take precautions
PB	Privacy breaches	S	Draw and share conclusions with others defenders
A	Authorities	R	Improve rights of affected individuals
I	Affected individuals	Sa	Sanctions
		D	Disclosure costs

Table 1: Literature Review on Security Information Sharing Regulations

This table summarizes the key characteristics of selected EU and US notification laws. It indicates that most disclosure regimes stipulate breach information sharing, which leads to disclosure costs for affected firms. Source: Laube, 2017

2.2 Research Gap in Voluntary Security Information Sharing

By contrast, although recent contributions stress the need to study the theoretical mechanisms of how, if at all, positive encouragement could increase SIS, such research is prominently absent in the literature to the best of our knowledge. Previous research has identified the study of how incentives are linked to SIS as a promising research gap (Hämmerli, Raam, & Franceschetti, 2013) and has expressed the need to develop and test theories linking incentives with SIS outcomes. This dissertation elaborates a theoretical understanding of which incentives would make agents voluntarily share SIS, as well as an understanding of the mechanisms by which they work (ENISA, 2010; Gal-Or & Ghose, 2005; Gordon et al., 2003; Harrison & White, 2012).

INTRODUCTION

Information type	...with firms (private)		...with all actors (public)		
	Actor type	Theoretical works	Empirical works	Theoretical works	Empirical works
Attack information sharing of ...					
defenders ...	Kamnan and Telang (2005) Cavusoglu et al. (2007) Li and Rao (2007) Arora et al. (2008) Moore et al. (2010)	Li and Rao (2007) Ransbotham et al. (2012) Vasek and Moore (2012) Finifter et al. (2013) Zhao et al. (2015) Cetin et al. (2016) Maillart et al. (2016)	Nizovtsev and Thursby (2007) Cavusoglu et al. (2007)	Arora et al. (2006b) Telang and Wattal (2007) Frei et al. (2010) Arora et al. (2010b) Moore and Clayton (2011) Tang et al. (2013) Mitra and Ransbotham (2015)	
firms ...	Gordon et al. (2003) Gal-Or and Ghose (2005) Ögüt et al. (2005) Hausken (2007) Liu et al. (2011) Gordon et al. (2015) Laube and Böhme (2015) Naghizadeh and Liu (2016)	Moore and Clayton (2008) Vasek et al. (2016)		Gordon et al. (2010) Wang et al. (2013)	
Control information sharing of ...					
firms ...	Gordon et al. (2003) Gal-Or and Ghose (2005) Ögüt et al. (2005) Hausken (2007) Liu et al. (2011) Gordon et al. (2015) Laube and Böhme (2015) Naghizadeh and Liu (2016)		Gal-Or and Ghose (2005) Arora et al. (2006a) August and Tunca (2008) Choi et al. (2010)	Rescorla (2003) Moores (2005) Arora et al. (2006b) Arora et al. (2010a) Gordon et al. (2010) Edelman (2011) Wang et al. (2013) Durumeric et al. (2014)	
Impact information sharing of ...					
firms ...	Gordon et al. (2003) Gal-Or and Ghose (2005) Ögüt et al. (2005) Hausken (2007) Liu et al. (2011) Gordon et al. (2015) Laube and Böhme (2015) Laube and Böhme (2016) Naghizadeh and Liu (2016)		Gal-Or and Ghose (2005) Hausken (2007) Romanosky et al. (2010) Laube and Böhme (2015) Laube and Böhme (2016) Naghizadeh and Liu (2016)	Campbell et al. (2003) Hovav and D'Arcy (2004) Cavusoglu et al. (2004a) Acquisti et al. (2006) Ko and Dorantes (2006) Ishiguro et al. (2006) Kannan et al. (2007) Gatzlaff and McCullough (2010) Gordon et al. (2010) Gordon et al. (2011) Wang et al. (2013) Kwon and Johnson (2015) Gay (2016) Ablon et al. (2016)	



Table 2: Systematic Literature Review on Voluntary Security Information Sharing

This table summarizes key reviewed publication on voluntary SIS. Source: Laube & Böhme, 2017

All in all, the literature suggests that human behavior may be significantly associated with the extent to which SIS occurs (if at all). It is therefore not surprising to see recent work emphasizing that the study of human behavior is key to the understanding of SIS (Böhme, 2016). More specifically, this work predicts that SIS can only be imperfectly understood unless the human motivation for (not) participating in SIS is studied (Harrison and White, 2012; Laube and Böhme, 2016; Vakili et al., 2017).

However, few contributions have addressed this research gap to date. Since Laube and Böhme, 2017 have provided an excellent account of the SIS literature, we refrain from replicating this account here. We rather point to the fact that this account shows that very few

INTRODUCTION

empirical studies on non-public SIS exist. These few studies focus on analyzing incident counts and aggregate data, but they do not study human behavior at the individual level of analysis (see Laube and Böhme, 2017: 28 for a tabulated overview).

My research intends to close this gap by proposing how and why human behavior and SIS may be associated, and by providing an empirical test of this association. As cybersecurity problems are unlikely to be resolved by information systems theory alone, I adopt an interdisciplinary approach as recommended by Anderson and Moore (2006). Recently, interdisciplinary studies were productive in showing the extent to which human behavior is associated with knowledge sharing (Yan et al., 2016; Safa and von Solms, 2016).

Human agents can benefit from receiving information from others but still refuse to share such information, thus *free riding* on the information value provided by others. As other agents anticipate this behavior, the overall level of sharing would be low and investment cost could not attain its efficient optimum. This research therefore proposes that agents will not engage in SIS unless they are incentivized appropriately. Both this theoretical link between incentives and SIS, as well as their conceptualization and empirical test, has not been dealt with in the existing literature.

2.3 Research Questions

This thesis addresses this research gap by providing a theoretical framework that links incentives to SIS. Before, very little was known about the particular incentives that actually increase voluntary SIS, or about the mechanisms by which they take effect. To the best of our knowledge, no theory linking incentives to SIS has yet been produced or tested. Whereas the collective benefits of SIS have been contrasted with the low levels of sharing actually observed, very little work has been done to identify and test the types of incentive that could actually increase the level of sharing. Therefore, this research closes this gap by answering one main research question which entails three consecutive sub-questions answered in three distinct parts:

Which incentives and barriers are likely to influence the SIS activity?

- I. *How to measure the SIS activity and its predictors?*
- II. *What are the empirical effects of those identified predictors on SIS?*
- III. *What are the preferred governance models for the SIS activity?*

INTRODUCTION

2.4 Theoretical Foundations

The underlying assumptions of this thesis are anchored in the position that the technical aspects of computer science alone are not sufficient to solve all cybersecurity problems. Therefore, methodologies and concepts from other disciplines are necessary (Anderson & Moore, 2009). Arguments have been presented in the psychology and sociology literature on the role of positive incentives in persuading agents that they can improve their economic situation by behaving in a particular way (Anderson & Moore, 2009). Extended research in behavioral economics has demonstrated that by using rewards and sanctions, we can channel human behavior towards particular options (Bauer & van Eeten, 2009). In these models, positive incentives offer the agent a Pareto-superior¹³ state vis-a-vis the current state, at the cost of behavioral compliance.

When applied to SIS, these models suggest that agents will share more information if they expect that the particular incentives provided will enable them to reduce their individual investment in cybersecurity (Anderson et al., 2007; Davidson, Fenn, & Cid, 2016). Finally, research on meta-governance suggests that governments must encourage networks to achieve their goal of increasing SIS (Dunn-Cavelty & Suter, 2009). Taken together, this literature suggests that human volition¹⁴ is changed as a result of expected costs and benefits associated with particular actions.

2.5 Research Methodology

This section summarizes the different tools and methods used to answer our three research questions. The detailed methodology can be found separately in each part of the thesis.

First, I build a multidisciplinary theoretical framework that links incentives, selected from published scientific literature, to SIS. On this basis, I conceptualize a model linking the identified incentives to SIS. I do not pre-suppose any particular institutional or organizational design; incentives could be provided by governments, through contractual arrangements

¹³ Pareto optimality is a state of allocation of resources from which it is impossible to reallocate so as to make any human agent better off without making at least one human agent worse off.

¹⁴ Volition is the cognitive process by which a human agent decides on a particular course of action.

INTRODUCTION

between participants, or by public-private partnerships. In particular, for my overarching theoretical mechanism, I design a two-step mechanism by which, in a first step, incentives change agents' expectations. In a second phase, these changed expectations then trigger individual actions that result in SIS.

Second, on the basis of this theoretical framework, I construct and empirically test my system model. Section 2.8 details why the model was adapted from two-step to one-step during the operationalization process. This thesis presents – to the best of my knowledge – the first empirical analysis of the effect of each incentive on SIS, and also possible moderation and mediation effects between incentives. To attain this goal, I operationalize and empirically test my framework with an exclusive dataset collected together with the Swiss *Reporting and Analysis Centre for Information Security* (MELANI) which operates an ISAC (MELANI-Net)¹⁵. The online survey was sent to the 424 participants of that closed SIS user group. The methods to design the questionnaire are interdisciplinary as they are at the intersection of economics (econometrics), psychology (psychometrics) and information assurance.

Based on that primary data, the SIS activity is regressed on previously identified motivational factors. Methods used for validating and/or falsifying hypotheses are related to econometrics/psychometrics, and more precisely on a tobit model (describing the relationship between a non-negative dependent variable and an independent variable) and a probit model, i.e. a regression where the dependent variable can take only two values. All the research was conducted at a micro-level of analysis, i.e. investigated under a microeconomic and/or psychological perspective related to preferences, resource allocation, incentives, motivations and human behavior.

Third, I present descriptive statistics illustrating an application of our framework in the context of critical infrastructure protection. Using my exclusive field-data, I investigate correlations between three governance models' preferences and institutional rules. Finally, I extend my pre-analysis to four other control variables in order to complement the preferences analysis.

¹⁵ <https://melani-net.ssl.admin.ch> (retrieved 10.03.2019)

INTRODUCTION

2.6 Fundamental Choice of Research Method

In principle, SIS can be fundamentally analyzed by looking at data or humans (Dillman et al., 2014; Nunnally and Bernstein, 2017). Previous researches have empirically investigated SIS by using (meta)data (Laube & Böhme, 2017) or by analyzing data from Security Information and Event Management (SIEM) software, that combine Security Event Management (SEM) and Security Information Management (SIM), i.e. the collection of data such as log files into a central repository for trend analysis.

A pre-analysis of the MELANI-Net log file and MELANI internal statistics confirmed that about half of the population has not shared any information during the past ten years. This confirms the presence of a free-rider problem, illustrated in a case study at the end of Part I. However, this data was unfit for empirical analysis, since it was collected for an internal satisfactory survey, and not empirical testing of hypothesis specifically investigating human behavior in SIS.

Therefore, I opted for a psychometric approach, which is a well-established method to measure, study and analyze human behavior. Psychometrics has existed as a research method since at least 1936 when Thurstone founded the American Psychometric Society, and it is a relevant and rigorous method for the analysis of human behavior (Kaplan and Saccuzzo, 2017).

From the questionnaire design through the estimation of the models, I followed established standards of good practice in psychometric methodology and empirical analysis (Dillman et al., 2014; Nunnally and Bernstein, 2017). At least two of the publications I cite and adapt scales from (Yan et al., 2016; Safa and von Solms, 2016) use psychometric methods in the IS domain to make contributions to both information systems research and to the interaction of technical systems and human behavior. Also, the models I used (ordered logistic regression, Tobit regression) are well-established in econometric analysis, see Greene (2017).

2.7 Choices About the Study of Human Behavior

Fundamentally, there are two main ways to study human behavior: (1) ethnographics and (2) psychometrics. An ethnographic study would imply real-time human interaction observation, for instance with a “spyware” recording human behavior on an ISAC. This approach is hard to

INTRODUCTION

implement but would allow SIS observation over time and the development of longitudinal studies.

My approach is not an ethnographic one, in that I would observe individuals in the wild as they socially interact. Rather, I collected survey data by which these individuals report about the nature and results of their social interactions. That is an inherent limitation of psychometric research, nevertheless, I believe the approach is acceptable since it follows the established standards of good practice in this field (Nunnally and Bernstein, 2017).

However, this approach was not feasible in my context for many technical and institutional barriers. Therefore, I have opted for the second approach, psychometrics, where humans self-report their behavior and experience with SIS. This approach offers numerous advantages in my sensitive context (MELANI and the Swiss Intelligence Community work closely together with) where respondent wish to remain anonymous. Hence, on ground of research ethics an ethnographic approach is not feasible.

2.8 Psychometric Operationalization

The three parts in this dissertation are linked psychometrically in the following order: Part I defines constructs on a theoretical ground and establishes theoretical measurement level, that Part II intends to test. However, in the course of this dissertation, important adaptation and modification to the measurement model as specified in Part I are made such that Part II presents a more advanced model. When Part I was presented and published in the post-proceedings of CRITIS'16 I have featured a two-step estimation procedure by which incentives would proceed expectations and behavior.

However, as my research progressed, I found that this model could be simplified to a more fundamental association between human behavior and SIS. This implied psychometric operationalization of the constructs directly as regards human behavior without going through intervening or mediating constructs. Hence, the two-step estimation theoretically proposed in Part I was adapted to a linear model that analyses the association between human behavior and SIS.

INTRODUCTION

2.9 Empirical Procedures

In principle, when working the psychometric constructs, models can be estimated either by econometric methods or by applying Structural Equation Modeling (SEM) (Nunnally and Bernstein, 2017). In this research, I opted for an econometric approach and this for the following reasons: SEM is a useful analytical tool, however in my case there are some limitations that make econometric estimation better.

First, SEM is appropriate when the researcher studies latent constructs whose theoretical content cannot or only imperfectly be observed in empirical reality, such that the measured data are collected with significant and structural measurement error. However, I do not theorize about latent constructs nor do I attempt to study any such construct. My study focuses on specific human behavior that can be directly reported by respondents. Particularly, since my questionnaire records self-reported measures, no external intervention from the side of the researcher is required for data collection, which limits the potential impact of measurement error.

Further, SEM should be preferred over econometric models if the relationship between the constructs is so complex that it cannot be adequately captured by either moderation, mediation, two-stage least square (2SLS), or three-stage least square (3SLS) analysis (Zellner & Theil, 1962). However, my approach attempts to identify a rather straightforward association between human behavior and SIS. This theoretical development does not specify complex relationships between the constructs I measure.

Finally, my theoretical development specifies interaction effects. The estimation of interaction effects is cumbersome in an SEM model. A few years ago, simpler methods to do this emerged (more technical documentation is available on request), but I do not believe these novel developments are established to an extent that they could be termed safe practice. Additionally, while these methods are easier to apply than their predecessors, they are still more cumbersome than calculating interaction effects in regression analyses.

2.10 Explanation of the Particular Constructs

As in the proceeding section, Part II presents more advanced empirical model than Part I, both in term of theoretical and their operationalization. In Part I, I had adopted psychometric scales

INTRODUCTION

from the literature but labeled these scales differently. This approach was problematic, because it led to inconsistencies between the construct as it was defined by the original authors and my subjective interpretation of those constructs.

Therefore, in Part II, I returned to the original scales as they were published. These psychometric scales are documented in the appendix to Part II. The constructs are chosen in both prior behavioral research, behavioral economics and social psychology. These measure important aspects of human behavior, which are particularly relevant in the context of SIS.

2.11 Research Context

This research uses the Swiss ISAC MELANI-Net both for illustration, data collection and policy recommendations. I do not study public knowledge sharing or Q&A forums like, e.g., Yan et al. (2016) do. I study an Information Sharing and Analysis Center (ISAC), and there is only one ISAC in Switzerland. An ISAC is an organization that brings together – in person, by face-to-face meetings – specialist managers that exchange information that is relevant for cybersecurity. See ENISA (2017) for a detailed description and historical background of different ISACs in European countries and the USA.

MELANI-Net is the national Swiss information security analysis center (ISAC). It is comparable to other national-level ISACs where information about cyberthreats and incidents relevant for the national economy, government institutions and critical infrastructures is shared by direct (social) interaction. Such ISACs exist in most developed countries. However, in contrast to many other countries, membership in MELANI-Net is voluntary. Within this ISAC, I have studied the closed user group, i.e. those senior management professionals who exchange highly sensitive data about security incidents, threats, and breaches. In the revised Part I have provided more background explanation regarding MELANI-Net, including the highly detailed report of Dunn Cavelty (2014: 39-54).

Any information exchange via MELANI-Net is restricted to the 424 members of the closed user group. Each and every member of this group must undergo government-led confirmation of their ID and personality before they are allowed access to the ISAC (hence, membership in MELANI-Net, unlike in Q&A forums, is restricted and subject to high-level legitimization procedures). There is no public forum, discussion, or dissemination.

INTRODUCTION

The operative problem of my study is to capture human behavior as it unfolds. An ethnographic approach was impossible since respondents wished to remain anonymous, such that ID'ing individuals and observing their interaction in real time was not feasible. I therefore resorted to an alternative approach. Within MELANI-Net, the very social exchange that constitutes SIS is often triggered by an initial message that an individual concerned with a cyberthreat posts on an internal message board. The focal individual can decide with whom (among the other members) this information is shared.

3. Thesis Structure and Outline

This cumulative thesis is divided into three parts, based on two double-blind peer-reviewed articles published in conference proceedings and one double-blind peer-reviewed publication revised and resubmitted in the *Journal of Cybersecurity*.¹⁶ The three parts can be read independently as standalone manuscripts. However, the weaknesses of this format are that it can lead to content redundancies and some small terminology differences across the different parts.

The three articles presented are developed in a chronological symbiosis order from the beginning of the PhD thesis. The first part establishes a novel theoretical framework linking incentives and SIS. A first version of the theoretical model is presented, and five SIS indicators are identified in order to analyze the SIS incentive mechanism. The second part provides empirical analyses by testing the hypotheses developed in Part I. The third part provides policy recommendations based on the same exclusive dataset as in Part II.

¹⁶ <https://academic.oup.com/cybersecurity> (retrieved on 28.10.2018)

INTRODUCTION

3.1 Part I: Theoretical Framework

The following conference paper was presented in October 2016 at the 11th *Critical Information Infrastructure Security*¹⁷ (CRITIS 2016), held in Paris, France:

- Mermoud, A., Keupp, M. M., Ghernaoui, S., & Percia David, D. (2016). Using Incentives to Foster Security Information Sharing and Cooperation: A General Theory and Application to Critical Infrastructure Protection. In *Lectures Notes in Computer Science* (pp. 150-162). Springer, Cham. https://doi.org/10.1007/978-3-319-71368-7_13

This paper was accepted as full paper among 22 other full papers and 8 short papers reviewed and selected from a total of 58 submissions. A revised version of the post-conference proceedings paper appears in Part I of this thesis.

3.2 Part II: Empirical Analysis

The following conference paper was presented in June 2018 at the 17th annual *Workshop on the Economics of Information Security*¹⁸ (WEIS 18), held in Innsbruck, Austria:

- Mermoud, A., Keupp, M. M., Huguenin, K., Palmié, M., & Percia David, D. (2018). Incentives for Human Agents to Share Security Information: A Model and an Empirical Test. In *Proceedings of the 17th Workshop on the Economics of Information Security* (WEIS), Innsbruck, Austria. https://weis2018.econinfosec.org/wp-content/uploads/sites/5/2018/05/WEIS_2018_paper_7.pdf

This paper was accepted as full paper among 22 other full paper reviewed and selected from a total of 57 submission. This conference paper has been revised and resubmitted to the *Journal of Cybersecurity* on the 28th of February 2019 and appears in Part II of this thesis, under the following title: *To Share or not to Share: A Behavioral Perspective on Human Participation in Security Information Sharing*.

¹⁷ <http://critis2016.org> (retrieved on 28.10.2018)

¹⁸ <https://weis2018.econinfosec.org> (retrieved on 28.10.2018)

INTRODUCTION

3.3 Part III: Policy Recommendations

The following conference paper was presented in September 2018 at the 13th International Conference on *Critical Information Infrastructure Security*¹⁹ (CRITIS 2018), held in Kaunas, Lithuania:

- Mermoud, A., Keupp, M. M., Percia David, D. (2019). Governance Models Preferences for Security Information Sharing: An Institutional Economics Perspective for Critical Infrastructure Protection. In *Lectures Notes in Computer Science* (pp. 179-190). Springer, Cham. https://doi.org/10.1007/978-3-030-05849-4_14

This paper was accepted as full paper among 16 other full papers and 3 short papers reviewed and selected from a total of 61 submissions. A revised version of the post-conference proceedings paper appears in Part III of this thesis.

4. Other Scientific Contributions

4.1 Conference Paper: CRITIS 2016

The following conference paper was presented in October 2016 at the 11th International Conference on *Critical Information Infrastructure Security*²⁰ (CRITIS 2016), held in Paris, France:

- Percia David, D., Keupp, M. M., Ghernaouti, S., & Mermoud, A. (2016). Cyber Security Investment in the Context of Disruptive Technologies: Extension of the Gordon-Loeb Model and Application to Critical Infrastructure Protection. In *International Conference on Critical Information Infrastructures Security* (pp. 296-301). Springer, Cham. https://doi.org/10.1007/978-3-319-71368-7_25

This paper was accepted as short paper among 22 other full papers and 8 short papers reviewed and selected from a total of 58 submissions.

¹⁹ <http://www.lei.lt/critis2018> (retrieved on 28.10.2018)

²⁰ <http://critis2016.org> (retrieved on 28.10.2018)

4.2 Journal Article: Computers in Human Behavior

The following journal article was accepted with major revisions in *Computers in Human Behavior*²¹ on the 3rd of January 2019:

- Percia David, D., Keupp, M. M., Mermoud, A. (2019). Opportunism is Not Enough: The Influence of Agent Behavior on the Perceived Performance of Security Information Sharing. *Computers in Human Behavior*.

This manuscript extends the findings in this dissertation by focusing on the perceived performance of SIS, arguing that the extent to which a human agent engages in SIS is a function of their individual performance expectation, i.e., of the net benefit they expect as a result of engaging in SIS. Combining theory with opportunistic action and altruistic punishment, we provide empirical analysis predictors of the perceived performance of SIS. Our results suggest that the frequency of sharing transactions, the perceived utility of resource allocation, reciprocity expectations, and trust have a significant effect on the formation of the perceived performance of SIS. These findings point to several opportunities to motivate human agents to show cooperative behavior.

4.3 Bachelor Thesis Supervision

During my time as PhD student I was lucky enough to supervise a bachelor thesis which received the 2018 award “Prix à l’innovation du domaine économie et services de la HES-SO”:

- Cuche, K., Madinier, H., Mermoud, A. (2018). Intelligence économique et politique : besoins et pratiques dans les principaux partis politiques suisses (bachelor dissertation). <https://doc.rero.ch/record/323603?ln=fr>

This work received some media coverage, for instance in the Swiss daily reference newspaper *Le Temps*:

- Mermoud, A. & Cuche, K. (2017). Le fédéralisme, meilleur antidote contre les manipulations politiques, in *Le Temps* (04.09.2017).²²

²¹ <https://www.journals.elsevier.com/computers-in-human-behavior> (retrieved on 28.10.2018)

²² <https://www.letemps.ch/opinions/federalisme-meilleur-antidote-contre-manipulations-politiques> (retrieved 11.01.2019)

5. Research Disseminations

This section lists research dissemination activities – in different languages and through different channels – provided to practitioners, experts, and students:

5.1 Lecturer at ETH Zurich

During the Autumn Semester 2018, I had the chance to become lecturer of the course 853-0102-00L *Military Business Administration II - Case Examples*²³ at the Swiss Federal Institute of Technology (ETH Zurich). This gave me the opportunity to transfer my research results to the students in German. The program of the course is organized into 14 units of 90 minutes each. The units combine the elements of lecture (where analytical concepts are taught) and application (where these concepts are applied). The program focuses on an analysis of hybrid warfare against Switzerland. Three main topics are highlighted: cyber defense, security of critical infrastructures, and security of supply.

5.2 Conference on Economic Warfare at ETH Zurich

In 2016, I had the opportunity to organize and coordinate the autumn conference of the Military Academy at ETH Zurich dedicated to the challenges and strategies of modern economic warfare. On the 10th of September 2016, around 200 guests from politics, the military, business and science attended the event. The conference leader, PD Dr. Marcus M. Keupp and four renowned experts explored the hybrid threat potential of modern economic warfare and developed defense strategies. I was also in charge of the overall coordination and edition of the conference proceedings:

- Keupp, M.M., Mermoud, A. (Gesamtredaktion). (2016). Der moderne Wirtschaftskrieg - Herausforderungen und Strategien. *Schriftenreihe MILAK-Herbsttagung vom 10.09.2016*. ISBN: 978-3-9524718-0-7.
<https://www.vtg.admin.ch/de/organisation/kdo-ausb/hka/milak.detail.news.html/vtg-internet/verwaltung/2016/16-09/16-09-10-milak.html>

²³<http://www.vorlesungsverzeichnis.ethz.ch/Vorlesungsverzeichnis/lerneinheit.view?lerneinheitId=124153&semkez=2018W&ansicht=KATALOGDATEN&lang=en> (retrieved on 28.10.2018)

INTRODUCTION

5.3 Massive Open Online Course (MOOC): The Economics of Cybersecurity

At the beginning of the year 2015, while writing my PhD thesis proposal, I had the opportunity to take the *DelftX - EconSec101x* MOOC²⁴ on the Economics of Cybersecurity. This online course was a great introduction to the topic and offered me the opportunity to interact informally through an internal forum with my research community at an early stage of my research. As the final part of this course, I had to write a short reflection essay on the economics of security information sharing which received several relevant feedbacks.

5.4 Invited Talks

During my period as a PhD candidate, I had the chance to give a few invited talks, for instance:

- On the 17th of February 2016, in French and German, for the *Höhere Stabsoffiziere (HSO) Seminar*, gathering all senior staff officers of the Swiss Armed Forces (in the rank of brigadier, major general or lieutenant general), held in Bern, Switzerland.
- On the 24th of May 2016, in French, for The *Swiss Association for Market Research, Competitive Intelligence and Strategic Planning (SMCS)*,²⁵ held in Geneva, Switzerland.
- On the 6th of December 2016, in French, for the *Association suisse de la sécurité de l'information (CLUSIS)*²⁶ held in Geneva, Switzerland.
- On the 13th of December 2016, in French, for the 30th *De Nouvelles Architectures pour les Communications (DNAC 2016)*²⁷ held at *Télécom ParisTech*, in Paris.

²⁴ <https://www.edx.org/course/cyber-security-economics-delftx-secon101x-0> (retrieved on 28.10.2018)

²⁵ <https://swissintell.ch> (retrieved on 28.10.2018)

²⁶ <https://clusis.ch> (retrieved on 28.10.2018)

²⁷ <https://dnac2016.dnac.org> (retrieved on 28.10.2018)

5.5 Professional and Trade Magazines, Newspapers and Book Chapters

During my time as a PhD candidate, I had the opportunity to coordinate (as associate editor) a special edition of the *Revue Militaire Suisse*²⁸ (RMS+ N°6 / 2018) dedicated to cybersecurity and threat intelligence. I also authored several vulgarized articles for information professionals and security experts:

- Mermoud, A. (2015). Comment la Suisse a gagné le Cyber Challenge 2015, in *Le Temps* (11.05.2015).
- Mermoud, A. & Percia David, D. (2016). La LRens, pour réduire le vide stratégique numérique, in *Le Temps* (21.09.2016).
- Mermoud, A., & Percia David, D. (2016). L'intelligence économique : Du renseignement militaire au renseignement privé, in *Revue Militaire Suisse* (RMS+) N°4.
- Percia David, D. & Mermoud, A. (2016). L'attractivité du service militaire : garantie d'un système sécuritaire efficace, in *Revue Militaire Suisse* (RMS+) N°6.
- Keupp M.M., Mermoud, A., & Percia David, D. (2017). Pour une approche économique de la cybersécurité, in *Military Power Revue* N°1.
- Keupp M.M., Mermoud, A., & Percia David, D. (2018). Teile und herrsche: Cybersicherheit durch Informationsaustausch, in *Allgemeine Schweizerische Militärzeitschrift* (ASMZ) N° 7.
- Keupp M.M., Percia David, D. & Mermoud, A. (2018). Teile und herrsche: Cybersicherheit durch Fusionszentren, in *Allgemeine Schweizerische Militärzeitschrift* (ASMZ) N°13.
- Mermoud, A., & Percia David, D. (2018). La souveraineté du renseignement : un besoin stratégique grandissant, in *Revue Militaire Suisse* (RMS+) N°6.
- Mermoud, A., & Percia David, D. (2018). Produire du renseignement grâce au partage d'information, in *Revue Militaire Suisse* (RMS+) N°6.
- Percia David, D. & Mermoud, A. (2018). Les fusion centers: le renseignement sous stéroïdes ?, in *Revue Militaire Suisse* (RMS+) N°6.
- Mermoud, A., Keupp, M. M. (2019). Using Incentives to Foster Security Information Sharing and Cooperation: A General Theory and Empirical Application to Critical Infrastructure Defense. Springer, Cham.

²⁸ The complete collection of the RMS archives is available online at e-periodica.ch via a project led by ETH Zurich.

INTRODUCTION

5.6 Consulting Services

During my time as a PhD candidate, I was lucky enough to offer some consulting services based on my research for the private sector and policy makers:

- Credit Suisse AG, Economic Research, Zurich.
- Canton of Geneva: permanent member of the Geneva Security Council.
- Canton of Fribourg: advisor to the Business Continuity Plan in Case of Network Breakdown.
- Military Intelligence Service, Swiss Armed Forces.

5.7 Cybersecurity Competitions

During my time as a PhD candidate, I had the opportunity to participate in two leading international cybersecurity competitions:

- Winner of the 2015 Cyber 9/12 Student Challenge²⁹ as head of team Switzerland, held in Geneva, Switzerland.
- Judge at the 2016 Cyber 9/12 Student Challenge, held in Geneva, Switzerland.

²⁹ <http://www.atlanticcouncil.org/resources/cyber-912-student-challenge-resources> (retrieved on 29.10.2018)

6. References

- Anderson, R. (2001). Why information security is hard - an economic perspective. In *Seventeenth Annual Computer Security Applications Conference* (pp. 358–365). IEEE. <https://doi.org/10.1109/ACSAC.2001.991552>
- Anderson, R., & Moore, T. (2006). The Economics of Information Security. *Science*, 314(5799), 610–613. <https://doi.org/10.1126/science.1130992>
- Anderson, R., & Moore, T. (2009). Information security: where computer science, economics and psychology meet. *Philosophical Transactions of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, 367(1898), 2717–2727. <https://doi.org/10.1098/rsta.2009.0027>
- Anderson, R., Moore, T., Nagaraja, S., & Ozment, A. (2007). Incentives and Information Security. In N. Nisan, R. Tim, E. Tardos, & V. Vazirani (Eds.), *Algorithmic Game Theory* (pp. 633–650). Cambridge: Cambridge University Press. <https://doi.org/10.1017/CBO9780511800481.027>
- Aviram, A., & Tor, A. (2003). Overcoming Impediments to Information Sharing. *Alabama Law Review*, 55(2), 231–280.
- Bauer, J., & van Eeten, M. (2009). Cybersecurity: Stakeholder incentives, externalities, and policy options. *Telecommunications Policy*, 33(10–11), 706–719. <https://doi.org/10.1016/j.telpol.2009.09.001>
- Böhme, R. 2016. Back to the roots: Information sharing economics and what we can learn for security. In: Second workshop on information sharing and collaborative security (WISCS), Denver CO, USA: ACM, 2015.
- Campbell, K., Gordon, L. A., Loeb, M. P., & Zhou, L. (2003). The economic cost of publicly announced information security breaches: empirical evidence from the stock market. *Journal of Computer Security*, 11(3), 431–448. <https://doi.org/10.3233/JCS-2003-11308>
- Davidson, A., Fenn, G., & Cid, C. (2016). A Model for Secure and Mutually Beneficial Software Vulnerability Sharing. In *Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security* (pp. 3–14). New York, NY, USA: ACM. <https://doi.org/10.1145/2994539.2994547>
- Dillman, D.A., Smyth, J., Christian, L.M. 2014. *Internet, Phone, Mail, and Mixed-Mode Surveys: The Tailored Design Method*. 4th ed. John Wiley & Sons.
- Dunn Cavelty, M. (2014). *Cybersecurity in Switzerland* (Springer Briefs in Cybersecurity). Cham: Springer International Publishing.
- Dunn-Cavelty, M., & Suter, M. (2009). Public–Private Partnerships are no silver bullet: An expanded governance model for Critical Infrastructure Protection. *International Journal of Critical Infrastructure Protection*, 2(4), 179–187. <https://doi.org/10.1016/j.ijcip.2009.08.006>

INTRODUCTION

- ENISA. (2010). *Incentives and Barriers to Information Sharing* (White report). Heraklion: European Union Agency for Network and Information Security. Retrieved from <https://www.enisa.europa.eu/publications/incentives-and-barriers-to-information-sharing>
- ENISA. (2015). *Cyber Security Information Sharing: An Overview of Regulatory and Non-regulatory Approaches* (White report). Heraklion: European Union Agency for Network and Information Security. Retrieved from <https://www.enisa.europa.eu/activities/cert/support/information-sharing/cybersecurity-information-sharing>
- Fehr, E., & Gächter, S. (2000). Fairness and Retaliation: The Economics of Reciprocity. *The Journal of Economic Perspectives*, 14(3), 159–181.
- Gal-Or, E., & Ghose, A. (2005). The Economic Incentives for Sharing Security Information. *Information Systems Research*, 16(2), 186–208. <https://doi.org/10.1287/isre.1050.0053>
- Gintis, H. (2000). Beyond Homo economicus: evidence from experimental economics. *Ecological Economics*, 35(3), 311–322. [https://doi.org/10.1016/S0921-8009\(00\)00216-0](https://doi.org/10.1016/S0921-8009(00)00216-0)
- Gordon, L. A., & Loeb, M. P. (2002). The Economics of Information Security Investment. *ACM Trans. Inf. Syst. Secur.*, 5(4), 438–457. <https://doi.org/10.1145/581271.581274>
- Gordon, L. A., Loeb, M. P., & Lucyshyn, W. (2003). Sharing information on computer systems security: An economic analysis. *Journal of Accounting and Public Policy*, 22(6), 461–485. <https://doi.org/10.1016/j.jaccpubpol.2003.09.001>
- Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Zhou, L. (2015a). Externalities and the Magnitude of Cyber Security Underinvestment by Private Sector Firms: A Modification of the Gordon-Loeb Model. *Journal of Information Security*, 06(01), 24–30. <https://doi.org/10.4236/jis.2015.61003>
- Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Zhou, L. (2015b). The impact of information sharing on cybersecurity underinvestment: A real options perspective. *Journal of Accounting and Public Policy*, 34(5), 509–519. <https://doi.org/10.1016/j.jaccpubpol.2015.05.001>
- Gordon, L. A., Loeb, M. P., & Sohail, T. (2010). Market Value of Voluntary Disclosures Concerning Information Security. *Management Information Systems Quarterly*, 34(3), 567–594. <https://doi.org/10.2307/25750692>
- Greene, W.H. 2017. *Econometric Analysis*. 8th ed. Pearson.
- Jacquet, C. Privacy aware sharing of IOCs in MISP. Ecole polytechnique de Louvain, Université catholique de Louvain, 2017. Prom. : Sadre, Ramin. <http://hdl.handle.net/2078.1/thesis:10600>
- Hämmerli, B., Raaum, M., & Franceschetti, G. (2013). Trust Networks among Human Beings: Analysis, Modeling, and Recommendations. In F. Flammini, R. Setola, & G. Franceschetti (Eds.), *Effective Surveillance for Homeland Security* (Vols. 1–0, pp. 21–50). New York: Chapman and Hall/CRC. Retrieved from <https://www.taylorfrancis.com/books/e/9781439883259/chapters/10.1201%2Fb14839-8>

INTRODUCTION

- Harrison, K., & White, G. (2012). Information sharing requirements and framework needed for community cyber incident detection and response. In *2012 IEEE Conference on Technologies for Homeland Security (HST)* (pp. 463–469). IEEE.
<https://doi.org/10.1109/THS.2012.6459893>
- Hausken, K. (2007). Information sharing among firms and cyber attacks. *Journal of Accounting and Public Policy*, 26(6), 639–688.
<https://doi.org/10.1016/j.jaccpubpol.2007.10.001>
- Hausken, K. (2015). A Strategic Analysis of Information Sharing Among Cyber Attackers. *Journal of Information Systems and Technology Management*, 12(2), 245–270.
<https://doi.org/10.4301/S1807-17752015000200004>
- Kahneman, D., & Tversky, A. (1979). Prospect Theory: An analysis of Decision under Risk. *Econometrica: Journal of the Econometric Society*, 47(2), 263–291.
- Laube, S., & Böhme, R. (2015). Mandatory Security Information Sharing with Authorities: Implications on Investments in Internal Controls. In *Proceedings of the 2Nd ACM Workshop on Information Sharing and Collaborative Security* (pp. 31–42). New York, NY, USA: ACM. <https://doi.org/10.1145/2808128.2808132>
- Laube S, Böhme R. The economics of mandatory security breach reporting to authorities. *Journal of Cybersecurity* 2016;2:29–41.
- Laube, S., & Böhme, R. (2017). Strategic Aspects of Cyber Risk Information Sharing. *ACM Computing Surveys (CSUR)*, 50(5), 77:1–77:36. <https://doi.org/10.1145/3124398>
- Luijff, E., & Klaver, M. (2015). On the Sharing of Cyber Security Information. In M. Rice & S. Sheno (Eds.), *Critical Infrastructure Protection IX* (pp. 29–46). Springer.
https://doi.org/10.1007/978-3-319-26567-4_3
- Moore, T. (2008). *Cooperative attack and defense in distributed networks* (Technical Report UCAM-CL-TR-718). University of Cambridge.
- Moore, T. (2010). The economics of cybersecurity: Principles and policy options. *International Journal of Critical Infrastructure Protection*, 3(3–4), 103–117.
<https://doi.org/10.1016/j.ijcip.2010.10.002>
- Moore, T., & Anderson, R. (2011). Economics and Internet Security: A Survey of Recent Analytical, Empirical, and Behavioral Research. Retrieved from
<https://dash.harvard.edu/handle/1/23574266>
- Moore, T., & Clayton, R. (2009). The impact of incentives on notice and take-down. In M. E. Johnson (Ed.), *Managing Information Risk and the Economics of Security* (pp. 199–223). Boston, MA: Springer. https://doi.org/10.1007/978-0-387-09762-6_10
- Moore, T., Pym, D., & Ioannidis, C. (2010). *Economics of Information Security and Privacy*. Springer Science & Business Media.
- Moran, T., & Moore, T. (2010). The Phish-Market Protocol: Securely Sharing Attack Data

INTRODUCTION

between Competitors. In R. Sion (Ed.), *Financial Cryptography and Data Security* (pp. 222–237). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-14577-3_18

Nunnally, J.C., Bernstein, I. 2017. *Psychometric Theory*. 3rd ed. McGraw-Hill.

Odlyzko, A. (2003). Economics, Psychology, and Sociology of Security. In R. N. Wright (Ed.), *Financial Cryptography* (Vol. 2742, pp. 182–189). Berlin, Heidelberg: Springer. https://doi.org/10.1007/978-3-540-45126-6_13

Safa NS, von Solms R. An information security knowledge sharing model in organizations. *Computers in Human Behavior* 2016;57:442–51.

Vakilinia I, louis SJ, Sengupta S. Evolving Sharing Strategies in Cybersecurity Information Exchange Framework. *Proceedings of the Genetic and Evolutionary Computation Conference Companion*. New York, NY, USA: ACM, 2017, 309–310.

Vasek, M., Weeden, M., and Moore, T. (2016). *Measuring the impact of sharing abuse data with web hosting providers*. In *ACM Workshop on Information Sharing and Collaborative Security*, pages 71--80. ACM.

Weiss, E. (2015). *Legislation to Facilitate Cybersecurity Information Sharing: Economic Analysis* (CRS Report). Congressional Research Service. Retrieved from <https://horizon.hozint.com/2014/12/crs-legislation-to-facilitate-cybersecurity-information-sharing-economic-analysis/>

Yan Z, Wang T, Chen Y et al. Knowledge sharing in online health communities: A social exchange theory perspective. *Information & Management* 2016;53:643–53.

PART I: Theoretical Framework

“People often represent the weakest link in the security chain and are chronically responsible for the failure of security systems.”

“Amateurs hack systems, professionals hack people.”

- Bruce Schneier

Using Incentives to Foster Security Information Sharing and Cooperation: A General Theory and Application to Critical Infrastructure Protection

Published in the proceedings of the 11th International Conference on Critical Information Infrastructures Security (CRITIS 2016)

Paris, France, October 10-12, 2016

Publisher: Springer, Lecture Notes in Computer Science book series (LNCS, volume 10242)

Abstract

There is a conspicuous lack of investment in cybersecurity. Various measures have been proposed to mitigate this. Investment models theoretically demonstrate the potential application of security information sharing (SIS) to critical infrastructure protection (CIP). However, the free-rider problem remains a major pitfall, preventing the full potential benefits of SIS from being realized. We closed an important research gap by providing a theoretical framework that links incentives with voluntary SIS. We applied this framework to CIP through a case study of the Swiss Reporting and Analysis Centre for Information Security, and we used the SIS model to analyze the incentive mechanisms that most effectively support SIS for CIP. Our work contributes to an understanding of the free-rider problem that plagues the provision of the public good that is cybersecurity and offer clues to its mitigation.

Keywords: cybersecurity economics; cybersecurity efficiency and effectiveness; investments and incentives of critical infrastructure protection; free-rider problem; security information sharing economics; information assurance.

1. Introduction

Investment in cybersecurity¹ remains Pareto sub-optimal due to the presence of externalities that cannot be completely internalized by the investor (Gordon, Loeb, Lucyshyn, & Zhou, 2015b). As a result, a Nash-stable yet inefficient equilibrium has emerged, in which each cybersecurity investor attempts to free ride on the investments of the others, consequently producing a Pareto sub-optimal global level of cybersecurity in the economy (Gordon, Loeb, Lucyshyn, & Zhou, 2015a). Although such free-rider problems are pervasive in the private sector and present significant risks to the national economy, the situation is exacerbated when national security is also taken into account (Gordon et al., 2015a). Universities, critical infrastructure (CI) providers, government, and the armed forces all rely heavily on information technology (IT) systems to fulfill their mandates. This makes them vulnerable to cyberattacks, which makes the consequences of cybersecurity breaches especially harmful for society as a whole (Gordon, Loeb, Lucyshyn, & Zhou, 2015a). Various measures have been proposed to mitigate this problem of under-investment, among which the sharing of cybersecurity-relevant information appears to be the most viable and relevant, as a way of simultaneously mitigating the externalities and increasing individual utility, inter-investor information, and social welfare (Gal-Or & Ghose, 2005). Furthermore, such sharing can reduce the information asymmetry between an attacker and the defender in the case of zero-day vulnerability attacks where the defender has little, if any, time to react (Laube & Böhme, 2016). By “sharing of cybersecurity-relevant information”, we refer to a process by which cybersecurity investors provide each other with information about threats, vulnerabilities, and successfully defended cyberattacks. For the sake of brevity, we will refer to this as “security information sharing” (SIS).² Part I of this thesis is organized as follows. In the first and second sections, we develop a theoretical framework and present our propositions. In Section 3, we report a case study. In Section 4, we discuss the limitations and possible extensions of the model. Our concluding remarks and proposals for future work are given in Section 5.

¹ In our study we use the term “cybersecurity” as a synonym for “information security,” referring to the protection of information that is transmitted over the Internet or any other computer network.

² “security information sharing” SIS can be defined as the mutual exchange of cybersecurity-relevant information on vulnerabilities, phishing, malware, and data breaches, as well as threat intelligence, best practices, early warnings, and expert advice and insight.

2. Theoretical Framework and Propositions

The importance of SIS for critical infrastructure protection (CIP) is widely acknowledged by academics, policy-makers, and industrial actors, as it can reduce risks, deter attacks, and enhance the resilience of the CI (Dunn-Cavelty & Suter, 2009). Cybercriminals and hackers have a long history of sharing experiences, tools, and vulnerabilities; this has contributed to the success of major cyberattacks. The timely introduction of SIS is therefore vital for CIP, because attackers sharing techniques erodes the effectiveness of traditional defense tools (de Bruijne & van Eeten, 2007). The Gordon-Loeb model theoretically demonstrates the potential application of SIS to CIP (Gordon, Loeb, & Lucyshyn, 2003). However, empirical studies have shown that a significant free-rider problem exists, preventing the full potential of SIS from being realized (ENISA, 2010). Although SIS offers a promising way of reducing the amount of total investment needed to establish cybersecurity, extant empirical research shows that both the frequency of SIS (i.e., the number of security information sharing transactions between investors in a given time interval) and its intensity (i.e., the depth of information shared in each transaction, represented by the number of comments related to each incident shared) remain at relatively low levels in the absence of any further intervention. In the absence of appropriate extra incentives, SIS is likely to be conducted at a sub-optimal level (Aviram & Tor, 2003).

2.1 Regulation Alone Cannot Solve the Free-Rider Problem

Incentives can be either positive, by increasing the economic and social benefits gained when investors share security information, or negative, by punishing investors that fail to share. Attempts to introduce negative incentives through regulation have been rather unsuccessful (ENISA, 2015). In the USA³ and in the EU,⁴ despite the introduction of several bills that encourage security-information sharing, the actual SIS remains at low levels (Gordon, Loeb, Lucyshyn, & Sohail, 2006). These bills were an attempt to impose legal requirements on both the private and public sectors when they share information, but to date such regulations do not seem to be producing the desired effect of increasing SIS (Hausken, 2007). When forced to share SIS, firms might even choose to share irrelevant or incomplete information, especially

³ In particular the 2002 Sarbanes-Oxley Act (SOX) and the 2015 Cybersecurity Information Sharing Act (CISA).

⁴ In December 2015, the European Parliament and Council agreed on the first EU-wide legislation on cybersecurity, adopting the EU Network and Information Security (NIS) Directive.

PART I: Theoretical Framework

with competitors (Moran & Moore, 2010). This regulatory failure does not seem to be country specific because attempts at negative incentivization by means of regulation, laws, and the imposition of punishments have also been unsuccessful elsewhere (Weiss, 2015).

2.2 Linking Incentives to Voluntary SIS

We propose an alternative approach to regulation. Security information, once obtained, can be either shared at a small marginal cost or kept private and hoarded by the producer. Therefore, a theoretical understanding of the mechanisms that would cause investors to voluntarily share SIS (Harrison & White, 2012) is needed. We propose that both the frequency and intensity of SIS will increase if investors are provided with appropriate positive incentives to share information (as opposed to being forced or encouraged to share through regulation). We do not presuppose any particular institutional or organizational design; incentives could be provided by government, through contractual arrangements between participants, or by public-private partnerships (PPPs). Although previous research has identified this as a promising approach (Hämmerli & Grudzien, 2015), very little is known about the particular incentives (if any) that actually increase voluntary SIS, or about the mechanisms by which they work. Past contributions have repeatedly stressed the need to develop and test theories linking incentives with SIS outcomes (Gal-Or & Ghose, 2005) but, to the best of our knowledge, no such theory has yet been produced or tested. As a result, the existing literature provides few serious discussions on the causal linkages by which incentives could be expected to increase the intensity and frequency of SIS. Whereas the collective benefits of SIS have been contrasted with the low levels of sharing actually observed, very little work has been done to identify the types of incentive that could successfully correct this. To close this gap, we propose a theoretical framework that links incentives with voluntary SIS. Our theory identifies the incentives that are expected to increase the frequency and intensity of voluntary SIS and clarifies the causal mechanisms by which they function.

2.3 A Holistic and Multidisciplinary Approach

In the psychology and sociology literature, arguments are presented on the role of positive incentives in persuading economic actors that they can improve their economic situation by behaving in a particular way (Anderson & Moore, 2009). For example, research in behavioral

PART I: Theoretical Framework

economics demonstrates that using incentives, rewards, and sanctions, can channel human behavior towards particular options (Bauer & van Eeten, 2009). More generally, this literature identifies human behavior as the weakest link in the cybersecurity chain (Ghernaouti, 2013). In these models, positive incentives offer the agent a Pareto-superior state vis-a-vis the current state, at the cost of behavioral compliance. When applied to SIS, these models suggest that investors will share information only if they expect that the particular incentives provided will enable them to reduce their individual investment in cybersecurity (Anderson, Moore, Nagaraja, & Ozment, 2007). Therefore, for our overarching theoretical mechanism, we propose that, for a first step, incentives “work” by changing investors’ expectations. These changed expectations then trigger individual actions that result in SIS. We primarily view both the frequency and intensity of SIS as functions of the change in agents’ expectations. It is the change that is the phenomenon of interest, rather than the particular incentive that induces it. In practice, a variety of incentives could be used to change expectations, and these are likely to be context-specific to particular countries, political and economic systems, and cultures. The current study differs from previous research in this domain by being grounded in empirical observations from an Information Sharing and Analysis Centre (ISAC)⁵. Our findings constitute an evidence base and an important contribution to the new fast-growing field of the “economics of cybersecurity”, and they are generalizable to other jurisdictions. Most importantly, our results will support the design of the next generation of ISACs, namely Information Sharing and Analysis Organizations (ISAOs),⁶ in which incentives and voluntary SIS will play a key role (PricewaterhouseCoopers (PwC), 2016). Fusion centers⁷ and the emerging threat intelligence platform (TPI) technology⁸ might also benefit from our findings, by providing the right incentives to their members to share more real-time threat data.

⁵ An ISAC is generally a non-profit organization that provides a platform for SIS, between the government and CIs.

⁶ Unlike ISACs, ISAOs are not directly tied to CIs and offer a flexible and voluntary approach for SIS.

⁷ A fusion center is an information sharing center designed to promote information sharing between different agencies.

⁸ The TPI technology helps organizations to analyze and aggregate real-time threat data to support defensive actions.

2.4 A Model Linking Incentives, Behavior, and SIS

Previous research suggests that four expectations are particularly relevant to the human interactions involved in sharing: reciprocity, value, institutional, and reputation (ENISA, 2010). We designed a two-stage SIS model. In the first step, incentives are provided to change the expectations of the agents. In the second step, these changed expectations trigger actions that result in an increase in SIS (Fig.1).

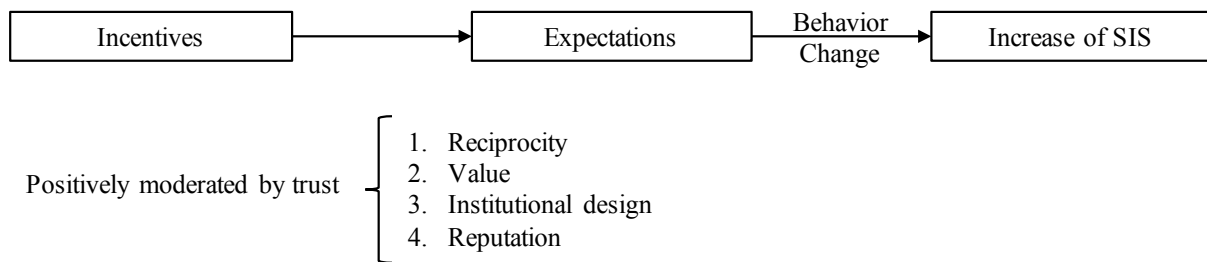


Figure 1: Design of a SIS Model

In summary, our model describes how incentives change expectations hence modifies the behavior of actors in order to improve voluntary SIS. We define frequency by the number of shared transactions between participants, and intensity by the depth of SIS in one single transaction. We further propose that the relationship between each of these effects and SIS is positively influenced by the degree of trust between individual agents.

2.5 Reciprocity Expectation

The extent to which human agents will engage in voluntary SIS depends on their expectations of reciprocity or recompense for the information they share (Xiong & Liu, 2004). For example, peer-to-peer (P2P) networks often confront the problem of free-riders (so-called “leechers”), because most participants would prefer to avoid seeding while enjoying the benefits of the network. As a result, most P2P networks either remove the free-riders or to force them to contribute by making seeding mandatory. Open-source studies have shown that, in the absence of an expectation of reciprocity, the benefits that a P2P network can provide are unlikely to be realized (von Hippel & von Krogh, 2003). Reciprocity can be self-reinforcing, because participants will share more when provided with an incentive that ensures reciprocity. Hence,

Proposition 1

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

Proposition 2

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

2.6 Value Expectation

Previous studies have identified the value of the information obtained as a result of sharing as an important precursor to SIS (ENISA, 2011). SIS and cooperation between industry peers can improve the relevance, quality, and value of information, because the actors often face similar cyberthreats. Collective intelligence and crowdsourcing studies show that organizations working together have greater threat awareness. SIS can also place extra burdens on the participants if they lack the resources to understand and analyze the security information that is shared with them. Therefore, each investor is expected to conduct a cost-benefit analysis before deciding whether or not to engage in SIS. The benefits are likely to increase as the value of the information increases; ideally, an investor should conclude that the benefits of the security information received outweigh the costs of the security information shared. Cost saving is generally the most direct and visible benefit of SIS to the participants. This makes the cost argument both subordinate to and linked with the value argument. Therefore, we make the following propositions:

Proposition 3

The frequency of SIS will increase to the extent that investors expect an increase in the value of the information they hold.

Proposition 4

The intensity of SIS will increase to the extent that investors expect an increase in the value of the information they hold.

2.7 Institutional Expectation

There is a consensus in the literature that the management and institutional design of an ISAC is key to building trust and facilitating effective SIS (Suter, 2012). A poorly designed ISAC can deter agents from joining, thus reducing the probability of an increase in SIS. Previous research identifies three elements that are key to an optimal structure: (1) leadership, (2) processing and labelling of shared information, and (3) secure storage and access to shared data (ENISA, 2016). A clear taxonomy is needed to create a common vocabulary and culture for participants. Next, minimal standards have to be implemented by the ISAC to organize the formation of the information that is shared. The central challenge in ISAC management is to create a core of quality participants, in order to encourage more quality participants to join and to avoid the introduction of free-riders (ENISA, 2009). Non-participants should perceive themselves to be missing access to important information. If the membership is too large, it is difficult to create relationships of trust; whereas if the membership is too small, the amount of shared data will be insufficiently attractive. A sound institutional design should result in a stable membership. Participants might be reluctant to engage in SIS activities if inappropriate actors are permitted to become members of the ISAC. It is essential that the platform applies up-to-date security standards, in order to provide a safe forum. Indeed, the high value of an ISAC database makes it a high-value target (HVT) for hackers. Therefore, we make the following propositions:

Proposition 5

The frequency of SIS will increase to the extent that investors trust the institutional management.

Proposition 6

The intensity of SIS will increase to the extent that investors trust the institutional management.

2.8 Reputation Expectation

Agents will evaluate the potential reputational benefits of their SIS activities, as well as the potential reputational risks. Participants are often reluctant to engage in SIS activities, fearing that the activities might be damaging to the reputation of the organization. Reputation is related to customer trust, the protection of customer data, and the quality of service offered (Gordon, Loeb, & Sohail, 2010). Common fears include information leaks and the use, by competitors,

PART I: Theoretical Framework

of critical information to damage the reputation of the client. Studies have shown that disclosing information on a cyberattack can reduce consumer trust, strongly affecting the market value of the company (Campbell, Gordon, Loeb, & Zhou, 2003). As a result, agents have a keen interest in protecting their reputation. However, some participants might see SIS as a means to cultivating their reputation as good corporate citizens; associating with government agencies can also enhance the reputation of participants. The fear of being publicly accused of being a free-rider might also provide an incentive to participate in SIS. As reputations are strongly moderated by trust, this can mitigate the reputational problem. If agents know and trust each other they will not exploit any revealed weaknesses. Therefore, we make the following propositions:

Proposition 7

The frequency of SIS will increase to the extent that investors expect an improvement in reputation.

Proposition 8

The intensity of SIS will increase to the extent that investors expect an improvement in reputation.

2.9 The Moderating Role of Trust

The psychology literature suggests that knowledge-based trust might be the most significant in the context of SIS (Hämmerli, Raaum, & Franceschetti, 2013). Our assumption is that trust is a necessary condition for SIS, but not a sufficient one. As a result, the four main effects noted above will each be positively moderated by trust, hence strengthened when trust between agents is present. In many jurisdictions, government and private industry work together to create ISACs that are neutral and anonymous facilitators of social networks, thereby supporting the emergence of trusted relationships between cybersecurity investors, the private sector, and the government (Fernández Vázquez, Acosta, Spirito, Brown, & Reid, 2012). The existence of networks of collaboration and trust in other fields of activity can be used for SIS. For instance, pre-existing relationships between the private and the public sector can be used to build trust (Dunn Cavelty, 2014). Hence,

Proposition 9

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

Proposition 10

The relationship between value expectations and SIS will positively reflect the degree of trust between the sharing agents.

Proposition 11

The relationship between institutional expectations and SIS will positively reflect the degree of trust between the sharing agents.

Proposition 12

The relationship between reputational expectations and SIS will positively reflect the degree of trust between the sharing agents.

3. Application of the Proposed Model to Critical Infrastructure Protection

Today, CIP is more of an economic policy than a technology policy. The capacity of a modern society to preserve the conditions of its existence is intimately linked to the proper operation of its CIs. Cybersecurity concerns are the main challenge faced by the operators of this infrastructure, not least because of the high degree of interconnection (Anderson & Fuloria, 2010). This raises the threat of a *cyber subprime scenario*, i.e. a cascading series of failures from an attack on a single point in the infrastructure.⁹ As a consequence, most OECD countries have adopted national CIP programs to increase preparedness and improve their response capabilities to critical cyber incidents. To illustrate our theoretical framework, we present a case study showing how SIS can improve cybersecurity in the financial sector, a particularly sensitive area of CIP. The national financial infrastructure of Switzerland is highly important for national security, given the presence of at least five systemically strategic (too big to fail) banks. For a potential attacker, the Swiss financial system is an attractive target that can be attacked at very little cost.

⁹ The interconnected 2008 global financial crisis bears several resemblances to a major cyber “risk nexus” scenario.

3.1 The Swiss Reporting and Analysis Centre for Information Security

The Swiss Reporting and Analysis Centre for Information Security (MELANI) is a forum in which participants from the information security technology sector and CI providers share security information. The Centre is organized as a PPP between the federal government and private industry. It operates an ISAC (MELANI-Net that brings together over 150 CI providers from all sectors in Switzerland (Dunn Cavelty, 2014). To conduct this case study, we were granted access to the MELANI-Net quantitative log-file, as well as to the qualitative results of a survey conducted in 2016.¹⁰ Each of the four main effects and the moderating role of trust are illustrated with real examples.

3.2 Reciprocity Expectation

Only half of the MELANI-Net participants are active on the platform. A first analysis of the logfile suggested the existence of a free-rider problem. The main reason for this seems to be that some participants have no information to share, or they believe that the information they hold is insufficiently relevant to justify sharing. This phenomenon might be unrelated to the provision of incentives or the free-rider problem. However, it is possible that participants use these arguments merely as an excuse to justify free riding. The most promising reciprocity incentive appears to be the sharing of best practices, i.e. the response to a cyber incident. The fear of free-riders seems to be an important barrier to engaging in SIS.

3.3 Value Expectation

Participants appreciate the aggregated information received from MELANI, which is perceived as the main added-value of SIS. MELANI recently developed an information radar that provides CIs with an aggregated overview of the cyber-threat landscape in Switzerland. This is the product that is most appreciated by the financial sector. It gives CI providers a strong incentive to engage in a wider range of SIS activities, because in the future this could provide the basis for an SIS-Early Warning System (EWS) that controls and mitigates the cascade effect

¹⁰ This internal survey does not conform to common practice in psychometrics. We could only use it to inspire future research and confirm the presence of a free-riding problem in our case study.

PART I: Theoretical Framework

(Alcaraz, Balastegui, & Lopez, 2010). Participants reduce their costs through participation in SIS by benefiting from free MELANI consulting, IT support, and access to exclusive and timely cyber-threat intelligence (CTI) from the government.

3.4 Institutional Expectation

Most participants believe MELANI to be well-managed. The financial sector regards the MELANI staff as reliable and credible. Switzerland offers a conducive environment for SIS, with a low corruption rate and strong trust between the government, the citizens, and the industry. More than half of the participants have been members of the platform for more than five years. In the financial sector, a clear taxonomy has been established and most participants believe that the platform has the right number of participants. However, impediments remain to the development of effective SIS, including legal issues that deter CI providers from engaging in SIS activities. These include antitrust laws, patent protection, national security laws, and data-privacy laws, such as the Swiss banking-secrecy law. This law makes sharing of client-related data problematic, especially in cross-border or multi-jurisdictional contexts.

3.5 Reputation Expectation

After the public disclosure of the Heartbleed security bug in 2014, the affected banks experienced a decrease in their market-share value. This event confirms that a security-information leak can seriously damage the reputation of participants. Therefore, participants need to trust the ISAC with their reputation and anonymity preservation. As a result, the shared data has to be properly sanitized, in order to make sure that competitors can never use the shared information to damage another participant's reputation.

3.6 Setting the Optimal Size of SIS Circles

The Swiss tradition of banking secrecy and non-cooperation in the financial sector is an established social norm that could act as an impediment to voluntary SIS. Surprisingly, the financial sector has the highest level of engagement in SIS activities and was the sector most willing to join MELANI at its foundation a decade ago. Over time, this has enabled the sector to build trust, based on already existing relationships and the regular face-to-face meetings at

PART I: Theoretical Framework

workshops or roundtables that take place between the MELANI staff and their contacts in the banks. Hence, the financial sector participants are satisfied, in general, with the service received and appreciate the importance of MELANI for their own activities, the financial sector overall, and Switzerland's national security.

The participants' willingness to engage in SIS activities reflects the levels of trust in three circles: the MELANI staff, the industry circle, and all of participants (Fig. 2). For each SIS transaction, participants can choose with which circle they want to engage. These established relationships enable the four effects discussed above to be moderated by trust. As a result, the trust that has been established over a long period in this sector positively influences our four expectations: reciprocity, value, institutional design, and reputation.

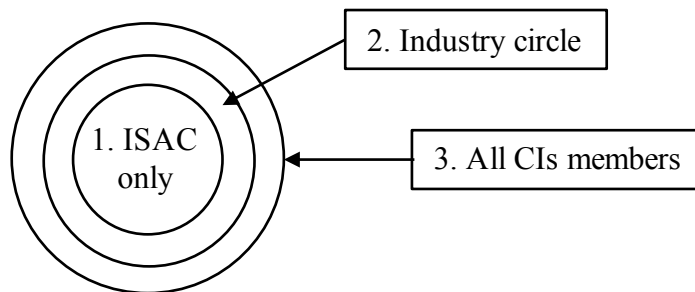


Figure 2: MELANI Trust-Circles (Adapted from the Onion Model)

4. Discussion

Unlike in other OECD countries, CIs in Switzerland are not usually in competition, because most are state owned, especially those in the energy sector. Privately owned CI providers might have incentives and barriers different than state-owned providers. This would require further research and investigation. Some CI operators sometimes fail to engage in SIS activities simply because they have no information to share, whereas other CIs share security information because they have security incidents to report. This phenomenon is unrelated to the provision of incentives or the free-rider problem. Another possible bias that should be considered is the many SIS activities that take place outside MELANI-Net, for instance bilaterally, in peer-to-peer groups, or through industry-based ISACs. This is typically the case in the financial industry, with its successfully established FS-ISAC (Liu, Zafar, & Au, 2014). Security solution vendors recently created the Cyber Threat Alliance, in order to engage in mutual SIS. A further example is the newly created Industrial Control System ISAC for threat intelligence sharing

among nations.¹¹ As a result, we were unable to observe the SIS activities that take place outside of MELANI-Net.

5. Concluding Comments and Next Steps

We provided a first blueprint for an innovative incentive-based SIS model, thus closing an important gap in the literature. This model can work as a complement to or an extension of the Gordon-Loeb model. Other economic and social incentives could be used to extend the expectations indicators in our model. The design and analysis of such alternative indicators is a task for future research. For instance, the criticality of a CI operator could be linked to the frequency and intensity of SIS. Indeed, systemic risks (too big to fail) and the large externalities associated with high criticality might provide an incentive to engage in extended SIS activities (Leu & Peter, 2016). This part is a conceptual work that is developed in Parts II and III. These developments, which focus on the generation of theories, are complemented by empirical propositions, testing, and policy recommendations at national and international levels. We hope that this study will inspire other researchers to extend and contribute to our model.

¹¹ The purpose of this platform is to bring together CI stakeholders in order to improve SIS at the international level.

6. References

- Alcaraz, C., Balastegui, A., & Lopez, J. (2010). Early Warning System for Cascading Effect Control in Energy Control Systems. In *Critical Information Infrastructures Security* (pp. 55–66). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-21694-7_5
- Anderson, R., & Fuloria, S. (2010). Security Economics and Critical National Infrastructure. In *Economics of Information Security and Privacy* (pp. 55–66). Springer, Boston, MA. https://doi.org/10.1007/978-1-4419-6967-5_4
- Anderson, R., & Moore, T. (2009). Information security: where computer science, economics and psychology meet. *Philosophical Transactions of the Royal Society of London A: Mathematical, Physical and Engineering Sciences*, 367(1898), 2717–2727. <https://doi.org/10.1098/rsta.2009.0027>
- Anderson, R., Moore, T., Nagaraja, S., & Ozment, A. (2007). Incentives and Information Security. In N. Nisan, R. Tim, E. Tardos, & V. Vazirani (Eds.), *Algorithmic Game Theory* (pp. 633–650). Cambridge: Cambridge University Press. <https://doi.org/10.1017/CBO9780511800481.027>
- Aviram, A., & Tor, A. (2003). Overcoming Impediments to Information Sharing. *Alabama Law Review*, 55(2), 231–280.
- Bauer, J., & van Eeten, M. (2009). Cybersecurity: Stakeholder incentives, externalities, and policy options. *Telecommunications Policy*, 33(10–11), 706–719. <https://doi.org/10.1016/j.telpol.2009.09.001>
- Campbell, K., Gordon, L. A., Loeb, M. P., & Zhou, L. (2003). The economic cost of publicly announced information security breaches: empirical evidence from the stock market. *Journal of Computer Security*, 11(3), 431–448. <https://doi.org/10.3233/JCS-2003-11308>
- de Bruijne, M., & van Eeten, M. (2007). Systems that Should Have Failed: Critical Infrastructure Protection in an Institutionally Fragmented Environment. *Journal of Contingencies and Crisis Management*, 15(1), 18–29. <https://doi.org/10.1111/j.1468-5973.2007.00501.x>
- Dunn Cavelty, M. (2014). *Cybersecurity in Switzerland*. Cham: Springer International Publishing. <https://doi.org/10.1007/978-3-319-10620-5>
- Dunn-Cavelty, M., & Suter, M. (2009). Public–Private Partnerships are no silver bullet: An expanded governance model for Critical Infrastructure Protection. *International Journal of Critical Infrastructure Protection*, 2(4), 179–187. <https://doi.org/10.1016/j.ijcip.2009.08.006>
- ENISA. (2009). *Good Practice Guide on Information Sharing* (White report). Heraklion: European Union Agency for Network and Information Security. Retrieved from <https://www.enisa.europa.eu/publications/good-practice-guide>
- ENISA. (2010). *Incentives and Barriers to Information Sharing* (White report). Heraklion: European Union Agency for Network and Information Security. Retrieved from <https://www.enisa.europa.eu/publications/incentives-and-barriers-to-information-sharing>
- ENISA. (2011). *Economic Efficiency of Security Breach Notification* (White report).

PART I: Theoretical Framework

Heraklion: European Union Agency for Network and Information Security. Retrieved from <https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/files/economic-efficiency-of-security-breach-notification/view>

ENISA. (2015). *Cyber Security Information Sharing: An Overview of Regulatory and Non-regulatory Approaches* (White report). Heraklion: European Union Agency for Network and Information Security. Retrieved from <https://www.enisa.europa.eu/activities/cert/support/information-sharing/cybersecurity-information-sharing>

ENISA. (2016). *Information sharing and common taxonomies between CSIRTs and Law Enforcement* (White report). Heraklion: European Union Agency for Network and Information Security. Retrieved from <https://www.enisa.europa.eu/publications/information-sharing-and-common-taxonomies-between-csirts-and-law-enforcement>

Fernández Vázquez, D., Acosta, O. P., Spirito, C., Brown, S., & Reid, E. (2012). Conceptual framework for cyber defense information sharing within trust relationships. In *2012 4th International Conference on Cyber Conflict (CYCON 2012)* (pp. 1–17).

Gal-Or, E., & Ghose, A. (2005). The Economic Incentives for Sharing Security Information. *Information Systems Research*, *16*(2), 186–208. <https://doi.org/10.1287/isre.1050.0053>

Ghernaouti, S. (2013). *Cyber Power: Crime, Conflict and Security in Cyberspace* (EPFL Press). Lausanne.

Gordon, L. A., Loeb, M. P., & Lucyshyn, W. (2003). Sharing information on computer systems security: An economic analysis. *Journal of Accounting and Public Policy*, *22*(6), 461–485. <https://doi.org/10.1016/j.jaccpubpol.2003.09.001>

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Sohail, T. (2006). The impact of the Sarbanes-Oxley Act on the corporate disclosures of information security activities. *Journal of Accounting and Public Policy*, *25*(5), 503–530. <https://doi.org/10.1016/j.jaccpubpol.2006.07.005>

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Zhou, L. (2015a). Externalities and the Magnitude of Cyber Security Underinvestment by Private Sector Firms: A Modification of the Gordon-Loeb Model. *Journal of Information Security*, *06*(01), 24–30. <https://doi.org/10.4236/jis.2015.61003>

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Zhou, L. (2015b). Increasing cybersecurity investments in private sector firms. *Journal of Cybersecurity*, *1*(1), 3–17. <https://doi.org/10.1093/cybsec/tyv011>

Gordon, L. A., Loeb, M. P., & Sohail, T. (2010). Market Value of Voluntary Disclosures Concerning Information Security. *Management Information Systems Quarterly*, *34*(3), 567–594. <https://doi.org/10.2307/25750692>

Hämmerli, B., & Grudzien, W. (2015). *Voluntary Information Sharing* (White report). European Union Agency for Network and Information Security. Retrieved from https://resilience.enisa.europa.eu/nis-platform/shared-documents/5th-plenary-meeting/chapter-3-wg2_final-for-discussion-may-27-2015/view

PART I: Theoretical Framework

- Hämmerli, B., Raaum, M., & Franceschetti, G. (2013). Trust Networks among Human Beings: Analysis, Modeling, and Recommendations. In F. Flammini, R. Setola, & G. Franceschetti (Eds.), *Effective Surveillance for Homeland Security* (Vols. 1–0, pp. 21–50). New York: Chapman and Hall/CRC. Retrieved from <https://www.taylorfrancis.com/books/e/9781439883259/chapters/10.1201%2Fb14839-8>
- Harrison, K., & White, G. (2012). Information sharing requirements and framework needed for community cyber incident detection and response. In *2012 IEEE Conference on Technologies for Homeland Security (HST)* (pp. 463–469). IEEE. <https://doi.org/10.1109/THS.2012.6459893>
- Hausken, K. (2007). Information sharing among firms and cyber attacks. *Journal of Accounting and Public Policy*, 26(6), 639–688. <https://doi.org/10.1016/j.jaccpubpol.2007.10.001>
- Laube, S., & Böhme, R. (2016). The economics of mandatory security breach reporting to authorities. *Journal of Cybersecurity*, 2(1), 29–41. <https://doi.org/10.1093/cybsec/tyw002>
- Leu, P. O., & Peter, D. (2016). Case Study: Information Flow Resilience of a Retail Company with Regard to the Electricity Scenarios of the Sicherheitsverbandsübung Schweiz (Swiss Security Network Exercise) SVU 2014. In E. Rome, M. Theocharidou, & S. Wolthusen (Eds.), *Critical Information Infrastructures Security* (pp. 159–170). Springer, Cham. https://doi.org/10.1007/978-3-319-33331-1_13
- Liu, C. Z., Zafar, H., & Au, Y. A. (2014). Rethinking FS-ISAC: An IT Security Information Sharing Network Model for the Financial Services Sector. *Communications of the Association for Information Systems*, 34(1), 15–36.
- Moran, T., & Moore, T. (2010). The Phish-Market Protocol: Securely Sharing Attack Data between Competitors. In R. Sion (Ed.), *Financial Cryptography and Data Security* (pp. 222–237). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-14577-3_18
- PricewaterhouseCoopers (PwC). (2016). *Information Sharing and Analysis Organizations: Putting theory into practice* (White report). Retrieved from <https://www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/pwc-information-sharing-and-analysis-organizations.pdf>
- Suter, M. (2012). *The governance of cybersecurity: an analysis of public-private partnerships in a new field of security policy*. ETH, Zurich.
- von Hippel, E., & von Krogh, G. (2003). Open Source Software and the “Private-Collective” Innovation Model: Issues for Organization Science. *Organization Science*, 14(2), 209–223. <https://doi.org/10.1287/orsc.14.2.209.14992>
- Weiss, E. (2015). *Legislation to Facilitate Cybersecurity Information Sharing: Economic Analysis* (CRS Report). Congressional Research Service. Retrieved from <https://horizon.hozint.com/2014/12/crs-legislation-to-facilitate-cybersecurity-information-sharing-economic-analysis/>
- Xiong, L., & Liu, L. (2004). PeerTrust: supporting reputation-based trust for peer-to-peer electronic communities. *IEEE Transactions on Knowledge and Data Engineering*, 16(7), 843–857. <https://doi.org/10.1109/TKDE.2004.1318566>

PART II: Empirical Analysis

“Any security technology whose effectiveness can't be empirically determined is indistinguishable from blind luck.”

- *Dan Geer's Law*

To Share or not to Share: A Behavioral Perspective on Human Participation in Security Information Sharing

*Published in the proceedings of the 17th Annual Workshop on the Economics of Information Security
Innsbruck, Austria, June 18-19, 2018*

*Revised and resubmitted to the Journal of Cybersecurity on the 28th of February 2019
Publisher: Oxford University Press*

Abstract

Security information sharing (SIS) is an activity whereby individuals exchange information that is relevant to analyze or prevent cybersecurity incidents. However, despite technological advances and increased regulatory pressure, human individuals still seem reluctant to share security information. Few contributions have addressed this research gap to date. Adopting an interdisciplinary approach, our study proposes a behavioral framework that theorizes how and why human behavior and SIS may be associated. We use psychometric methods to test these associations, analyzing a unique sample of 262 human Information Sharing and Analysis Centre (ISAC) members who share real security information. We also provide a dual empirical operationalization of SIS by introducing the measures of SIS frequency and intensity. We find significant associations between human behavior and SIS. Thus, the study contributes to clarifying why SIS, while beneficial, is underutilized by pointing to the pivotal role of human behavior for economic outcomes. It therefore adds to the growing field of the economics of information security. By the same token, it informs managers and regulators about the significance of human behavior as they propagate goal alignment and shape institutions. Finally, the study defines a broad agenda for future research on SIS.

Key words: security information sharing; psychometrics; economics of information security; behavioral economics; behavioral psychology.

1. Introduction

Security information sharing (SIS) is an activity whereby individuals exchange information that is relevant to analyze or prevent cybersecurity incidents. Such information includes, but is not limited to, the identification of information system vulnerabilities, phishing attempts, malware, and data breaches, as well as results of intelligence analysis, best practices, early warnings, expert advice and general insights (Luijff and Klaver, 2015).

Prior research has proposed that SIS makes every unit of security investment more effective, such that individuals can reduce investments dedicated to generate cybersecurity in their organization. As a result of these individual improvements, total welfare is also likely to increase (Gordon et al., 2003; Gal-Or and Ghose, 2005). Hence, SIS likely contributes to strengthening the cybersecurity of firms, critical infrastructures, government, and society (Gordon et al., 2010, 2015a, 2015b; Hausken, 2015; Böhme, 2016).

However, these theoretical expectations hardly seem to materialize. Recent contributions have noted that SIS is at suboptimal levels, implying negative consequences for the cybersecurity of organizations and society (Böhme, 2016). Game-theoretic simulation suggests that individuals may free-ride on the information provided by others while not sharing any information themselves (Gordon et al., 2003; Hausken, 2007). Researchers and international organizations have been warning for years that human individuals seem reluctant to share security information, although the technical infrastructure for information exchange does exist (Campbell et al., 2003; ENISA, 2010, 2016; Naghizadeh and Liu, 2016). In an attempt to alleviate this problem, legislators and regulators have attempted to make SIS mandatory.¹ However, reviews suggest that despite these attempts, individuals still seem reluctant share security information (Ghose and Hausken, 2006; Moran and Moore, 2010; Bisogni, 2015; Weiss, 2015). They may even ‘game’ the system in an attempt to circumvent regulation (Anderson and Fuloria, 2010; Moore, 2010; Moran and Moore, 2010).

All these findings imply that human behavior may be significantly associated with the extent to which SIS occurs (if at all). It is therefore not surprising to see recent work emphasizing that the study of human behavior is key to the understanding of SIS (Böhme,

¹ For example, the USA created the 2002 Sarbanes-Oxley Act and the 2015 Cybersecurity Information Sharing Act (CISA). The Health Insurance Portability and Accountability Act (HIPAA) requires organizations to report breaches of protected health information (PHI) to the U. S. Department of Health and Human Services (HHS). In December 2015, the European Parliament and Council agreed on the first EU-wide legislation on cybersecurity by proposing the EU Network and Information Security (NIS) Directive.

2016). More specifically, this work predicts that SIS can only be imperfectly understood unless the human motivation to (not) participate in SIS is studied (Harrison and White, 2012; Laube and Böhme, 2016; Vakili et al., 2017).

However, few contributions have addressed this research gap to date. Since Laube and Böhme (2017) have provided an excellent account of the SIS literature, we refrain from replicating this account here. We rather point to the fact that this account shows that very few empirical studies on non-public SIS exist. These few studies concentrate on analyzing incident counts and aggregate data, but they do not study human behavior at the individual level of analysis (see Laube and Böhme, 2017: 28 for a tabulated overview).

Our study intends to address this gap by proposing how and why human behavior and SIS may be associated, and by providing an empirical test of this association. As cybersecurity problems are unlikely to be resolved by information systems theory alone, we adopt an interdisciplinary approach as recommended by Anderson and Moore (2006). Recently, interdisciplinary studies were productive in showing the extent to which human behavior is associated with knowledge sharing (Yan et al., 2016; Safa and von Solms, 2016).

We build a theoretical framework anchored in behavioral theory, arguing that SIS is associated with human behavior. We use psychometric methods to test these associations, analyzing a unique sample of 262 human ISAC members who share real security information. The remainder of this paper is structured as follows. Section 2 develops the behavioral framework and deduces testable hypotheses from this framework. Section 3 details the sampling context, measures, and empirical. The results are explained in section 4. Section 5 discusses both the theoretical, empirical and practical contributions our study makes and points to some limitations of our approach that open up paths for future research.

2. Theoretical framework and hypotheses

Behavioral research relativized some of the strong formal assumptions that neoclassical economics had ascribed to human behavior, particularly those of rationality, perfect information, and selfish utility maximization (*homo oeconomicus*). By contrast, it showed that human beings have bounded instead of perfect rationality. They often violate social expectations, have limited information processing capacity, use heuristics when making decisions, are affected by emotion while doing so, and retaliate even if the cost of retaliation exceeds its benefits (Simon, 1976; Kahneman and Tversky, 1979; Fehr and Gächter, 2002; Bazerman, 2005; DellaVigna, 2009).

PART II: Empirical Analysis

Moreover, humans do not necessarily maximize higher-level (i.e., organizational, societal) goals, even if it would be economically rational for them to do so. Theoretical work on SIS has suggested early that individual and organizational interests may not always be aligned and that the individual is not necessarily an indifferent agent (Gal-Or and Ghose, 2004). Goal-framing theory suggests that individual goals may not necessarily be congruent with higher-level goal frames, implying that the individual can defect from organizational maximization goals (Lindenberg and Foss, 2011). Particularly in the case of collective action, the individual may behave in ways that is not conducive to the overall group goal (Olson, 1965; Oliver, 1980). For the context of SIS, this research implies that individually, humans might not necessarily participate in SIS although it would be optimal to do so for society as a whole.

Particularly, human exchange relationships are not necessarily characterized by rational economic optimization, but instead by human expectations about fairness, reciprocity, and trust (Malhotra, 2004; Fehr and Gächter, 2000, 2002; Fehr and Schmidt, 1999). Therefore, the argument can be made that SIS may be associated with human behavior. Indeed, prior research argues that the understanding of SIS requires an analysis of what behavior may motivate humans to participate in SIS, and what may deter them from doing so (Aviram and Tor, 2003; Bauer and van Eeten, 2009).

Human behavior is the result of human motivation, intention and volition. It manifests itself in goal-directed (i.e., nonrandom) and observable actions (Watzlawick et al., 2011; Smith and Winterhalder, 2017; Tomasello et al., 2005). Sharing information implies human action from at least the side of the individual who shares. Moreover, SIS constitutes an economic transaction by which knowledge resources are *shared*, rather than acquired (Bock et al., 2005). Hence, SIS differs from discrete arm's length transactions whereby a single individual simply trades financial means for access to information. Instead, SIS is characterized by continued social interaction among many individuals who mutually exchange information assets (Yan et al., 2016).

Therefore, humans are unlikely to *randomly* participate in SIS, such that SIS does not occur 'naturally'. Hence, theorizing is required regarding how and why human behavior may be associated with SIS. Applying prior behavioral research to our research context, we develop testable hypotheses about five salient constructs which may be associated with SIS. In all of these hypotheses, our focal individual is an indifferent human individual who, independently of the motives of other individuals, ponders whether or not to participate in SIS. We believe

PART II: Empirical Analysis

this perspective is conservative and conducive to empirical analysis since it neither requires assumptions about the behavior of other individuals nor a dyadic research setting.

2.1 Attitude

Behavioral theory suggests that attitudes have a directive influence on human behavior (Ajzen, 1996). Attitude is a psychological tendency that is expressed by evaluating a particular entity with some degree of favor or disfavor (Eagly and Chaiken, 1993). Hence, an individual's favorable or unfavorable attitude towards a particular behavior predicts the extent to which this behavior actually occurs (Ajzen and Fishbein, 1980; Ajzen and Madden, 1986).

Much empirical work has confirmed and detailed this attitude-behavior link, particularly in the context of information systems adoption and intention to use (see Belletier et al., 2018 and Kroenung and Eckhard, 2015 for extensive literature reviews). More specifically, Bock et al. (2005) find that this attitude-behavior link influences individuals' intention to share knowledge.

Drawing on prior empirical work in behavioral psychology, Safa and von Solms (2016) also found support for the hypothesis that an affirmative attitude towards knowledge sharing positively influences participation rates. Descriptive work has conjectured (though not tested or confirmed) that individual attitudes about the meaningfulness of SIS might be associated with actual participation in SIS (ENISA, 2010). Therefore, if the focal individual has a positive attitude towards SIS, s/he should be more likely to participate in SIS. Therefore,

***H1:** SIS is positively associated with the extent to which the focal individual has a positive attitude towards SIS.*

2.2 Reciprocity

Behavioral theory suggests that human behavior is characterized by inequity aversion (Fehr and Schmidt, 1999). As they socially interact with others, humans expect to receive equitable compensation whenever they voluntarily give something to others, and they punish those unwilling to give something in return (Brosnan and de Waal, 2003; Tricomi et al., 2010). Hence, when humans are treated in a particular way, they reciprocate, i.e., they respond likewise (Fehr

PART II: Empirical Analysis

and Gächter, 2000). As a result, reciprocity is a shared behavioral norm among human beings that governs their social cooperation (Gouldner, 1960; Fehr and Gintis, 2007).

Economic exchange relationships are therefore shaped by the reciprocity expectations of the participants involved in this exchange (Kolm and Ythier, 2006). In such relationships, reciprocity is a dominant strategy that is conducive to a socially efficient distribution of resources (Andreoni, 1995; Bolton and Ockenfels, 2000). Therefore, the extent to which the focal individual participates in information exchange is likely associated with that individual's expectation that his/her efforts are reciprocated.

For example, reciprocal fairness is an important variable in the design of peer selection algorithms in peer-to-peer networks. By integrating reciprocal response patterns such as 'tit-for-tat', operators can optimize peer-to-peer traffic (Wang et al., 2011). The value of a unit of security information is proportional to the incremental security enhancement that this unit is supposed to provide to the recipient (Bodin et al., 2018; Gordon et al., 2016). Hence, whenever the focal individual shares such information units, it creates value for the counterparty. By the above arguments, the focal individual likely refuses to participate in future exchanges unless such value creation is reciprocated by the counterparty.

On the one hand, the focal individual may expect that information sharing is reciprocated by 'hard rewards', i.e. in monetary terms, by a higher status inside the ISAC or his or her own organization, or in terms of career prospects (transactional reciprocity). On the other hand, the focal individual may also expect that whenever s/he shares a unit of information, s/he receives useful information in return, such that a continuous social interaction that is beneficial to both parties emerges (social reciprocity). Prior research suggests that both these types of reciprocity are associated with information exchange patterns between individuals (Kwahk and Park, 2016; Siegrist et al., 2004; Paese and Gilin, 2000). Therefore,

H2a: *SIS is positively associated with the extent to which the focal individual expects his or her information sharing to be transactionally reciprocated.*

H2b: *SIS is positively associated with the extent to which the focal individual expects his or her information sharing to be socially reciprocated.*

2.3 Executional Cost

Behavioral theory suggests that humans are loss-averse, i.e. they attempt to avoid economic losses more than they attempt to realize economic benefits. Much experimental research has confirmed this tendency (Kahneman and Tversky, 1979; Tversky & Kahneman, 1991, 1992; Tom et al., 2007).

An economic exchange relationship can be fraught with significant transaction cost, i.e. the time, material, and financial resources that the focal individual must commit before an exchange is made (Williamson, 1981). Hence, if SIS is associated with high transaction costs for participation, the focal individual is likely to avoid the necessary resource commitments to finance this cost. For example, Yan et al. (2016) argue that when knowledge contribution requires significant time, sharing tends to be inhibited. Consistent with their conceptualization, we term such transaction costs ‘executional cost’.

As a result, in the presence of high executional cost, the focal individual likely adapts his or her behavior in an attempt to avoid these costs. For instance, if the focal individual learns that in a given ISAC environment, SIS is taking too much time, is too laborious, or requires too much effort, the individual likely reduces or terminates participation in SIS (Luijff and Klaver, 2015). For example, an abundance of procedural rules that govern the processing and labelling of shared information and the secure storage and access to shared data likely stalls information sharing activity (ENISA, 2016). Thus, high executional cost likely dissuades the focal individual from participating in SIS. Therefore,

H3: SIS is negatively associated with the extent to which the focal individual expects information sharing to be fraught with executional cost.

2.4 Reputation

Behavioral theory suggests that humans deeply care about being recognized and accepted by others (Baumeister and Leary, 1995; Bénabou and Tirole, 2006). Many philosophers have argued that the desire for social esteem fundamentally influences human behavior and, as a result, economic action (Brennan and Pettit, 2004).

Depending on the outcomes of particular social interactions with other individuals, the focal individual earns or loses social esteem. Hence, over time each individual builds a reputation, i.e. a socially transmitted assessment by which other individuals judge the focal

PART II: Empirical Analysis

individual's social esteem (Emler, 1990; McElreath, 2003). For example, academic researchers strive to increase the reputation of their department by publishing scholarly work (Keith and Babchuk, 1998). The desire to earn a reputation as a competent developer is a strong motivator for individuals to participate in open source software development although they receive no monetary compensation for the working hours they dedicate to this development (von Hippel and von Krogh, 2003).

When this reasoning is transferred to the context of SIS, the focal individual may be inclined to share information because s/he hopes to build or improve his or her reputation among the other participants of SIS. Prior research suggests that this desire constitutes an extrinsic motivation that may be associated with an individual's intention to share information (Chang and Chuang, 2011; Park et al., 2014), and intention is a precursor of behavior. Therefore,

***H4:** SIS is positively associated with the extent to which the focal individual expects information sharing to promote his or her reputation in the sharing community.*

2.5 Trust

Behavioral theory suggests that humans simplify complex decision-making by applying heuristics (Petty and Cacioppo, 1986; Tversky and Kahneman, 1992), particularly when they attempt to reduce the cost of information acquisition and valuation (Gabaix et al., 2006).

Whenever a focal individual is unable or unwilling to objectively evaluate information conveyed by other individuals, s/he likely resorts to heuristics to simplify the evaluation process (Chaiken, 1980). In the context of SIS, this implies that whenever the focal individual receives security information from another individual, s/he cannot necessarily be sure about the extent to which (if any) this information is valuable or useful. This assessment is associated with significant transaction cost, e.g. for due diligence procedures that attempt to value the information received. The individual may also lack technological competence and expertise, such that time-consuming discussions with experts are required for proper valuation. All in all, upon the receipt of a particular unit of information, the focal individual is faced with a complex valuation problem which s/he may seek to simplify by applying heuristics.

Trust is an implicit set of beliefs that the other party will behave in a reliable manner (Gefen et al., 2003). This set of beliefs is a particularly effective heuristic because it can reduce the transaction cost associated with this valuation. If the focal individual trusts the information

PART II: Empirical Analysis

received is useful and valuable, s/he can simplify evaluation procedures, and particularly so if the involved individuals interact in dense networks with agreed standards of behavior. Therefore, trust is a facilitator of economic organization and interaction (McEvily et al., 2003; Granovetter, 1985). For example, mutual trust among the participants of peer-to-peer networks can reduce transactional uncertainty (Xiong and Liu, 2004). Moreover, trust can mitigate information asymmetry by reducing transaction-specific risks (Ba and Pavlou, 2002). It is also a significant predictor of participation in virtual knowledge sharing communities (Ridings et al., 2002).

Such trust, in turn, is positively associated with knowledge sharing in both direct and indirect ways (Hsu et al., 2002), whereas distrust is an obstacle to knowledge sharing (Amayah, 2013). More specifically, trust is a facilitator in information security knowledge sharing behavior (Safa and von Solms, 2016). Thus, the extent to which the focal individual trusts the information s/he receives is valuable should be positively associated with his or her propensity to participate in SIS. Therefore,

***H5:** SIS is positively associated with the extent to which the focal individual trusts that the counterparty provides valuable information.*

2.6 Interaction Effects

By consequence, we suggest that trust negatively moderates the associations between attitude and reciprocity on the one hand and SIS on the other hand. We argued that trust is a facilitator of economic exchange. In other words, trust likely reduces the focal individual's perceived cost of engaging in SIS, in that s/he requires fewer or lesser alternative stimuli (Lindenberg and Foss, 2011). A neutral focal individual who has not participated in SIS before is unlikely to participate unless s/he has a positive attitude towards SIS. That individual must hence construct the meaningfulness of SIS *internally*, i.e. convince him- or herself that SIS is useful. By contrast, if the focal individual trusts that the information s/he receives will be useful, s/he uses the counterparty to *externally* confirm such meaningfulness of SIS. The process of the internal construction of the meaningfulness of SIS is therefore at least partially substituted by the external, trust-based affirmation of such meaningfulness. We would hence expect that the significance of the association between attitude and SIS decreases with the extent to which the focal individual trusts the information s/he receives will be useful.

PART II: Empirical Analysis

By the same token, since trust is a facilitator of economic exchange, it likely reduces the association between reciprocity and SIS. An indifferent focal individual cannot be completely sure about the behavior of the exchange counterparty, such that s/he requires continuous transactional or social reciprocity for SIS to perpetuate the exchange. In the absence of any trust that the information received is useful, SIS likely ends as soon as this reciprocity requirement is no longer met. By contrast, whenever the focal individual trusts that the information s/he receives will be useful, s/he has a motive to participate in SIS that is independent of such reciprocity concerns. Hence, trust is likely to act at least partially as a substitute for reciprocity, such that the focal individual should emphasize to a lesser extent that reciprocity will be required if s/he is expected to begin or perpetuate SIS. Therefore,

H6a-c: The extent to which the focal individual trusts that information received from the counterparty is effective negatively moderates the respective positive associations between attitude, transactional, and social reciprocity on the one hand and SIS on the other hand.

3. Methods

3.1 Sampling Context and Population

Our study focused on the 424 members of the closed user group of the Swiss national ISAC, the *Reporting and Analysis Centre for Information Assurance* (MELANI-Net). An ISAC is an organization that brings together cybersecurity managers in person to facilitate SIS between operators of critical infrastructures. For a general introduction to the concept of an ISAC, see Zhao and White (2012). For some illustrative examples of ISACs across different countries, see ENISA (2017). For a detailed description of MELANI-Net, its organization and history, see Dunn Caveltly (2014: 39-54). The ISAC we study is organized as a public-private partnership between the government and private industry; it operates on a not-for-profit basis. Membership in MELANI-Net is voluntary. In Switzerland, there is no regulation that makes SIS mandatory, hence, individuals are free to share or not share information, and they can also control the group of individuals with whom they want to share the information. This implies our study design can capture the full range of human behavior from perfect cooperation to total refusal.

The members of the closed user group are all senior managers in charge of providing cybersecurity for their respective organizations. They come from both private critical infrastructure operators and from the public sector. They have to undergo government

PART II: Empirical Analysis

identification and clearance procedures as well as background checks before being admitted for ISAC membership. They share classified, highly sensitive information the leaking or abuse of which may cause significant economic damage. There is no interaction of these members with the public whatsoever, and no external communication to the public or any publication of SIS results is made. For all of these members, the exchange of SIS can be assumed to be relevant, as they manage critical infrastructures that are ultimately all connected and operate with similar IT systems, such that cybersecurity problems that relate to any particular individual are likely of interest to other participants too.

Within this closed user group, individuals can contact each other by an internal message board whenever a particular individual has shared information about a threat that is of interest to other members. They do so by commenting on the initial information shared in order to establish a first contact which then leads to further social exchange between the two individuals. Once contact is made by a short reply to the threat information, the individuals involved in the conversation meet on their own initiative to share detailed security information between them (e.g., informally over lunch, in group meetings, or small industry-specific conferences, but always face-to-face). Each individual decides for him- or herself if s/he wants to meet, with whom, and in what form. They also freely decide about the extent of the information shared (if any). MELANI-Net officials neither force nor encourage individuals to interact; both in terms of social interaction in general and regarding the sharing of any particular unit of information.

3.2 Measures

Our study analyzes human behavior on the individual level of analysis. We therefore chose a psychometric approach to operationalize our constructs (Nunnally and Bernstein, 2017). We adopted psychometric scales from the extant measurement literature wherever possible and kept specific adaptations to our population context to a minimum. Table 1 explains and details all variables, their item composition and wording (if applicable), dropped items (if any), factor loadings, and Cronbach alphas and cites the sources they were taken from.

SIS is operationalized dually by the two constructs *frequency* and *intensity*. Intensity measures the extent to which the focal individual reacts to any threat information shared by another individual and thus begins social interaction with that other individual. Intensity is thus a reactive measure of how intensely the focal individual engages in knowledge sharing with

PART II: Empirical Analysis

others *upon being informed* of a threat.² Since information sharing is not mandatory, this measure captures the individual's free choice to (not) engage in exchange relationships with other individuals. By contrast, *frequency* is a proactive measure; it captures how often an individual shares security information that *s/he possesses him- or herself*.

To capture respondent heterogeneity, we controlled for gender, age, and education level. Further, we controlled for the individual's ISAC membership duration in years, because a respondent's sharing activity may co-evolve with the length of ISAC membership. *Gender* was coded dichotomously (male, female). *Age* was captured in four mutually exclusive categories (21-30, 31-40, 41-50, 50+ years). *Education* was captured by six mutually exclusive categories (none, bachelor, diploma, master, PhD, other). We also controlled for the industry affiliation of the organization that the individual represents.

3.3 Implementation

Data for all variables was collected from individual respondents by a questionnaire instrument. We followed the procedures and recommendations of Dillman et al. (2014) for questionnaire design, pre-test, and implementation. Likert-scaled items were anchored at "strongly disagree" (1) and "strongly agree" (5) with "neutral" as the midpoint. Categories for the measure *intensity* were ordered hierarchically.

The questionnaire was developed as a paper instrument first. It was pre-tested with seven different focus groups from academia and the cybersecurity industry. Feedback obtained was used to improve the visual presentation of the questionnaire and to add additional explanations. This feedback also indicated that respondents could make valid and reliable assessments.

Within the closed user group, both MELANI-Net officials and members communicate with each other in English. Switzerland has four official languages, none of which is English, and all constructs we used for measurement were originally published in English. We therefore chose to implement the questionnaire in English to rule out any back-translation problems. Before implementation, we conducted pre-tests to make sure respondents had the necessary

² The measure *intensity* is ordered and categorical in that it asks respondents to provide an estimate rather than an exact percentage figure. We preferred this approach in order to give respondents an opportunity to provide an estimate, such that they would not be deterred by the need to provide an exact figure. For the same reason, we preferred a scale-based over a percentage measure for *frequency*. We also captured an alternative measure of intensity by a Likert scale, but found that models with the ordered categorical measure fit the data better.

PART II: Empirical Analysis

language skills. The cover page of the survey informed respondents about the research project and our goals and also made clear that we had no financial or business-related interest.

The paper instrument was then implemented as a web-based survey using *SelectSurvey* software provided by the Swiss Federal Institute of Technology Zurich. For reasons of data security, the survey was hosted on the proprietary servers of this university. The management of MELANI-Net invited all closed user group members to respond to the survey by sending an anonymized access link, such that the anonymity of respondents was guaranteed at all times. Respondents could freely choose whether or not to reply. As a reward for participation, respondents were offered a research report free of charge that summarized the responses. Respondents could freely choose to save intermediate questionnaire completions and return to the survey and complete it at a later point in time.

The online questionnaire and the reminders were sent to the population by the Deputy Head of MELANI-Net together with a letter of endorsement. The survey link was sent in an e-mail describing the authors, the data, contact details for IT support, the offer of a free report, and the scope of our study. Data collection began on October 12, 2017 and ended on December 1, 2017. Two reminders were sent on October 26 and November 9, 2017. Of all 424 members, 262 had responded when the survey was closed, for a total response rate of 62%.

3.4 Analysis

Upon completion of the survey, sample data were exported from the survey server, manually inspected for consistency and then converted into a STATA dataset (Vol. 15) on which all further statistical analysis was performed. Post-hoc tests suggested no significant influence of response time on any measure. There was no significant overrepresentation of individuals affiliated with any particular organization, suggesting no need for a nested analytical design.

We performed principal component factor analysis with oblique rotation on all items. Validity was tested by calculating item-test, item-rest, and average inter-item correlations. Reliability was measured by Cronbach alpha. High direct factor-loadings and low cross-loadings indicate a high degree of convergent validity (Hair et al., 2009). The final matrix suggested seven factors with an eigenvalue above unity. The first factor explained 14.56% of the total variance, suggesting the absence of significant common method variance in the sample (Podsakoff and Organ, 1986). The detailed factor-loadings and their diagnostic measures are given in Table 2. Upon this analysis, three items were dropped (viz. Table 1) because they had

PART II: Empirical Analysis

low direct and high cross factor loadings. Finally, for any scale, individual item scores were added, and this sum was divided by the number of items in the scale (Reinholt et al., 2011; Trevor and Nyberg, 2008).

The construct *intensity* is ordered and categorical, therefore we estimated ordered probit models. A comparison with an alternative ordered logit estimation confirmed the original estimations and indicated the ordered probit model fit the data slightly better. The construct *frequency* is conditioned on values between 1 and 5, therefore we estimated Tobit models. Both models were estimated with robust standard errors to neutralize any potential heteroscedasticity. Consistent with the recommendation of Cohen et al. (2002), we incrementally built all models by entering only the controls in a baseline model first, then added the main effects, and finally entered the interaction effects. In both estimations, we mean centered the measures before entering them into the analysis. Model fit was assessed by repeated comparisons of Akaike and Bayesian information criteria between different specifications.

4. Results

Table 3 provides descriptive statistics for all variables. Table 4 specifies Spearman correlations; for the sake of brevity, correlates for controls are omitted. Table 5 documents the two final, best-fitting models and their respective diagnostic measures.

H1 is partially supported. A positive attitude towards SIS is positively associated with the intensity ($p < 0.05$), but not with the frequency of SIS. This may suggest that whenever the focal individual believes SIS is an effective activity, his or her behavior is responsive to information shared by other individuals.

H2a is fully supported. Social reciprocity is associated with both the intensity ($p < 0.01$) and the frequency of SIS ($p < 0.05$). This finding is in line with our theoretical expectation that individuals seek equitable exchange relationships in which cooperative behavior is rewarded. Future research may longitudinally study such social interaction over time with a dyadic research setting, studying how exchange patterns of repeated reciprocation develop over time.

H2b is partially supported. Transactional reciprocity is associated with the frequency of SIS ($p < 0.01$), but not with its intensity. This may imply that transactional rewards such as bonuses or promotion motivate individuals to share knowledge, they already possess with others in order to signal a high level of productive activity vis-à-vis their superiors.

PART II: Empirical Analysis

H3 is fully supported. Consistent with our theoretical expectation, executional cost is negatively associated with both the frequency ($p < 0.05$) and the intensity ($p < 0.001$) of SIS. This not only signals that executional cost constitutes a form of transaction cost that may deter individuals from sharing, as we hypothesized. The negative association with intensity is much stronger, suggesting that the negative association of executional cost is larger when the focal individual reacts to information shared by others. In other words, in the presence of high executional cost, individuals seem to be punished for reacting. Since our research design only accounted for the presence of executional cost, more research is required to identify the institutional or organizational sources of this cost.

H4 is not supported. Contrary to what we hypothesized, we find no support for the claim that an individuals' expectation to increase his or her status or social esteem is associated with SIS. Our measure of reputation is neither significantly associated with the intensity nor with the frequency of SIS. This negative result may be due to the fact that Yan et al. (2016) introduced their measure of reputation (which we use in our empirical study) in the context of public knowledge sharing among private individuals who vie for public social esteem. By contrast, we study a population of security professionals in the context of a private setting in which sensitive and classified information is shared. This may imply that, insofar as *security* information sharing is concerned, future research should propose alternative measures of reputation that are congruent with this context.

H5 is partially supported. The extent to which the focal individual trusts the information received will be useful is positively associated with the frequency ($p < 0.01$), but not with the intensity of SIS. This may imply that a focal individual who has such trust would be more willing to share knowledge s/he already possesses. In this respect, more research is required regarding the relationship between initial trust among individuals and the evolution of such trusts as exchange relationships unfold.

As regards the interaction effects, we find that H6a is partially supported. The extent to which the focal individual trusts the information received will be useful negatively moderates the relationship between attitude and the intensity ($p < 0.05$), but not the frequency of SIS. This may imply that trust can function as a partial substitute for attitude, in that the focal individual needs to convince him- or herself to a lesser extent that SIS is useful in general if that individual trusts the particular information s/he is about to receive is useful.

PART II: Empirical Analysis

H6b is not supported. The extent to which the focal individual trusts the information received will be useful neither moderates the positive association of social reciprocity with the intensity of SIS nor that with the frequency of SIS. This may imply that, unlike in the above case for H6a, the focal individual's trust that any particular unit of information is useful cannot function as a substitute for the importance of social reciprocity in the exchange relationship as such.

H6c is fully supported. The extent to which the focal individual trusts the counterparty provides valuable information, negatively moderates both the association of transactional reciprocity with the frequency ($p < 0.01$) and with the intensity ($p < 0.05$) of SIS. In line with our theoretical reasoning, this result may suggest that trust can help the focal individual to convince him- or herself that the exchange relationship is equitable (since the information s/he is about to receive is trusted to be useful), such that the focal individual has to rely less on the expectation that s/he will be compensated by monetary or career benefits whenever s/he participates in exchange relationships.

Finally, the fact that we find partial support for H1, H2b, H5 and H6a suggests that a differentiation of the theoretical construct SIS into different measurement constructs is productive. Future research may further develop the measures of frequency and intensity we have proposed here or develop yet other detailed operationalizations.

As regards our control variables, we find no significant association of respondents' demographic heterogeneity, length of membership in MELANI-Net, or industry affiliation with SIS. The latter non-finding also alleviates concerns of overrepresentation of a particular industry or firm among the responses. For the controls *age*, *industry*, and *education*, a benchmark category was automatically selected during estimation for every control (viz. footnote b to Table 5).

The only significant association we find relates to the control *education* in the model for the frequency of SIS. Since the education category 'other' is used as the benchmark, the results suggest that in comparison to individuals with an education captured by 'other', the remaining individuals in all other education categories share significantly less in terms of frequency ($p < 0.01$, respectively), whereas no association with intensity is presented. Since all other categories capture academic degrees and the case of no education, this may imply that individuals who have a non-academic education (e.g., vocational training) share knowledge they possess more often with other individuals, probably because they are industry practitioners

who wish to propagate information, they possess throughout respective their industries to strengthen organizational practice.

5. Discussion

Building on prior research in the field of the economics of information security and adopting a behavioral framework to organize our theoretical reasoning, we have proposed how and why human behavior should be associated with SIS. To the best of our knowledge, this study is the first that associates the actual sharing of sensitive information among real human individuals inside a private Information Sharing and Analysis Centre (ISAC) with the behavior of these individuals. We also provide a dual empirical operationalization of SIS by introducing the measures of SIS frequency and intensity. Our study thus provides a first step towards an empirical corroboration of prior theoretical and game-theoretic reasoning on SIS. It also confirms that interdisciplinary approaches which attempt to integrate thinking from economics and psychology are useful when SIS is studied (Anderson and Moore, 2006).

Our study also contributes to prior work that has both theoretically predicted and descriptively noted that SIS, while beneficial, is underutilized (Campbell et al., 2003; ENISA, 2010, 2016; Naghizadeh and Liu, 2016; Ghose and Hausken, 2006; Moran and Moore, 2010; Bisogni, 2015; Weiss, 2015). We provide some first empirical evidence on the association of particular human behaviors with SIS among individuals in a private ISAC setting. The study also contributes to understanding the theoretical prediction that actual SIS may not reach its societally optimal level (Gordon et al., 2003; Gal-Or and Ghose, 2005) by suggesting that human behavior may be at the core of this problem. At the same time, we would caution regulators and researchers to infer that SIS should be mandated (i.e., that individuals should be forced to share) as a consequence of this problem. Adjusting sanction levels for failure to comply with mandatory SIS could be difficult, if not impossible (Laube and Böhme, 2016). Moreover, regulations that attempt to solve the ‘sharing dilemma’ in SIS should try to fix causes, not symptoms (Böhme, 2016). Our study neither employed a longitudinal research design nor did we collect time-series data, therefore, we cannot establish causal relationships between human behavior and SIS. Nevertheless, the negative and significant association between executional cost and both the frequency and intensity of SIS that we identify confirms prior research that finds that institutions shape human interaction and behavior. Institutions are formal and informal rules which govern human behavior by rewarding desirable actions and making undesirable actions more expensive or punishable (Baumol, 1990; North, 1990, 2005).

PART II: Empirical Analysis

The organization of an ISAC is shaped by both internal institutions (i.e., rules voluntarily agreed to among ISAC participants and organizers) and external institutions (i.e., rules imposed onto them by government and regulatory authorities). Since high executional cost can be attributed to both effects, legislators and regulators should be careful to predict the impact and consequences of intended regulation for the executional cost of SIS. The association between executional cost and SIS that our study identifies suggests that humans are likely to assess the economic consequences of external institutions in terms of executional costs and adapt their behavior accordingly. Moreover, we find that both social and transaction reciprocity are positively associated with both the frequency and the intensity of SIS. Since reciprocity is a social norm, it cannot be forced by formal regulation and constraint, and the attempt to do so may induce individuals to comply with the letter rather than the spirit of the law by sharing irrelevant, non-timely, or false information (Burr, 2015).

We believe that the future study of these issues opens up promising paths for research that can both explain why individuals attempt to circumvent SIS regulation and suggest more conducive institutions. In this way, our study provides a stepping stone on which researchers can build to resolve the paradox that actual SIS, while considered highly useful in general, is at low levels, and that individuals attempt to circumvent regulation that makes SIS mandatory (Anderson and Fuloria, 2010; Moore, 2010; Moran and Moore, 2010; ENISA, 2010, 2016). At this time, we speculate that a liberal institutional environment that attempts to make individuals comply by ‘nudging’ them is probably more conducive than the attempt to enforce compliance by coercion (Thaler and Sunstein, 2009). We leave it to future research to either corroborate or refute this speculation, suggesting that irrespective of any institutional arrangement, human behavior is significantly associated with SIS, and that human behavior as regards SIS responds to institutional arrangements.

From a practical perspective, our findings support the presumption that the ‘biggest obstacles [for SIS] are economic (dis)incentives, not a lack of technology’ (Böhme, 2016). Our empirical approach takes the technological context as a given and focuses on identifying associations between human behavior and SIS. Cybersecurity managers in organizations can benefit from these results as they attempt to make individuals comply with organizational goals. Our results suggest that both the frequency and the intensity of SIS are associated with human behavior. Managers should therefore be careful to study these associations when they define organizational goals and accept that individual human behavior does not necessarily comply with these unless appropriate goal alignment is provided (Lindenberg and Foss, 2011; Hume,

PART II: Empirical Analysis

2000). For example, managers may facilitate an individual's participation in SIS by reducing the executional cost of information exchange, or they may provide the focal individual with intelligence on counterparties to help them assess the likelihood with which information sharing may be reciprocated.

Our study is pioneering in the sense that it studies real human beings and their self-reported behavior in the context of a real ISAC. Nevertheless, it merely studies a single, centrally organized ISAC in a single country. Hence, future research should generalize our approach to alternative models of ISAC organization and explore diverse national and cultural settings by replicating our study with different ISACs and nation-states. We believe our approach is conducive to such generalization since neither our theoretical framework, nor any one of our behavioral constructs, nor the empirical measures we used to operationalize these are context-specific to any particular national or cultural context. Our measures and the theory in which they are grounded rather represent fundamental aspects of human behavior which, in our view, should apply globally. Thus, future work could complement our study with data from different ISACs, such that a transnational continuum of sharing intensities and frequencies could be constructed. This continuum would allow researchers to identify commonalities and differences in information exchange patterns and use these insights to propose expedient policy options.

Finally, the ISACs that exist as of today have evolved from trade associations, government agencies, and public-private partnerships. However, the evolution of such historical trajectories is subject to technological change (Nelson and Winter, 1982). We therefore believe that novel technologies could facilitate human interaction in future ISAC configurations. For example, since the cost of reputation losses upon security breaches can be interpreted as privacy risk (Böhme, 2016), insights from privacy research and secure distributed computation and interaction (e.g., Ezhei and Ladani, 2017) might be used to construct distributed ISACs with safe real-time participation. Future research may use our study to consider the impact of such novel technological approaches on human behavior to prevent unintended consequences.

From a broader perspective, our study design has some limitations that point to opportunities for future research.³ First, both as regards the level and the unit of analysis, our study focuses on the human individual. This implies that interactions between the individual

³ We thank two anonymous reviewers for providing us with suggestions how our approach may be expanded and generalized.

PART II: Empirical Analysis

and the organizational and institutional contexts within which the focal individual acts are beyond the scope of this study. Nevertheless, our setting may be expanded both theoretically and empirically to incorporate such multilevel interactions. For example, the organizational-level performance implications of SIS could be studied, in that future research would analyze the association of individual behavior with organizational results, such as increased cybersecurity or increased performance.

In particular, future research may analyze the extent to which different organizational processes, cultures, and risk management approaches are associated with SIS by way of human behavior. For example, critical infrastructure providers who face significant risks of business interruption and going concern if their cybersecurity is compromised may emphasize more than other organizations that SIS is desirable and hence direct their employees to act accordingly. Thus, organizational policy may mediate the association between human behavior and SIS. Future research could build on our approach by developing more complex multilevel study designs that can incorporate such additional sources of variance.

Finally, our study design is cross-sectional, implying that we can only claim association, but not causation. While we believe this is acceptable given the pioneering nature of this study, longitudinal study designs are required to establish causality. Such studies may ethnographically analyze human interaction within an ISAC over time, log how and why behavior changes, and infer how this behavioral evolution operates on SIS outcomes.

6. References

- Ajzen, I. (1996). The directive influence of attitudes on behavior. In P. M. Gollwitzer & J. A. Bargh (Eds.), *The psychology of action: Linking cognition and motivation to behavior* (pp. 385-403). New York, NY, US: Guilford Press.
- Ajzen, I., Fishbein, M. 1980. *Understanding attitudes and predicting social behavior*. Englewood Cliffs, NJ: Prentice-Hall.
- Ajzen, I., Madden, T.J. 1986. Prediction of goal-directed behavior: attitudes, intentions, and perceived behavioral control. *Journal of Experimental Social Psychology*, 22: 453-474.
- Amayah, A. T. (2013). Determinants of knowledge sharing in a public sector organization. *Journal of Knowledge Management* 17(3): 454-471.
- Anderson R, Fuloria S. Security Economics and Critical National Infrastructure. In: Moore T, Pym D, Ioannidis C (eds.). *Economics of Information Security and Privacy*. Springer, Boston, MA, 2010, 55–66.
- Anderson R, Moore T. The Economics of Information Security. *Science* 2006;314:610–3.
- Andreoni, J. (1995) Cooperation in public-goods experiments: kindness or confusion? *The American Economic Review*. 85 (4), 891–904.
- Aviram A, Tor A. Overcoming Impediments to Information Sharing. *Alabama Law Review* 2003;55:231–80.
- Ba, S., Pavlou, P. 2002. Evidence of the effect of trust building technology in electronic markets: Price premiums and buyer behavior. *MIS Quarterly* 26(3): 243-268.
- Bauer, J., & van Eeten, M. (2009). Cybersecurity: Stakeholder incentives, externalities, and policy options. *Telecommunications Policy*, 33(10–11), 706–719.
- Baumeister, R.F. and Leary, M.R. (1995). The need to belong: Desire for interpersonal attachments as a fundamental human motivation. *Psychological Bulletin* 117, 497-529.
- Baumol WJ (1990) Entrepreneurship: Productive, unproductive, and destructive. *Journal of Political Economy* 98:893–921
- Bazerman, M.H. (2005). *Judgement in Managerial Decision Making*. New York: Wiley.
- Belletier, C., Robert, A., Motak, L., Izaute, M. 2018. Toward explicit measures of intention to predict information system use: An exploratory study of the role of implicit attitudes. *Computers in Human Behavior* 86 : 61-68.
- Bénabou, R., Tirole, J. (2006). Incentives and prosocial behavior. *American Economic Review* 96(5): 1652-1678.
- Bisogni F. 2015. Data Breaches and the Dilemmas in Notifying Customers. *Workshop on the Economics of Information Security (WEIS)*, Delft.
- Bock, G.W., Zmud, R.W., Kim, Y.G., Lee, J.N. 2005. Behavioral intention formation in

PART II: Empirical Analysis

knowledge sharing: examining the roles of extrinsic motivators, social–psychological forces, and organizational climate. *MIS Quarterly* 29(1) : 87–112.

Bodin LD, Gordon LA, Loeb MP et al. Cybersecurity insurance and risk-sharing. *Journal of Accounting and Public Policy* 2018;37:527–44.

Böhme, R. 2016. Back to the roots: Information sharing economics and what we can learn for security. In: Second workshop on information sharing and collaborative security (WISCS), Denver CO, USA: ACM, 2015.

Bolton, G.E., Ockenfels, A. 2000. ERC: A Theory of Equity, Reciprocity, and Competition. *American Economic Review* 90(1): 166-193.

Brennan, G. Pettit, P. (2004). *The Economy of Esteem*. Oxford: Oxford University Press.

Brosnan, S.F., de Waal, F. 2003. Monkeys reject unequal pay. *Nature* 425: 297–299.

Burr R. 2015. S.754 - To improve cybersecurity in the United States through enhanced sharing of information about cybersecurity threats, and for other purposes. Washington DC: 114th United States Congress.

Campbell K, Gordon LA, Loeb MP et al. The economic cost of publicly announced information security breaches: empirical evidence from the stock market. *Journal of Computer Security* 2003;11:431–48.

Chaiken, S. 1980. Heuristic versus systematic information processing and the use of source versus message cues in persuasion. *Journal of Personality and Social Psychology* 39: 752–766.

Chang, H. H., Chuang, S.-S. (2011). Social capital and individual motivations on knowledge sharing: participant involvement as a moderator. *Information & Management*, 48(1), 9-18

Cohen, J., Cohen, P., West, S.G., Aiken, L.S. 2002. *Applied Multiple Regression/Correlation Analysis for the Behavioral Sciences*. 3rd ed. Taylor & Francis.

DellaVigna, S: 2009. Psychology and economics: Evidence from the field. *Journal of Economic Literature* 47(2): 315-372.

Dillman, D.A., Smyth, J., Christian, L.M. 2014. *Internet, Phone, Mail, and Mixed-Mode Surveys: The Tailored Design Method*. 4th ed. John Wiley & Sons.

Dunn Cavelty, M. (2014). *Cybersecurity in Switzerland* (Springer Briefs in Cybersecurity). Cham: Springer International Publishing.

Eagly, A.H., Chaiken, S. 1993. *The psychology of attitudes*. Fort Worth, TX: Harcourt et al.

Emler N. 1990. A Social Psychology of Reputation. *European Review of Social Psychology*, 1(1): 171-193.

ENISA. *Incentives and Barriers to Information Sharing*. Heraklion: European Union Agency for Network and Information Security, 2010.

PART II: Empirical Analysis

- ENISA. Information Sharing and Common Taxonomies between CSIRTs and Law Enforcement. Heraklion: European Union Agency for Network and Information Security, 2016.
- ENISA. Information Sharing and Analysis Centres (ISACs). Cooperative models. Heraklion: European Union Agency for Network and Information Security, 2017.
- Ezhei M, Ladani BT. Information sharing vs. privacy: A game theoretic analysis. *Expert Systems with Applications* 2017;88:327–37.
- Fehr E, Gächter S. Fairness and Retaliation: The Economics of Reciprocity. *Journal of Economic Perspectives* 2000;14:159–81.
- Fehr, E., and Gächter, S. (2002). Altruistic punishment in humans. *Nature*, 415, 137-140.
- Fehr, E., Gintis, H. 2007. Human Motivation and Social Cooperation: Experimental and Analytical Foundations. *Annual Review of Sociology*, 33: 43-64.
- Fehr, E., Schmidt, K. 1999. A theory of fairness, competition, and cooperation. *The Quarterly Journal of Economics*, 114: 817-868.
- Gabaix, X., Laibson, D., Moloche, G., Weinberg, S., 2006. Costly Information Acquisition: Experimental Analysis of a Boundedly Rational Model. *American Economic Review* 96(4): 1043–1068.
- Gal-Or E, Ghose A. The Economic Incentives for Sharing Security Information. *Information Systems Research* 2005;16:186–208.
- Gal-Or E., Ghose A. (2004) The Economic Consequences of Sharing Security Information. In: Camp L.J., Lewis S. (eds) Economics of Information Security. Advances in Information Security, vol 12. Springer, Boston, MA
- Gefen, D., Karahanna, E., Straub, D.W., 2003. Trust and TAM in online shopping: an integrated model. *MIS Quarterly* 27(1), 51–90.
- Ghose A, Hausken K. 2006. A Strategic Analysis of Information Sharing Among Cyber Attackers. *SSRN Electronic Journal* 12(2).
- Gordon LA, Loeb MP, Lucyshyn W et al. Externalities and the Magnitude of Cyber Security Underinvestment by Private Sector Firms: A Modification of the Gordon-Loeb Model. *Journal of Information Security* 2015a;06:24–30.
- Gordon LA, Loeb MP, Lucyshyn W et al. The impact of information sharing on cybersecurity underinvestment: A real options perspective. *Journal of Accounting and Public Policy* 2015b;34:509–19.
- Gordon LA, Loeb MP, Lucyshyn W. Sharing information on computer systems security: An economic analysis. *Journal of Accounting and Public Policy* 2003;22:461–85.
- Gordon LA, Loeb MP, Sohail T. Market Value of Voluntary Disclosures Concerning Information Security. *MIS Quarterly* 2010;34:567–94.

PART II: Empirical Analysis

- Gordon LA, Loeb MP, Zhou L. Investing in Cybersecurity: Insights from the Gordon-Loeb Model. *Journal of Information Security* 2016;07:49.
- Gouldner AW. The Norm of Reciprocity: A Preliminary Statement. *American Sociological Review* 1960;25:161–78.
- Granovetter M. Economic Action and Social Structure: The Problem of Embeddedness. *American Journal of Sociology* 1985;91:481–510.
- Hair JF, Black WC, Babin BJ, Anderson RE. 2009. *Multivariate Data Analysis*. 5th ed. Upper Saddle River N.J: Prentice Hall, 1998.
- Harrison K, White G. Information sharing requirements and framework needed for community cyber incident detection and response. 2012 IEEE Conference on Technologies for Homeland Security (HST). IEEE, 2012, 463–9.
- Hausken K. A Strategic Analysis of Information Sharing Among Cyber Attackers. *Journal of Information Systems and Technology Management* 2015;12:245–70.
- Hausken K. Information sharing among firms and cyber attacks. *Journal of Accounting and Public Policy* 2007;26:639–88.
- Hsu, M.-H., Ju, T.L., Yen, C.-H., Chang, C.-M. 2002. Knowledge sharing behavior in virtual communities: The relationship between trust, self-efficacy, and outcome expectations. *International Journal of Human-Computer Studies* 65(2): 153-169.
- Hume D (2000) *A treatise of human nature*. Oxford University Press, New York
- Kahneman D, Tversky A. Prospect Theory: An analysis of Decision under Risk. *Econometrica: Journal of the Econometric Society* 1979;47:263–291.
- Kahneman, D., Tversky, A. 1979. Prospect theory – an analysis of decision under risk. *Econometrica* 47: 263-291.
- Keith, B., Babchuk, N. 1998. The Quest for Institutional Recognition: A Longitudinal Analysis of Scholarly Productivity and Academic Prestige among Sociology Departments. *Social Forces* 76(4): 1495–1533.
- Kolm, S.-C., Ythier, J.M. 2006. *Handbook of the Economics of Giving, Altruism and Reciprocity*. Elsevier.
- Kroenung, J., Eckhardt, A. 2015. The attitude cube—A three-dimensional model of situational factors in IS adoption and their impact on the attitude–behavior relationship. *Information & Management* 52: 611–627.
- Kwahk K-Y, Park D-H. The effects of network sharing on knowledge-sharing activities and job performance in enterprise social media environments. *Computers in Human Behavior* 2016;55, Part B:826–39.
- Laube S, Böhme R. Strategic Aspects of Cyber Risk Information Sharing. *ACM Computing Surveys (CSUR)* 2017;50:77:1–77:36.

PART II: Empirical Analysis

- Laube S, Böhme R. The economics of mandatory security breach reporting to authorities. *Journal of Cybersecurity* 2016;2:29–41.
- Lindenberg, S., Foss, N. 2011. Managing joint production motivation: the role of goal framing and governance mechanisms. *Academy of Management Review* 36(3): 500-525.
- Luijff E, Klaver M. On the Sharing of Cyber Security Information. In: Rice M, Sheno S (eds.). *Critical Infrastructure Protection IX*. Springer, 2015, 29–46.
- Malhotra, Deepak (2004). Trust and Reciprocity Decisions: The Differing Perspectives of Trustors and Trusted Parties. *Organizational Behavior and Human Decision Processes* 94(2), 61-73.
- McElreath, R. 2003. Reputation and the Evolution of Conflict. *Journal of Theoretical Biology* 220: 345-357.
- McEvily, B., Perrone, V., Zaheer, A. 2003. Trust as an organizing principle. *Organization Science* 14: 91-103.
- Moore, T. (2010). The economics of cybersecurity: Principles and policy options. *International Journal of Critical Infrastructure Protection*, 3(3–4), 103–117.
- Moran T, Moore T. The Phish-Market Protocol: Securely Sharing Attack Data between Competitors. In: Sion R (ed.). *Financial Cryptography and Data Security*. Springer, Berlin, Heidelberg, 2010, pp. 222–37.
- Naghizadeh P, Liu M. Inter-temporal incentives in security information sharing agreements. 2016 Information Theory and Applications Workshop (ITA). IEEE, 2016, 1–8.
- Nelson RR, Winter SG (1982) *An evolutionary theory of economic change*. Belknap Press, Cambridge
- North DC (1990) *Institutions, institutional change and economic performance*. Cambridge University Press, Cambridge
- North DC (2005) *Understanding the process of economic change*. Cambridge University Press, Cambridge
- Nunnally, J.C., Bernstein, I. 2017. *Psychometric Theory*. 3rd ed. McGraw-Hill.
- Oliver, P. 1980. Rewards and punishments as selective incentives for collective action: Theoretical investigations. *American Journal of Sociology* 85(6): 1356-1375.
- Olson M (1965) *The logic of collective action*. Harvard University Press, Cambridge MA
- Paese PW, Gilin DA. When an Adversary is Caught Telling the Truth: Reciprocal Cooperation Versus Self-Interest in Distributive Bargaining. *Pers Soc Psychol Bull* 2000;26:79–90.
- Park, J. H., Gu, B., Leung, A. C. M., & Konana, P. (2014). An investigation of information sharing and seeking behaviors in online investment communities. *Computers in Human Behavior*, 31: 1-12.

PART II: Empirical Analysis

- Petty, R.E., Cacioppo, J.T. 1986. The Elaboration Likelihood Model of Persuasion. *Advances in Experimental Social Psychology* 19: 123-205.
- Podsakoff, P. M., MacKenzie, S., & Podsakoff, N. P. (2012). Sources of method bias in social science research and recommendations on how to control it. *Annual Review of Psychology*, 63(1), 539–569.
- Podsakoff PM, Organ DW. Self-Reports in Organizational Research: Problems and Prospects. *Journal of Management* 1986;12:531–44.
- Reinholt, M. I. A., Pedersen, T., & Foss, N. J. (2011). Why a central network position isn't enough: The role of motivation and ability for knowledge sharing in employee networks. *Academy of Management Journal*, 54(6): 1277-1297.
- Ridings, C.M., Gefen, D., Arinze, B., 2002. Some antecedents and effects of trust in virtual communities. *Strategic Information Systems* 11(3-4), 271–295.
- Safa NS, von Solms R. An information security knowledge sharing model in organizations. *Computers in Human Behavior* 2016;57:442–51.
- Siegrist J, Starke D, Chandola T et al. The measurement of effort–reward imbalance at work: European comparisons. *Social Science & Medicine* 2004;58:1483–99.
- Simon, H.A. (1976). *Administrative Behavior: A Study of Decision-Making Processes in Administrative Organization*. Free Press, New York.
- Smith, E.A., Winterhalder, B. (Eds.) 2017. *Evolutionary ecology and human behavior*. New York: Routledge.
- Thaler RH, Sunstein CR. *Nudge: Improving Decisions About Health, Wealth, and Happiness*. New York: Penguin Books, 2009.
- Tom, S., Fox, C., Trepel, C., Poldrack, R. 2007. The neural basis of loss aversion in decision-making under risk. *Science* 315: 515-518.
- Tomasello, M., Carpenter, M., Call, J., Behne, T., Moll, H. 2005. Understanding and sharing intentions: The origins of cultural cognition. *Behavioral and Brain Sciences* 28(5): 675-691.
- Trevor, C. O., & Nyberg, A. J. (2008). Keeping your headcount when all about you are losing theirs: Downsizing, voluntary turnover rates, and the moderating role of HR practices. *Academy of Management Journal* 51(2): 259–276.
- Tricomi, E., Rangel, A., Camerer, C., O'Doherty, J. 2010. Neural evidence for inequality-averse social preferences. *Nature* 463: 1089–1091.
- Tversky, A., Kahneman, D. 1991. Loss aversion in riskless choice: a reference dependent model. *The Quarterly Journal of Economics*. 106 (4), 1039–1061
- Tversky, A., Kahneman, D. 1992. Advances in Prospect Theory: Cumulative Representation of Uncertainty. *Journal of Risk and Uncertainty* 5: 297-323
- Vakilinia I, louis SJ, Sengupta S. Evolving Sharing Strategies in Cybersecurity Information

PART II: Empirical Analysis

- Exchange Framework. Proceedings of the Genetic and Evolutionary Computation Conference Companion. New York, NY, USA: ACM, 2017, 309–310.
- von Hippel E, von Krogh G. Open Source Software and the “Private-Collective” Innovation Model: Issues for Organization Science. *Organization Science* 2003;14:209–23.
- Wang W-T, Hou Y-P. Motivations of employees’ knowledge sharing behaviors: A self-determination perspective. *Information and Organization* 2015;25:1–26.
- Wang, J.H., Wang, C., Yang, J., An, C. 2011. A study on key strategies in P2P file sharing systems and ISPs’ P2P traffic management. *Peer-to-Peer Networking and Applications*, 4(4): 410-419.
- Watzlawick, P., Bavelas, J.B., Jackson, D.D. 2011. *Pragmatics of human communication*. Norton & Company.
- Weiss E. 2015. *Legislation to Facilitate Cybersecurity Information Sharing: Economic Analysis*. Washington DC: Congressional Research Service.
- Williamson, O.E. (1981). The Economics of Organization: The Transaction Cost Approach. *American Journal of Sociology*. 87(3): 548–577
- Xiong L, Liu L. PeerTrust: supporting reputation-based trust for peer-to-peer electronic communities. *IEEE Transactions on Knowledge and Data Engineering* 2004;16(7): 843-857.
- Yan Z, Wang T, Chen Y et al. Knowledge sharing in online health communities: A social exchange theory perspective. *Information & Management* 2016;53:643–53.
- Zhao, W., White, G. 2012. A collaborative information sharing framework for Community Cyber Security. *IEEE Conference on Technologies for Homeland Security (HST)*, Waltham, MA: 457-462.

PART II: Empirical Analysis

7. Appendix

Table 1: Constructs, Items and Scales Used in the Survey

Measures (Source)	Type	Item	Text	Factor loading	Cronbach alpha
<i>SIS constructs</i>					
Intensity of SIS (novel)	Ordered categorical measure	n/a	How often do you comment on shared information? * Never * Rarely, in less than 10% of the chances when I could have * Occasionally, in about 30% of the chances when I could have * Sometimes, in about 50% of the chances when I could have * Frequently, in about 70% of the chances when I could have * Usually, in about 90% of the chances I could have * Every time	n/a	n/a
Frequency of SIS (Safa & von Solms, 2016)	Likert scale	ISKS1 ISKS2 ISKS3 ISKS4 ISKS5	I frequently share my experience about information security with MELANI I frequently share my information security knowledge with MELANI I frequently share my information security documents with MELANI I frequently share my expertise from my information security training with MELANI I frequently talk with others about information security incidents and their solutions in MELANI workshops	0.8075 0.8903 0.8850 0.8600 0.6898	0.8945
<i>Behavioral constructs</i>					
Attitude (Safa & von Solms, 2016)	Likert scale	AT1 AT2 AT3 AT4	I think SIS behavior is a valuable asset in the organization I believe SIS is a useful behavioral tool to safeguard the organization's information assets My SIS has a positive effect on mitigating the risk of information security breaches SIS is a wise behavior that decreases the risk of information security incidents	dropped 0.7751 0.6376 0.7849	0.6761
Transactional reciprocity (Wang and Hou, 2015)	Likert scale	HR1 HR2 HR3	I expect to be rewarded with a higher salary in return for sharing knowledge with other participants I expect to receive monetary rewards (i.e., additional bonus) in return for sharing knowledge with other participants I expect to receive opportunities to learn from others in return for sharing knowledge with other participants	0.8822 0.8743 dropped	0.7956

PART II: Empirical Analysis

Social reciprocity (Kwahk and Park, 2016)	Likert scale	HR4	I expect to be rewarded with an increased job security in return for sharing knowledge with other participants	0.7499	
		NOR1	I believe that it is fair and obligatory to help others because I know that other people will help me some day	dropped	
		NOR2	I believe that other people will help me when I need help if I share knowledge with others through MELANI	0.8464	
		NOR3	I believe that other people will answer my questions regarding specific information and knowledge in the future if I share knowledge with others through MELANI	0.8714	0.8003
		NOR4	I think that people who are involved with MELANI develop reciprocal beliefs on give and take based on other people's intentions and behavior	0.6946	
Executorial cost (Yan et al., 2016)	Likert scale	EC1	I cannot seem to find the time to share knowledge in the community	0.6964	
		EC2	It is laborious to share knowledge in the community	0.6950	0.7882
		EC3	It takes me too much time to share knowledge in the community	0.8626	
		EC4	The effort is high for me to share knowledge in the community	0.7913	
Reputation (Yan et al., 2016)	Likert scale	R1	Sharing knowledge can enhance my reputation in the community	0.6312	
		R2	I get praises from others by sharing knowledge in the community	0.6890	
		R3	I feel that knowledge sharing improves my status in the community	0.7922	0.6996
		R4	I can earn some feedback or rewards through knowledge sharing that represent my reputation and status in the community	0.7039	
Trust (Safa & von Solms, 2016)	Likert scale	TR1	I believe that my colleague's information security knowledge is reliable	0.7510	
		TR2	I believe that my colleague's information security knowledge is effective	0.8688	
		TR3	I believe that my colleague's information security knowledge mitigates the risk of information security breaches	0.8460	0.8598
		TR4	I believe that my colleague's information security knowledge is useful	0.8039	
		TR5	I believe that my colleagues would not take advantage of my information security knowledge that we share	dropped	

PART II: Empirical Analysis

Table 2: Final Set of Factor Loadings after Oblique Rotation^a

Item	Loading on oblimin-rotated factor							Commonality
	factor 1	factor 2	factor 3	factor 4	factor 5	factor 6	factor 7	
ISKS1	0.8075							0.27
ISKS2	0.8903							0.19
ISKS3	0.885							0.20
ISKS4	0.86							0.21
ISKS5	0.6898							0.44
AT2							0.7751	0.32
AT3	0.3412						0.6376	0.38
AT4							0.7849	0.31
NOR2					0.8464			0.23
NOR3					0.8714			0.18
NOR4					0.6946			0.36
HR1				0.8822				0.16
HR2				0.8743				0.19
HR4				0.7499				0.41
EC1			0.6964					0.49
EC2			0.695					0.45
EC3			0.8626					0.21
EC4			0.7913					0.32
R1						0.6312		0.49
R2						0.689		0.51
R3						0.7922		0.29
R4						0.7039		0.44
TR1		0.751						0.36
TR2		0.8688						0.21
TR3		0.846						0.26
TR4		0.8039						0.29
<i>Eigenvalue</i>	3.786	2.951	2.502	2.329	2.24	2.142	1.851	
<i>Proportion of variance explained</i>	14.56%	11.35%	9.62%	8.96%	8.62%	8.24%	7.12%	
<i>Cumulative variance explained</i>	14.56%	25.91%	35.53%	44.49%	53.11%	61.34%	68.46%	

Notes to Table 2.

a. Blank cells represent factor loadings smaller than 0.30.

PART II: Empirical Analysis

Table 3: Descriptive Statistics on all Variables

Variable	Obs	Mean	Std. Dev.	Min	Max
Frequency	240	2.68	0.78	1	5
Intensity	228	2.34	1.20	1	7
Attitude	208	4.10	0.53	3	5
Reciprocity (social)	195	3.88	0.60	1.66	5
Reciprocity (transactional)	195	2.16	0.75	1	4
Executorial cost	208	3.14	0.65	1.25	5
Trust	190	3.82	0.55	1.25	5
Gender	260	1.04	0.20	1	2
Age category	261	2.87	0.86	1	4
Education category	260	2.58	1.25	1	6
Membership duration	260	7.05	5.35	1	18

Table 4: Correlations Among Dependent and Independent Variables^a

	Frequency	Intensity	Attitude	Reciprocity (social)	Reciprocity (transactional)	Executorial cost	Trust
Frequency	1						
Intensity	0.3547***	1					
Attitude	0.2436***	0.2742***	1				
Reciprocity (social)	0.2602***	0.2750***	0.3798***	1			
Reciprocity (transactional)	0.1836**	0.0456	-0.0901	0.000	1		
Executorial cost	-0.2238**	-0.1694*	-0.0976	-0.0314	0.1533*	1	
Trust	0.2279**	-0.0101	0.2471***	0.0269***	-0.1321	-0.1857*	1

Notes to Table 4.

a. Spearman correlations. * $p < 0.05$; ** $p < 0.01$; *** $p < 0.001$.

PART II: Empirical Analysis

Table 5: Final Results of Model Estimations^{a,b}

	Intensity of SIS (ordered probit estimation)	Frequency of SIS (Tobit estimation)
	<i>Coefficient (std. error)</i>	<i>Coefficient (std. error)</i>
Attitude	0.3627* (0.1672)	0.1895 (0.1111)
Reciprocity (social)	0.4045** (0.1526)	0.2150* (0.1046)
Reciprocity (transactional)	0.1860 (0.1118)	0.2361** (0.0816)
Executorial cost	-0.4833*** (0.1314)	-0.2336* (0.0962)
Reputation	0.0932 (0.1895)	-0.1121 (0.1232)
Trust	-0.1847 (0.1501)	0.2964** (0.1036)
Attitude x Trust	-0.6544* (0.2874)	-0.3490 (0.2311)
Reciprocity (social) x Trust	0.1969 (0.2431)	0.2055 (0.1813)
Reciprocity (transactional) x Trust	-0.4561* (0.2119)	-0.3839** (0.1378)
Gender	-0.2106 (0.4788)	0.1837 (0.1773)
Age 21-30	-0.1361 (0.4204)	0.2057 (0.2378)
Age 31-40	0.1139 (0.2293)	0.0051 (0.1513)
Age 41-50	0.0096 (0.1820)	0.0171 (0.1243)
Education none	-0.7239 (0.6388)	-0.8152** (0.2441)
Education Master	-0.8336 (0.6368)	-0.7984** (0.2671)
Education Bachelor	-0.3198 (0.6202)	-0.7678** (0.2324)
Education PhD	-0.9997 (0.6382)	-0.9345** (0.3181)
Membership duration	0.0184 (0.0164)	0.0213 (0.0112)
Government	-0.2945 (0.3082)	-0.0097 (0.2288)
Banking & Finance	-0.1515 (0.2472)	0.0304 (0.2064)
All other industries	-0.1576 (0.2982)	-0.3748 (0.2395)
Energy	-0.1007 (0.3217)	0.1867 (0.2399)
Health	-0.2958 (0.3528)	0.0465 (0.2759)
<i>Constant</i>		3.0939*** (0.4718)
Log pseudolikelihood	-246.50	-197.92
Pseudo R ²	0.0896	0.1564
F (23 d.f., 165); $p > F$		5.25; 0.000***
Wald χ^2 (23 d.f.); $p > \chi^2$	64.02; 0.000***	
Observations	188	188
- of which left-censored		10
- of which right-censored		1

Notes to Table 5.

a. Two-tailed tests. Robust standard errors are given between parentheses.

* $p < 0.05$; ** $p < 0.01$; *** $p < 0.001$

b. Age category “above 50”, education category “other” and the telecommunication/IT industry serve as the respective control variable benchmarks.

PART II: Empirical Analysis

Table 6: Documentation of Pre-Tests

Participant	Test 1	Test 2	Test 3	Results
Professor I	X		X	Adaptation of scales to context
Professor II		X		Adaptation of scales to context
PhD student I	X			Wording adaptation
PhD student II		X		Usability improvements
PhD student III			X	Implementation of idioms explanation and support of the study leader
Professional I	X			Questionnaire shortened
Professional II			X	Text field for general comments added
Industry expert I	X			Wording adaptation
Industry expert II		X	X	Wording adaptation

PART III: Policy Recommendations

“If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology.”

- *Bruce Schneier*

Governance Models Preferences for Security Information Sharing: An Institutional Economics Perspective for Critical Infrastructure Protection

Published in the proceedings of the 13th International Conference on Critical Information Infrastructure Security (CRITIS 2018)

Kaunas, Lithuania, September 24-26, 2018

Publisher: Springer, Lecture Notes in Computer Science book series (LNCS, volume 11260)

Abstract

Empirical studies have analyzed the incentive mechanisms for sharing security information between human agents, a key activity for critical infrastructure protection. However, recent research shows that most Information Sharing and Analysis Centers do not perform optimally, even when properly regulated. Using a meso-level of analysis (i.e. information sharing organizations), we close an important research gap by presenting a theoretical framework that links institutional economics and security information sharing. We illustrate this framework with a dataset collected through an online questionnaire addressed to all critical infrastructures (N=262) operating at a Swiss Reporting and Analysis Centre for Information Security. Using descriptive statistics, we investigate how institutional rules offer human agents an institutional freedom to self-design an efficient security information sharing artifact. Our results show that a properly designed artifact can positively reinforce human agents to share security information and find the right balance between three governance models: (a) public-private partnership, (b) private, and (c) government-based. Overall, our work lends support to a better institutional design of security information sharing and the formulation of policies that can avoid non-cooperative and free-riding behaviors that plague cybersecurity.

Keywords: economics of information security; security information sharing; new institutional economics; information sharing and analysis center; critical infrastructure protection; information assurance.

1. Introduction

In recent years, critical infrastructures (CIs) have grown more dependent on Supervisory Control and Data Acquisition (SCADA) systems and the Internet network to operate properly (Eden et al., 2015). Therefore, the cybersecurity of CIs is increasingly recognized as a public good that is essential in the daily life of human agents, organizations, and governments (Mermoud, Keupp, Ghernaouti, & Percia David, 2016). The need for managing critical infrastructure protection (CIP) is of vital importance for national security because cascading effects caused by mutual dependencies across different CIs and their services are considered to be a systemic risk (E. Luijff, Nieuwenhuijs, Klaver, Eeten, & Cruz, 2008; Percia David, Keupp, Ghernaouti, & Mermoud, 2016; van Eeten, Nieuwenhuijs, Luijff, Klaver, & Cruz, 2011).

Previous research has shown that security information sharing (SIS)¹ is a key activity for producing information security for CIP (Laube & Böhme, 2016; E. Luijff & Klaver, 2015). SIS is widely acknowledged by policy-makers and industrial actors, as it can reduce risks, deter attacks, and enhance the overall resilience of CIs (Laube & Böhme, 2017). For the last two decades, Information Sharing and Analysis Centers (ISACs) have been the preferred way for CIs to organize and coordinate SIS.² Even though no empirical evidences demonstrate the link between the SIS activity and an observed enhancement of information security, most scholars and practitioners are convinced that such an activity contributes to foster cybersecurity and social welfare as a whole (Gordon, Loeb, Lucyshyn, & Zhou, 2015; Laube & Böhme, 2016).

Although empirical studies have investigated the incentive mechanisms that support voluntary SIS at a micro-level (i.e., between human agents), most ISACs do not perform at their theoretical Pareto-optimal level,³ even when properly regulated (Mermoud, Keupp, Huguenin, Palmié, & Percia David, 2018). This leads to the following research question: What are the most efficient institutional rules for designing a SIS artifact? To the best of our knowledge, no scientific study has investigated this aspect. To address it, we propose a set of institutional rules for the design of efficient SIS artifacts at a meso-level, i.e., a theoretically

1

² ISACs are non-profit organizations that provide a central resource for gathering information on cyber threats by providing a two-way sharing process, often involving both the private and the public sector.

³ Pareto efficiency describes a state of allocation of resources from which it is impossible to reallocate so as to make any human agent better off without making at least one human agent worse off.

PART III: Policy Recommendations

“ideal” SIS center. Using descriptive statistics from a primary set of field-data, we present three generalizable SIS governance models, thus suggesting how human agents would self-organize SIS if these particular rules are implemented.

The remainder of this part is structured as follows: In Section 2, we survey related work and connect different streams of economic theories in order to generate a novel theoretical framework. In Section 3, we conceptualize a set of institutional rules linked to an SIS artifact. We document our population and how the dataset was collected, Section 4. And in Section 5, we present descriptive statistics illustrating our framework in the context of CIP. We present concluding remarks, limitations and future work are presented in Section 6.

2. Theoretical Framework and Related Work

This part is premised on the belief that a computer security-based approach, although necessary, is not sufficient to handle the information security issues of CIs. Therefore, in this section, we connect different streams of theories from institutional economics and security of information systems in order to create a multi-disciplinary theoretical framework.

2.1 An Institutional Economics Perspective of SIS

The driving forces leading to the creation of the ISAC differ; in some cases, the private sector takes the lead, whereas in others, the public sector brings all stakeholders together.⁴ In both cases, it is crucial for the ISAC to find the right balance of collaboration between the public and private sectors, usually formalized into a public–private partnership (PPP)⁵ (ENISA, 2018a). Our research is premised on the idea that ISACs are institutions that were not designed in the most efficient way, because they were historically initiated and regulated by governments, which are more focused on complying to security principles, rather than on ensuring a security efficiency (Boettke, Coyne, & Leeson, 2013).

⁴ Some EU legislation nourishes the existing ISACs and the creation of new ones. For example, in December 2015, the European Parliament and Council agreed on the first EU-wide legislation on cybersecurity, adopting the EU Network and Information Security (NIS) Directive. The EU General Data Protection Regulation (GDPR) aims to harmonize and unify existing EU privacy-breach reporting obligations. On the other hand, some regulations, such as the US Freedom of Information Act might represent a barrier to SIS.

⁵ A PPP is a cooperation between two or more private and public sectors. In this study, we do not differentiate whether the public or the private sector are owning and/or managing the PPP.

PART III: Policy Recommendations

From an organizational-theory perspective, ISACs perform differently as they operate under different institutional rules (ENISA, 2018a). With each industry or government being free to set up their ISAC, these sharing institutions widely differ in quality, structure, and in how they are funded, managed and operated (ENISA, 2015; Prieto, 2006). Consequently, by applying an economic perspective on ISACs, it is possible to understand the quality, performance and problems of a particular institution. An institutional economic analysis can reveal why human agents behave differently depending on how the sharing institution is designed. This can explain why suboptimal performance appears to be pervasive, even in the next generation of ISACs, for instance in Information Sharing and Analysis Organization (ISAOs) or so-called “fusion centers” (PricewaterhouseCoopers (PwC), 2015, 2016; Weiss, 2015), which are supposed to aggregate and manage the flow of information across all levels and sectors. To address this problem, we propose a set of institutional rules for the design of efficient SIS artifacts, i.e., a theoretically “ideal” SIS center designed at a meso-level, i.e. a level of analysis that falls between the micro- and macro-levels, such as a community or an organization.

The New Institutional Economics (NIE) literature offers insights on how legal norms and rules (i.e., institutions) underlie an economic activity, such as SIS (Zenger, Lazzarini, & Poppo, 2002). The NIE theory describes how rules affect human behavior, as institutions have different political, economic and social conditions (Furubotn & Richter, 2005; Richter, 2015). Institutions set the rules on how an economic system works and create incentives and threats to orient human agents’ actions such as for SIS (Bauer & van Eeten, 2009). Thus, human agents cannot be expected to voluntarily engage in SIS, unless they are provided with a safe and conducive institutional design that facilitates SIS (Mermoud et al., 2018). As a result, the decisive criteria for SIS performance are not related to funding or regulations, but rather to the design of “good” institutions. As there is an ongoing global debate about whether SIS should be mandatory, our research contributes to the formulation of policies based on voluntary SIS that can avoid non-cooperative and free-riding behaviors that plague cybersecurity (Luijff & Kernkamp, 2015).

3. Research Artifact and Set of Rules

In this section, we develop an SIS artifact based on a set of institutional rules.

3.1 Institutional Design of an SIS Artifact

Design science research (DSR) focuses on the creation, development and performance evaluation of artifacts typically including research models, algorithms, knowledge and human-computer interfaces (Gregor & Hevner, 2013). We use the DSR theory to conceptualize our SIS artifact as a generic information center which is not necessarily related to ISACs as such. In our study, we use the NIE methodology to design a theoretical “ideal” SIS artifact with the intention of improving the functional performance iteratively. Figure 1 presents nine institutional rules which can generate institutional incentives for SIS. Depending on how the rules are implemented, the performance and governance models will differ, because human agents can self-organize SIS and select the right balance of partnership between the public and private sector. The lack of cooperation between the public and private sector remains a major pitfall for SIS and the global security (Prieto, 2006), especially in a “post-Snowden” context where trust has been broken.

3.2 Set of Universal Rules for SIS

Using a free-market economy approach, we suggest that, if human agents can self-design an SIS artifact, the market will select the best model on the long run (Hayek, 2005). Previous research suggests that nine universal institutional rules are particularly relevant for a design-efficient SIS artifact (ENISA, 2018a, 2018b):

1. ***Investment / sharing freedom*** guarantees that participation in SIS is voluntary and not forced by any regulations and/or constraints. Participants can determine what they share and are allowed to leave the artifact at any time.
2. ***SIS security*** is guaranteed that the artifact is built, managed and audited with the highest cybersecurity standards. An application programming interface (API) should be designed to enable tokenization, i.e. substituting a sensitive data element with a non-sensitive equivalent. This process should facilitate a secured SIS process and meet the

PART III: Policy Recommendations

security requirements of US and EU regulators (e.g., regarding sensitive customer data).

3. **SIS privacy** is guaranteed by the participants' ability to seclude themselves, or information about themselves, thus engaging in SIS selectively. Therefore, participants can access, modify and delete their (meta)data at any time and have a right to be forgotten. Participants can determine with whom they share security information according to the circle theory (e.g., participants can choose to share information only with the government or only with their industry) (Mermoud et al., 2016). Upon request, the (meta)data can be anonymized in order to protect the participants' identities. The data will not be used for other purposes than producing information security.
4. **A trust** mechanism process is implemented in order to build trust among participants (e.g., with workshops or events). Trust can also be built on existing relationships or collaborations.
5. **Information exclusivity** is a rule that ensures that the shared information is timely, relevant, actionable and exclusive, thus making the artifact more attractive for participants.
6. **Financial rewards** are organized in order to motivate participants with a financial reward mechanism that recognizes their involvement in the SIS activity.
7. **Social rewards** are organized in order to motivate participants with a reciprocal altruism mechanism. As in the tit-for-tat strategy, evolutionary biology defines reciprocal altruism as a behavior where an organism acts in a manner that temporarily reduces its fitness while increasing another organism's fitness, with the expectation that the other organism will act in a similar manner, and eventually increase its own fitness.
8. **Cooperation** is implemented by altruistic punishment mechanisms and is measured by the frequency and intensity of the SIS activity. Such a cooperation is triggered by the intention to engage in the SIS activity, which was triggered by the belief that the SIS activity is performing in terms of information security.
9. **Institutional design (ID)** guarantees that the most efficient rules are implemented, audited and controlled iteratively. Participants should be able to choose their

PART III: Policy Recommendations

organizational and governance standards, for instance between: 9a) centralized sharing model such as a relational database (e.g., a forum) and 9b) decentralized sharing model such as a distributed database (e.g., a blockchain). This rule is also defined by 9c) formalization and 9d) standardization. Formalization is the extent to which work roles are structured in an organization, and the activities of the participants are governed by rules and procedures. Standardization is the process of implementing and developing technical standards based on the consensus of different parties.

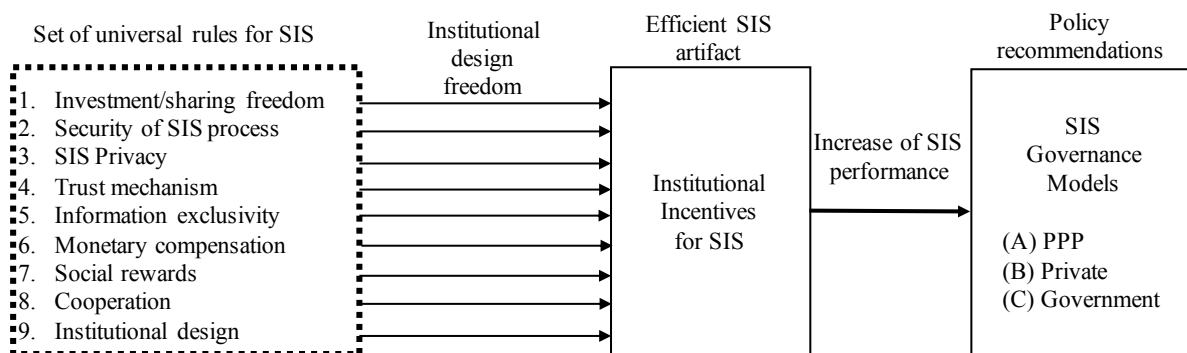


Figure 1: Security Information Sharing Artifact

This figure describes a set of institutional rules that offer human agents an institutional freedom to design an efficient SIS artifact. The artifact positively reinforces human agents to share security information in three generic governance models; (a) public–private partnership, (b) private, and (c) government-based.

4. Application to Critical Infrastructure Protection

In this section, we present how our data set was collected and three different generic governance models that can be applied to CIP.

4.1 Population and Data Collection

We conducted our study with the Swiss Reporting and Analysis Centre for Information Security (MELANI). The center was created in 2005 as PPP between the federal government and the private industry. It operates an ISAC (MELANI-Net) that brings together over 150 CI

PART III: Policy Recommendations

operators from all sectors in Switzerland. The questionnaire⁶ was sent to the 424 participants of that closed SIS user group. These human agents freely decide whether to share information, such that their individual behavior also determines the behavior of the CIs they represent. The closed user group comprises senior managers from diverse industries; all are in charge of providing cybersecurity for their respective firms.

Data collection began on October 12, 2017 and finished on December 1, 2017. Two reminders were sent on October 26 and November 9, 2017. When data collection ended, 262 responses had been collected, of which 189 fully completed questionnaires (72%). Overall, the survey response rate was 63%.

4.2 Possible Governance Models for SIS

We posit that human agents – positively reinforced by institutional rules – will self-organize for SIS and find the right balance between three main generic SIS governance models based on previous studies (ENISA, 2016, 2018a):

- A) *The public–private partnership* model typically brings together cybersecurity stakeholders to organize SIS. Therefore, a strong cooperation between CIs and governments is needed in order to address cybersecurity issues. In this model, trust is hard to achieve, because of the high cultural heterogeneity. This governance model is the result of a mixed economy, i.e., a system bringing together elements of free market and planned economies. The government often has a role of facilitator but is not the driving force behind the governance model.

- B) *The private industry model* is typically a sector-specific model focusing on organizing SIS for CIs within the same sector, in order to generate sectorial knowledge and trend analysis. This governance model is likely to be joined by highly competitive international industries, such as banking and finance or air transport. This governance model is the result of a market economy, because the driving force is the private industry.

⁶ The full questionnaire with items and scales is to be found in the appendix or can be downloaded at the following address <https://drive.switch.ch/index.php/s/DgYt2lWZcgVSyMP>

C) *The government model* is typically a country-centered approach focusing on gathering public CIs and cybersecurity agencies, such as governmental computer emergency response team (CERTs). This governance model is often funded by government subsidies where participation is either mandatory or voluntary for both public and private CIs (e.g., mandates stemming from EU directives, such as breach reporting mentioned at the art. 13a of the Telecom Law). This governance model is usually the result of a planned economy, because the driving force is the government.

5. Results

In this section, we present descriptive statistics illustrating an application of our framework in the context of CIP. Using the collected field-data, we investigated correlations between governance model preferences and institutional rules. We extended our pre-analysis to four other control variables in order complement the preferences analysis: Organization size, participations in trust building events, and sector of activity.

5.1 Correlations between Institutional Rules and Governance Model Preferences

Table 1 shows the correlation coefficients between the governance model preferences and the nine rules measured at a micro-level. These latter are represented by proxies that have been gathered through specific psychometric questions.⁷ Our results show relatively low correlations between pre-established institutional rules and human agents' preferences for respective generic governance models, namely PPP-, private-, or government- ISACs. Moreover, only a few correlations (seven out of thirty-six) are statistically significant. Concerning the following rules, namely: 2) Security, 4) Trust, 5) Information exclusivity, PPP are preferred (positive signs). Yet, despite statistically significant results, those correlation coefficients remain at low levels. However, rule 8) Cooperation is highly statistically significant for the PPP preference, despite remaining at a relatively low level as well. This rule also shows a statistically significant correlation coefficient for the Private model preference, but also remains at a low level. Rule 3) Privacy is interestingly showing a negative and

⁷ t-test and analysis of variance (ANOVA) were performed in order to analyze the differences and statistical significance among group means. The detail of those analysis and proxies selection are available upon request from the corresponding author.

PART III: Policy Recommendations

statistically significant correlation between the Government model and the Privacy rule. Despite an also low level, it instinctively indicates trust suspicions between human agents and the government. Due to the correlation coefficients low levels, and the general lack of statistically significant results, at this stage, no direct link between institutional rules and preferred generic governance models can be deducted. Therefore, future work on what defines governance model preferences is needed at the meso-level.

Set of universal rules for SIS	(a) PPP	(b) Private	(c) Government
1) Investment/sharing freedom (Q7)	-0.09	-0.02	0.06
2) Security (Q15)	0.15*	-0.00	-0.03
3) Privacy (Q95)	0.10	0.01	-0.15*
4) Trust (Q16)	0.15*	0.04	-0.09
5) Information exclusivity (Q17)	0.15*	0.05	0.03
6) Financial rewards (Q48)	-0.02	-0.01	0.05
7) Social rewards (Q51)	0.11	0.05	-0.02
8) Cooperation (Q54)	0.26***	0.15	0.03
9a) ID: centralization (Q56)	0.08	0.00	-0.02
9b) ID: decentralization (Q57)	0.06	0.00***	0.12
9c) ID: formalization (Q58)	0.09	0.10	0.00
9d) ID: standardization (Q59)	-0.10	0.06	0.01

Table 1: Governance Model Preferences for Security Information Sharing

This table shows the governance model preferences ($N_1=137$) correlated with a set of rules measured at a micro-level, represented by proxies that have been gathered through specific psychometric questions. Each response score was measured on a scale anchored at 1 (lowest score, e.g., “never”, “not content at all”) to 5 (highest score, e.g. “always”, “highly content”). Hence, the larger the score in the table, the greater the satisfaction or involvement

PART III: Policy Recommendations

with the specific governance model. For corresponding significance levels: * $p < 0.1$, ** $p < 0.05$, *** $p < 0.01$.

5.2 Governance Model Preferences by Organization Size

Fig. 2 shows the governance model preferences ($N_2=260$) related to the organization size. This confirms that PPP-based and private-based governance models are generally preferred. Overall, private-based and PPP-based governance models are preferred. Large organizations (>250 employees) slightly prefer private-based and PPP-based governance models. Such a result can be explained by the fact that larger organizations are likely to be international organizations that are more subject to experiencing more competitive environment, thus are more familiar with a free market setup. As such a setup has the tendency of obeying fewer regulations, a private-based governance model would be a better fit for them. According to their experience, most participants perceive the number of participants in their closed circle to be optimal (45%) and sometimes too large (24%) or too small (31%).

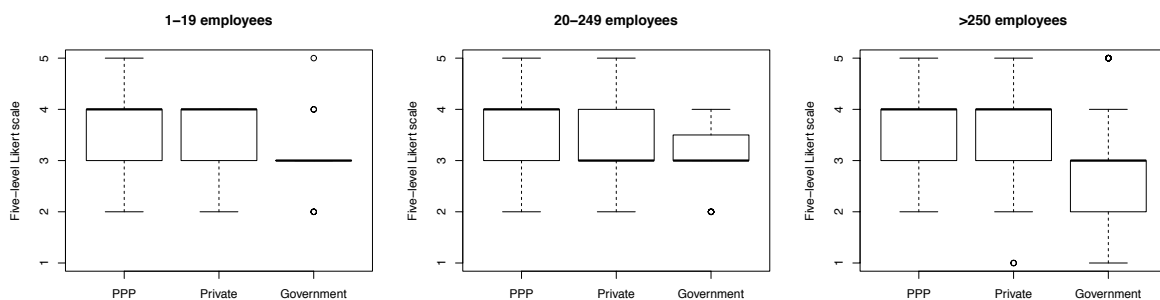


Figure 2: Governance Model Preferences by Organization Size

This figure shows governance model preferences ($N_2=260$) related to the organization size measured by the number of employees. Each response score was measured on a scale from 1 (lowest score, e.g., “strongly disagree”) to 5 (highest score, e.g., “strongly agree”).

5.3 Governance Model Preferences by Participation in Trust Building Events

We measured the governance model preferences ($N_{fa}=260$) related to the participation in trust building events, such as workshops. Each response score was measured on a dichotomous scale anchored at 1 (“Yes”) to 2 (“No”). Our results show no clear differences between governance model preferences between operators who have participated in workshops and those who have

PART III: Policy Recommendations

not. However, participating in such events helps build trust among operators. The slight preference for private-based governance models of operators who have participated in workshops (3.75) with respect to those who have not (3.51) might be explained by this participation in trust building events. They might prefer privately-based SIS or in PPPs (3.70), instead of government-based SIS (2.88) as the trust they create among themselves is not directly related to the government. This shows, however, that the government is important for creating initial trust and setting the rules for a conducive environment for the SIS activity.

5.4 Governance Model Preferences by Sector of Activity

Figure 3 shows sector-wide governance model preferences trends. Surprisingly, among the administration population ($N_3=36$), private-based and PPP-based governance models are preferred over the government-based models. PPP-based models is the most preferred option, and the private-based option is not far behind. Such statistics are relevant as the administration is part of the government. This can be explained by the fact that the information-security expertise of the private sector is an attribute that administrators are keen to take advantage of by sharing the knowledge between the private industry and the government. Among those in the banking and finance population ($N_4=57$), private-based and PPP-based governance models are also preferred with respect to government-based models. Such statistics are not surprising as the banking and finance sector is highly competitive and obeys to a free-market setup. Moreover, a government-based option is the least preferred, corroborating the idea that less regulation is better for that specific sector. In the transport and logistic sector ($N_5=7$), the PPP governance model is the preferred one, probably because this specific industry has a long history of collaboration between the private and public sector. Furthermore, this sector is predominantly composed of fully state-owned limited companies regulated by public law. Further research could investigate the relationship between shareholding and governance model preferences, in order to develop sector-wide tailored policy options.

PART III: Policy Recommendations

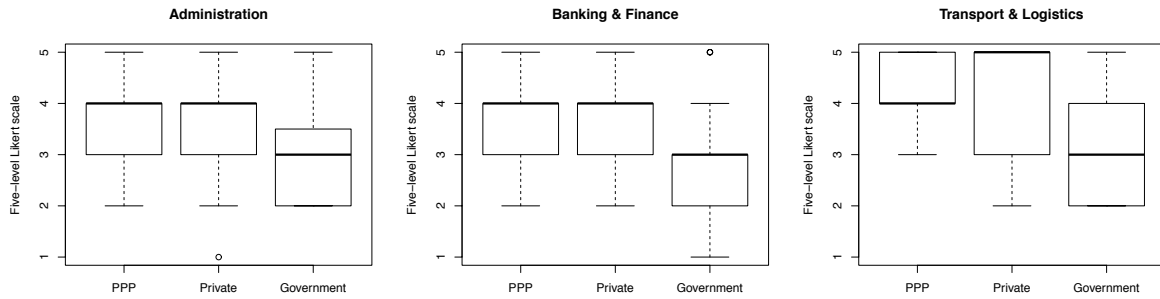


Figure 3: Governance Model Preferences by Sectors

This figure shows sector-wide governance model preferences trends. Each response score was measured on a scale anchored at 1 (lowest score, e.g., “strongly disagree” to 5 (highest score, e.g., “strongly agree”).

6. Concluding Remarks, Limitations and Future Work

To the best of our knowledge, this work is the first study linking institutional rules with a conducive environment that could foster SIS at a meso-level. Using descriptive statistics from a primary set of field-data, we have presented three preferences generic SIS governance models, suggesting how human agents could self-organize SIS if these particular rules are implemented. Our results suggest that a properly designed artifact may positively reinforces human agents to share security information and find the right balance between three governance models. Overall, our work lends support to a better institutional design of SIS and the formulation of policies that can avoid non-cooperative and free-riding behaviors that plague cybersecurity.

This study has some limitations. First, we recognize socioeconomic biases, such as an overrepresentation of male respondents. Second, in some cases we note a tension between the micro-level measurements and some analysis performed at a meso-level. However, the analysis of those two distinct levels is meticulously distinguished. Even though respondents’ answers are measured at a micro-level, their preferences shed some light on their meso-level preferences.

Our research could be extended in several ways. First, our model could be generalized to other contexts, for instance, cross-border information sharing among intelligence agencies, which remains a major pitfall for fusion centers established after the 9/11 attacks [22]. As the presented rules are universal, they could probably be implemented in other cultures and contexts, for instance, in information exchanges between tax authorities. Second, engaging in the SIS economy is not only a matter of incentives and institutional design. As SIS is a human activity (even when partially automatized) that takes place only if it is perceived as effective

PART III: Policy Recommendations

by those who are likely to implement it. A positive performance perception that SIS can bring to information security is thus a sine qua non condition for engaging in SIS. Such a motivational approach could in fine also support the information security of CIs.

7. References

- Bauer, J., & van Eeten, M. (2009). Cybersecurity: Stakeholder incentives, externalities, and policy options. *Telecommunications Policy*, 33(10–11), 706–719. <https://doi.org/10.1016/j.telpol.2009.09.001>
- Boettke, P., Coyne, C., & Leeson, P. (2013). Comparative historical political economy. *Journal of Institutional Economics*, 9(3), 285–301. <https://doi.org/10.1017/S1744137413000088>
- Eden, P., Blyth, A., Burnap, P., Cherdantseva, Y., Jones, K., Soulsby, H., & Stoddart, K. (2015). A Cyber Forensic Taxonomy for SCADA Systems in Critical Infrastructure. In E. Rome, M. Theocharidou, & S. Wolthusen (Eds.), *Critical Information Infrastructures Security* (pp. 27–39). Springer, Cham. https://doi.org/10.1007/978-3-319-33331-1_3
- ENISA. (2015). *Cyber Security Information Sharing: An Overview of Regulatory and Non-regulatory Approaches* (White report). Heraklion: European Union Agency for Network and Information Security. Retrieved from <https://www.enisa.europa.eu/activities/cert/support/information-sharing/cybersecurity-information-sharing>
- ENISA. (2016). *Information sharing and common taxonomies between CSIRTs and Law Enforcement* (White report). Heraklion: European Union Agency for Network and Information Security. Retrieved from <https://www.enisa.europa.eu/publications/information-sharing-and-common-taxonomies-between-csirts-and-law-enforcement>
- ENISA. (2018a). *Information Sharing and Analysis Center (ISACs) - Cooperative models* (White report). Heraklion: European Union Agency for Network and Information Security. Retrieved from <https://www.enisa.europa.eu/publications/information-sharing-and-analysis-center-isacs-cooperative-models>
- ENISA. (2018b). *Public Private Partnerships (PPP) - Cooperative models* (White report). Heraklion: European Union Agency for Network and Information Security. Retrieved from <https://www.enisa.europa.eu/publications/public-private-partnerships-ppp-cooperative-models>
- Furubotn, E. G., & Richter, R. (2005). *Institutions and Economic Theory: The Contribution of the New Institutional Economics*. University of Michigan Press. Retrieved from <http://www.jstor.org/stable/10.3998/mpub.6715>
- Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Zhou, L. (2015). Externalities and the Magnitude of Cyber Security Underinvestment by Private Sector Firms: A Modification of the Gordon-Loeb Model. *Journal of Information Security*, 06(01), 24–30. <https://doi.org/10.4236/jis.2015.61003>
- Gregor, S., & Hevner, A. R. (2013). Positioning and presenting design science research for maximum impact. *MIS Quarterly*, 37(2), 337–355.
- Hayek, F. A. (2005). *The Road to Serfdom*. London: Institute of Economic Affairs.
- Laube, S., & Böhme, R. (2016). The economics of mandatory security breach reporting to

PART III: Policy Recommendations

authorities. *Journal of Cybersecurity*, 2(1), 29–41. <https://doi.org/10.1093/cybsec/tyw002>

Laube, S., & Böhme, R. (2017). Strategic Aspects of Cyber Risk Information Sharing. *ACM Computing Surveys (CSUR)*, 50(5), 77:1–77:36. <https://doi.org/10.1145/3124398>

Luijff, E., & Klaver, M. (2015). On the Sharing of Cyber Security Information. In M. Rice & S. Sheno (Eds.), *Critical Infrastructure Protection IX* (pp. 29–46). Springer. https://doi.org/10.1007/978-3-319-26567-4_3

Luijff, E., Nieuwenhuijs, A., Klaver, M., Eeten, M. van, & Cruz, E. (2008). Empirical Findings on Critical Infrastructure Dependencies in Europe. In R. Setola & S. Geretshuber (Eds.), *Critical Information Infrastructure Security* (pp. 302–310). Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-03552-4_28

Luijff, H. A. M., & Kernkamp, A. C. (2015). *Sharing Cyber Security Information: Good Practice Stemming from the Dutch Public-Private-Participation Approach*. Den Haag: TNO. <https://doi.org/10.13140/RG.2.1.4321.7442>

Mermoud, A., Keupp, M. M., Ghernaouti, S., & Percia David, D. (2016). Using Incentives to Foster Security Information Sharing and Cooperation: A General Theory and Application to Critical Infrastructure Protection. In *Critical Information Infrastructures Security* (pp. 150–162). Springer, Cham. https://doi.org/10.1007/978-3-319-71368-7_13

Mermoud, A., Keupp, M. M., Huguenin, K., Palmié, M., & Percia David, D. (2018). Incentives for Human Agents to Share Security Information: a Model and an Empirical Test. In *17th Workshop on the Economics of Information Security (WEIS)* (pp. 1–22). Innsbruck, Austria. Retrieved from <https://hal.archives-ouvertes.fr/hal-01753984>

Percia David, D., Keupp, M. M., Ghernaouti, S., & Mermoud, A. (2016). Cyber Security Investment in the Context of Disruptive Technologies: Extension of the Gordon-Loeb Model and Application to Critical Infrastructure Protection. In *Critical Information Infrastructures Security* (pp. 296–301). Springer. https://doi.org/10.1007/978-3-319-71368-7_25

PricewaterhouseCoopers (PwC). (2015). *Study and considerations on Information Sharing and Analysis Organizations* (White report). Retrieved from <https://www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/pwc-study-considerations-on-information-sharing-analysis-organizations-final.pdf>

PricewaterhouseCoopers (PwC). (2016). *Information Sharing and Analysis Organizations: Putting theory into practice* (White report). Retrieved from <https://www.pwc.com/us/en/increasing-it-effectiveness/publications/assets/pwc-information-sharing-and-analysis-organizations.pdf>

Prieto, D. B. (2006). Information Sharing with the Private Sector: History, Challenges, Innovation, and Prospects. In *Seeds of Disaster, Roots of Response: How Private Action Can Reduce Public Vulnerability*. Retrieved from <https://www.belfercenter.org/index.php/node/89667>

Richter, R. (2015). *Essays on New Institutional Economics*. Cham: Springer International Publishing. <https://doi.org/10.1007/978-3-319-14154-1>

van Eeten, M., Nieuwenhuijs, A., Luijff, E., Klaver, M., & Cruz, E. (2011). The State and the

PART III: Policy Recommendations

Threat of Cascading Failure Across Critical Infrastructures: The Implications of Empirical Evidence from Media Incident Reports. *Public Administration*, 89(2), 381–400.
<https://doi.org/10.1111/j.1467-9299.2011.01926.x>

Weiss, E. (2015). *Legislation to Facilitate Cybersecurity Information Sharing: Economic Analysis* (CRS Report). Congressional Research Service. Retrieved from <https://horizon.hozint.com/2014/12/crs-legislation-to-facilitate-cybersecurity-information-sharing-economic-analysis/>

Zenger, T., Lazzarini, S. G., & Poppo, L. (2002). Informal and Formal Organization in New Institutional Economics. <http://dx.doi.org/10.2139/ssrn.319300>

CONCLUSION

“A problem shared is a problem halved.”

CONCLUSION

In this dissertation, I have explored several research questions, published as three independent articles. Although the three parts of this thesis have their own conclusions, here, I summarize my main contributions and results, limitations and critical reflections, as well as leads for future work.

1. Main Contributions

For over forty years, economists have analyzed information sharing between organizations, most of the time with the involvement of proxies (e.g., trade associations) (Gal-Or & Ghose, 2005). About twenty years ago, these “old” models were taken up by security economics when information security emerged as a new application domain for economic reasoning (Böhme, 2016; Garrido-Pelaz, Gozalez-Manzano, & Pastrana, 2016). Today, extensive scientific literature confirms that SIS among human agents who operate information systems is conducive for improving the cybersecurity of these systems (Laube & Böhme, 2017). Empirical analysis, however, shows that “sharing centers” (such as ISACs) do not always work optimally (Murdoch & Leaver, 2015).

In order to improve SIS, the technical literature usually focuses on the identification of the correct exchange format, on data models or on the adoption of the right technology (Burger, Goodman, Kampanakis, & Zhu, 2014) or sharing conventions, such as the Traffic Light Protocol.¹ This approach neglects the fact that SIS is a human activity, hence people need incentives to properly use it. My behavioral approach extends the SIS literature with several contributions on the human factor in SIS (Mermoud, Keupp, Ghernaouti, & Percia David, 2016; Mermoud, Keupp, Huguenin, Palmié, & Percia David, 2018; Mermoud, Keupp, & Percia David, 2018); they are provided in three different, but complementary parts listed below.

1.1 Results Synthesis Part I: Theoretical Framework

My first goal was to provide a novel theoretical framework that – based on a thorough literature review – links SIS and selected incentives. SIS is a relatively low-cost and uncomplicated way to give defenders an advantage over attackers, in a context where cybersecurity can be reduced

¹ The Traffic Light Protocol (TLP) was created in the early 2000s by the UK Government's National Infrastructure Security Coordination Centre to encourage greater sharing of sensitive information between individuals and organizations in a trusted and controlled way. Source: <https://www.cpni.gov.uk/> (retrieved 13.03.2019)

CONCLUSION

to an arms race for information. However, SIS is a human activity which is fragile. Its biggest obstacles are not a lack of technology to facilitate information exchange, but economic (dis)incentives. Therefore, in order to better understand the determinants and barriers to SIS, I developed a first theoretical incentive-based and human-centric SIS system model that is based on five propositions which are operationalized into hypothesis in Part II.

1.2 Results Synthesis Part II: Empirical Analysis

My second goal was to operationalize the theory developed in Part I and empirically test my hypotheses, using a psychometric questionnaire answered by 262 firms (with a response rate of 63% of the 424 asked) participating in a Swiss ISAC. The research hypotheses are (1) that sharing has to be reciprocated; (2) that valuable information should be obtained; (3) that there would be low executional costs; (4) there would be a positive effect on reputation; and (5) that sharers would trust each other. Hypothesis 4 was not supported; (1) and (3) were supported strongly, and (2) and (5) were supported to some extent.

1.3 Results Synthesis Part III: Policy Recommendations

My third goal was to formulate policy recommendations that could avoid the non-cooperative and free-riding behaviors that plague SIS. The preferred governance model for SIS is a public-private partnership. Our results also suggest that a properly designed artifact can positively reinforce human agents and encourage them to voluntarily share security information, even in a world where SIS tends to become mandatory through specific regulations (GDPR, NIS directive, CISA, etc.).

2. Limitations and Critical Reflections

Although the three parts of this thesis have their own discussion section, here, I summarize the main overall limitations of the thesis. The three articles in this dissertation are all published or under revision and hence stand as they were published or submitted. This implies that published text cannot be changed, but now as I stand at the end of my dissertation process, some critical reflection that encompasses the entire manuscript is adequate. To this purpose this section is

CONCLUSION

detailed into various points with no particular order that each address an important issue that should be considered in the context with what was published.

An important limitation is that the data collected for this research are cross-sectional, not longitudinal, and hence I can only claim association, but not causation. The thesis manuscript was completely revised after the private defense with this limitation in mind, and any instances that might be interpreted as over-claiming have been removed in the revised version. Instead of such over-claiming, I have now provided more paths for future research whereby future work can refute or corroborate the associations I identify.

In Part I, I attempted to construct a theoretical model on the basis of pure theory and illustration alone. As I attempted to operationalize this model for empirical testing, I researched the empirical literature to identify measures by which I could operationalize my theoretical constructs. This created a problem that theoretical labels not intended by the authors of this measurement were ascribed to them. For example, the scale “attitude” as published by Safa and von Solms (2016) was used with the label “value” in Part II. Also, what Yan et al. (2016) termed “executional costs” I interpreted as “institutional barriers”. I did so in an attempt to align the theoretical model I had constructed in Part I with measurement literature. However, I found that these ascribed levels complicated theory development in Part II and upon due criticism, I decided to use the empirical measures as they were published and reframed from using any ascribed level from my side. This led to a more substantial and profound theoretical foundation of the hypothesis and also prevented inaccurate claims.

As a result, Part II features empirical constructs as they were published under their original name. In this sense, Part I and II are inconsistent in that Part II provides a stronger and better substantiated theoretical model that is also aligned with the empirical literature. Thus, the development of Part I to Part II illustrates the learning process as I advanced my knowledge in behavioral economics, behavioral psychology and research methods.

My dissertation is not a game theoretic piece and hence it does not contribute to analyzing externalities of SIS. In this respect, the introduction of Part I overstates what I can find in my analysis. What I do find however is that human behavior is significantly associated with SIS, which is the more fundamental problem with the current underutilization of SIS. Therefore, it seems to be a lack of focus on the human factor in SIS. As all externalities ultimately reside in human behavior, the understanding of *free-riding* and *underutilization* requires a prior understanding of human behavior.

CONCLUSION

In this sense, my dissertation provides a very first step towards a deeper understanding of the economic effects of SIS. More research is required to further explore how human behavior and SIS outcomes are related ideally by longitudinal approaches which can infer causal relationships and hence bridge the gap between game theoretic work and empirical measurement.

3. Discussion on Policy Recommendations and ISAC organization

By the research design I use, my dissertation does not study reasons why humans would *not* share information. However, it does inform the reader about which behavior and why is associated with SIS. This implies the question of whether or not an individual shares information is more related to the expectation that the individual has for any particular exchange relationship. The empirical results I find in Part II suggest that if the focal individual has trust a positive attitude and expectations will be reciprocated, that individual is likely to share knowledge and to react to information provided by others. Future research should hence enquire into the behavioral causes of the non-sharing of information considering the extent to which any individual poses information that can be shared (if any).

Overall, this PhD thesis provides some food for thoughts regarding the future of SIS. ISACs as we know them today are inherited from the past. For the future, it will be important to mitigate this path dependence and investigate about alternative “information sharing” institutions, which are responsive to human behavior *by design*. Since human behavior is significantly associated with SIS, information sharing organizations must follow human behavior. If the SIS institution is not aligned with human behavior, this institution will not perform well. This touches fundamental aspects of human organizations, which could be theoretically investigated and empirically tested in future work.

My dissertation, in particular Part III, gives some hints of what respondents in my sample think is a conducive environment for SIS and what is not a “good” organization for SIS. Particularly the strong negative correlation I find with the “executional costs” suggest that mandatory sharing is probably not as productive as trying to motivate human agents to cooperate voluntarily.

In the future, alternative ISAC configuration or similar “information sharing institution” could emerge. For instance, an ISAC could be organized according to the private-collective innovation model by von Hippel & von Krogh (2003), i.e. by “crowdsourcing” intelligence

CONCLUSION

from a larger open source community. That way of organizing would be “something in the middle” between state and private ISAC organization, hence could constitute an alternative way of ISAC organization that Part III does not consider. Section 3.2 describes an example of how the future of automated SIS could look like.

4. Outlook

This dissertation opens multiple research opportunities for future work. First, I present two research works (in-progress) that are built on the findings of this dissertation. Second, I investigate new research opportunities based on (meta)data generated by recent SIS regulations.

4.1 The Influence of Agent Behavior on the Perceived Performance of SIS (submitted)

This research project extends the findings in this dissertation by focusing on the perceived performance of SIS, arguing that the extent to which a human agent engages in SIS is a function of their individual performance expectation, i.e., of the net benefit they expect as a result of engaging in SIS. Combining theory with opportunistic action and altruistic punishment, we provide empirical analysis predictors of the perceived performance of SIS. Our results suggest that the frequency of sharing transactions, the perceived utility of resource allocation, reciprocity expectations, and trust have a significant effect on the formation of the perceived performance of SIS. These findings point to several opportunities to motivate human agents to show cooperative behavior. This journal article was accepted (major revisions) in *Computers in Human Behavior*² on the 3rd of January 2019. We are currently revising it and will resubmit it on the 15th of May, 2019:

- Percia David, D., Keupp, M. M., Mermoud, A. (2019). Opportunism is Not Enough: The Influence of Agent Behavior on the Perceived Performance of Security Information Sharing. *Computers in Human Behavior*.

4.2 Setting the Optimal Size of SIS Groups (work-in-progress)

This project is work in-progress explores a neglected area of SIS, specifically the optimal size of SIS groups. Based on the findings of this dissertation, our research group is extending our

² <https://www.journals.elsevier.com/computers-in-human-behavior> (retrieved on 28.10.2018)

CONCLUSION

results by revisiting the Olson's Paradox (Dejean, Pénard, & Suire, 2010) with empirical analysis on the optimal SIS group size among different industries and sectors, in order to furnish tailor-made optimization recommendations according to the environment specifications (i.e., different industries and thus different sharing cultures). Findings could point to several optimization opportunities related to the optimal size of SIS platforms, and ultimately foster the performance of the SIS activity.

Practitioners' experiences suggest that the performance of SIS platforms does not grow linearly with the number of participants. If the shortage of members leads to a weak SIS activity, too many members seems to lead to the same result, due to the lack of trust between participants (inverted U-curve due to oversharing effects). We propose to empirically investigate the influence of the SIS platform size (i.e., the number of members) on the performance of the SIS activity itself (measured by the number of shared cyber incidents/cyber threats in a given SIS platform). To the best of our knowledge, this relationship has never been investigated. Future results could be of interest for both academics and practitioners, as it could shed some light on how to set institutional rules for avoiding congestion, thus enhance and even maximize the SIS performance.

Hypotheses will be tested by using a new dataset from the Open Threat Exchange Platform (OTX),³ the world's largest crowd-sourced computer-security platform with over 80'000 participants who share on average, about 19 million daily cyber threats.

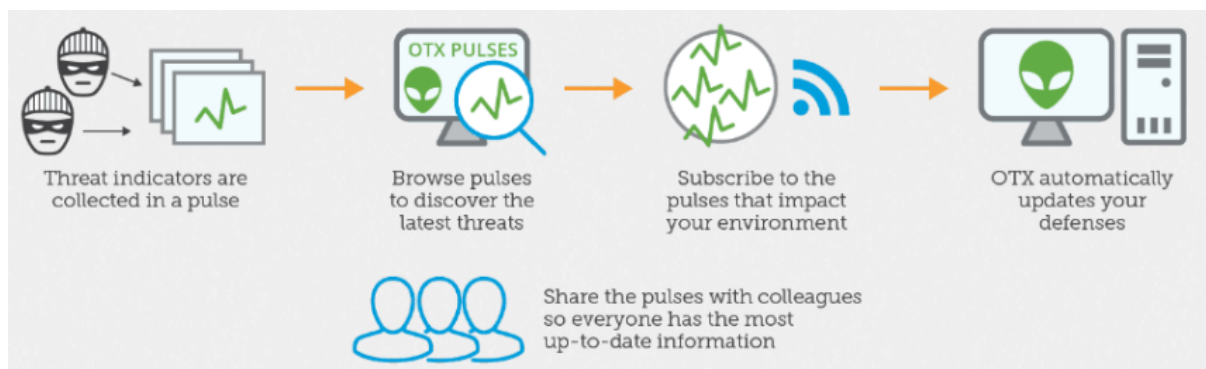


Figure 1: The Open Source OTX Platform Allows the Creation of ISAC-Like Groups

Since 2016, the OTX platform has enabled participants to create private communities and discussions groups in order to share information about cyber threats. Organizations can create their own sector wide "ISAC-like groups" at very little cost, without the administrative burden and institutional barriers associated with "official" ISACs. Source: <https://www.alienvault.com>

³ <https://otx.alienvault.com/> (retrieved 05.11.2018)

CONCLUSION

This platform, acquired in August 2018 by AT&T, is already partially automated and enables interoperability through APIs, as well as the integration of natural language processing and machine learning. The automation of SIS also has the advantage of eliminating or reducing inappropriate human behaviors. In recent years, other private initiatives have come to fill the shortcomings of the ISACs, often considered too slow and too bureaucratic by practitioners.

For instance, Facebook⁴ and IBM⁵ have launched similar threat exchange platforms in recent years. Empirical analysis based on data provided by such platforms could point to several optimization opportunities related to the optimal size of SIS platforms, and ultimately foster the performance of the SIS activity. These findings could be corroborated or falsified by a second phase consisting of setting a lab experiment in order to train and evaluate a classifier. Further research could also use data from SIEM software, such as log files that offer real-time analysis of security alerts, correlation of events, and audit trail. Future results could point to several optimization opportunities related to the optimal size of SIS platforms and aimed at fostering the performance of the SIS activity. This work will be submitted to the 2019 *Workshop on the Economics of Information Security* (WEIS 19),⁶ to be held at Harvard University:

- Percia David, D., Keupp, M. M., Mermoud, A. (2019). Size Does Matter: Setting the Optimal Size of Security Information Sharing Platforms for Fostering Cybersecurity – An Empirical Analysis.

4.3 Empirical Analysis of Mandatory SIS with Authorities (work-in-progress)

As regulators will likely implement new laws to encourage SIS in the future, it would be interesting to empirically analyze the (meta)data generated by the laws intended to foster SIS. For instance, researchers could collaborate with authorities in the EU member states that are already engaged in SIS through article 33 of the GDPR.⁷ In the US and the EU, other major regulatory efforts are underway to strengthen information sharing.

⁴ <https://developers.facebook.com/programs/threatexchange/> (retrieved 05.11.2018)

⁵ <https://exchange.xforce.ibmcloud.com/> (retrieved 05.11.2018)

⁶ <https://weis2019.econinfosec.org> (retrieved on 28.10.2018)

⁷ <http://www.privacy-regulation.eu/en/33.htm> (retrieved 01.11.2018)

CONCLUSION

In Switzerland, following the recent adoption of the National Strategy for Switzerland's protection against cyber risks (NCS),⁸ the Federal Council has begun to work on regulations that would make SIS partially mandatory. In the summer of 2019, a formal decision will be taken for the regulation of SIS in Switzerland.⁹ Economic analysis will be very much needed to shed light onto the effectiveness of such laws, as our current policy recommendations support the view that the effectiveness of mandatory security-breach reporting to authorities is probably limited. Further interdisciplinary research (at the frontier of law and economics) could also explore the privacy / utility trade-off of SIS with authorities, in order to expand the (security) information sharing economics literature.

⁸ https://www.isb.admin.ch/isb/en/home/ikt-vorgaben/strategien-teilstrategien/sn002-nationale_strategie_schutz_schweiz_cyber-risiken_ncs.html (retrieved 01.11.2018)

⁹ <https://www.parlament.ch/fr/ratsbetrieb/suche-curia-vista/geschaeft?AffairId=20183562> (retrieved 01.11.2018)

CONCLUSION

5. References

- Böhme, R. (2016). Back to the Roots: Information Sharing Economics and What We Can Learn for Security. In *Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security - WISCS'16* (pp. 1–2). New York, NY, USA: ACM Press. <https://doi.org/10.1145/2994539.2994540>
- Burger, E. W., Goodman, M. D., Kampanakis, P., & Zhu, K. A. (2014). Taxonomy Model for Cyber Threat Intelligence Information Exchange Technologies. In *Proceedings of the 2014 ACM Workshop on Information Sharing & Collaborative Security* (pp. 51–60). New York, NY, USA: ACM Press. <https://doi.org/10.1145/2663876.2663883>
- Dejean, S., Pénard, T., & Suire, R. (2010). Olson's Paradox Revisited: An Empirical Analysis of incentives to contribute in P2P File-Sharing Communities. <https://doi.org/10.2139/ssrn.1299190>
- Gal-Or, E., & Ghose, A. (2005). The Economic Incentives for Sharing Security Information. *Information Systems Research*, 16(2), 186–208. <https://doi.org/10.1287/isre.1050.0053>
- Garrido-Pelaz, R., Gozalez-Manzano, L., & Pastrana, S. (2016). Shall we collaborate? A model to analyse the benefits of information sharing. Retrieved from <https://arxiv.org/abs/1607.08774>
- Laube, S., & Böhme, R. (2017). Strategic Aspects of Cyber Risk Information Sharing. *ACM Comput. Surv.*, 50(5), 77:1–77:36. <https://doi.org/10.1145/3124398>
- Mermoud, A., Keupp, M. M., Ghernaouti, S., & Percia David, D. (2016). Using Incentives to Foster Security Information Sharing and Cooperation: A General Theory and Application to Critical Infrastructure Protection. In *Critical Information Infrastructures Security* (pp. 150–162). Springer, Cham. https://doi.org/10.1007/978-3-319-71368-7_13
- Mermoud, A., Keupp, M. M., Huguenin, K., Palmié, M., & Percia David, D. (2018). Incentives for Human Agents to Share Security Information: a Model and an Empirical Test. In *17th Workshop on the Economics of Information Security (WEIS)* (pp. 1–22). Innsbruck, Austria. Retrieved from <https://hal.archives-ouvertes.fr/hal-01753984>
- Mermoud, A., Keupp, M. M., & Percia David, D. (2018). Governance Models Preferences for Security Information Sharing: An Institutional Economics Perspective for Critical Infrastructure Protection (Vol. Lectures Notes in Computer Science (LNCS)). Presented at the In Proceedings of the 13th International Conference on Critical Information Infrastructures Security (CRITIS), Kaunas, Lithuania: Springer.
- Murdoch, S., & Leaver, N. (2015). Anonymity vs. Trust in Cyber-Security Collaboration. In *Proceedings of the 2Nd ACM Workshop on Information Sharing and Collaborative Security* (pp. 27–29). New York, NY, USA: ACM. <https://doi.org/10.1145/2808128.2808134>
- Safa NS, von Solms R. An information security knowledge sharing model in organizations. *Computers in Human Behavior* 2016;57:442–51.
- Yan Z, Wang T, Chen Y et al. Knowledge sharing in online health communities: A social exchange theory perspective. *Information & Management* 2016;53:643–53.

APPENDIX

1. Resume – Dr. Alain Mermoud

As a PhD candidate, Alain Mermoud worked under the co-supervision of PD Dr. Marcus Matthias Keupp (ETH Zurich) and Prof. Kévin Huguenin (UNIL). He started his PhD research in 2015, while working as a scientific collaborator at the department of Defense Management at the Military Academy (MILAC) at ETH Zurich. Prior to that, he worked 5+ years in the banking industry, including at the Bank for International Settlements in Basel and at the Credit Suisse Economic Research department in Zurich. He earned his MSc in Business Administration in 2011 and his BSc in Information Science in 2008 from the University of Applied Sciences Western Switzerland as a Hirschmann-scholarshipholder.

Professional Courses

- **Lecturer** at ETH Zurich, Business Administration and Cyber Defense Management, fall semester 2018
- **Invited Lecturer** at the University of Geneva, Master of Advanced Studies (MAS) in Global Security and Conflict Resolution, Geneva, 2017 – present
- **Scientific Collaborator**, Department of Defense Management, Military Academy at ETH Zurich, Nov. 2014 – present
- **Member of the Board (President since Mai 2018)**, The Swiss Association for Market Research, Competitive Intelligence and Strategic Planning, Swisintell.org, Bern, 2013 – present
- **Senior Information Specialist (Vice-President)**, Credit Suisse AG, Economic Research / Private Banking, Zurich, Jun. 2011 – Mar. 2015
- **Intelligence Officer (Captain)**, Military Intelligence Service, Bern, Jul. 2014 – present
- **Information Specialist (Deputy Secretary General)**, Bibliothek Information Schweiz, Bern, Apr. 2010 – Mai 2011
- **Information Specialist (Analyst)**, Bank for International Settlements, Basel, Oct. 2008 – Apr. 2009

Education (Swiss matriculation number: 03579562)

- **PhD**, Information Systems, Faculty of Business and Economics (HEC Lausanne) of the University of Lausanne, 2015 – 2019
- **MBA**, Strategic Management and Business Intelligence (MSIE 19), ESLSCA Business School Paris, 2013 – 2014
- **MSc**, Business Administration, University of Applied Sciences Western Switzerland, 2009 – 2011
- **BSc**, Information Science, University of Applied Sciences Western Switzerland, 2004 – 2008
- **Certificat Fédéral de Capacité (CFC) de Médiaticien avec Maturité Professionnelle Commerciale (MPC)**, Centre Professionnel du Nord Vaudois, 1998 – 2002

APPENDIX

Full Publication List and On-line Profiles

- Information Security and Privacy Lab at the University of Lausanne
<https://people.unil.ch/kevinhuguenin/members/alain-mermoud>
- Department of Defense management at the Military Academy at ETH Zurich
<http://tiny.cc/n6pp1y>
- ResearchGate
https://www.researchgate.net/profile/Alain_Mermoud
- LinkedIn
<https://www.linkedin.com/in/alainmermoud>
- ORCID
<https://orcid.org/0000-0001-6471-772X>
- QR code to ORCID public record with full profile & scientific publications



Contact details

- ✉ ProtonMail end-to-end encrypted email: alain.mermoud@protonmail.com
- ✉ Gmail homemade address: gmail@alain-mermoud.ch
- ☎ Threema end-to-end encrypted voice calls and instant messaging: +4179 335 39 17

2. Online Questionnaire

07/12/2017

Last page

Incentives and Security Information Sharing

This study is endorsed by :



Pascal Lamia
Head of MELANI

pascal.lamia@isb.admin.ch
058 463 45 06



Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra



PD Dr. Marcus M. Keupp
Head of Defense Management

mkeupp@ethz.ch
058 484 82 47



Alain Mermoud, PhD candidate
Study leader

alain.mermoud@milak.ethz.ch
058 484 82 99

You can verify the authenticity of this study and the identity of the authors on the official website of their institutions

[Pascal Lamia](#) (Swiss Confederation)
[Marcus Matthias Keupp](#) (Military Academy at ETH Zurich)
[Alain Mermoud](#) (Military Academy at ETH Zurich)

Or by calling MELANI +4158 46 34506

Dear member of the MELANI closed circle,
Sehr geehrte Mitglieder des "Geschlossenen Kundenkreises" (GK),
Chers membres du cercle fermé,

We are doing a research study in the domain of human aspects of security information sharing in organisations. We would like to understand your incentives and barriers to cybersecurity-relevant information sharing with the Swiss Reporting and Analysis Centre for Information Assurance (MELANI). Your responses will be extremely valuable to build a safer and more resilient Cyberspace. Please find below some information on:

The authors

- This survey is being conducted by the military academy at ETH Zurich with the support of MELANI
- Data collection is led by PD Dr. Marcus M. Keupp and his assistant Alain Mermoud, who is a PhD candidate at the University of Lausanne

The data

- All your responses are collected in Switzerland and treated strictly anonymously

<https://www.selectsurvey.ethz.ch/Print.aspx?SurveyID=78L24661&Title=Y&Breaks=N&AllPages=Y&Pages=>

1/10

APPENDIX

07/12/2017

Last page

- The collected data will be deleted after all analyses have been performed
- This survey is purely academic and has no financial or business-related interest

Your reward

- You will receive a free study which will support your organisation in the security information sharing process
- Upon request, you will be delivered with a precise picture of how your organisation compares to others. If you decide to receive this reward, only your e-mail address will be disclosed to the study leader.

The questionnaire

- The template is responsive, but we strongly recommend to answer the survey on a desktop or laptop with a trustworthy Internet connection
- The questionnaire takes about 15-20 minutes to complete
- The questionnaire is only available in English, but the study leader can support you in French and German
- Please direct any questions directly to alain.mermoud@milak.ethz.ch or +4158 484 82 99

Definition and scope

- Security information sharing is an activity consisting of sharing cybersecurity-relevant information between cybersecurity stakeholders. For the sake of brevity, we will refer to this activity as "security information sharing" (SIS) throughout the questionnaire
- Organisations typically exchange information on vulnerabilities, phishing, malware, and data breaches, as well as threat intelligence, best practices, early warnings, and expert advices and insights (Luijck & Klaver, 2015)
- Please note that this study attempts to capture your SIS activities with MELANI only. Please ignore other SIS activities, such as SIS with other Information Sharing and Analysis Centers (ISACs) or bilateral SIS
- The unit of analysis is yourself. **Please answer the questions based on your personal experiences, and not on behalf of your organisation!**

Incentives and Security Information Sharing

Controls

Control variables are necessary to eliminate distortions.

Please answer the questions based on your personal experiences, and not on behalf of your organisation!

1. Gender*

- Male Female

Other, please specify

2. What is your mother tongue?*

- German French English Italian

Other, please specify

3. What is your age group?*

- Below 21 21 to 30 31 to 40 41 to 50 above 50

4. Which education level did you achieve?*

- No education Diploma Bachelor Master PhD

Other, please specify

5. What is your position in your organisation?*

- Employee Chief employee Middle management Management Member of the board

Other, please specify

6. In which field does your organisation operate?*

Chemical / Pharmaceutical

<https://www.selectsurvey.ethz.ch/Print.aspx?SurveyID=78L24661&Title=Y&Breaks=N&AllPages=Y&Pages=>

2/10

APPENDIX

07/12/2017

Last page

- - Banking & Finance
 - Administration
 - Energy
 - Telecommunication / IT
 - Insurance
 - Transport and logistic
 - Industry
 - Health
 - Other, please specify
-

7. How many years have you overseen Security Information Sharing (SIS)?*
- Not in charge less than 1 1 to 3 3 to 6 over 6
8. What is the workload related to SIS in your organisation (in full-time equivalent)?*
- 0
 0-1
 1-2
 2-3
 over 3
9. How would you rate your general level of IT knowledge*
- Excellent Good Neutral Fair Poor
10. How many people work in your organisation?*
- 1 1 - 20 20 - 100 100 - 250 over 250
11. In which year did your organisation become a member of MELANI?*
-
12. Have you participated in MELANI workshops / events?*
-
13. What is the level of IT outsourcing in your organisation?*
- Very Significant Significant Neutral Insignificant Very Insignificant
14. What is the level of internationalisation of your organisation (shareholding, clients, subsidiaries, etc.)?*
- Very Significant Significant Neutral Insignificant Very Insignificant
15. What is your level of satisfaction with MELANI services?*
- Very Satisfied Satisfied Neutral Dissatisfied Very Dissatisfied
16. How are your personal relationships with your peers (other MELANI participants)?*
- Very Friendly Friendly Neutral Unfriendly Very Unfriendly
17. Which amount of exclusive information do you receive through SIS with MELANI?
- Very Small Small Neutral Large Very Large

Incentives and Security Information Sharing

Frequency

<https://www.selectsurvey.ethz.ch/Print.aspx?SurveyID=78L24661&Title=Y&Breaks=N&AllPages=Y&Pages=>

3/10

APPENDIX

07/12/2017

Last page

Please answer the questions based on your personal experiences, and not on behalf of your organisation!

18. Generally, I have a lot of information to share*
- Strongly Agree Agree Neutral Disagree Strongly Disagree
19. I frequently share my experience about information security with MELANI*
- Strongly Agree Agree Neutral Disagree Strongly Disagree
20. I frequently share my information security knowledge with MELANI*
- Strongly Agree Agree Neutral Disagree Strongly Disagree
21. I frequently share my information security documents with MELANI*
- Strongly Agree Agree Neutral Disagree Strongly Disagree
22. I frequently share my expertise from my information security training with MELANI*
- Strongly Agree Agree Neutral Disagree Strongly Disagree
23. I frequently talk with others about information security incidents and their solutions in MELANI workshops*
- Strongly Agree Agree Neutral Disagree Strongly Disagree
24. I share a new information with other participants*
- Never
- Rarely, in less than 10% of the chances when I could have
- Occasionally, in about 30% of the chances when I could have
- Sometimes, in about 50% of the chances when I could have
- Frequently, in about 70% of the chances when I could have
- Usually, in about 90% of the chances I could have
- Every time

Incentives and Security Information Sharing

Intensity

Please answer the questions based on your personal experiences, and not on behalf of your organisation!

25. How often do you comment on shared information?*
- Never
- Rarely, in less than 10% of the chances when I could have
- Occasionally, in about 30% of the chances when I could have
- Sometimes, in about 50% of the chances when I could have
- Frequently, in about 70% of the chances when I could have
- Usually, in about 90% of the chances I could have
- Every time
26. How intensely do you react to the comments of other participants?*
- Not at all
- Little
- Moderate
- Significant
- Always

27. I often react to comments in the community*

<https://www.selectsurvey.ethz.ch/Print.aspx?SurveyID=78L24661&Title=Y&Breaks=N&AllPages=Y&Pages=>

4/10

APPENDIX

07/12/2017

Last page

- Strongly Agree Agree Neutral Disagree Strongly Disagree
28. I often use the community to provide comments*
- Strongly Agree Agree Neutral Disagree Strongly Disagree
29. I comment in the community as much as possible*
- Strongly Agree Agree Neutral Disagree Strongly Disagree
30. I am very interested in sharing knowledge with MELANI*
- Strongly Agree Agree Neutral Disagree Strongly Disagree
31. I usually spend a lot of time reacting to comments*
- Strongly Agree Agree Neutral Disagree Strongly Disagree
32. I usually actively share my knowledge with MELANI*
- Strongly Agree Agree Neutral Disagree Strongly Disagree

Incentives and Security Information Sharing

Value of information

Please answer the questions based on your personal experiences and not on behalf of your organisation!

33. I believe SIS is a useful behavioral tool to safeguard the organization's information assets*
- Strongly Agree Agree Neutral Disagree Strongly Disagree
34. My SIS has a positive effect on mitigating the risk of information security breaches*
- Strongly Agree Agree Neutral Disagree Strongly Disagree
35. SIS is a wise behavior that decreases the risk of information security incidents*
- Strongly Agree Agree Neutral Disagree Strongly Disagree
36. SIS would decrease the time needed for my job responsibilities*
- Strongly Agree Agree Neutral Disagree Strongly Disagree
37. SIS would increase the effectiveness of performing job tasks*
- Strongly Agree Agree Neutral Disagree Strongly Disagree
38. Considering all aspects, SIS would be useful*
- Strongly Agree Agree Neutral Disagree Strongly Disagree
39. I can't seem to find the time to share knowledge in the community*
- Strongly Agree Agree Neutral Disagree Strongly Disagree
40. It is laborious to share knowledge in the community*
- Strongly Agree Agree Neutral Disagree Strongly Disagree
41. It takes me too much time to share knowledge in the community*
- Strongly Agree Agree Neutral Disagree Strongly Disagree
42. The effort is high for me to share knowledge in the community*

<https://www.selectsurvey.ethz.ch/Print.aspx?SurveyID=78L24661&Title=Y&Breaks=N&AllPages=Y&Pages=>

5/10

APPENDIX

07/12/2017

Last page

Strongly Agree Agree Neutral Disagree Strongly Disagree

Incentives and Security Information Sharing

Reciprocity

Please answer the questions based on your personal experiences and not on behalf of your organisation!

43. I believe that it is fair and obligatory to help others because I know that other people will help me some day*
 Strongly Agree Agree Neutral Disagree Strongly Disagree
44. I believe that other people will help me when I need help if I share knowledge with others through MELANI*
 Strongly Agree Agree Neutral Disagree Strongly Disagree
45. I believe that other people will answer my questions regarding specific information and knowledge in the future if I share knowledge with others through MELANI*
 Strongly Agree Agree Neutral Disagree Strongly Disagree
46. I think that people who are involved with MELANI develop reciprocal beliefs on give and take based on other people's intentions and behavior*
 Strongly Agree Agree Neutral Disagree Strongly Disagree
47. I expect to be rewarded with a higher salary in return for sharing knowledge with other participants*
 Strongly Agree Agree Neutral Disagree Strongly Disagree
48. I expect to receive monetary rewards (i.e. additional bonus) in return for sharing knowledge with other participants*
 Strongly Agree Agree Neutral Disagree Strongly Disagree
49. I expect to receive opportunities to learn from others in return for sharing knowledge with other participants*
 Strongly Agree Agree Neutral Disagree Strongly Disagree
50. I expect to be rewarded with an increased job security in return for sharing knowledge with other participants*
 Strongly Agree Agree Neutral Disagree Strongly Disagree
51. My acts of knowledge sharing and seeking strengthen the ties of obligation between existing participants*
 Strongly Agree Agree Neutral Disagree Strongly Disagree
52. My acts of knowledge sharing and seeking create the obligations with other members within MELANI*
 Strongly Agree Agree Neutral Disagree Strongly Disagree
53. My acts of knowledge sharing and seeking expand the scope of my association with other members within MELANI*
 Strongly Agree Agree Neutral Disagree Strongly Disagree
54. My acts of knowledge sharing and seeking will encourage cooperation among MELANI participants in the future*
 Strongly Agree Agree Neutral Disagree Strongly Disagree
55. My acts of knowledge sharing and seeking create strong relationships with members who have common interests within MELANI*
 Strongly Agree Agree Neutral Disagree Strongly Disagree

APPENDIX

07/12/2017

Last page

Incentives and Security Information Sharing

Institutional design

Please answer the questions based on your personal experiences and not on behalf of your organisation!

56. A centralized sharing model - such as a relational database like a forum - would allow me to engage in more SIS activities*
- Strongly Agree Agree Neutral Disagree Strongly Disagree
57. A decentralized sharing model - such as a distributed database like blockchain - would encourage me to engage in more SIS activities*
- Strongly Agree Agree Neutral Disagree Strongly Disagree
58. Formalization would allow me to engage in more SIS activities*
Formalization is the extent to which work roles are structured in an organization, and the activities of the employees are governed by rules and procedures.
- Strongly Agree Agree Neutral Disagree Strongly Disagree
59. Standardization would allow me to engage in more SIS activities*
Standardization is the process of implementing and developing technical standards based on the consensus of different parties.
- Strongly Agree Agree Neutral Disagree Strongly Disagree
60. SIS is of value in my organization*
- Strongly Agree Agree Neutral Disagree Strongly Disagree
61. The management appreciates employees for their SIS*
- Strongly Agree Agree Neutral Disagree Strongly Disagree
62. The management awards employees for their SIS*
- Strongly Agree Agree Neutral Disagree Strongly Disagree
63. The management encourages employees to utilise SIS*
- Strongly Agree Agree Neutral Disagree Strongly Disagree

Incentives and Security Information Sharing

Reputation

Please answer the questions based on your personal experiences and not on behalf of your organisation!

64. Sharing knowledge can enhance my reputation in the community*
- Strongly Agree Agree Neutral Disagree Strongly Disagree
65. I get praises from others by sharing knowledge in the community*
- Strongly Agree Agree Neutral Disagree Strongly Disagree
66. I feel that knowledge sharing improves my status in the community*
- Strongly Agree Agree Neutral Disagree Strongly Disagree

67. I can earn some feedback or rewards through knowledge sharing that represent my reputation and status in the community*

<https://www.selectsurvey.ethz.ch/Print.aspx?SurveyID=78L24661&Title=Y&Breaks=N&AllPages=Y&Pages=>

7/10

APPENDIX

07/12/2017

Last page

- community*
- Strongly Agree Agree Neutral Disagree Strongly Disagree
68. My colleagues respect me when I share my information security knowledge*
 Strongly Agree Agree Neutral Disagree Strongly Disagree
69. The others have a positive opinion when I share my information security knowledge*
 Strongly Agree Agree Neutral Disagree Strongly Disagree
70. The management asked me to help others in terms of information security*
 Strongly Agree Agree Neutral Disagree Strongly Disagree
71. Employees have a positive image about me due to their evaluation of my information security knowledge*
 Strongly Agree Agree Neutral Disagree Strongly Disagree

Incentives and Security Information Sharing

Trust

Please answer the questions based on your personal experiences and not on behalf of your organisation!

72. I believe that my colleague's information security knowledge is reliable*
 Strongly Agree Agree Neutral Disagree Strongly Disagree
73. I believe that my colleague's information security knowledge is effective*
 Strongly Agree Agree Neutral Disagree Strongly Disagree
74. I believe that my colleague's information security knowledge mitigates the risk of information security breaches*
 Strongly Agree Agree Neutral Disagree Strongly Disagree
75. I believe that my colleague's information security knowledge is useful*
 Strongly Agree Agree Neutral Disagree Strongly Disagree
76. I believe that my colleagues would not take advantage of my information security knowledge that we share*
 Strongly Agree Agree Neutral Disagree Strongly Disagree
77. I believe that people in my network give credit for each other's knowledge where it is due*
 Strongly Agree Agree Neutral Disagree Strongly Disagree
78. I believe that people in my network respond when I am in need*
 Strongly Agree Agree Neutral Disagree Strongly Disagree
79. I believe that people in my network use each other's knowledge appropriately*
 Strongly Agree Agree Neutral Disagree Strongly Disagree
80. I believe that my requests for knowledge will be answered*
 Strongly Agree Agree Neutral Disagree Strongly Disagree
81. I believe that people in my network share the best knowledge that they have*
 Strongly Agree Agree Neutral Disagree Strongly Disagree

APPENDIX

07/12/2017

Last page

Incentives and Security Information Sharing

You are almost at the end of the survey

Please answer the questions based on your personal experiences and not on behalf of your organisation!

82. SIS satisfies my desire for acquiring information security skills*
 Strongly Agree Agree Neutral Disagree Strongly Disagree
83. SIS satisfies my sense of curiosity*
 Strongly Agree Agree Neutral Disagree Strongly Disagree
84. I enjoy it when I gain knowledge about information security through knowledge sharing*
 Strongly Agree Agree Neutral Disagree Strongly Disagree
85. I feel pleasure when I share my knowledge about information security*
 Strongly Agree Agree Neutral Disagree Strongly Disagree
86. I am interested in SIS*
 Strongly Agree Agree Neutral Disagree Strongly Disagree
87. I have the necessary knowledge about information security to share with the other staff*
 Strongly Agree Agree Neutral Disagree Strongly Disagree
88. I have the ability to share information security knowledge to mitigate the risk of information security breaches*
 Strongly Agree Agree Neutral Disagree Strongly Disagree
89. SIS is an easy and enjoyable task for me*
 Strongly Agree Agree Neutral Disagree Strongly Disagree
90. I have the useful resources to share SIS with the other employees*
 Strongly Agree Agree Neutral Disagree Strongly Disagree
91. I am willing to share my information security knowledge because of its potential to reduce cyber risks*
 Strongly Agree Agree Neutral Disagree Strongly Disagree
92. I will share my information security experiences with my colleagues to increase their cyber threat awareness*
 Strongly Agree Agree Neutral Disagree Strongly Disagree
93. I will inform the other staff about new methods and software that can reduce the risk of information security*
 Strongly Agree Agree Neutral Disagree Strongly Disagree
94. I will share the report on information security incidents with others, in order to reduce the risk*
 Strongly Agree Agree Neutral Disagree Strongly Disagree

Incentives and Security Information Sharing

<https://www.selectsurvey.ethz.ch/Print.aspx?SurveyID=78L24661&Title=Y&Breaks=N&AllPages=Y&Pages=>

9/10

APPENDIX

07/12/2017

Last page

Last page

Please answer the questions based on your personal experiences and not on behalf of your organisation!

95. According to your experience, the number of participants in the MELANI closed circle is*

- Very Small Small Neutral Large Very Large

96. I prefer to engage in SIS activities that involves participants from the entire Critical Infrastructure closed circle ("Geschlossene Kundenkreis" / "cercle fermé")*

- Strongly Agree Agree Neutral Disagree Strongly Disagree

97. I prefer to engage in SIS activities that involves participants from my industry*

- Strongly Agree Agree Neutral Disagree Strongly Disagree

98. I prefer to engage in SIS activities that involves participants from the MELANI staff only*

- Strongly Agree Agree Neutral Disagree Strongly Disagree

99. Do you want to leave a general comment on this study?

For instance, you can describe your personal incentives and barriers to engage in SIS activities or your favorite service provided by MELANI.

100. Upon request, you will be delivered with a precise picture of how your organisation compares to others. If you decide to receive this reward, please enter your e-mail address below. It will only be disclosed to the study leader.

Again, thank you very much for your cooperation! Best regards,
Alain Mermoud, PhD candidate
Study leader
alain.mermoud@milak.ethz.ch
+4158 484 82 99

APPENDIX

3. Certificate of Achievement Economics of Cybersecurity



4. Certificate from the UNIL Graduate Campus

