To share or not to share: A behavioral perspective on human participation in security information sharing

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

JOURNAL OF CYBERSECURITY

Journal of Cybersecurity, 2019, 1–13
doi: 10.1093/cybsec/tyz006
Research paper

Research paper

To share or not to share: a behavioral perspective on human participation in security information sharing

Alain Mermoud [1,2,*], Marcus Matthias Keupp[2,3], Kévin Huguenin [1], Maximilian Palmié[4] 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 (MILAC) at ETH Zurich, 8903 Birmensdorf, Switzerland; [3]University of St. Gallen, Dufourstrasse 50, 9000 St. Gallen, Switzerland; [4]Institute of Technology Management, University of St. Gallen, Dufourstrasse 40a, 9000 St. Gallen, Switzerland

*Corresponding address: Tel: +41 58 484 82 99; E-mail: alain.mermoud@gmail.com

Received 21 July 2018; revised 17 May 2019; accepted 14 June 2019

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, individuals still seem reluctant to share security information. Few contributions have addressed this conundrum 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 human Information Sharing and Analysis Center 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 extends 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

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 [67].

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 [41, 47]. Hence, SIS likely contributes to strengthening the cybersecurity of firms, critical infrastructures, government, and society [19, 45, 46, 48, 54].

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 [19]. Game-theoretic simulation suggests that individuals may free-ride on the information provided by others while not sharing any information themselves [47, 55]. Researchers and international

organizations have been warning for years that individuals seem reluctant to share security information, although the technical infrastructure for information exchange does exist [32, 33, 47, 73]. Legislators have attempted to resolve this problem by creating regulation that makes SIS mandatory.[1] However, reviews suggest that despite these attempts, individuals still seem reluctant to share security information [16, 44, 72, 103]. They may even 'game' the system in an attempt to circumvent regulation [5, 71, 72].

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 [19]. More specifically, this work predicts that SIS can only be imperfectly understood unless the human motivation to (not) participate in SIS is studied [53, 65, 98].

However, few contributions have addressed this research gap to date. Since an excellent account of the SIS literature exists [64], 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 Ref. [64] 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. Following prior recommendations [6], we adopt an interdisciplinary approach. Recently, interdisciplinary studies were productive in showing the extent to which human behavior is associated with knowledge sharing [87, 106].

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 members of an Information Sharing and Analysis Center (ISAC) who share real security information. The remainder of this article is structured as follows. Section 2 develops the behavioral framework and deducts testable hypotheses from this framework. Section 3 details the sampling context, measures, and empirical methods. 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.

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"). In 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 [13, 27, 37, 58, 59, 89].

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 [42]. 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 [66]. Particularly in the case of collective action, the individual may behave in ways that are not conducive to the overall group goal [78, 79]. 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 [36, 37, 39, 68]. 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 [8, 10].

Human behavior is the result of human motivation, intention, and volition. It manifests itself in goal-directed (i.e. nonrandom) and observable actions [90, 93, 102]. 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 [17]. 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 [106].

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 individual who, independently of the motives of other individuals, ponders whether or not to participate in SIS. We believe 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.

Attitude

Behavioral theory suggests that attitudes have a directive influence on human behavior [1]. Attitude is a psychological tendency that is expressed by evaluating a particular entity with some degree of favor or disfavor [30]. Hence, an individual's favorable or unfavorable attitude towards a particular behavior predicts the extent to which this behavior actually occurs [2, 3].

Much empirical work has confirmed and detailed this attitude–behavior link, particularly in the context of information systems adoption and intention to use (see Refs [14] and [62] for extensive literature reviews). More specifically, this attitude-behavior link influences individuals' intention to share knowledge [17]. Moreover, an affirmative attitude towards knowledge sharing positively influences participation rates [87]. 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 [32]. 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.

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.

Reciprocity

Behavioral theory suggests that human behavior is characterized by inequity aversion [39]. 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 [22, 95]. Hence, when humans are treated in a particular way, they reciprocate, that is, they respond likewise [36]. As a result, reciprocity is a shared behavioral norm among human beings that governs their social cooperation [38, 50].

Economic exchange relationships are therefore shaped by the reciprocity expectations of the participants involved in this exchange [61]. In such relationships, reciprocity is a dominant strategy that is conducive to a socially efficient distribution of resources [7, 20]. 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 [101]. 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 [18, 49]. 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," that is, 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 [63, 80, 88]. 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.

Executional Cost

Behavioral theory suggests that humans are loss-averse, that is, they attempt to avoid economic losses more than they attempt to realize economic benefits. Much experimental research has confirmed this tendency [58, 59, 92, 96, 97].

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 [104]. 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, Ref. [106] 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 [67]. 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 [33]. 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.

Reputation

Behavioral theory suggests that humans deeply care about being recognized and accepted by others [11, 15]. Many philosophers have argued that the desire for social esteem fundamentally influences human behavior and, as a result, economic action [21].

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, that is, a socially transmitted assessment by which other individuals judge the focal individual's social esteem [31, 69]. For example, academic researchers strive to increase the reputation of their department by publishing scholarly work [60]. 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 [99].

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 [25, 81], 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.

Trust

Behavioral theory suggests that humans simplify complex decision-making by applying heuristics [82, 97], particularly when they attempt to reduce the cost of information acquisition and valuation [40].

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 [24]. 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, for example, 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 [43]. 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 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 [51, 70]. For example, mutual trust among the participants of peer-to-peer networks can reduce transactional uncertainty [105]. Moreover, trust can mitigate information asymmetry by reducing transaction-specific risks [9]. It is also a significant predictor of participation in virtual knowledge sharing communities [86].

Such trust, in turn, is positively associated with knowledge sharing in both direct and indirect ways [56], whereas distrust is an obstacle to knowledge sharing [4]. More specifically, trust is a facilitator in information security knowledge sharing behavior [87]. 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.

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 [66]. 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," that is, 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.

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. In 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.

Methods

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 Ref. [107]. For some illustrative examples of ISACs across different countries, see Ref. [34]. For a detailed description of MELANI-net, its organization, and history, see Ref. [29]. 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 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.

Measures

Our study analyzes human behavior on the individual level of analysis. We therefore chose a psychometric approach to operationalize our constructs [77]. We adopted psychometric scales from the extant literature wherever possible and kept specific adaptions 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 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. In 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 by 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 and combined these into five categories (government, banking and finance, energy, health, telecom and IT, all others).

Implementation

Data for all variables were collected from individual respondents by a questionnaire instrument. We followed the procedures and recommendations of Ref. [28] 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.[3] 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 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 12 October 2017 and ended on 1 December 2017. Two reminders were sent on 26 October and 9 November 2017. Of all 424 members, 262 had responded when the survey was closed for a total response rate of 62%.

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 [52]. 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 [84]. 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 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 [85, 94].

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 Ref. [26], 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. Since all the categorical controls age, education and industry are exhaustive and hence perfectly collinear, Stata automatically chose a benchmark category for each of these (cf. footnotes b to Tables 5 and 6).

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. 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. We also contrasted the Tobit model that used the scale-based measure for *frequency* with an alternative ordered probit model that used a categorical specification of that variable, but found that the former model fit the data much better.

3 Further detailed information about these pre-tests is available from the corresponding author.

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

Measures (source)	Type	Item	Text	Factor loading	Cronbach alpha
SIS constructs					
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 [87]	Likert scale	ISKS1	I frequently share my experience about information security with MELANI	0.8075	0.8945
		ISKS2	I frequently share my information security knowledge with MELANI	0.8903	
		ISKS3	I frequently share my information security documents with MELANI	0.8850	
		ISKS4	I frequently share my expertise from my information security training with MELANI	0.8600	
		ISKS5	I frequently talk with others about information security incidents and their solutions in MELANI workshops	0.6898	
Behavioral constructs					
Attitude [87]	Likert scale	AT1	I think SIS behavior is a valuable asset in the organization	Dropped	0.6761
		AT2	I believe SIS is a useful behavioral tool to safeguard the organization's information assets	0.7751	
		AT3	My SIS has a positive effect on mitigating the risk of information security breaches	0.6376	
		AT4	SIS is a wise behavior that decreases the risk of information security incidents	0.7849	
Transactional reciprocity [100]	Likert scale	HR1	I expect to be rewarded with a higher salary in return for sharing knowledge with other participants	0.8822	0.7956
		HR2	I expect to receive monetary rewards (i.e. additional bonus) in return for sharing knowledge with other participants	0.8743	
		HR3	I expect to receive opportunities to learn from others in return for sharing knowledge with other participants	Dropped	
		HR4	I expect to be rewarded with an increased job security in return for sharing knowledge with other participants	0.7499	
Social reciprocity [63]	Likert scale	NOR1	I believe that it is fair and obligatory to help others because I know that other people will help me some day	Dropped	0.8003
		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	
		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	
Executional cost [106]	Likert scale	EC1	I cannot seem to find the time to share knowledge in the community	0.6964	0.7882
		EC2	It is laborious to share knowledge in the community	0.6950	
		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 [106]	Likert scale	R1	Sharing knowledge can enhance my reputation in the community	0.6312	0.6996
		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	
		R4	I can earn some feedback or rewards through knowledge sharing that represent my reputation and status in the community	0.7039	
Trust [87]	Likert scale	TR1	I believe that my colleague's information security knowledge is reliable	0.7510	0.8598
		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	
		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	

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

Item	Loading on oblimin-rotated factor							Uniqueness
	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
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	

[a]Blank cells represent factor loadings smaller than 0.30.

Results

Table 3 provides descriptive statistics for all variables. Table 4 specifies Spearman correlations; for the sake of brevity, correlates for controls are omitted. Tables 5 and 6 document all models and their respective diagnostic measures. Since we handled missing data conservatively by list-wise deletion, the sample size of the respective models is smaller than that of the full sample.

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 explore 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.

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 Ref. 106 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. In 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 trust 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.

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. footnotes b to Tables 5 and 6).

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 and across industries to strengthen organizational practice.

Table 3: Descriptive statistics on all variables

Variable	Obs	Mean	SD	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
Executional cost	208	3.14	0.65	1.25	5
Reputation	190	3.46	0.47	1.5	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

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 self-reported sharing of sensitive information among real individuals inside a private Information Sharing and Analysis Center (ISAC) with the behavior of these individuals. We also provide a dual empirical

Table 4: Correlations among dependent and independent variables[a]

	Frequency	Intensity	Attitude	Reciprocity (social)	Reciprocity (transactional)	Executional cost	Reputation	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			
Executional cost	−0.2238**	−0.1694*	−0.0976	−0.0314	0.1533*	1		
Reputation	−0.0226	0.0968	0.1227	0.3069***	0.0270	0.1148	1	
Trust	0.2279**	−0.0101	0.2471***	0.0269***	−0.1321	−0.1857*	0.1042	1

[a]Spearman correlations.
*$P < 0.05$; **$P < 0.01$; ***$P < 0.001$.

Table 5: Models for intensity of SIS (ordered probit estimation)[a,b]

	Baseline Coefficient (robust standard error)	Main effects Coefficient (robust standard error)	Full model Coefficient (robust standard error)
Attitude		0.4973 (0.1609)**	0.3627 (0.1672)*
Reciprocity (social)		0.3481 (0.1549)*	0.4045 (0.1526)**
Reciprocity (transactional)		0.2254 (0.1138)*	0.1860 (0.1118)
Executional cost		−0.3949 (0.1198)***	−0.4833 (0.1314)***
Reputation		0.0083 (0.1905)	0.0932 (0.1895)
Trust		−0.2250 (0.1577)	−0.1847 (0.1501)
Attitude × trust			−0.6544 (0.2874)*
Reciprocity (social) × trust			0.1969 (0.2431)
Reciprocity (transactional) × trust			−0.4561 (0.2119)*
Gender	0.2045 (0.3712)	−0.1507 (0.4480)	−0.2106 (0.4788)
Age 21–30	−0.0920 (0.3434)	−0.1286 (0.4063)	−0.1361 (0.4204)
Age 31–40	0.0567 (0.2031)	0.0896 (0.2220)	0.1139 (0.2293)
Age 41–50	−0.0001 (0.1762)	−0.0138 (0.1777)	0.0096 (0.1820)
Education none	−0.2253 (0.4789)	−0.7976 (0.5208)	−0.7239 (0.6388)
Education Master/Diploma	−0.3512 (0.4649)	−0.8990 (0.4964)	−0.8336 (0.6368)
Education Bachelor	0.0206 (0.4635)	−0.3347 (0.4924)	−0.3198 (0.6202)
Education PhD	−0.4581 (0.4984)	−0.8959 (0.5322)	−0.9997 (0.6382)
Membership duration	0.0257 (0.0134)	0.0184 (0.0165)	0.0184 (0.0164)
Government	−0.1539 (0.2729)	−0.2662 (0.3125)	−0.2945 (0.3082)
Banking and Finance	−0.0672 (0.2098)	−0.1598 (0.2527)	−0.1515 (0.2472)
All other industries	−0.0472 (0.2473)	−0.1649 (0.2977)	−0.1576 (0.2982)
Energy	0.0283 (0.2931)	−0.0650 (0.3260)	−0.1007 (0.3217)
Health	−0.3250 (0.2638)	−0.2498 (0.3260)	−0.2958 (0.3528)
Log pseudolikelihood	−318.98	−249.82	−246.50
Pseudo R^2	0.0214	0.0773	0.0896
Wald χ^2 (df)	16.10 (14)	55.43 (20)***	64.02 (23)***
Observations	225	188	188
AIC ‖ BIC	677.97 ‖ 746.29	551.65 ‖ 635.80	551.02 ‖ 644.87

[a]Two-tailed tests.

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

*$P < 0.05$; **$P < 0.01$; ***$P < 0.001$.

operationalization of SIS by introducing the measures of SIS frequency and intensity. Finally, our study confirms that interdisciplinary approaches which attempt to integrate thinking from economics and psychology are useful when SIS is studied [6].

Our study also contributes to prior work that has both theoretically predicted and descriptively noted that SIS, while beneficial, is underutilized [16, 32, 33, 44, 47, 72, 73, 103]. 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 [41, 47] 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 [65]. Moreover, regulation that attempts to solve the "sharing dilemma" in SIS should try to fix causes, not symptoms [19]. Our study has collected cross-sectional data, and hence 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 [12, 75, 76]. 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 transactional reciprocity are positively associated with both the frequency and the intensity of SIS. Since reciprocity is a social norm, it cannot be enforced 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 [23].

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 future research can build. The extant literature has documented well that actual SIS, while considered highly useful in general, is at low levels, and that individuals attempt to circumvent regulation that makes SIS mandatory [5, 32, 33, 71, 72]. Our study adds to these findings by suggesting that this economic problem of

Table 6: Models for frequency of SIS (Tobit estimation)[a,b]

	Baseline Coefficient (robust standard error)	Main effects Coefficient (robust standard error)	Full model Coefficient (robust standard error)
Attitude		0.2797 (0.1214)*	0.1895 (0.1111)
Reciprocity (social)		0.1807 (0.1195)	0.2150 (0.1046)*
Reciprocity (transactional)		0.2734 (0.0824)**	0.2361 (0.0816)**
Executional cost		−0.1872 (0.0911)*	−0.2336 (0.0962)*
Reputation		−0.1827 (0.1243)	−0.1121 (0.1232)
Trust		0.2689 (0.1058)*	0.2964 (0.1036)**
Attitude × trust			−0.3490 (0.2311)
Reciprocity (social) × trust			0.2055 (0.1813)
Reciprocity (transactional) × trust			−0.3839 (0.1378)**
Gender	0.4851 (0.1681)**	0.2412 (0.1791)	0.1837 (0.1773)
Age 21–30	0.1852 (0.2131)	0.2595 (0.2387)	0.2057 (0.2378)
Age 31–40	−0.0365 (0.1567)	0.0218 (0.1528)	0.0051 (0.1513)
Age 41–50	0.0294 (0.1222)	0.0040 (0.1264)	0.0171 (0.1243)
Education none	−0.6274 (0.1705)***	−0.9126 (0.2210)***	−0.8152 (0.2441)**
Education Master/Diploma	−0.6063 (0.1462)***	−0.8749 (0.2291)***	−0.7984 (0.2671)**
Education Bachelor	−0.5872 (0.1531)***	−0.8089 (0.2062)***	−0.7678 (0.2324)**
Education PhD	−0.5392 (0.2667)*	−0.8892 (0.2976)**	−0.9345 (0.3181)**
Membership duration	0.0277 (0.0112)*	0.0211 (0.0118)	0.0213 (0.0112)
Government	−0.1629 (0.2039)	0.0130 (0.2373)	−0.0097 (0.2288)
Banking and Finance	−0.0613 (0.1694)	0.0328 (0.2142)	0.0304 (0.2064)
All other industries	−0.5292 (0.1947)**	−0.4016 (0.2430)	−0.3748 (0.2395)
Energy	0.1054 (0.2236)	0.2191 (0.2485)	0.1867 (0.2399)
Health	−0.0909 (0.2115)	0.0767 (0.2787)	0.0465 (0.2759)
Constant	2.6652 (0.2705)***	3.0954 (0.3520)***	3.0939 (0.3577)***
Log pseudolikelihood	−274.73	−202.46	−197.92
Pseudo R^2	0.0538	0.1370	0.1564
F (df)	4.10 (14, 223)***	5.25 (20, 168)***	5.25 (23, 165)***
Observations (left ‖ right censored)	237 (12 ‖ 1)	188 (10 ‖ 1)	188 (10 ‖ 1)
AIC ‖ BIC	581.47 ‖ 636.96	448.93 ‖ 520.13	445.84 ‖ 526.75

[a]Two-tailed tests.

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

*$P < 0.05$; **$P < 0.01$; ***$P < 0.001$.

underutilization is difficult to resolve unless regulators and lawmakers consider the association of human behavior and SIS outcomes. 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 [91]. We leave it to future research to either corroborate or refute this speculation, suggesting that irrespective of any particular institutional arrangement, human behavior is significantly associated with SIS and hence likely responds to changes in institutional configuration. All in all, our study suggests that future research can productively employ behavioral theory and methods as it attempts to further develop SIS research by considering the human interaction that precedes actual acts of sharing.

In a broader sense, our work develops prior conceptual ideas that human aspects matter at least as much as technological ones when SIS is concerned [19]. 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 [57, 66]. 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 [74]. 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 [19], insights from privacy research and secure distributed computation and interaction [35] 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.[4] First, both as regards the level and the unit of analysis, our study focuses on the individual. This implies that interactions between the individual 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 financial 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 moderate 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, controlled experiments are required to establish causality. We encourage future work to introduce such methods. Further, future studies could also 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.

Conflict of interest statement. None declared.

Acknowledgments

Comments received from Tyler Moore, Thomas Maillart, Mauro Cherubini, and three anonymous reviewers all helped to improve previous versions of this article. We thank the Swiss Federal Institute of Technology Zurich for providing free software and IT support during the survey implementation phase. The usual disclaimer applies.

References

1. Ajzen I. The directive influence of attitudes on behavior. In: Gollwitzer PM and Bargh JA (eds), *The Psychology of Action: Linking Cognition and Motivation to Behavior*. New York, NY: Guilford Press, 1996, 385–403.
2. Ajzen I, Fishbein M. *Understanding Attitudes and Predicting Social Behavior*. Englewood Cliffs, NJ: Prentice-Hall, 1980.
3. Ajzen I, Madden TJ. Prediction of goal-directed behavior: attitudes, intentions, and perceived behavioral control. *J Exp Soc Psychol* 1986;**22**:453–74.
4. Amayah AT. Determinants of knowledge sharing in a public sector organization. *J Knowledge Manage* 2013;**17**:454–71.
5. Anderson R, Fuloria S. Security economics and critical national infrastructure. In: Moore T, Pym D, Ioannidis C (eds), *Economics of Information Security and Privacy*. Boston, MA: Springer, 2010, 55–66.
6. Anderson R, Moore T. The economics of information security. *Science* 2006;**314**:610–13.
7. Andreoni J. Cooperation in public-goods experiments: kindness or confusion? *Am Econ Rev* 1995;**85**:891–904.
8. Aviram A, Tor A. Overcoming impediments to information sharing. *Ala Law Rev* 2003;**55**:231–80.
9. Ba S, Pavlou P. Evidence of the effect of trust building technology in electronic markets: price premiums and buyer behavior. *MIS Quart* 2002;**26**:243–68.
10. Bauer J, van Eeten M. Cybersecurity: stakeholder incentives, externalities, and policy options. *Telecommun Policy* 2009;**33**:706–19.
11. Baumeister RF, Leary MR. The need to belong: desire for interpersonal attachments as a fundamental human motivation. *Psychol Bull* 1995;**117**:497–529.
12. Baumol WJ. Entrepreneurship: productive, unproductive, and destructive. *J Political Econ* 1990;**98**:893–921.
13. Bazerman MH. *Judgement in Managerial Decision Making*. New York, NY: Wiley, 2005.
14. Belletier C, Robert A, Motak L, *et al*. Toward explicit measures of intention to predict information system use: an exploratory study of the role of implicit attitudes. *Comput Human Behav* 2018;**86**:61–8.
15. Bénabou R, Tirole J. Incentives and prosocial behavior. *Am Econ Rev* 2006;**96**:1652–78.
16. Bisogni F. Data breaches and the dilemmas in notifying customers. In: *Workshop on the Economics of Information Security (WEIS)*, Delft, 2015.
17. Bock GW, Zmud RW, Kim YG, *et al*. Behavioral intention formation in knowledge sharing: examining the roles of extrinsic motivators, social–psychological forces, and organizational climate. *MIS Quart* 2005;**29**:87–112.
18. Bodin LD, Gordon LA, Loeb MP, *et al*. Cybersecurity insurance and risk-sharing. *J Account Pub Policy* 2018;**37**:527–44.
19. Böhme R. 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: ACM, 2015.
20. Bolton GE, Ockenfels A. ERC: a theory of equity, reciprocity, and competition. *Am Econ Rev* 2000;**90**:166–93.
21. Brennan G, Pettit P. *The Economy of Esteem*. Oxford: Oxford University Press, 2004.
22. Brosnan SF, de Waal F. Monkeys reject unequal pay. *Nature* 2003;**425**:297–99.
23. Burr R. *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, 2015.
24. Chaiken S. Heuristic versus systematic information processing and the use of source versus message cues in persuasion. *J Pers Soc Psychol* 1980;**39**:752–66.
25. Chang HH, Chuang S-S. Social capital and individual motivations on knowledge sharing: participant involvement as a moderator. *Inf Manage* 2011;**48**:9–18.
26. Cohen J, Cohen P, West SG, *et al*. *Applied Multiple Regression/Correlation Analysis for the Behavioral Sciences*. 3rd ed. London: Taylor & Francis, 2002.

4 We thank two anonymous reviewers for sharing ideas about how our approach may be expanded and generalized.

27. DellaVigna S. Psychology and economics: evidence from the field. *J Econ Lit* 2009;**47**:315–72.
28. Dillman DA, Smyth J, Christian LM. *Internet, Phone, Mail, and Mixed-Mode Surveys: The Tailored Design Method*, 4th edn. Hoboken, New Jersey: John Wiley & Sons, 2014.
29. Dunn Cavelty M. *Cybersecurity in Switzerland. Springer Briefs in Cybersecurity*. Cham: Springer International Publishing, 2014.
30. Eagly AH, Chaiken S. *The Psychology of Attitudes*. Fort Worth, TX: Harcourt et al., 1993.
31. Emler N. A social psychology of reputation. *Eur Rev Soc Psychol* 1990; **1**:171–93.
32. ENISA. *Incentives and Barriers to Information Sharing*. Heraklion: European Union Agency for Network and Information Security, 2010.
33. ENISA. *Information Sharing and Common Taxonomies between CSIRTs and Law Enforcement*. Heraklion: European Union Agency for Network and Information Security, 2016.
34. ENISA. *Information Sharing and Analysis Centres (ISACs). Cooperative Models*. Heraklion: European Union Agency for Network and Information Security, 2017.
35. Ezhei M, Ladani BT. Information sharing vs. privacy: a game theoretic analysis. *Expert Syst Appl* 2017;**88**:327–37.
36. Fehr E, Gächter S. Fairness and retaliation: the economics of reciprocity. *J Econ Perspect* 2000; **14**:159–81.
37. Fehr E, Gächter S. Altruistic punishment in humans. *Nature* 2002;**415**: 137–40.
38. Fehr E, Gintis H. Human motivation and social cooperation: experimental and analytical foundations. *Annu Rev Sociol* 2007;**33**:43–64.
39. Fehr E, Schmidt K. A theory of fairness, competition, and cooperation. *Quart J Econ* 1999;**114**:817–68.
40. Gabaix X, Laibson D, Moloche G, *et al*. Costly information acquisition: experimental analysis of a boundedly rational model. *Am Econ Rev* 2006;**96**:1043–68.
41. Gal-Or E, Ghose A. The economic incentives for sharing security information. *Inf Syst Res* 2005;**16**:186–208.
42. Gal-Or E, Ghose A. The economic consequences of sharing security information. In: Camp LJ, and Lewis S (eds), *Economics of Information Security. Advances in Information Security*, Vol. **12**. Boston, MA: Springer, 2004.
43. Gefen D, Karahanna E, Straub DW. Trust and TAM in online shopping: an integrated model. *MIS Quart* 2003;**27**:51–90.
44. Ghose A, Hausken K. A strategic analysis of information sharing among cyber attackers. *SSRN Electron J* 2006;**12**:1–37.
45. 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;**6**:24–30.
46. 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**:509–519.
47. Gordon LA, Loeb MP, Lucyshyn W. Sharing information on computer systems security: an economic analysis. *J Account Public Policy* 2003;**22**: 461–85.
48. Gordon LA, Loeb MP, Sohail T. Market value of voluntary disclosures concerning information security. *MIS Quart* 2010;**34**:567–94.
49. Gordon LA, Loeb MP, Zhou L. Investing in cybersecurity: insights from the Gordon-Loeb model. *J Inf Secur* 2016;**7**:49.
50. Gouldner AW. The norm of reciprocity: a preliminary statement. *Am Sociol Rev* 1960;**25**:161–78.
51. Granovetter M. Economic action and social structure: the problem of embeddedness. *Am J Sociol* 1985;**91**:481–510.
52. Hair JF, Black WC, Babin BJ, *et al*. *Multivariate Data Analysis*, 5th edn. Upper Saddle River, NJ: Prentice Hall, 2009.
53. Harrison K, White G. Information sharing requirements and framework needed for community cyber incident detection and response. In: *2012 IEEE Conference on Technologies for Homeland Security (HST)*, Waltham, IEEE, 2012, 463–69.
54. Hausken K. A strategic analysis of information sharing among cyber attackers. *J Inf Syst Technol Manage* 2015;**12**:245–70.
55. Hausken K. Information sharing among firms and cyber attacks. *J Account Public Policy* 2007;**26**:639–88.
56. Hsu M-H, Ju TL, Yen C-H, *et al*. Knowledge sharing behavior in virtual communities: the relationship between trust, self-efficacy, and outcome expectations. *Int J Human-Comput Stud* 2007;**65**:153–69.
57. Hume D. *A Treatise of Human Nature*. New York, NY, Oxford University Press, 2000.
58. Kahneman D, Tversky A. Prospect theory: an analysis of decision under risk. *Econometrica* 1979;**47**:263–91.
59. Kahneman D, Tversky A. Prospect theory—an analysis of decision under risk. *Econometrica* 1979;**47**:263–91.
60. Keith B, Babchuk N. The quest for institutional recognition: a longitudinal analysis of scholarly productivity and academic prestige among sociology departments. *Social Forces* 1998;**76**:1495–1533.
61. Kolm S-C, Ythier JM. *Handbook of the Economics of Giving, Altruism and Reciprocity*. Amsterdam: Elsevier, 2006.
62. Kroenung J, Eckhardt A. The attitude cube—a three-dimensional model of situational factors in IS adoption and their impact on the attitude–behavior relationship. *Inf Manage* 2015;**52**:611–27.
63. Kwahk K-Y, Park D-H. The effects of network sharing on knowledge-sharing activities and job performance in enterprise social media environments. *Comput Human Behav* 2016;**55**:826–39.
64. Laube S, Böhme R. Strategic aspects of cyber risk information sharing. *ACM Comput Surv (CSUR)* 2017;**50**:1–77.
65. Laube S, Böhme R. The economics of mandatory security breach reporting to authorities. *J Cybersecur* 2016;**2**:29–41.
66. Lindenberg S, Foss N. Managing joint production motivation: the role of goal framing and governance mechanisms. *Acad Manage Rev* 2011;**36**:500–25.
67. Luiijf E, Klaver M. On the sharing of cyber security information. In: Rice M, Shenoi S (eds), *Critical Infrastructure Protection IX*. Cham: Springer, 2015, 29–46.
68. Malhotra D. Trust and reciprocity decisions: the differing perspectives of trustors and trusted parties. *Org Behav Human Decis Process* 2004;**94**: 61–73.
69. McElreath R. Reputation and the evolution of conflict. *J Theor Biol* 2003;**220**:345–57.
70. McEvily B, Perrone V, Zaheer A. Trust as an organizing principle. *Org Sci* 2003;**14**:91–103.
71. Moore T. The economics of cybersecurity: principles and policy options. *Int J Crit Infrastruct Prot* 2010;**3**:103–17.
72. Moran T, Moore T. The Phish-Market protocol: securely sharing attack data between competitors. In: Sion R (ed.), *Financial Cryptography and Data Security*. Berlin-Heidelberg: Springer, 2010, 222–37.
73. Naghizadeh P, Liu M. Inter-temporal incentives in security information sharing agreements. In: *2016 Information Theory and Applications Workshop (ITA)*. IEEE, 2016, 1–8.
74. Nelson RR, Winter SG. *An Evolutionary Theory of Economic Change*. Cambridge: Belknap Press, 1982.
75. North DC. *Institutions, Institutional Change and Economic Performance*. Cambridge: Cambridge University Press, 1990.
76. North DC. *Understanding the Process of Economic Change*. Cambridge: Cambridge University Press, 2005.
77. Nunnally JC, Bernstein I. 2017. *Psychometric Theory*, 3rd edn. New York: McGraw-Hill.
78. Oliver P. Rewards and punishments as selective incentives for collective action: theoretical investigations. *Am J Sociol* 1980;**85**:1356–75.
79. Olson M. *The Logic of Collective Action*. Cambridge, MA: Harvard University Press, 1965.
80. 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.
81. Park JH, Gu B, Leung ACM, *et al*. An investigation of information sharing and seeking behaviors in online investment communities. *Comput Human Behav* 2014;**31**:1–12.

82. Petty RE, Cacioppo, JT. The elaboration likelihood model of persuasion. *Adv Exp Soc Psychol* 1986;**19**:123–205.
83. Podsakoff PM, MacKenzie S, Podsakoff NP. Sources of method bias in social science research and recommendations on how to control it. *Annu Rev Psychol* 2012;**63**:539–69.
84. Podsakoff PM, Organ DW. Self-reports in organizational research: problems and prospects. *J Manage* 1986;**12**:531–44.
85. Reinholt MIA, Pedersen T, Foss NJ. Why a central network position isn't enough: the role of motivation and ability for knowledge sharing in employee networks. *Acad Manage J* 2011;**54**:1277–97.
86. Ridings CM, Gefen D, Arinze B. Some antecedents and effects of trust in virtual communities. *Strategic Inf Syst* 2002;**11**:271–95.
87. Safa NS, von Solms R. An information security knowledge sharing model in organizations. *Comput Human Behav* 2016;**57**:442–51.
88. Siegrist J, Starke D, Chandola T, *et al*. The measurement of effort–reward imbalance at work: European comparisons. *Soc Sci Med* 2004;**58**:1483–99.
89. Simon HA. *Administrative Behavior: A Study of Decision-Making Processes in Administrative Organization*. New York, NY: Free Press, 1976.
90. Smith EA, Winterhalder B. (eds) *Evolutionary Ecology and Human Behavior*. New York, NY: Routledge, 2017.
91. Thaler RH, Sunstein CR. *Nudge: Improving Decisions about Health, Wealth, and Happiness*. New York, NY: Penguin Books, 2009.
92. Tom S, Fox C, Trepel C, *et al*. The neural basis of loss aversion in decision-making under risk. *Science* 2007;**315**:515–518.
93. Tomasello M, Carpenter M, Call J, *et al*. Understanding and sharing intentions: the origins of cultural cognition. *Behav Brain Sci* 2005;**28**:675–91.
94. 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.
95. Tricomi E, Rangel A, Camerer C, *et al*. Neural evidence for inequality-averse social preferences. *Nature* 2010;**463**:1089–1091.
96. Tversky A, Kahneman D. Loss aversion in riskless choice: a reference dependent model. *Quart J Econ* 1991;**106**:1039–61.
97. Tversky A, Kahneman D. Advances in prospect theory: cumulative representation of uncertainty. *J Risk Uncertainty* 1992;**5**:297–323.
98. Vakilinia I, Louis SJ, Sengupta S. Evolving sharing strategies in cybersecurity information exchange framework. In: *Proceedings of the Genetic and Evolutionary Computation Conference Companion*. New York, NY: ACM, 2017, 309–10.
99. von Hippel E, von Krogh G. Open source software and the "private-collective" innovation model: issues for organization science. *Org Sci* 2003;**14**:209–23.
100. Wang W-T, Hou Y-P. Motivations of employees' knowledge sharing behaviors: a self-determination perspective. *Inf Org* 2015;**25**:1–26.
101. Wang JH, Wang C, Yang J, *et al*. A study on key strategies in P2P file sharing systems and ISPs' P2P traffic management. *Peer-to-Peer Network Appl* 2011;**4**:410–19.
102. Watzlawick P, Bavelas JB, Jackson DD. *Pragmatics of Human Communication*, New York, Norton & Company, 2011.
103. Weiss E. *Legislation to Facilitate Cybersecurity Information Sharing: Economic Analysis*. Washington, DC: Congressional Research Service, 2015.
104. Williamson OE. The economics of organization: the transaction cost approach. *Am J Sociol* 1981;**87**:548–77.
105. Xiong L, Liu L. PeerTrust: supporting reputation-based trust for peer-to-peer electronic communities. *IEEE Trans Knowledge Data Eng* 2004;**16**:843–57.
106. 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.
107. Zhao W, White G. A collaborative information sharing framework for Community Cyber Security. In: *IEEE Conference on Technologies for Homeland Security (HST)*, Waltham, MA: IEEE, 2012, 457–62.