Incentives for Human Agents to Share Security Information: a Model and an Empirical Test

Alain Mermoud, Marcus Matthias Keupp, Kévin Huguenin, Maximilian Palmié, Dimitri Percia David

▶ **To cite this version:**

Alain Mermoud, Marcus Matthias Keupp, Kévin Huguenin, Maximilian Palmié, Dimitri Percia David. Incentives for Human Agents to Share Security Information: a Model and an Empirical Test. 17th Workshop on the Economics of Information Security (WEIS), Jun 2018, Innsbruck, Austria. pp.22. hal-01753984

HAL Id: hal-01753984
https://hal.science/hal-01753984

Submitted on 25 May 2018

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Incentives for Human Agents to Share Security Information: a Model and an Empirical Test

Alain Mermoud[1,2,*], Marcus Matthias Keupp[2,3], Kévin Huguenin[1], Maximilian Palmié[3], and Dimitri Percia David[1,2]

[1]Department of Information Systems, Faculty of Business and Economics (HEC Lausanne), University of Lausanne (UNIL), 1015 Lausanne, Switzerland; [2]Department of Defence Management, Military Academy at ETH Zurich, 8903 Birmensdorf, Switzerland; [3]Institute of Technology Management, University of St. Gallen, Dufourstrasse 40a, 9000 St. Gallen, Switzerland.

*Corresponding author: E-mail: alain.mermoud@unil.ch

Abstract

In this paper, we investigate the role of incentives for Security Information Sharing (SIS) between human agents working in institutions. We present an incentive-based SIS system model that is empirically tested with an exclusive dataset. The data was collected with an online questionnaire addressed to all participants of a deployed Information Sharing and Analysis Center (ISAC) that operates in the context of critical infrastructure protection (N=262). SIS is measured with a multidimensional approach (intensity, frequency) and regressed on five specific predicators (reciprocity, value of information, institutional barriers, reputation, trust) that are measured with psychometric scales. We close an important research gap by providing, to the best of our knowledge, the first empirical analysis on previous theoretical work that assumes SIS to be beneficial. Our results show that institutional barriers have a strong influence on our population, i.e., SIS decision makers in Switzerland. This lends support to a better institutional design of ISACs and the formulation of incentive-based policies that can avoid non-cooperative and free-riding behaviours. Both frequency and intensity are influenced by the extent to which decision makers expect to receive valuable information in return for SIS, which supports the econometric structure of our multidimensional model. Finally, our policy recommendations support the view that the effectiveness of mandatory security-breach reporting to authorities is limited. Therefore, we suggest that a conducive and lightly regulated SIS environment – as in Switzerland – with positive reinforcement and indirect suggestions can "nudge" SIS decision makers to adopt a productive sharing behaviour.

Key words: security information sharing; incentives; psychometrics; economics of information security; behavioural economics

1. Introduction

The vital importance of information systems in almost every aspect of human life implies the need for investment in the security of the systems. However, in practice, such cybersecurity investments hardly ever reach their theoretical optimum [1,3]. This under-investment causes substantial economic costs, risks, and welfare losses [2] and threatens national security [3]. To alleviate this problem, cybersecurity research proposes that security information sharing (SIS) among human agents should increase cybersecurity investment because such sharing would increase information efficiency hence lower investment costs for any given level of cybersecurity [3].

SIS is an activity consisting of human agents exchanging cybersecurity-relevant information, such as vulnerabilities, phishing, malware, and data breaches, as well as threat intelligence analysis, best practices, early warnings, expert advice and general insights [4]. This activity is typically organized in processes on public-private platforms (or forums) provided by Information Sharing and Analysis Centers (ISACs).[2] Further studies confirm the positive results of such cooperation for both individual human agents [1,5], government authorities [6], market values of firms in the private sector [7], and economic welfare in general [8].

Several game-theoretic models investigate the benefits of SIS for individual agents [3,5]. Game theory strategies, such as "tit-for-tat" (an effective strategy for the iterated prisoner's dilemma) suggest positive outcome for SIS, whereas empirical validation is often missing [9,10]. We close an important research gap by providing the first-ever empirical analysis based on a psychometric approach to previous theoretical work that assumes SIS to be beneficial. For our study, we secured access to a Swiss ISAC that has organized SIS between critical infrastructure (CI) operators (our population) since 2005. This organization – MELANI[3] – is a Swiss government-organized ISAC that aims to improve the cybersecurity level of CI operators by encouraging them to share security-relevant information.

SIS also likely reduces information asymmetry costs that defenders of information systems face, making it particularly relevant in the context of the detection of zero-day vulnerabilities [8]. Collective intelligence and crowdsourcing studies have shown that organizations which cooperate in cyberdefence activities have greater threat awareness [12]. Any individual human agent can likely reduce the cost of attaining the optimal level of cybersecurity investment when they engage in SIS [13], hence any particular agent should have a strong motivation to act accordingly.

Cybersecurity threats are particularly relevant for critical infrastructure operators due to the extent of the potential loss due to business interruption, physical damage, and collateral damage for the population and economy as a whole. The capacity of a modern society to preserve the conditions of its existence is intimately linked to the proper operation of its critical infrastructures. Cybersecurity concerns are the main challenge faced by the operators of such infrastructures, not least because of the high degree of interconnection [14]. This raises the threat of a so-called "cyber subprime scenario", i.e., a cascading series of failures from an attack that aims to exploit this interconnectivity.[4] Because of this situation, many agents

[2] ISACs have been introduced following the Presidential Decision Directive-63 (PDD-63) in 1998. PDD-63 recognized the potential for the critical infrastructures of the USA to be attacked either through physical or cyber means with the intent to affect the military or economic power of the country.

[3] The Reporting and Analysis Centre for Information Assurance (Melde- und Analysestelle Informationssicherung - MELANI) is a public-private-partnership (PPP) that gathers Swiss critical infrastructures and other partners active in the area of information systems and Internet security.

[4] In a 2014 report, the Atlantic Council and Zurich Insurance revealed that the interconnected 2008 global financial crisis bears several resemblances to what could happen in a major cyber "risk nexus" scenario (Atlantic Council, Zurich Insurance, Risk Nexus Report, 2014).

interested in sharing security information can likely be found in this context, such that data availability was facilitated. Indeed, prior research has highlighted the potential contribution of SIS to critical infrastructure protection [9].

The remainder of this paper is structured as follows: Section 2 surveys related work and connects different streams of theories in order to link SIS and incentives. A system model and various hypotheses are presented in Section 3. The research methodology, the data collection process, and the demography of the participants are described in Section 4. Detailed results and the corresponding insights are presented in Section 5; the tables containing the raw results in full can be found in the appendix. The conclusion, limitations, and future work are described in Section 6.

2. Related Work

In this section, we survey works related to SIS in four main categories.

Free-Riding

Human cooperation is fraught with negative externalities that cannot be completely internalized. A particular human agent may benefit by receiving information from others while refusing to share such information, making him or her free-ride on the value of security information provided by others. As other agents anticipate this behaviour, they would refuse to share such information. As a result, a Nash-stable, yet inefficient, equilibrium emerges in which each cybersecurity agent attempts to free-ride on the investments of others. Hence, the overall level of SIS would be low and cybersecurity investment would – again – fail to attain its efficient optimum [16,17]. As a result, the global level of cybersecurity in the economy is unlikely to ever reach its theoretical optimum, unless human agents are incentivized to mutually participate in SIS activities [10,14,15,17].

Link between SIS and Incentives

Therefore, the under-investment problem cannot be alleviated unless human agents are provided with appropriate incentives to engage in SIS [19]. Recent research has therefore stressed the need to study the link between incentives and SIS [12, 27]. A theoretical understanding of which incentives would encourage humans to engage in SIS (and why) is required to solve the cybersecurity investment problem [8,13,20,21]. However, to the best of our knowledge, such contributions do not yet exist as of today. This paper therefore constitutes a first attempt to propose a theory linking incentives and SIS, and to empirically test this theory. In principle, human agents can be motivated positively (i.e., with rewards if they behave in the desired way) or negatively (by forcing them to comply and threatening them with punishment if they do not). As a result, incentives for SIS can be provided either positively, by increasing the economic and social rewards reaped when agents share security information, or negatively, by punishing agents that fail to share [22–24].[5]

Regulation

To date, governments have experimented with regulation, by attempting to force government institutions and private sector firms to engage in SIS and by defining sanctions for failing to

[5] 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 [9].

comply. However, reviews suggest that such regulatory attempts, as well as "walls of shame"[6], did not seem to produce the desired effect of increased SIS [3,11,22,23,24]. This disappointing result might be due to the effect that, when forced to share security information, human agents choose to share irrelevant or incomplete information, especially so if they are compelled to share information with competitors [26]. This regulatory failure does not seem to be country-specific, as regulatory attempts in other countries have also produced limited results [27].

Model

Our theoretical system model focuses on a positive reinforcement: we argue that SIS will increase if agents are provided with appropriate positive incentives to share information. As cybersecurity problems are unlikely to be solved by information systems theory alone, we adopt an interdisciplinary approach, as recommended by recent work [30]. Existing behavioural, sociological and psychological research shows that human agents are motivated to act in a particular way when they believe that, as a result of such actions, they can improve their economic or social position [30,31,32,33]. All in all, the literature suggests that human volition (i.e., a choice made by will) is changed as a result of the expected costs and benefits associated with particular actions: human agents ask themselves what would make them share security information. We therefore propose that SIS is a function of different incentives.

3. Theoretical Framework and Hypotheses

Although many incentives exist, prior conceptual and exploratory works suggest five main incentives that each should significantly increase human agents' willingness to engage in SIS [17,35,36]. These incentives are all based on the expectation that (1) sharing will be reciprocated; (2) the information received from the transaction partner will be valuable; (3) sharing will be facilitated by an effective institutional design; (4) sharing will be beneficial for the reputation of the organization the agent works for; and (5) the transaction partner can be trusted. We posit that these expectations change the individual agents' assessments of the potential outcomes of a sharing transaction. Hence, their positive expectations of these issues would motivate them to engage in actual SIS. Figure 1 below illustrates our proposed model.

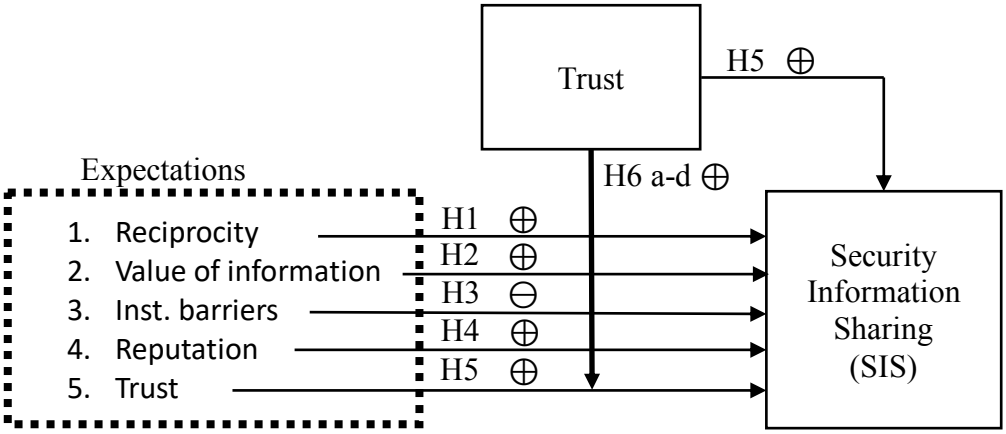

Figure 1: System model linking incentives and SIS where trust between human agents is both a moderator and predicator. Incentives change expectations, modifying the behaviour of human agents to increase voluntary SIS.

[6] The Health Insurance Portability and Accountability Act (HIPAA) requires reporting breaches of protected health information (PHI) to the U. S. Department of Health and Human Services (HHS). Public access to current reported breaches should give regulated entities more incentive to maintain high privacy and security standards, in order to stay off of the "wall of shame".

Reciprocity refers to the effect that the propensity of human agents to engage in a particular behaviour depends on the extent to which such behaviour is reciprocated by the transaction partner. Hence, the expectations of such reciprocity should be the basis for the extent to which they share information [29]. Social psychology research suggests that when agents are treated in a particular way, they respond likewise (reciprocate). For example, peer-to-peer (P2P) systems often confront the problem of free riders (or so called 'leechers'), because most participants often prefer to avoid contributing while enjoying the benefits of the network. As a result, most P2P networks have been forced to remove free riders, or to turn them into forced riders by making contributions mandatory. As in the "tit-for-tat" strategy, evolutionary biology defines reciprocal altruism as a behaviour 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 [30]. 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 [31]. Reciprocity can be self-reinforcing, because participants will share more when provided with an incentive that ensures reciprocity [32]. Hence,

Hypothesis 1: *SIS will increase with the extent to which a human agent expects SIS to be reciprocated.*

Value of Information measures the benefit that an agent expects to gain from a good and/or a service. A convenient proxy for this measure is the maximum amount of money a specific agent is willing to pay for a good or service [33]. Previous studies have identified the value expectation of the information obtained by sharing as an important precursor to SIS [21]. SIS and cooperation between industry peers can improve the relevance, quality, and value of information, because different human agents often face similar cyber-threats [34].

Nevertheless, SIS can be an extra burden on the participants if they lack the resources to understand and analyse the security information that is shared with them. Therefore, each agent is expected to conduct a cost-benefit analysis before deciding whether or not to engage in SIS. The benefits would increase as the value expectation of the information increases; ideally, an agent will conclude that the benefits of the security information received outweigh the costs of the security information shared. For the participants, cost saving is generally the most direct and visible benefit of SIS. Hence,

Hypothesis 2 (H2): *SIS will increase with the extent to which a human agent expects to receive valuable information in return.*

Institutional Barriers are an important precursor to sharing outcomes. For example, contractual rules regarding the processing and labelling of shared information, as well as the secure storage and access to shared data, influence sharing outcomes [12]. Moreover, a clear taxonomy and framework is needed to create a common terminology and culture for participants before sharing transactions can be made [4]. Such basic arrangements could serve as a precursor to actual sharing and this is likely to be implemented by contractual institutions that define common standards of language use and processes. Hence, the motivation for human agents to engage in SIS is likely influenced by the extent to which they expect an effective institutional design that facilitates sharing transactions. For example, such effective institutions restrict membership in sharing organizations to make SIS attractive to an outside agent, to secure minimum quality standards for the information shared, and to avoid the entry of free riders into the sharing process [12]. Hence,

Hypothesis 3 (H3): *SIS will increase with the extent to which a human agent expects SIS to be facilitated by effective institutions.*

Reputation indicates a value judgment about an agent's attributes. Corporate reputation, for instance, evolves over time as a result of consistent performance, and is reinforced by effective communication [35]. Agents can evaluate the potential reputational benefits of their SIS activities, as well as potential reputational risks. Participants are often reluctant to share information about cybersecurity incidents, as such information might reveal discomforting incidents such as security breaches, data theft, or blackmailing [36]. Reputation is based on customer trust, the protection of customer data, and the quality of service offered [7]. Common fears include information leaks and the use by competitors of critical information to damage the reputation of the client [37]. Disclosing information about cyber-attacks might therefore reduce consumer trust hence negatively influence a firm's market value [2]. As a result, agents have a strong incentive to engage in SIS if they believe that by sharing they can limit their firm's exposure to reputational risks. Hence,

Hypothesis 4 (H4): *SIS will increase with the extent to which a human agent expects a positive effect of SIS on corporate reputation.*

Trust is a belief that a particular human agent is honest, reliable, good and effective [38]. This belief is formed within agents over time as a result of repeated personal interactions that lead to positive outcomes for the sharing agent [54]. Hence, trust is a significant predictor of a human agent's willingness to engage in SIS because such belief reduces the reluctance that exists when any particular human agent is asked to share security information with an unknown stranger [2,46,48]. Therefore,

Hypotheses 5 (H5): *SIS will increase with the extent to which human agents that share security information trust each other.*

Besides this direct effect of trust on SIS, we believe that trust should also positively moderate each relationship postulated in H1 through H4. Hence, the four main effects hypothesized would be even stronger as the trust increases among the agents. First, trust reduces the transaction cost of human interaction and creates a belief among the sharing agents that another transaction will be just as beneficial to them as prior transactions. Pre-existing trust in an exchange relationship has been shown to positively influence the reciprocity of subsequent exchanges [49,50]. Hence, trust should positively moderate the reciprocity expectation because in a trusted relationship there is less risk associated with an act of sharing not being reciprocated. In other words, past transactions that have created trust among the sharing agents can positively influence future transactions [42]. Second, in the absence of trust, the value of information received in a sharing transcation can only imperfectly be predicted by the receiving agent. However, in the presence of trust the agent likely anticipates that the information received will be valuable with high probabilty hence should have a stronger motivation to share. Third, behavioural research suggests that institutions are more effective when prior trust between human agents exists [51,52,53]. Fourth and finally, in many jurisdictions, governments and private industries have worked together to create networks in an attempt to support the emergence of trusted relationships between human agents [45,46]. Human agents active in such networks are likely to communicate their membership to external stakeholders and the public in order to improve corporate reputation. Hence,

Hypotheses 6a-d (H6 a-d): *The relationships between the value of information (reciprocity, institutional barriers, reputation) expectation and SIS are positively moderated by the extent to which human agents in a sharing transaction trust each other.*

4. Methods

Specification and Measurement of Constructs

We operationalized and tested our hypotheses as follows. As we postulate relationships between individual-level expectation and perception, modelling the influence of these on individual behaviour (i.e., sharing information), our study is set at the individual level of analysis. Hence, the individual who decides to share, or not, security-relevant information is the unit of analysis. For these reasons, we opted for a psychometric approach [48] that measures all constructs directly at the individual level. Data on all constructs was collected from individual respondents through a questionnaire instrument. Validated academic procedures of questionnaire design [49] informed its production. The questionnaire was developed as a paper instrument first. Then we pretested it with focus groups from academia and the cybersecurity industry; we used the feedback to improve the visual presentation of the questionnaire and to add additional explanations. The feedback received during this phase indicated that respondents could make valid and reliable assessments, which alleviated concerns about the approximation nature of shared unit-level constructs [50].

Population

The questionnaire was implemented among the 424 participants of the closed user group of the Swiss Reporting and Analysis Centre for Information Assurance (MELANI).[7] This organization is an ISAC, i.e., a government organization that provides a platform to facilitate SIS between Critical Infrastructures (CIs). These agents decide freely whether or not to share information, such that their individual behaviour also determines the behaviour of the firm or government organization they represent. The sharing environment is organized as a forum in which participants from the information security technology sector and CI providers share security information. MELANI is organized as a public-private partnership between the Swiss federal government and the private sector. The closed user group in this organization comprises senior industry managers from diverse industries; who all are in charge of providing cybersecurity for their respective firms. For all of these members, the exchange of SIS is important, as they operate critical infrastructures[8] that are ultimately all connected. Hence, if they share they can learn from each other and make individual protection stronger if they share. This group of 424 individuals constitutes an ideal population from which we drew our sample to empirically test our hypotheses. We used the number of years a particular manager was a member with MELANI served as a proxy to control for prior SIS experience.

Implementation

Within this closed user group, both MELANI 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 also implemented the questionnaire[9] in the English language to exclude any back-translation problems from the onset. Before implementation, we conducted pre-tests to make sure respondents had the necessary 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.

We implemented the questionnaire as an online survey, employing the SelectSurvey software, provided free of charge by the Swiss Federal Institute of Technology in Zurich

[7] https://www.melani.admin.ch/melani/en/home.html (last accessed January 12, 2018).

[8] They are professionally affiliated with the banking and finance (38% of all members), government (26%), energy (11%), telecommunication / IT (6%), insurance (6%) transport and logistics (6%), industry (3%), health (3%) and the chemical / pharmaceutical industries (1%).

[9] For limited space reasons, the original questionnaire is available upon request from the corresponding author.

(ETHZ).[10] For reasons of data security, the survey was hosted on proprietary servers of the ETHZ. The data were captured in an anonymized and voluntary way. The management of MELANI 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 were free to reply, and no pressure from MELANI or the authors of this paper was exerted at any time. As a reward for participation, respondents were offered a free of charge research report free of charge that summarized the responses.

Dependent Variables

To capture sharing activities in a multidimensional way, we operationalize SIS by two distinct dependent variables: *frequency* and *intensity* (of sharing). Frequency measures the amount of times information is shared between agents, whereas intensity measures the depth of sharing interaction. A simple count could be deceptive, as many sharing transactions do not necessarily indicate that important information is shared in each transaction, and vice versa, as much highly relevant information be shared in very few or even a single transaction. *Frequency* was operationalized by a multi-item scale adopted from the literature (viz. Table 1 on p. 18 in the appendix). *Intensity* was measured by an ordered categorical variable that captured how intensely MELANI members would respond to a particular sharing transaction. The variable comprised seven categories (never; rarely, in less than 10% of the chances when I could have; occasionally, in about 30% of the chances when I could have, etc., until "every time"). We opted for this ordered-categorical approach, so people could estimate and would not be deterred by the need to provide exact percentage figures. We also captured an alternative measure by means of a Likert scale, but during the empirical analysis, we found that the ordered categorical variable fits the data better.

Independent Variables

All independent variables are measured by psychometric scales that each comprise several items. They were adapted from prior empirical literature [9] wherever possible, in order to establish good measurement accuracy by using validated measurement instruments. These scales, their items and Cronbach alphas are all detailed in Table 1 on p.17 of the appendix. All of the items these scales comprise are Likert-scaled; respondents could express their view vis-à-vis each item by choosing from a five-point scale anchored at "strongly disagree" and "strongly agree", with "neutral" as the midpoint. To construct each scale, we added its individual item scores and subsequently divided the sum by the number of items in it [51]. All independent variables were measured in a single construct, with the exception of reciprocity which was captured by two variables. *Reciprocity (social)* captured respondents' expectations to be socially rewarded for SIS, whereas *reciprocity (transactional)* captured the expectation that SIS constitute an arm's-length transaction for which concrete compensation in monetary or career terms is expected.

Controls

To capture heterogeneity among individuals, we controlled for the respondent's gender, age, education level, and length of membership with MELANI, because expectation of SIS gained during membership might influence a respondent's sharing behaviour. *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 (Bachelor, Diploma, Master, none, other, PhD). We finally controlled for the industry

[10] IT support received free of charge during implementation is gratefully acknowledged.

affiliation of the firm the respondent is affiliated with. The selection of relevant controls was informed by prior empirical research in the field of economics of cybersecurity [52].

Data Collection

The online questionnaire and the reminders were sent to the population by the Deputy Head of MELANI, which gave a strong credibility and endorsement to the participants. The survey link was sent in an e-mail describing the authors, the data, the contact for support, as well as the reward and the definition and scope of the study. 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 is 63%. Statistical analysis was done with STATA.[11]

Post-hoc Tests

We tested response patterns for systematic differences between "early" and "late" replies and for a potential influence of total response time as respondents could save intermediate questionnaire completions and return to the survey and complete it at a later point in time. The analysis did not suggest any specific influence. After data collection was complete, we tested the reliability and validity of both our items and our scales by using diverse approaches. All of these methods consistently indicate high levels of reliability and validity. The reliability of our items was tested by calculating item-test, item-rest, and average inter-item correlations, and the reliability of our scales was verified by calculating Cronbach's alpha [48]. The convergent validity of our scales was assessed by applying the principal component factor analysis with oblique rotation. This analysis suggested eight factors with an eigenvalue about unity. High direct factor-loadings and low cross-loadings indicate a high degree of convergent validity [53]. The first factor explained 13.4% of the total variance. Hence, according to Harman's one-factor test, there seemed to be no significant common method variance in the sample [54]. The detailed factor-loadings and their diagnostic measures are given in Table 2 on p.20 of the appendix.

Estimation

For the dependent variable *intensity*, we estimated ordered probit models, as the variable is measured by six mutually exclusive and hierarchical categories. Akaike information criteria were used to compare the goodness of fit. For the dependent variable *frequency*, we estimated tobit models as this variable is conditioned on values between 1 and 5 [55]. We incrementally built all models by first entering only the controls in a baseline model and then adding the covariates one by one. In both estimations, we mean centered the independent variables before entering them into the analysis.

5. Results

Table 3 provides descriptive statistics for all variables. Table 4 specifies Spearman correlations; for the sake of brevity, correlates are shown between dependent and independent variables only. Table 5 documents the two final, best-fitting models and their respective diagnostic measures.[12] We judged our hypotheses on the basis of these final models. H1 is

[11] When data collection was complete, the data were exported from the survey application, manually inspected for consistency and then converted into a STATA (v.13) dataset on which all further statistical analysis was performed.

[12] Further detailed information about these procedures is available from the corresponding author.

partially supported. The value of information a human agent expects to receive as a result of sharing security information significantly increases the intensity of SIS ($p < 0.05$), but not its frequency. H2 is fully supported insofar as social reciprocity is concerned, and partially insofar as transactional reciprocity is concerned. Social reciprocity significantly increases both the intensity ($p < 0.05$) and the frequency ($p < 0.05$) of SIS. Transactional reciprocity significantly increases the frequency of sharing ($p < 0.01$), but not its intensity. H3 is strongly supported. Effective institutional design significantly increases both frequency ($p < 0.001$) and intensity ($p < 0.01$) of SIS. Note that the negative sign on both coefficients is due to the variable *institutional barriers* being reverse-coded, such that ineffective institutional design reduces both frequency and intensity of SIS (in line with our theoretical expectation). H4 is not supported. Reputation is neither a significant predictor for the frequency nor for the intensity of SIS. H5 is partially supported.

Trust between human agents significantly increases the frequency ($p < 0.01$), but not the intensity of sharing. Finally, partial support is found for the moderating role of trust. It negatively and significantly moderates the relationship between value and the intensity ($p < 0.05$), but not the frequency ($p < 0.05$) of SIS, lending partial support to Hypothesis 6a. It also negatively and significantly moderates the relationship between transactional reciprocity and SIS, both for frequency ($p < 0.05$) and intensity ($p < 0.01$), thus lending full support to Hypothesis 6b. All other interaction effects are insignificant, hence Hypotheses 6c and 6d are rejected. Education, regardless of the education level, is negatively associated with the frequency (each $p < 0.05$), but not the intensity of SIS. Neither gender, nor the age, length of membership in MELANI, nor industry affiliation is a significant predictor of SIS.

6. Discussion

To the best of our knowledge, our paper represents the first empirical study of security information sharing (SIS) among human agents in an actual Information Sharing and Analysis Centre (ISAC). We have provided a theoretical explanation for SIS in an interdisciplinary way by drawing on prior behavioural economics, psychology, and information systems research. Five specific predictors (reciprocity, value, institutional barriers, reputation, trust) were elaborated from these prior works, and SIS is regressed on these. Furthermore, we have offered a multidimensional measure of SIS by differentiating between the frequency and the intensity of security information shared.

The results suggest that the frequency and the intensity of SIS are caused by different motivations. The expectation of both social and transactional returns, as well as the level of trust between sharing agents, seems to be a strong incentive for frequency. Whereas, the expected value of the information received in return, as well as reciprocity, seems to be a motivating factor for intensity. Hence, the frequency of SIS resembles a pattern of continuous, business-like exchange that intensifies as trust is built by continuous cooperation, whereas the intensity of SIS seems to be primarily based on the value an agent expects to receive in return. In this regard, trust is not a significant predictor, implying that agents will not share in-depth information unless they can reasonably expect an equal return. Expectations about reciprocity significantly influence both dimensions of SIS. Our results confirm that both social and transactional reciprocity are powerful adaptive mechanisms that can trigger feelings of indebtedness even when faced with an uninvited favour [56,57]. Hence, once agents reasonably believe that, in the long term, the beneficial results of reciprocity will win out over short term self-interest, they would more likely share security information. This finding is in line with prior theoretical expectations [58].

Generalisation

All in all, our findings point to the importance of human behaviour when studying information systems. To date, theoretical information systems research dominates the study of information security, whereas interdisciplinary approaches are desirably, but largely missing [59]. To our knowledge of the literature, very few contributions study SIS among actual human agents, and none is empirical [6]. Given that SIS, when done successfully, is an activity generating social benefits [6], this lack of evidence seems problematic.

Our paper is a first attempt towards closing this gap, and we propose that actual information sharing between human agents should be studied in a variety of contexts. We obtained our results by analysing a sample of decision-making agents who operate and protect critical infrastructures in a single country. However, we do not believe that our results are necessarily limited to those particular contexts. None of the explanatory constructs we offer is contingent on particular nation-states, cultures, or idiosyncratic contexts. They rather represent basic traits of human volition and organization that can be identified globally.

Furthermore, our results inform about research on behavioural aspects in information security by showing how and why expectations about future benefits can provide incentives for human agents to exhibit particular actions [28]. Our results can thus serve help to formulate policies and institutional designs that replace non-cooperation and free-riding by productive sharing behaviour. Specifically, we suggest how human agents could be ‘nudged’ to cooperate by providing them with conducive expectations that sharing will improve their position and benefit. Our results support the view that the effectiveness of regulation in stimulating productive human behaviour is limited, and that positive reinforcement and indirect suggestions should be used instead [60].

Recommendations

In both models, the variable *institutional barriers* variable is a negative and significant predictor for both the frequency and the intensity of SIS. These results point to the importance of proper institutional design. Human agents cannot be expected to voluntarily engage in SIS unless they are provided with a safe and conducive organizational environment that facilitates SIS. As there is an ongoing global debate about whether or not SIS should be mandatory, policymakers should be cautious about preferring regulation as they attempt to incentivize human agents to engage in SIS. Our results show that reciprocity is a significant predictor for both the frequency and the intensity of SIS. Reciprocity is a social norm of responding to a positive action with another positive action and cannot be instituted by regulation and constraint. If forced, agents might even share irrelevant, non-timely, or false information [61]. Adjusting sanction levels for failure to comply with mandatory SIS could also be difficult, if not impossible [6]. All in all, our results suggest that providing positive incentives seems to be a more promising way to encourage human agents share security information – thus confirming propositions formulated before [62]. We propose that a liberal environment is probably more conducive for information security than a coercive one, at least insofar as the cooperation of human agents is required. For example, in the ISAC we studied, human agents' fears about data leaks are mitigated by the introduction of 'trust circles' that reflect a particular agent's willingness to engage in SIS. Participants can share security information with ISAC staff only (first circle), selected industry peers (second circle) or all members (third circle). For each SIS transaction, participants can choose which circle (i.e., the level of privacy) they want to communicate with. We believe that such effective institutional designs are more conducive than formal regulation, when it comes to incentivizing agents to engage in SIS.

This study differs from prior work in the sense that empirical observations are provided from observing actual human agents in an actual ISAC. Consequently, the results have important implications for the development of the IT security industry. As our results confirm the negative influence of institutional obstacles both for the frequency and the intensity of SIS, they point to the fact that effective sharing is not only about human behaviour, but also about a conducive institutional environment. Switzerland offers an ideal environment for SIS (high level of trust in institutions, low corruption rate).

Our findings both inform the reviews of existing ISACs, as well as the design of formally established Information Sharing and Analysis Organizations (ISAOs). Furthermore, given that 'big data' analytics implicate disruptive technological change in the IT security industry, our results are likely relevant for the technical and institutional design of information security operation centres or fusion centres, i.e., organizations designed to promote information sharing between national and international agencies [63]. For example, both the *threat intelligence platform* and *cyber-threat intelligence* technologies must rely on effective SIS as agents are expected to mutually share real-time threat data. Therefore, the creation of these technologies should not only be informed from an information systems viewpoint but be corroborated with an institutional perspective.

Future Work

Future research could build on our work in a variety of ways. The authors of this study are currently preparing a policy recommendations paper at a meso-level of analysis in order to deliver insights for legislators willing to design better ISACs. Our empirical approach focused on four main effects that together explain about 68% of the sample variance. Additional explanatory variables could be conceived to expand our model. For example, in our research we did not consider altruism. Human agents can share information although they do not necessarily expect a social or transactional return, as a gesture of goodwill, or as an initial step to build trust among participants. Future studies could also consider predictors that model

individual perception of risk, as the willingness to share information among human agents can be expected to grow with the risk of economic damage as a result of information not shared. For example, human agents whose organizations exhibit systemic risks (e.g., 'too big to fail' banks) might be more inclined towards SIS if provided with appropriate incentives.

Future studies could set the level of analysis on the industry rather than on human agents. 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. This has enabled the sector to build trust over time, based on already existing relationships and the regular face-to-face meetings at workshops or roundtables that take place between the MELANI staff and their contacts in the banks. Even though impediments remain to the development of effective SIS in this specific industry, including legal issues that deter CI providers from engaging in SIS activities: including antitrust laws, patent protection, national security laws, and data privacy laws, such as the Swiss banking secrecy laws. These legal issues make problematic the sharing of client-related data, especially in cross-border or multi-jurisdictional contexts, where attackers can find multiple "offshore" entry points to an organization.

References

1. Gordon LA, Loeb MP, Lucyshyn W *et al.* The impact of information sharing on cybersecurity underinvestment: A real options perspective. *J Account Public Policy* 2015;**34**:509–19.

2. Campbell K, Gordon LA, Loeb MP *et al.* The Economic Cost of Publicly Announced Information Security Breaches: Empirical Evidence from the Stock Market. *J Comput Secur* 2003;**11**:431–448.

3. 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. *J Inf Secur* 2015;**06**:24–30.

4. Luiijf E, Klaver M. On the Sharing of Cyber Security Information. In: Rice M, Shenoi S (eds.). *Critical Infrastructure Protection IX*. Springer, 2015, 29–46.

5. Hausken K. A strategic analysis of information sharing among hackers. *JISTEM - J Inf Syst Technol Manag Online* 2015;**12**:245–70.

6. Laube S, Böhme R. The economics of mandatory security breach reporting to authorities. *J Cybersecurity* 2016;**2**:29–41.

7. Gordon L, Loeb M, Sohail T. Market Value of Voluntary Disclosures Concerning Information Security. *Manag Inf Syst Q* 2010;**34**:567–94.

8. Gal-Or E, Ghose A. The Economic Incentives for Sharing Security Information. *Inf Syst Res* 2005;**16**:186–208.

9. Laube S, Böhme R. Strategic Aspects of Cyber Risk Information Sharing. *ACM Comput Surv* 2017;**50**:77:1–77:36.

10. 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.

11. Hausken K. Information sharing among firms and cyber attacks. *J Account Public Policy* 2007;**26**:639–88.

12. ENISA. *Information Sharing and Common Taxonomies between CSIRTs and Law Enforcement*. 2016.

13. Gordon LA, Loeb MP, Lucyshyn W. Sharing information on computer systems security: An economic analysis. *J Account Public Policy* 2003;**22**:461–85.

14. 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 US, 2010, 55–66.

15. De Bruijne M, Van Eeten M. Systems that Should Have Failed: Critical Infrastructure Protection in an Institutionally Fragmented Environment. *J Contingencies Crisis Manag* 2007;**15**.

16. Mermoud A, Keupp MM, Ghernaouti S *et al.* Using Incentives to Foster Security Information Sharing and Cooperation: A General Theory and Application to Critical Infrastructure Protection. *Critical Information Infrastructures Security*. Springer, Cham, 2016, 150–62.

17. Ezhei M, Tork Ladani B. Information sharing vs. privacy: A game theoretic analysis. *Expert Syst Appl* 2017;**88**:327–37.

18. Gao X, Zhong W, Mei S. A game-theoretic analysis of information sharing and security investment for complementary firms. *J Oper Res Soc* 2014;**65**:1682–91.

19. Aviram A, Tor A. Overcoming Impediments to Information Sharing. *Ala Law Rev* 2003;**55**:231.

20. Harrison K, White G. Information sharing requirements and framework needed for community cyber incident detection and response. *Homeland Security (HST), 2012 IEEE Conference on Technologies For*. 2012, 463–9.

21. ENISA. *Incentives and Barriers to Information Sharing*. 2010.

22. Gal-or E, Ghose A. The economic consequences of sharing security information. *Workshop on Economics and Information Security, 2003*. Kluwer Academic Publishers, 2004, 95–104.

23. Ghose A, Hausken K. *A Strategic Analysis of Information Sharing Among Cyber Attackers*., 2006.

24. Bisogni F. Data Breaches and the Dilemmas in Notifying Customers. 2015.

25. Nolan A. Cybersecurity and Information Sharing: Legal Challenges and Solutions. *Digit Libr* 2015.

26. Moran T, Moore T. The Phish-Market Protocol: Securely Sharing Attack Data between Competitors. In: Sion R (ed.). *Financial Cryptography and Data Security*. Springer, 2010.

27. Weiss E. United States | CRS | Legislation to Facilitate Cybersecurity Information Sharing: Economic Analysis. *HORIZON* 2015.

28. Kahneman D, Tversky A. Prospect theory: An analysis of decision under risk. *Econom J Econom Soc* 1979:263–291.

29. Xiong L, Liu L. PeerTrust: supporting reputation-based trust for peer-to-peer electronic communities. *IEEE Trans Knowl Data Eng* 2004;**16**, DOI: 10.1109/TKDE.2004.1318566.

30. Trivers RL. The Evolution of Reciprocal Altruism. *Q Rev Biol* 1971;**46**:35–57.

31. von Hippel E, von Krogh G. *Open Source Software and the "Private-Collective" Innovation Model: Issues for Organization Science*., 2003.

32. Theodorakopoulos G, Boudec JYL, Baras JS. Selfish Response to Epidemic Propagation. *IEEE Trans Autom Control* 2013;**58**:363–76.

33. Varian HR. Microeconomic Analysis. *N Y WW Nort* 1992;**3**.

34. Petrenj B, Lettieri E, Trucco P. Information sharing and collaboration for critical infrastructure resilience - a comprehensive review on barriers and emerging capabilities. *Int J Crit Infrastruct* 2013;**9**:304–29.

35. Gray ER, Balmer JMT. Managing Corporate Image and Corporate Reputation. *Long Range Plann* 1998;**31**:695–702.

36. Campbell K, Gordon LA, Loeb MP *et al.* The economic cost of publicly announced information security breaches: empirical evidence from the stock market. *J Comput Secur* 2003;**11**:431–448.

37. Naghizadeh P, Liu M. Inter-temporal incentives in security information sharing agreements. *2016 Information Theory and Applications Workshop (ITA)*. 2016, 1–8.

38. Safa NS, Von Solms R. An information security knowledge sharing model in organizations. *Comput Hum Behav* 2016;**57**:442–51.

39. Hämmerli B, Grudzien W. *Voluntary Information Sharing*. NISP Chapter 3, 2014.

40. Rocha Flores W, Antonsen E, Ekstedt M. Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture. *Comput Secur* 2014;**43**:90–110.

41. Fukuyama F. *Trust: The Social Virtues and The Creation of Prosperity*. 1st Free Press Pbk. Ed edition. New York, NY: Free Press, 1996.

42. Molleman L, van den Broek E, Egas M. Personal experience and reputation interact in human decisions to help reciprocally. *Proc R Soc B Biol Sci* 2013;**280**, DOI: 10.1098/rspb.2012.3044.

43. Leakey RE, Lewin R. *People of the Lake: Mankind & Its Beginnings*. Reissue edition. New York: Avon Books, 1979.

44. Ridley M. *The Origins of Virtue*. New Ed edition. London: Penguin, 1997.

45. Fernandez Vazquez D, Pastor Acosta O, Brown S *et al*. Conceptual framework for cyber defense information sharing within trust relationships. *CYCON*. 2012, 1–17.

46. Haemmerli B, Raaum M, Franceschetti G. Trust Networks among Human Beings: Analysis, Modeling, and Recommendations. *Effective Surveillance for Homeland Security*. Chapman and Hall/CRC, 2013, 21–50.

47. Kollars NA, Sellers A. Trust and information sharing: ISACs and U.S. Policy†. 2016, DOI: 10.1080/23738871.2016.1229804.

48. Nunnally JC, Bernstein I. *Psychometric Theory*. 3rd Revised edition. New York: McGraw Hill Higher Education, 1994.

49. Clayton W. Faubion, Jason D. Andrew. Book Review: Dillman, D. A. (2000). Mail and Internet Surveys: The Tailored Design Method (2nd ed.). New York: Wiley 464 pp., $47.50 (hardcover). *Rehabil Couns Bull* 2001;**44**:178–80.

50. Kozlowski S, Klein K. *A Multilevel Approach to Theory and Research in Organizations: Contextual, Temporal, and Emergent Processes.*, 2012.

51. Trevor CO, Nyberg AJ. Keeping Your Headcount When All About You Are Losing Theirs: Downsizing, Voluntary Turnover Rates, and The Moderating Role of HR Practices. *Acad Manage J* 2008;**51**:259–76.

52. Safa NS, Von Solms R. An Information Security Knowledge Sharing Model in Organizations. *Comput Hum Behav* 2016;**57**:442–451.

53. Hair JF ed. *Multivariate Data Analysis*. 5th ed. Upper Saddle River N.J: Prentice Hall, 1998.

54. Philip M. Podsakoff, Dennis W. Organ. Self-Reports in Organizational Research: Problems and Prospects. *J Manag* 1986;**12**:531–44.

55. Greene WH. *Econometric Analysis*. 7 edition. Boston: Pearson, 2011.

56. 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.

57. Kwahk K-Y, Park D-H. The effects of network sharing on knowledge-sharing activities and job performance in enterprise social media environments. *Comput Hum Behav* 2016;**55**, **Part B**:826–39.

58. Fehr E, Gächter S. Fairness and Retaliation: The Economics of Reciprocity. *J Econ Perspect* 2000;**14**:159–81.

59. Anderson R, Moore T. The Economics of Information Security. *Science* 2006;**314**:610–3.

60. Thaler RH, Sunstein CR. *Nudge: Improving Decisions About Health, Wealth, and Happiness*. Updated. New York: Penguin Books, 2009.

61. Burr R. *S.754 - 114th Congress (2015-2016): Cybersecurity Information Sharing Act of 2015*., 2015.

62. Flora SR. *Power of Reinforcement, The*. SUNY Press, 2012.

63. David DP, Keupp MM, Ghernaouti S *et al.* Cyber Security Investment in the Context of Disruptive Technologies: Extension of the Gordon-Loeb Model and Application to Critical Infrastructure Protection. *Critical Information Infrastructures Security*. Springer, Cham, 2016, 296–301.

64. Wang W-T, Hou Y-P. Motivations of employees' knowledge sharing behaviors: A self-determination perspective. *Inf Organ* 2015;**25**:1–26.

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

APPENDIX

Table 1: Constructs, items and scales used in the survey

Scale / Construct	Item	Wording	Sources from which items were adapted	Cronbach alpha
Frequency	ISKS1	I frequently share my experience about information security with MELANI	[52]	0.8945
	ISKS2	I frequently share my information security knowledge with MELANI		
	ISKS3	I frequently share my information security documents with MELANI		
	ISKS4	I frequently share my expertise from my information security training with MELANI		
	ISKS5	I frequently talk with others about information security incidents and their solutions in MELANI workshops		
Value of information	AT2	I believe SIS is a useful behavioural tool to safeguard the organization's information assets	[52]	0.6761
	AT3	My SIS has a positive effect on mitigating the risk of information security breaches		
	AT4	SIS is a wise behaviour that decreases the risk of information security incidents		
Reciprocity (transactional)	HR1	I expect to be rewarded with a higher salary in return for sharing knowledge with other participants	[64]	0.7956
	HR2	I expect to receive monetary rewards (i.e., additional bonus) in return for sharing knowledge with other participants		
	HR4	I expect to be rewarded with an increased job security in return for sharing knowledge with other participants		
Institutional barriers	EC1	I cannot seem to find the time to share knowledge in the community	[4]	0.7882
	EC2	It is laborious to share knowledge in the community		
	EC3	It takes me too much time to share knowledge in the community		
	EC4	The effort is high for me to share knowledge in the community		

Reciprocity (social)	NOR2	I believe that other people will help me when I need help if I share knowledge with others through MELANI	[4]	0.7882
	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		
	NOR4	I think that people who are involved with MELANI develop reciprocal beliefs on give and take based on other people's intentions and behaviour		
Reputation	R1	Sharing knowledge can enhance my reputation in the community	[65]	0.6996
	R2	I get praises from others by sharing knowledge in the community		
	R3	I feel that knowledge sharing improves my status in the community		
	R4	I can earn some feedback or rewards through knowledge sharing that represent my reputation and status in the community		
Trust	TR1	I believe that my colleague's information security knowledge is reliable	[52]	0.8598
	TR2	I believe that my colleague's information security knowledge is effective		
	TR3	I believe that my colleague's information security knowledge mitigates the risk of information security breaches		
	TR4	I believe that my colleague's information security knowledge is useful		

Table 2: Final set of factor loadings after oblique rotation[a]

Item	Loading on oblimin-rotated factor							
	factor 1	factor 2	factor 3	factor 4	factor 5	factor 6	factor 7	Commonality
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
Eigenvalue	*3.786*	*2.951*	*2.502*	*2.329*	*2.24*	*2.142*	*1.851*	
Proportion of variance explained	*14.56%*	*11.35%*	*9.62%*	*8.96%*	*8.62%*	*8.24%*	*7.12%*	
Cumulative variance explained	*14.56%*	*25.91%*	*35.53%*	*44.49%*	*53.11%*	*61.34%*	*68.46%*	

Notes to Table 2.
a. Blank cells represent factor loadings of less than abs < 0.30

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
Value of information	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
Institutional design	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	Value	Reciprocity (social)	Reciprocity (financial)	Institutional design	Trust
Frequency	1						
Intensity	0.3547***	1					
Value of information	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		
Institutional design	-0.2238**	-0.1694*	-0.0976	-0.0314	0.1533*	1	
Trust	0.2279**	-0.0101	0.2471***	0.0269***	-0.1321	-0.1857*	

Notes to Table 4.
a. Spearman correlations. *p < 0.05; **p < 0.01; ***p < 0.001.

Table 5: Final results of model estimations[a,b]

	Intensity of SIS (ordered probit estimation)	**Frequency of SIS (tobit estimation)**
	Coefficient (std. error)	*Coefficient (std. error)*
Value of information	0.3964* (0.1862)	0.1627 (0.1165)
Reciprocity (social)	0.3793* (0.1648)	0.2066* (0.1010)
Reciprocity (transactional)	0.1614 (0.1194)	0.2276** (0.0749)
Institutional barriers	-0.4928*** (0.1396)	-0.232** (0.0849)
Reputation	0.1199 (0.1971)	-0.091 (0.1243)
Trust	-0.154 (0.1684)	0.3189** (0.1060)
Value x Trust	-0.6254* (0.3159)	-0.3260 (0.1960)
Reciprocity (social) x Trust	0.1770 (0.2665)	0.1383 (0.1665)
Reciprocity (transactional) x Trust	-0.428* (0.2174)	-0.3777** (0.1371)
Institutional design x Trust	0.2400 (0.2495)	-0.163 (0.1558)
Reputation x Trust	0.4013 (0.3943)	0.1261 (0.2495)
Gender	-0.2311 (0.4152)	0.2014 (0.2601)
Age 21-30	-0.1101 (0.3911)	0.2082 (0.2444)
Age 31-40	0.1620 (0.2414)	0.0097 (0.1515)
Age 41-50	0.0386 (0.2002)	0.0191 (0.1261)
Education none	-0.5686 (0.5732)	-0.8007* (0.3612)
Education Master	-0.6672 (0.5621)	-0.7931* (0.3544)
Education Bachelor	-0.1803 (0.5533)	-0.7385* (0.3499)
Education PhD	-0.8225 (0.6173)	-0.9552* (0.3883)
Membership duration	0.0161 (0.0165)	0.0200 (0.0105)
Government	-0.2845 (0.3367)	-0.0057 (0.2119)
Banking / finance / industry	-0.1578 (0.3025)	0.0307 (0.1900)
All other industries	-0.1950 (0.3378)	-0.3791 (0.2127)
Energy	-0.0862 (0.3705)	0.2025 (0.2326)
Health	-0.2942 (0.3985)	0.0291 (0.2490)
Constant		3,058175*** (0.4718)
Log likelihood	-245.65	-197.15
Pseudo R^2	0.0928	0.1596
LR χ^2 (25 d.f.)	50.23	74.90
$p > \chi^2$	0.002**	0.000***
Observations	188	188

Notes to table 5.
a. Two-tailed tests. Standard errors are given between parentheses. *p < 0.05; **p < 0.01; ***p < 0.001
b. Age category “above 50”, education category “PhD” and the telecommunication/IT industry serve as the respective control variable benchmarks.