Computers in Human Behavior 106 (2020) 106255

Contents lists available at ScienceDirect

Computers in Human Behavior

journal homepage: www.elsevier.com/locate/comphumbeh

Knowledge absorption for cyber-security
The role of human beliefs

Dimitri Percia David [a,b,*], Marcus Matthias Keupp [b,c], Alain Mermoud [a,b,d]

[a] Department of Information Systems, Faculty of Business and Economics (HEC Lausanne), University of Lausanne (UNIL), 1015 Lausanne, Switzerland
[b] Department of Defence Management, Military Academy at ETH Zurich, 8903 Birmensdorf, Switzerland
[c] Institute of Technology Management, University of St. Gallen, 9000 St. Gallen, Switzerland
[d] EPFL Cyber-Defence Campus, armasuisse Science and Technology, 1015 Lausanne, Switzerland

ARTICLE INFO

Keywords:
Cyber-security
Security economics
Information sharing
Organizational learning
Knowledge-based view
Tacit knowledge
Knowledge absorption

ABSTRACT

We investigate how human beliefs are associated with the absorption of specialist knowledge that is required to produce cyber-security. We ground our theorizing in the knowledge-based view of the firm and transaction-cost economics. We test our hypotheses with a sample of 262 members of an information-sharing and analysis center who share sensitive information related to cyber-security. Our findings suggest that resource belief, usefulness belief, and reciprocity belief are all positively associated with knowledge absorption, whereas reward belief is not. The implications of these findings for practitioners and future research are discussed.

1. Introduction

For both public and private organizations, effective cyber-security is required to prevent business interruption and thus to ensure operational continuity (Fransen, Smulders, & Kerkdijk, 2015; Furnell & Clarke, 2012; Gordon, Loeb, & Zhou, 2016; Luiijf & Klaver, 2015; Skopik, Settanni, & Fiedler, 2016; Tounsi & Rais, 2018). The production of such cyber-security is a knowledge-intensive task (Ben-Asher & Gonzalez, 2015; Jakobson, 2011). Despite the fact that hardware and software components required for this defense are relatively homogeneous and readily available at low cost or even for free (Anderson, 2001; Hofmann & Ramaj, 2011), highly specialist knowledge is required to combine and deploy these components effectively for organizational defense — for instance, by designing resilient systems architectures and implementing them efficiently (Etzioni, 2011; Lee, Bagheri, & Kao, 2015). Hence, cyber-security is a complex capability that is not readily created by the purchasing of technological components; rather, it is the skilled knowledge of how to organize and orchestrate these components that creates the actual defense (Anderson, 2001; Hofmann & Ramaj, 2011; Solms & Niekerk, 2013). Furthermore, due to the swift technological evolution and short technology life-cycles of these components, knowledge required to produce cyber-security becomes obsolete (Casas et al., 2017; Chen, Chiang, & Storey, 2012; Mahmood & Afzal, 2013; Wang et al., 2014). Organizations are hence under continuous pressure to update existing and acquire novel knowledge to keep up with the evolution of cyber-threats (Bauer & van Eeten, 2009; Cardenas, Manadhata, & Rajan, 2013; Casas et al., 2017; Chen et al., 2012; Cui & He, 2016; Laube & Böhme, 2017; Mahmood & Afzal, 2013; Ransbotham, Kane, & Lurie, 2012; Sait et al., 2015; Singh & Nene, 2013; Terzi, Terzi, & Sagiroglu, 2017; Wang et al., 2014, 2014).

Any organization that has to organize cyber-security might thus be interested in a continuous absorption of such specialist knowledge. Knowledge absorption is an organizational capability to transfer, integrate, and utilize new knowledge obtained from external sources (Cohen & Levinthal, 1989; Grant, 1996a, 1996b; Park, 2011; Tsai, 2001). Prior research suggests that if the organization succeeds at this knowledge absorption, the investment cost for any given level of information security is reduced (Gal-Or & Ghose, 2005), as are inefficient duplications of effort (Feledi, Fenz, & Lechner, 2013). Furthermore, the effectiveness of security solutions improves (Parsons et al., 2014; Safa & Von Solms, 2016).

As organizations can absorb knowledge only by the learning of their existing members or the recruitment of new members (March, 1991; Simon, 1991), our study of knowledge absorption puts the individual level of analysis to the fore. After all, it is humans who learn and develop specialist knowledge, and who use this knowledge to orchestrate the technical components for effective cyber-defense. Therefore, it is not surprising that recent research has emphasized that any understanding of cyber-security is incomplete unless the association of

* Corresponding author at: Department of Information Systems, Faculty of Business and Economics (HEC Lausanne), University of Lausanne (UNIL), 1015 Lausanne, Switzerland.
E-mail address: dimitri.percia.david@protonmail.ch (D. Percia David).

https://doi.org/10.1016/j.chb.2020.106255
Received 18 October 2018; Received in revised form 7 November 2019; Accepted 7 January 2020
Available online 11 January 2020

individual action and cyber-security outcomes is studied (Anderson, 2001; Anderson & Fuloria, 2010; Anderson & Moore, 2006; Gordon, Loeb, & Lucyshyn, 2003; Laube & Böhme, 2017). However, few such studies exist to date. A recent overview of the related literature by Laube and Böhme (2017) suggests that almost all research on cyber-security information exchange (and subsequent knowledge absorption) is characterized by the following limitations. First, the overwhelming majority of this literature does not analyze individuals, but analyzes impersonal information such as log-files (Flegel, 2002; Forte, 2004; Maillart et al., 2017; Masud et al., 2008; Moore & Clayton, 2011). Much literature is also restricted to pure game theory or simulation (Cavusoglu, Raghunathan, & Yue, 2008; Fielder et al., 2014; Gal-Or & Ghose, 2005; Gordon et al., 2003; Grossklags, Christin, & Chuang, 2008; Hausken, 2007; Kunreuther & Heal, 2003; Manshaei et al., 2013; Shiva, Roy, & Dasgupta, 2010). Second, a cyber-security context often requires sensitive and classified information that is unlikely to be shared or disseminated by public channels (Bisogni, 2015; Gal-Or & Ghose, 2005; Hausken, 2007; Laube & Böhme, 2017; Moran & Moore, 2010; Weiss, 2014). Third, the knowledge required to build cyber-security is expert knowledge and hence is highly tacit, i.e., bound in personal experience. Such tacit knowledge is not only hard to describe objectively (e.g., by documentation in manuals or textbooks), but it can also not readily be transferred among individuals, unless by intense social interaction between sender and recipient (Nonaka & Takeuchi, 1995; Polanyi, 1962; Siesfeld, Cefola, & Neef, 2009). Although some work on cyber-security studies the transfer of explicit knowledge that can be documented in forums and databases (e.g., Yan et al. (2016) and Safa and Von Solms (2016)), we are not aware of any empirical work that would analyze the transfer and absorption of tacit knowledge in a cyber-security context. This lack of attention constitutes an important research gap (Wang & Noe, 2010). Fourth and finally, even if the absorption of tacit knowledge requires human interaction, the social process alone does not necessarily imply that knowledge is actually absorbed. Human interaction can be futile if the possessor of any knowledge is unable or unwilling to transfer it to other individuals. To the best of our knowledge, the existing literature focuses on attitudes, motivations and contexts that influence an individual's propensity to (not) share information (Jeon, Kim, & Koh, 2011; Naghizadeh & Liu, 2016; Pi, Chou, & Liao, 2013; Safa & Von Solms, 2016; Ter Wal, Criscuolo, & Salter, 2017; Tosh et al., 2017; Wagner et al., 2018; Wang & Hou, 2015; Zibak & Simpson, 2019). In contrast, we are not aware of any contribution that measures the extent to which (i.e., the success with which) actual knowledge absorption for cyber-security has occurred as a result of social interaction.

The purpose of our paper is to address all of these limitations. We study the extent to which an individual successfully absorbs knowledge in a private, collaborative setting in which sensitive, non-public and tacit knowledge required to build cyber-security is absorbed through information sharing. Hence, both the focus and the unit of analysis are on the individual level. Recent work has highlighted that the study of such collaborative-information sharing should lead to a better understanding of cyber-security (Laube & Böhme, 2017). We go one step further by not only studying elements associated with such information sharing, but also its outcomes in terms of individual knowledge absorption.

We first build a framework that is anchored in the knowledge-based view of the firm, arguing that the absorption of tacit knowledge is associated with human beliefs (Section 2). Using ordered probit regression, we then test this model with psychometric data from 262 members of the closed user group of MELANI-net, the national information sharing and analysis center (ISAC) in Switzerland (Section 3). Our results suggest that resource belief, usefulness belief, and reciprocity belief are positively associated with knowledge absorption, whereas belief in hard rewards is not (Section 4). We discuss the implications of our findings and provide recommendations for future research and managerial practice (Section 5).

2. Theoretical framework and hypotheses

In this section, we present our hypotheses related to potential associations between human beliefs and knowledge absorption.

The knowledge-based view of the firm suggests that knowledge is a valuable, scarce, and imperfectly imitable resource and hence is a significant source of competitive advantage for organizations (Barney, 1991; Foss, 1996; Grant, 1996a, 1996b; Kogut, 2000; Nickerson & Zenger, 2004; Phelan & Lewin, 2000; Spender, 1996). More specifically, specialist knowledge is a significant contributor to product, process and service innovation (Grant, 1996a, 1996b; Scarbrough, 2003; Schilling, 2010; Tether & Tajar, 2008). Hence, an organization must continuously absorb specialist knowledge to be able to generate innovations that can provide cyber-security for its IT components and systems architecture.

Organizational knowledge absorption is the result of individual (i.e., human) learning. An organization absorbs knowledge only by the learning of its current members, or by the inclusion of new members (Grant, 1996a, 1996b; March, 1991; Simon, 1991). In this article, we focus on the learning of existing organization members.[1] In this perspective, novel organizational knowledge is created by the individual knowledge absorption of these members (Bock & Kim, 2002).

However, for any individual member, knowledge absorption from beyond the boundary of the organization is not a free activity. Typically, an individual incurs significant transaction costs before any economic exchange is completed. Such costs include time spent and financial resources dedicated to receiving information, making decisions, and the process of interacting with others (Williamson, 1981). In the context of an ISAC, these costs are incurred once the individual begins to interact with others, as intensive social interaction is required for a successful transfer of tacit knowledge between any two individuals (Kogut & Zander, 1993; Nonaka & Takeuchi, 1995; Polanyi, 1962; Teece, 1977, 1983). Prior research also suggests that if information sharing takes too much time, is too laborious, or requires too much effort, an individual engages less in knowledge transfer, and the amount of knowledge transferred is reduced (ENISA, 2010, 2018; Luiijf & Klaver, 2015; Yan et al., 2016). Furthermore, the knowledge may be classified or irrelevant from the individual's perspective. We therefore propose that before making any specific assessment, the individual might estimate whether or not the knowledge present in the ISAC is generally worth the transaction cost required to absorb this knowledge. Unless this assessment is positive, the individual is unlikely to engage in any profound interaction at all.

2.1. H1: Resource belief

When individuals must make such considerations, they typically use cues and heuristics to simplify the decision-making process (Gabaix et al., 2006; Petty & Cacioppo, 1986). By such cues, objective and impersonal assessment is replaced by a subjective, belief-based assessment of whether or not the information to be received is useful at all (Bosch, Volberda, & Boer, 1999; Kogut & Zander, 1993; Polanyi, 1962). Whenever such a belief is present, individuals are more prone to engage in social interactions that precede knowledge absorption (Lichtenthaler & Ernst, 2007). Hence, knowledge absorption might be positively associated with the extent to which the individual believes the knowledge available in the ISAC constitutes a valuable, rare, and imperfectly imitable asset – i.e., a resource (Barney, 1991) – that is worth absorbing (resource belief). Hence,

H1: *Knowledge absorption is positively associated with resource belief.*

[1] We consider the discussion of recruiting strategies for novel members beyond our scope, because this context would transcend both the individual level of analysis and the boundary of the firm.

H1 is therefore related to the individual's belief that the transaction costs of knowledge sharing will be outweighed by the benefits that will come from such a social interaction (i.e., knowledge sharing); such benefits being concertized by knowledge absorption resulting from knowledge sharing.

2.2. H2: Usefulness belief

While this resource belief may induce the individual to interact with others at all, it does not necessarily imply the knowledge available is directly applicable for the specific job tasks the individual is charged with. For example, ISAC participants may exchange information that is useful to the industry or the organization in general, but that information may offer no specific guidance for any particular job task.

Prior research suggests that individuals do not necessarily act altruistically – i.e., only in the interest of the organization (Nagin et al., 2002). Goal-alignment theory suggests that individual and organizational goals are not necessarily congruent (Hume, 2000; Lindenberg & Foss, 2011). Consequently, an individual would not only consider the general usefulness of any knowledge available from other ISAC members – i.e., whether or not this knowledge constitutes a resource that is worth the transaction cost – but also the extent to which this knowledge is specifically useful for any particular job task.

As the job performance evaluation of the individual might be considered as a specific contribution to organizational cyber-security, the individual has an incentive to study the specific usefulness of any information with this job-related assessment in mind (Feldman & March, 1981; Luiijf & Klaver, 2015; Nagin et al., 2002). Hence, knowledge absorption might be positively associated with the extent to which individuals believe the knowledge available in the ISAC specifically contributes to fulfilling their job tasks (usefulness belief). Hence,

H2: *Knowledge absorption is positively associated with usefulness belief.*

If H1 is related to the individual's fundamental assessment that determines if engaging in knowledge sharing is worth it (i.e., the transaction costs of such a social interaction will be outweighed by the benefits coming from the resulting knowledge absorption in general), H2 reaches one step further by suggesting that knowledge absorption might be useful for the individual's job tasks.

2.3. H3: Reward belief

Further, goal alignment theory also suggests that the individual may choose to not disclose the specialist knowledge absorbed to other members of the organization. Typically, individuals align their behavior with their return goals; hence they expect to be rewarded whenever they exhibit behavior that is in the organization's interest (Nagin et al., 2002).

Unless individuals believe that the organization will provide such rewards, they may choose to exploit their ISAC membership on an individual basis (e.g., by hoarding knowledge to make oneself irreplaceable in the organization, by starting up a firm or by selling private consultancy services to the industry). Hence, the individual would not absorb knowledge in the interest of the organization, but rather in the interest of private business. To solve this incentivization problem, organizations typically offer — hard reward so whenever knowledge is absorbed and shared for the benefit of the organization. Such rewards include job promotions, greater job security, salary increases, or more power and responsibility in the organization (Bock & Kim, 2002; Centers & Bugental, 1966; Kalleberg, 1977; Ryan & Deci, 2000). For example, Buckman Laboratories distinguishes its 100-top information-sharers at an annual conference located at a resort (Singh, 2005). Lotus Development, an IBM division, rewards employees for information sharing activities (Davenport & Glaser, 2002). Prior research suggests

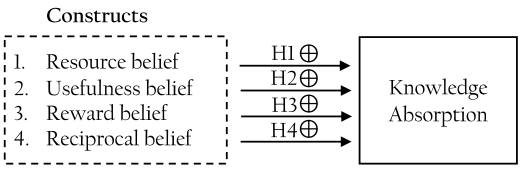

Fig. 1. Knowledge-Absorption Model. Notes to Fig. 1: Each construct and its respective hypothesis (H1 to H4) are potentially positively associated with the dependent variable – i.e., knowledge absorption.

that such rewards positively contribute to individuals' hours worked, dedication, and performance (Encinosa, Gaynor, & Rebitzer, 2007; Gaynor, Rebitzer, & Taylor, 2001).

Therefore, the more individuals believe they will receive such – 'hard rewards' for successful knowledge absorption (reward belief), the more they should be likely to concentrate on realizing such absorption. Hence,

H3: *Knowledge absorption is positively associated with reward belief.*

If H2 is related to the individual's assessment that determines if engaging in knowledge sharing will help the fulfillment of their job tasks (i.e., the transaction costs of such a social interaction will be outweighed by the benefits coming from the resulting knowledge absorption in terms of job tasks fulfillment), H3 suggests that knowledge absorption might be fostered if such absorption is compensated by rewards delivered by the organization.

2.4. H4: Reciprocity belief

Given that knowledge is a valuable, scarce and imperfectly imitable resource, the value of a unit of cyber-security knowledge is proportional to the incremental cyber-security enhancement that this unit is supposed to provide (Bodin et al., 2018; Gordon, Loeb, Lucyshyn, & Zhou, 2015). As individuals are probably aware that any knowledge they share delivers such benefits to others, they may expect to receive adequate knowledge in return. Typically, humans prefer such equitable exchanges over any other arrangement (Andreoni, 1995; Bolton & Ockenfels, 2000; Kolm & Mercier-Ythier, 2006), and they punish those who defect from this principle of equity or refuse to reciprocate when another individual provides something valuable (Brosnan & Waal, 2003; Fehr & Gächter, 2000, 2002; Tricomi et al., 2010). For example, reciprocal fairness is an important variable in the design of peer-selection algorithms in peer-to-peer (P2P) networks. As a result, the operators of such networks have developed ways to remove – 'leechers' who demand information without providing any (Wang et al., 2011). The extent to which an individual can absorb tacit knowledge by social exchange might depend on the extent to which this individual is willing to reciprocate whenever they receive information from others (Xiong & Liu, 2004).

Therefore, unless the individual believes that original knowledge sharing will be reciprocated (reciprocity belief), they might terminate social interaction with others. As such interaction is a prerequisite of effective absorption, any prior level of knowledge absorption would significantly decrease. Hence,

H4: *Knowledge absorption is positively associated with reciprocity belief.*

The following illustration summarizes the different constructs – i.e., the set of independent variables and their respective hypothesis –, and emphasizes their potential association with the dependent variable, i.e., knowledge absorption.

By testing the above-mentioned model, we suggest to explore with which intensity (if at all) the variable of *knowledge absorption* is associated with the individual's beliefs.

3. Data and methods

In this section, we present the sampling context and population of this study, how we measured our independent variable, items and constructs, how we implemented the questionnaire in order to measure our items and constructs, as well as how we proceeded with our analysis.

3.1. Sampling context and population

As our theoretical reasoning focuses on knowledge absorption by social interaction, the sampling context must fit this research interest. We therefore collected our data from the closed user-group of MELANI-net — the Swiss national information sharing and analysis center (ISAC). An ISAC is a nonprofit organization that brings together cyber-security managers in person to facilitate interpersonal information exchange between critical-infrastructure providers (CIP).[2] Both the survey and the related dataset we exploit are identical to those described in Mermoud et al. (2019).

This setting is particularly useful for our context as individuals in the closed user-group participate on behalf of their organizations, share highly sensitive and classified information in a private and exclusive setting, and interact socially as they share and absorb tacit knowledge. The 424 members of the closed user-group are all managers and specialists who must provide cyber-security for their respective organizations. They come from both private and public CIP. They have to undergo government identification and clearance procedures, as well as background checks before being admitted for ISAC membership. There is no interaction whatsoever between these members and the public, and no external communication to the public or any publication of relevant knowledge is made. Hence, this setting matches our proposition that the knowledge needed to produce cyber-security is not only classified and difficult to identify, but also tacit and grounded in personal experience, such that social interaction between individuals is required to transfer it.

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

3.2. Measures

Our study follows individuals who self-report about their beliefs. We therefore chose a psychometric approach to operationalize our constructs (Nunnally & Bernstein, 2017).

We introduce a novel ordinal indicator to capture individual knowledge absorption. It asks respondents to state which amount of exclusive information they receive through security information exchange with the other participants inside the ISAC.

To measure the different beliefs we hypothesized, extant psychometric scales were used. Adaptions of these scales to our population context were kept to a minimum. Table 1 details all constructs, their sources, item composition and wording, dropped items (if any), factor loadings; and Cronbach alphas.

To capture respondent heterogeneity, we controlled for gender, age, and education level. Gender was coded dichotomously (male, female). Age was captured by four mutually exclusive categories (21–30, 31–40, 41–50, 50+ years). Education level was captured by six mutually exclusive categories (none, bachelor, diploma, master, PhD, other).[3]

We further captured the respondent's hierarchical position in the organization (employee, chief employee – i.e., intermediary supervisor position –, middle management, management, member of the board, other), as this position may influence both the propensity of sharing knowledge as such, and the intensity with which knowledge is actually shared (Cai et al., 2013).

We also controlled for the number of years the individual had experience with collaborative-information sharing (prior information sharing experience: not in charge, less than 1, 1 to 3, 3 to 6, over 6), as such experience is significantly associated with information sharing intention (Lee & Ma, 2012).

Further, the extent to which the respondent can absorb knowledge can co-evolve with the length of ISAC membership, as individuals gain more insight over time and develop interpersonal relationships. Hence, we controlled for membership duration and calculated it as the difference between 2017 and the year the individual became an ISAC member.

Also, individual experience from past social interactions can influence the respondent's beliefs (Haemmerli, Raaum, & Franceschetti, 2013; Vázquez et al., 2012). We therefore asked respondents to state whether or not they had already participated in prior ISAC meetings and events (dichotomously coded yes/no).

Sympathy and antipathy in peer relations might influence the extent to which individuals interact and learn; hence, the quality of any peer relation may influence the extent to which knowledge absorption can occur (Chow & Chan, 2008; Coolahan et al., 2000). We therefore asked respondents to rate their individual perception of the personal relationships they had with their peers among ISAC members (very friendly, friendly, neutral, unfriendly, very unfriendly).

We also asked respondents to rate their potential individual contribution by indicating the extent to which they felt they (generally) had much information to share (strongly agree, agree, neutral, disagree, strongly disagree). We insert this control into the model as an individual's intention to share knowledge might be associated with how much the individual knows already. Further, individuals who have little to share might receive less information from their peers as these feel less compelled to reciprocate if they receive little in the first place (Chang & Chuang, 2011; Davenport, Prusak, et al., 1998).

Finally, we controlled for the industry heterogeneity (government, banking/finance, energy, health, all other industries) by logging each respondent's self-reported affiliation. This information was used to construct dichotomous indicators ('dummy variables') that group respondents into the five industry categories, government, banking & finance, energy, health, and all other industries. Each dummy variable takes on the value 1 if a respondent is affiliated with a particular industry, and has a value of 0 otherwise.

[2] For a general introduction to the concept of an ISAC and illustrative examples, see Powner (2005) and ENISA (2018). For a detailed description of MELANI-net, its organization and history, see Cavelty (2014).

[3] For instance, an individual who has a master's degree has necessarily a bachelor's degree, and therefore will be flagged only in the master's degree category. The term *diploma* refers to the Swiss *CFC*, i.e., a *Federal Certificate of Competence*, which is a diploma awarded for an apprenticeship of 3 to 4 years and successful completion of a final examination.

Table 1
Constructs.

Measure	Type	Item	Text	Fact. l.	Cr. α
[Publication]					
Dependent					
Knowledge absorption (Novel)	Ordered categorical indicator	n/a	Which amount of exclusive information do you receive through security information exchange with MELANI? * Very Small * Small * Neutral * Large * Very Large	n/a	n/a
Independent					
Resource belief (Carol, Davison, & Wong, 2016)	Likert scale	RES1	I believe that people in my network give credit for each other's knowledge where it is due	Dropped	0.82
		RES2	I believe that people in my network respond when I am in need	0.81	
		RES3	I believe that people in my network use each other's knowledge appropriately	0.82	
		RES4	I believe that my requests for knowledge will be answered	0.86	
		RES5	I believe that people in my network share the best knowledge that they have	Dropped	
Usefulness belief (Tamjidyamcholo et al., 2014)	Likert scale	US1	SIS would decrease the time needed for my job responsibilities	0.85	0.71
		US2	SIS would increase the effectiveness of performing job tasks	0.86	
		US3	Considering all aspects, SIS would be useful	0.64	
Reward belief (Wang & Hou, 2015)	Likert scale	HR1	I expect to be rewarded with a higher salary in return for sharing knowledge with other participants	0.91	0.81
		HR2	I expect to receive monetary rewards (i.e., additional bonus) in return for sharing knowledge with other participants	0.90	
		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	0.73	
Reciprocity belief (Kwahk & Park, 2016)	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	0.8
		NOR2	I believe that other people will help me when I need help if I share knowledge with others through MELANI	0.82	
		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	0.87	
		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	0.79	

3.3. Implementation

Data for all variables was collected from individual respondents by a questionnaire instrument. We followed the procedures and recommendations of Dillman, Smyth, and Christian (2014) for questionnaire design, pretest, and implementation. Likert-scaled items were anchored at – 'strongly disagree' (1) and – 'strongly agree' (5) with 'neutral' as the midpoint (3). The questionnaire was first developed as a paper instrument. It was pretested with seven different focus groups from academia and the cyber-security industry. The 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 pretests 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 it also made clear that we had no financial or business-related interests. We followed Podsakoff, MacKenzie, et al. (2003), as far as this was possible for a cross-sectional research design, to alleviate common method bias concerns from the onset.

The paper instrument was then implemented as a web-based survey by using the *Select-Survey* software provided by the Swiss Federal Institute of Technology Zurich (ETH). 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, free of charge, a research report that summarized the responses. Respondents could freely choose to save intermediate questionnaire completions and to return to the survey and complete it at a later point in time.

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

3.4. Analysis

Upon completion of the survey, the 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 over-representation of individuals affiliated with any particular organization, thus suggesting no need for a nested analytical design.

By calculating item-test, item-rest, and average inter-item correlations, the validity of each construct was tested (Hair, 2006). The reliability was measured by Cronbach alpha. We performed iterative principal component factor analysis with oblique rotation until total variance explained was maximized and each item clearly loaded on one factor. During this process, four items were dropped because they did not meet these criteria. Table 2 details the results of this procedure, and Table 1 documents the dropped items. The high direct factor-loadings and low cross-loadings of the final four factors we identified indicate a high degree of convergent validity (Hair, 2006). All of these have an eigenvalue above unity. The first factor explained 19.1% of the total variance, suggesting the absence of significant common method variance in the sample (Podsakoff & Organ, 1986). To construct the scale values, individual item scores were added, and this sum was divided by the number of items in the scale (Reinholt, Pedersen, & Foss, 2011; Trevor & Nyberg, 2008).

Our dependent construct is ordered and categorical, therefore we estimated an ordered probit model. A comparison with an alternative ordered logit estimation confirmed the original estimations and indicated that the ordered probit model slightly better fit the data. The model was estimated with robust standard errors to neutralize any potential heteroscedasticity. For the controls age, industry, and education, a benchmark category was automatically selected during estimation (cf. footnote *b* of Table 5). Consistent with the recommendation of Cohen et al. (2002), we incrementally built all models by entering only the controls in a baseline model first, then, we added the main effects. In both estimations, we mean-centered all measures before entering them into the analysis. Model fit was assessed by repeated comparisons of Akaike and Bayesian information criteria between different specifications.

4. Results

Table 3 provides summarized descriptive statistics. 95% of respondents are male, 32% are below and 68% above the age of 40. Practitioners without a formal degree constitute 20% of the sample, whereas 68% have a certificate of competence or a bachelor degree. Only 4.6% have a master degree or a PhD. The majority of the sample is composed of two groups: employees or intermediate supervisors (42% of respondents), and middle or line managers (51%). Only 2.7% are top managers or board members. 43% of respondents have up to three years of experience with collaborative information sharing, and 48% have more than three years of such experience. 52% had already participated in one of more prior ISAC meetings or event.

Since our dependent variable is ordinal, a monotonic correlation analysis is necessary. Moreover, data for ordinal variables need not be distributed normally. Table 4 therefore provides Spearman rather than Pearson correlations. For the sake of brevity, correlates for controls are omitted. Table 5 documents the final best-fitting model, together with its diagnostic measures.

H1 is supported. Resource belief is positively associated with knowledge absorption at $p < 0.05$. This suggests that whenever an individual believes valuable knowledge can be acquired, they are more willing to invest the transaction cost for tacit knowledge absorption and are able to absorb such knowledge to a greater extent.

H2 is supported. Usefulness belief is positively associated with knowledge absorption at $p < 0.01$. This finding is in line with our theoretical expectation that individuals seek knowledge absorption not for its own sake, but in order to augment the efficiency and effectiveness of their cyber-security production.

H3 is not supported. Reward belief is not significantly associated with knowledge absorption. In context with the above findings for H1 and H2, this signals that the individual's decision to participate in a knowledge-transfer process is primarily intrinsically motivated. Moreover, this non-finding might be due to the fact that Wang and Hou (2015) introduce their measure of reward belief (which we adapted for our study) in the context of public information-sharing and absorption, implying that in a private setting of knowledge absorption, intrinsic motivations for absorption might outweigh extrinsic ones.

H4 is supported. Reciprocity belief is significantly associated with the extent to which the individual absorbs knowledge at $p < 0.01$. This finding is in line with our theoretical expectation that knowledge absorption is ultimately the result of reciprocated human interaction.

Although all control variables and industry dummy variables capture variance, only one of them is significant at $p < 0.05$. We find that knowledge absorption is not associated with an individual's job position, prior information-sharing experience, size of the organization

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	Uniqueness
HR1	0.91				0.14
HR2	0.90				0.18
HR4	0.73				0.44
US1				0.85	0.26
US2				0.86	0.22
US3				0.64	0.39
NOR2			0.82		0.26
NOR3			0.87		0.21
NOR4			0.79		0.36
RES2		0.81			0.28
RES3		0.82			0.28
RES4		0.86			0.24
Eigenvalue	2.29	2.29	2.22	1.94	
Proportion of variance explained	19.10%	19.05%	18.48%	16.20%	
Cumulative variance explained	19.10%	38.16%	56.64%	72.84%	

[a]Blank cells represent factor loadings (x) such as $|x| < 0.3$.

Table 3
Descriptive statistics.

Variable	Obs	Mean	Std. Dev.	Min	Max
Knowledge absorption	260	3.13	0.86	1	5
Resource belief	190	3.82	0.52	1.67	5
Usefulness belief	208	3.78	0.62	1.67	5
Reward belief	195	2.16	0.75	1	4
Reciprocity belief	195	3.89	0.61	1.67	5
Size of the organization	260	4.57	0.90	1	5
Quality of peer relationships	260	3.93	0.70	3	5
Potential individual contribution	243	3.07	0.91	1	5
Membership duration	260	6.05	5.35	0	17

that employs an individual, quality of peer relationships, potential individual contribution, an individual's gender, age, education level, industry affiliation, or length of ISAC membership. These non-findings do not only alleviate concerns about unobserved heterogeneity among respondents, but the non-significance of the industry dummies also alleviates concerns of over-representation of a particular industry or firm among the responses.

The one significant effect we do find suggests that participation in prior ISAC events (such as group meetings, conferences, and industry-specific talks) is positively associated with knowledge absorption. This finding suggests that knowledge absorption positively evolves over time, as individuals build social relationships during such events.

5. Discussion

In this last section, we present our concluding comments, the policy recommendations resulting from concluding comments, we discuss the limitations of this study and suggest paths for further research.

In this article, we argue that the production of organizational cyber-security is associated with the extent to which the members of this organization, i.e., human beings, can absorb the tacit knowledge required for this production. Framing this argument in the knowledge-based view of the firm and transaction cost economics, we empirically show that human beliefs are significantly associated with the extent to which an individual absorbs knowledge.

To the best of our knowledge, our study is the first empirical contribution that analyzes knowledge absorption in a private setting, where sensitive knowledge required for cyber-security products and services is shared and absorbed. Prior to our approach, scholars analyzed human interaction in the context of cyber-security, but almost exclusively in public settings. We develop this empirical literature by focusing on tacit knowledge-transfer in a private setting, thus suggesting this research design corresponds more closely with both the type of knowledge required to produce cyber-security and the transmission channels by which this sensitive and classified knowledge is shared.

We also contribute to filling the significant gap that Laube and Böhme (2017) note in their tabulation of the recent literature. Through this research, we help to extend the literature on the economics of information security by suggesting that cyber-security is not solely a technical issue. Whereas many technological solutions to cyber-security have been proposed, few of these are successful unless an economic perspective is adopted (Anderson, 2001; Anderson & Moore, 2006). Our study therefore strengthens the proposition that interdisciplinary approaches which attempt to integrate thinking from economics and psychology when considering cyber-security are useful (Anderson & Moore, 2006; Furnell & Clarke, 2012). For the same reason, we suggest that a proper understanding of subjective human beliefs and behaviors can complement the analysis of objective data such as log files. We argue that humans consider the transaction costs of knowledge absorption before they engage in any related activities. We therefore caution future research from depicting humans as neutral – 'tools' that work only for the production of a public good or social welfare (Gordon et al., 2015). Instead, in this study, we contribute to resolving the paradox that humans are often reluctant to provide cyber-security knowledge, despite the fact that they are aware that the absorption of this knowledge by others is conducive to producing individual and collective cyber-security (ENISA, 2010, 2018; Gal-Or & Ghose, 2005; Gordon et al., 2003; Naghizadeh & Liu, 2016).

We propose to interpret effective knowledge absorption as the result of a multi-stage decision-making process. Our findings suggest that individuals first consider the transaction cost of social exchange that precedes knowledge absorption (resource belief). If this decision is affirmative, they begin social interaction, absorb some first knowledge elements, and assess the extent to which these are relevant for their job tasks (usefulness belief). Once they believe so, they likely adapt their social behavior in order to facilitate further knowledge absorption, i.e., they reciprocate to maintain the exchange process (reciprocity belief). As a result, collaborative and collective knowledge sharing perpetuates. While we can only propose such a process, and while we cannot establish any sequential or causal order with the data we have, future research may test this proposition from a longitudinal perspective.

Much prior research analyzed associations between human attitudes and intentions on the one hand and human behavior on the other hand (Jeon et al., 2011; Pi et al., 2013; Safa & Von Solms, 2016; Wang & Hou, 2015). Although this research is useful, our study goes one step further by associating beliefs with a performance outcome on the individual level, i.e., the extent to which an individual has effectively absorbed knowledge as a result of the social exchange with other ISAC

Table 4
Correlation analysis.[a]

	Knowledge absorption	Resource belief	Usefulness belief	Reward belief	Reciprocity belief
Knowledge absorption	1				
Resource belief	0.2860***	1			
Usefulness belief	0.2779***	0.2042**	1		
Reward belief	0.0258	−0.1568	−0.0602	1	
Reciprocity belief	0.3543***	0.3500***	0.2489***	−0.0001	1

[a] ρ: * $p < 0.05$; ** $p < 0.01$; *** $p < 0.001$.

Table 5
Results of model estimation (Ordered probit regression).[a,b]

Knowledge absorption		
Constructs	Coefficient	(Robust std. error)
Resource belief	0.4256*	(0.1695)
Usefulness belief	0.4167**	(0.1601)
Reward belief	0.0973	(0.1203)
Reciprocity belief	0.4012**	(0.1525)
Control variables		
Position in the organization	−0.0769	(0.0567)
Prior information sharing experience	−0.1285	(0.0934)
Size of the organization	0.0412	(0.0916)
Participation in prior ISAC events	0.4267*	(0.2000)
Quality of peer relationships	0.3066	(0.1706)
Potential individual contribution	−0.0377	(0.1009)
Gender	0.4955	(0.3388)
Age 21–30	0.0116	(0.4230)
Age 31–40	−0.3392	(0.2386)
Age 41–50	−0.3595	(0.2060)
Education none	−0.2416	(0.4354)
Education Master	−0.0153	(0.4207)
Education Bachelor	−0.1350	(0.4003)
Education PhD	−0.4339	(0.4700)
Membership duration	−0.0130	(0.0196)
Government	0.5862	(0.3693)
Banking & Finance	0.5474	(0.3486)
All other industries	0.5160	(0.3636)
Energy	0.5717	(0.3900)
Health	0.4981	(0.4362)
Log pseudolikelihood	−204.23	
Pseudo R^2	0.1385	
Wald χ^2 *(24 d.f.)*	83.95	
$p>\chi^2$	0.000***	
Observations[c]	188	

[a] Two-tailed tests: * $p < 0.05$; ** $p < 0.01$; *** $p < 0.001$.

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

[c] The difference between the number of respondents (=262) and the number of observations of the model (=188) is due to our conservative estimation approach that prefers list-wise deletion over imputation or modification.

participants. Future studies could continue our line of work by expanding our setting to the organizational level of analysis, studying how and why tacit knowledge, individually absorbed, contributes to the production of organizational cyber-security. Furthermore, the organizational context could moderate or even impede this production as the — 'not-invented- here' syndrome could obstruct the integration of knowledge from beyond the boundary of the firm into the internal cyber-security production processes (Antonelli, 1998; Antons & Piller, 2015; Huber, 2001; Katz & Allen, 1982; Lichtenthaler & Ernst, 2006), as could political divergences, processual impediments, and organizational bureaucracy. Today, the microfoundations of the organizational processes by which individually acquired tacit cyber-security knowledge is combined with other knowledge assets and material resources into actual cyber-security are largely unknown. Future research might study both the resource configuration and the combination process of these assets to a greater extent in order to bridge the research gap between individual knowledge absorption and organizational cyber-security.

Our dependent construct is an ordinal indicator, and its ability to measure effective knowledge absorption is limited. Receiving exclusive information through security information exchange is a necessary but not a sufficient condition for effective knowledge absorption, since both the integration of this information with prior individual knowledge and the transfer of this integrated knowledge to the organization is required for a full performance analysis (Hiebert & Lefevre, 1986; Knight & Liesch, 2002; Li & Kettinger, 2006; Nonaka & Takeuchi, 1995).[4] Since such a multi-step process of absorption cannot be readily measured by psychometric methods, our dependent measure should be seen as a first step towards providing such full measurement, and we invite future research to develop more complex measure that can consider the absorption process more comprehensively.

We suggest that any such future measures should be conceptualized on the individual level of analysis, as individual learning typically precedes organizational learning. While our ordinal indicator of knowledge absorption is far from being exhaustive, it is worthwhile to note that few empirical measures study individual absorption. Much work still uses measures defined at the organizational level, such as R&D intensity (Camisón & Forés, 2010; Cohen & Levinthal, 1989, 1990; Griffith, Redding, & Reenen, 2003; Liao, Fei, & Chen, 2007; Schmidt, 2010), patent cross-citation indicators (George et al., 2001; Peri, 2005), or the number of engineers the firm employs (Jane Zhao & Anand, 2009).

Our results also have implications for ISAC managers. The organizational design of an ISAC is relevant as it influences the behavior of the participants (Sedenberg & Dempsey, 2018). ISAC managers can attempt to increase participation rates by emphasizing that, in their ISAC, transaction costs of participation are low, participants bring valuable knowledge assets to the table, and interpersonal exchange is facilitated. At the same time, they should be careful to reduce transaction costs by only novel, technology-enabled forms of organization. For example, recommendations to construct distributed ISACs by adopting methods from cryptology and secure distributed computation (e.g., Ezhei and Ladani (2017)) might be useful if the goal is the quick absorption of explicit knowledge. However, the high demands that tacit knowledge absorption puts on the intensity of social, i.e., close interactions of individuals might reduce the value of such technology-based solutions. Hence, and somewhat ironically, the more sensitive the technological knowledge is to cyber-security, the less likely this knowledge will be shared inside the cyber-sphere.

Also, the specialists who absorb knowledge by participating in ISAC meetings and other forms of social exchange do not need to be the same people as those who are generally in charge of organizing the production of cyber-security. Our results should caution those who organize the production of cyber-security to not rely on monetary or career incentives as they attempt to give incentives to the group. Although many organizations have created reward systems to encourage their employees to share information with others (Bartol & Srivastava, 2002), we find no support for the hypothesis that knowledge absorption is associated with reward belief. Hence, goal alignment between individual and organizational interests is unlikely to be produced by the promise of monetary and career rewards. Hence, managers should concentrate on measures that reduce transaction cost by facilitating

[4] We thank an anonymous reviewer for providing this discussion point.

social exchange, helping to establishing long-term human relationships, and emphasizing the usefulness of knowledge absorption for the individual's personal job.

Finally, our research design has some limitations that future research could help relax. First, we studied a single, centrally organized ISAC in one country. Hence, future research should generalize our approach to alternative models of ISAC organizations 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 as neither our theoretical framework, nor any one of our measurement 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 represent fundamental aspects of human economic decision-making that, in our view, should apply globally. At the same time, this focus implies a limitation of scope. Our study does not deliver a multidimensional account of information sharing, nor do we attempt to introduce dynamic or dyadic settings. Our perspective is that of an individual who self-reports on the extent to which they have realized knowledge absorption. Future work could therefore build on our approach by studying the context and dynamics of human knowledge absorption over time.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

Anderson, Ross (2001). Why information security is hard – an economic perspective. In *Seventeenth annual computer security applications conference*, *Annual computer security applications conference* (pp. 358–365). New Orleans, USA: IEEE, ISBN: 0-7695-1405-7, http://dx.doi.org/10.1109/ACSAC.2001.991552.

Anderson, Ross, & Fuloria, Shailendra (2010). Security economics and critical national infrastructure. In Tyle Moore, David Pym, & Christos Ioannidis (Eds.), *Economics of information security and privacy* (pp. 55–66). Springer, ISBN: 978-1-4419-6967-5.

Anderson, Ross., & Moore, Tyler (2006). The economics of information security. *Science*, *314*(5799), 610–613.

Andreoni, James (1995). Cooperation in public-goods experiments: Kindness or confusion? *The American Economic Review*, *85*(4), 891–904.

Antonelli, Cristiano (1998). Localized technological change, new information technology and the knowledge-based economy: The european evidence. *Journal of Evolutionary Economics*, *8*(2), 177–198.

Antons, David, & Piller, Frank T. (2015). Opening the black box of "not invented here": Attitudes, decision biases, and behavioral consequences. *Academy of Management Perspectives*, *29*(2), 193–217.

Barney, Jay (1991). Firm resources and sustained competitive advantage. *Journal of Management*, *17*(1), 99–120.

Bartol, Kathryn M., & Srivastava, Abhishek (2002). Encouraging knowledge sharing: The role of organizational reward systems. *Journal of Leadership & Organizational Studies*, *9*(1), 64–76.

Bauer, Johannesa M., & van Eeten, Michel J. G. (2009). Cybersecurity: Stakeholder incentives, externalities, and policy options. *Telecommunications Policy*, *33*(10), 706–719.

Ben-Asher, Noam, & Gonzalez, Cleotilde (2015). Effects of cyber security knowledge on attack detection. *Computers in Human Behavior*, *48*, 51–61.

Bisogni, Fabio (2015). Data breaches and the dilemmas in notifying customers. In *Proceedings of the workshop on the economics of information security*. Delft, Netherlands.

Bock, Geea W., & Kim, Young-Gul (2002). Breaking the myths of rewards: An exploratory study of attitudes about knowledge sharing. *Information Resources Management Journal (IRMJ)*, *15*(2), 14–21.

Bodin, Lawrence D., et al. (2018). Cybersecurity insurance and risk-sharing. *Journal of Accounting and Public Policy*, *37*(6), 527–544.

Bolton, Garya E., & Ockenfels, Axel (2000). ERC: A theory of equity, reciprocity, and competition. *American Economic Review*, *90*(1), 166–193.

Bosch, Frans A. J. van den, Volberda, Henk W, & Boer, Michiel de (1999). Coevolution of firm absorptive capacity and knowledge environment: Organizational forms and combinative capabilities. *Organization Science*, *10*(5), 551–568.

Brosnan, Saraha F., & Waal, Frans B. M. de (2003). Monkeys reject unequal pay. *Nature*, *425*(6955), 297–299.

Cai, Shun, et al. (2013). Knowledge sharing in collaborative supply chains: Twin effects of trust and power. *International Journal of Productions Research*, *51*(7), 2060–2076.

Camisón, César, & Forés, Beatriz (2010). Knowledge absorptive Capacity: New insights for its conceptualization and measurement. *Journal of Business Research*, *63*(7), 707–715.

Cardenas, Alvaroa A., Manadhata, Pratyusa K., & Rajan, Sreeranga P. (2013). Big data analytics for security. *IEEE Security & Privacy*, *11*(6), 74–76.

Carol, X. J. Ou, Davison, Robert M., & Wong, Louie H. M. (2016). Using interactive systems for knowledge sharing: the impact of individual contextual preferences in China. *Information & Management*, *53*(2), 145–156.

Casas, Pedro, et al. (2017). Network security and anomaly detection with big-dama, a big data analytics framework. In *IEEE 6th international conference on cloud networking* (pp. 1–7). IEEE.

Cavelty, Myriama Dunn (2014). *Cybersecurity in Switzerland*. Springer, ISBN: 978-3-319-10620-5.

Cavusoglu, Huseyin, Raghunathan, Srinivasan, & Yue, Wei T (2008). Decision-theoretic and game-theoretic approaches to IT security investment. *Journal of Management Information Systems*, *25*(2), 281–304.

Centers, Richard, & Bugental, Daphne E. (1966). Intrinsic and extrinsic job motivations among different segments of the working population. *Journal of Applied Psychology*, *50*(3), 193–197.

Chang, Hsina Hsin, & Chuang, Shuang-Shii (2011). Social capital and individual motivations on knowledge sharing: Participant involvement as a moderator. *Information & Management*, *48*(1), 9–18.

Chen, Hsinchun, Chiang, Roger H. L., & Storey, Vedaa C. (2012). Business intelligence and analytics: From big data to big impact. *MIS Quarterly*, *36*(4), 1165–1188.

Chow, Wing S., & Chan, Laia Sheung (2008). Social network, social trust and shared goals in organizational knowledge sharing. *Information & Management*, *45*(7), 458–465.

Cohen, Wesley M., & Levinthal, Daniel A. (1989). Innovation and learning: The Two Faces of R&D. *The Economic Journal*, *99*(397), 569–596.

Cohen, Wesley M., & Levinthal, Daniel A (1990). Absorptive capacity: A new perspective on learning and innovation. *Administrative Science Quarterly*, *35*(1), 128–152.

Cohen, Jacob, et al. (2002). *Applied multiple regression/correlation analysis for the behavioral sciences, Vol. 1* (third ed.). Didcot, UK: Taylor & Francis, ISBN: 978-0-8058-2223-6.

Coolahan, Kathleen, et al. (2000). Preschool peer interactions and readiness to learn: Relationships between classroom peer play and learning behaviors and conduct. *Journal of Educational Psychology*, *92*(3), 458.

Cui, Baojiang, & He, Shanshan (2016). Anomaly detection model based on hadoop platform and weka interface. In *10th international conference on innovative mobile and internet services in ubiquitous computing* (pp. 84–89). IEEE.

Davenport, Thomas H., & Glaser, John (2002). Just-in-time delivery comes to knowledge management. *Harvard Business Review*, *80*(7), 107–111.

Davenport, Thomas H., Prusak, Laurence, et al. (1998). *Working knowledge: How organizations manage what they know*. Harvard Business Press.

Dillman, Dona A., Smyth, Jolene D., & Christian, Leaha Melani (2014). *Internet, phone, mail, and mixed-mode surveys: The tailored design method* (fourth ed.). Hoboken, USA: John Wiley & Sons, ISBN: 978-1-118-45614-9.

Encinosa, William E., Gaynor, Martin, & Rebitzer, James B. (2007). The sociology of groups and the economics of incentives: Theory and evidence on compensation systems. *Journal of Economic Behaviour and Organization*, *62*(2), 187–214.

ENISA (2010). *Incentives and barriers to information sharing*. Heraklion, Greece: European Union Agency for Network Information Security.

ENISA (2018). *INformation Sharing and Analysis Centres (ISACs): Cooperative models*. Attiki, Greece: European Union Agency for Network Information Security.

Etzioni, Amitai (2011). Cybersecurity in the private sector. *Issues in Science and Technology*, *28*(1), 58–62.

Ezhei, Mansooreh., & Ladani, BehrouzTork (2017). Information sharing vs. privacy: a game theoretic analysis. *Expert Systems with Applications*, *88*, 327–337.

Fehr, Ernst, & Gächter, Simon (2000). Fairness and retaliation: The economics of reciprocity. *Journal of Economic Perspectives*, *14*(3), 159–181.

Fehr, Ernst., & Gächter, Simon (2002). Altruistic punishment in humans. *Nature*, *415*(6868), 137–140.

Feldman, M. S., & March, J. G. (1981). Information in organizations as signal and symbol. *Administrative Science Quarterly*, *26*(2), 171–186.

Feledi, Daniel, Fenz, Stefan, & Lechner, Lukas (2013). Toward web-based information security knowledge sharing. *Information Security Technical Report*, [ISSN: 1363-4127] *17*(4), 199–209.

Fielder, Andrew, et al. (2014). Game theory meets information security management. In Nora Cuppens-Boulahia, et al. (Eds.), *ICT systems security and privacy protection*, *IFIP international information security conference, Vol. 428* (pp. 15–29). Berlin, Heidelberg, Germany: Springer.

Flegel, Ulrich (2002). Pseudonymizing unix log files. In *Infrastructure security*, *International conference on infrastructure security* (pp. 162–179). Berlin, Heidelberg, Germany: Springer, ISBN: 978-3-540-45831-9.

Forte, Darioa Valentino (2004). "The art" of log correlation: Tools and techniques for correlating events and log files. *Computer Fraud & Security*, *2004*(8), 15–17.

Foss, N. J. (1996). More critical comments on knowledge-based theories of the firm. *Organization Science*, *7*(5), 519–523.

Fransen, Frank, Smulders, Andre, & Kerkdijk, Richard (2015). Cyber security information exchange to gain insight into the effects of cyber threats and incidents. *Elektrotechnik und Informationstechnik*, *132*(2), 106–112.

Furnell, Steven, & Clarke, Nathan (2012). Power to the people? The evolving recognition of human aspects of security. *Computers & Security*, *31*(8), 983–988.

Gabaix, Xavier, et al. (2006). Costly information acquisition: Experimental analysis of a boundedly rational model. *American Economic Review*, *96*(4), 1043–1068.

Gal-Or, Esther, & Ghose, Anindya (2005). The economic incentives for sharing security information. *Information Systems Research*, *16*(2), 186–208.

Gaynor, Martin, Rebitzer, James B., & Taylor, Lowella J. (2001). *Incentives in HMOs*. (w8522), Cambridge, USA: National Bureau of Economic Research.

George, Gerard, et al. (2001). The effects of alliance portfolio characteristics and absorptive Capacity on performance: A study of biotechnology firms. *The Journal of High Technology Management Research*, *12*(2), 205–226.

Gordon, Lawrence A., Loeb, Martin P., & Lucyshyn, William (2003). Sharing information on computer systems security: An economic analysis. *Journal of Accounting and Public Policy*, *22*(6), 461–485.

Gordon, Lawrence A., Loeb, Martin P., Lucyshyn, William, & Zhou, Lei (2015). Externalities and the magnitude of cyber security underinvestment by private sector firms: A modification of the Gordon-Loeb model. *Journal of Information Security*, *6*(1), 24–30.

Gordon, Lawrence A., Loeb, Martin P., & Zhou, Lei (2016). Investing in cybersecurity: Insights from the Gordon-Loeb model. *Journal of Information Security*, *7*, 49–59.

Grant, R. M. (1996a). Prospering in dynamically-competitive environments: Organizational capability as knowledge integration. *Organization Science*, *7*(4), 359–467.

Grant, Roberta M. (1996b). Toward a knowledge-based theory of the firm. *Strategic Management Journal*, *17*, 109–122.

Griffith, Rachel, Redding, Stephen, & Reenen, John van (2003). R&D and absorptive capacity: Theory and Empirical Evidence. *Scandinavian Journal of Economics*, *105*(1), 99–118.

Grossklags, Jens, Christin, Nicolas, & Chuang, John (2008). Secure or insure?: A game-theoretic analysis of information security games. In *Proceeding of the 17th international conference on world wide web* (pp. 209–218). Beijing, China: ACM Press, ISBN: 978-1-60558-085-2.

Haemmerli, Bernhard, Raaum, Margrete, & Franceschetti, Giorgio (2013). Trust networks among human beings: Analysis, modeling, and recommendations. In *Effective surveillance for homeland security* (pp. 21–50). Chapman Hall/CRC.

Hair, J. F. (2006). *Multivariate data analysis, Vol. 1* (fifth ed.). Taramani, India: Pearson Education India.

Hausken, Kjell (2007). Information sharing among firms and cyber attacks. *Journal of Accounting and Public Policy*, *26*(6), 639–688.

Hiebert, James, & Lefevre, Patricia (1986). Conceptual and procedural knowledge in mathematics: An introductory analysis. In *Conceptual and procedural knowledge: The case of mathematics, Vol. 2* (pp. 1–27).

Hofmann, Annette, & Ramaj, Hidajet (2011). Interdependent risk networks: the threat of cyber attack. *International Journal of Management and Decision Making*, *11*(5), 312–323.

Huber, George P. (2001). Transfer of knowledge in knowledge management systems: Unexplored issues and suggested studies. *European Journal of Information Systems*, *10*(2), 72–79.

Hume, David (2000). *A treatise of human nature, Vol. 1*. New York, USA: Oxford University Press, ISBN: 978-0-19-875172-4.

Jakobson, Gabriel (2011). Mission cyber security situation assessment using impact dependency graphs. In *14th international conference on information fusion* (pp. 1–8). IEEE.

Jane Zhao, Zheng, & Anand, Jaideep (2009). A multilevel perspective on knowledge transfer: Evidence from the chinese automotive industry. *Strategic Management Journal*, *30*(9), 959–983.

Jeon, Suhwan, Kim, Young-Gul, & Koh, Joon (2011). An integrative model for knowledge sharing in communities of practice. *Journal of Knowledge Management*, *15*(2), 251–269.

Kalleberg, Arne L. (1977). Work values and job rewards: A theory of job satisfaction. *American Sociological Review*, *42*(1), 124–143.

Katz, R., & Allen, T. J. (1982). Investigating the Not Invented Here (NIH) syndrome: a look at the performance, tenure, and communication patterns of 50 R&D Project Groups. *R&D Management*, *12*(1), 7–20.

Knight, Gary A., & Liesch, Peter W (2002). Information internalisation in internationalising the firm. *Journal of Business Research*, *55*(12), 981–995.

Kogut, Bruce (2000). The network as knowledge: Generative rules and the emergence of structure. *Strategic Management Journal*, *21*(3), 405–425.

Kogut, Bruce, & Zander, Udo (1993). Knowledge of the firm and the evolutionary theory of the multinational corporation. *Journal of International Business Studies*, *24*(4), 625–645.

Kolm, Serge-Christophe, & Mercier-Ythier, Jean (Eds.), (2006). *Handbook of the economics of giving, altruism and reciprocity, Vol. 1*. Amsterdam, Netherlands: Elsevier, ISBN: 978-0-08-047821-0.

Kunreuther, Howard., & Heal, Geoffrey (2003). Interdependent security. *Journal of Risk and Uncertainty*, *26*(2), 231–249.

Kwahk, Kee-Young, & Park, Do-Hyung (2016). The effects of network sharing on knowledge-sharing activities and job performance in enterprise social media environments. *Computers in Human Behavior*, *55*, 826–839.

Laube, Stefan, & Böhme, Rainer (2017). Strategic aspects of cyber risk information sharing. *ACM Computing Surveys (CSUR)*, *50*(5), 77.

Lee, Jay., Bagheri, B., & Kao, Hung-An (2015). A cyber-physical systems architecture for industry 4.0-based manufacturing systems. *Manufacturing Letters*, *3*(5), 18–23.

Lee, Cheia Sian, & Ma, Long (2012). News sharing in social media: The effect of gratifications and prior experience. *Computers in Human Behavior*, *28*(2), 331–339.

Li, Yuan, & Kettinger, William J. (2006). An evolutionary information-processing theory of knowledge creation. *Journal of the Association for Information Systems*, *7*(1), 25.

Liao, Shu-Hsien, Fei, Wu-Chen, & Chen, Chih-Chiang (2007). Knowledge sharing, absorptive Capacity, and innovation Capability: an empirical study of Taiwan's knowledge-intensive industries. *Journal of Information Science*, *33*(3), 340–359.

Lichtenthaler, Ulrich, & Ernst, Holger (2006). Attitudes to externally organising knowledge management tasks: a review, reconsideration and extension of the NIH syndrome. *R&D Management*, *36*(4), 367–386.

Lichtenthaler, Ulrich, & Ernst, Holger (2007). Developing reputation to overcome the imperfections in the markets for knowledge. *Research Policy*, *36*(1), 37–55.

Lindenberg, Siegwart, & Foss, Nicolai (2011). Managing joint production motivation: The role of goal framing and governance mechanisms. *Academy of Management Review*, *36*(3), 500–525.

Luiijf, Eric, & Klaver, Marieke (2015). On the sharing of cyber security information. In *Critical infrastructure protection IX: 466, International conference on critical infrastructure protection, Vol. 466* (pp. 29–46). Cham, Switzerland: Springer, ISBN: 978-3-319-26567-4.

Mahmood, Tariq, & Afzal, Uzma (2013). Security analytics: Big data analytics for cybersecurity: a review of trends, techniques and tools. In *2013 2nd national conference on information assurance* (pp. 129–134). Rawalpindi, Pakistan: IEEE, ISBN: 978-1-4799-1288-9.

Maillart, Thomas, et al. (2017). Given enough eyeballs, all bugs are shallow? Revisiting eric raymond with bug bounty programs. *Journal of Cybersecurity*, *3*(2), 81–90.

Manshaei, Mohammada Hossein, et al. (2013). Game theory meets network security and privacy. *ACM Computing Surveys*, *45*(3), 25.

March, James G. (1991). Exploration and exploitation in organizational learning. *Organization Science*, *2*(1), 71–87.

Masud, Mohammada M., et al. (2008). Flow-based identification of botnet traffic by mining multiple log files. In *2008 first international conference on distributed framework and applications* (pp. 200–206). Penang, Malaysia: IEEE, ISBN: 978-1-4244-2313-2.

Mermoud, Alain, et al. (2019). To share or not to share: A behavioral perspective on human participation in security information sharing. *Journal of Cybersecurity*, *5*(1).

Moore, Tyler W., & Clayton, Richard (2011). The impact of public information on phishing attack and defense. *Communications and Strategies*, (81), 45–68.

Moran, Tal, & Moore, Tayler (2010). The phish-market protocol: Securely sharing attack data between competitors. In *International conference on financial cryptography and data security* (pp. 222–237). Berlin, Heidelberg, Germany: Springer, ISBN: 978-3-642-14577-3.

Naghizadeh, Parinaz., & Liu, Mingyan (2016). Inter-temporal incentives in security information sharing agreements. In *2016 information theory and applications workshop* (pp. 1–8). La Jolla, USA: IEEE, ISBN: 978-1-5090-2529-9.

Nagin, Daniel S., et al. (2002). Monitoring, motivation, and management: The determinants of opportunistic behavior in a field experiment. *American Economic Review*, *92*(4), 850–873.

Nickerson, Jack A., & Zenger, Todda R. (2004). A knowledge-based theory of the firm — the problem-solving perspective. *Organization Science*, *15*(6), 617–632.

Nonaka, Ikujiro., & Takeuchi, Hirotaka (1995). *The knowledge-creating company : How Japanese companies create the dynamics of innovation* (first ed.). New York, USA: Oxford University Press, ISBN: 978-0-19-509269-1.

Nunnally, Jum C., & Bernstein, Ira H. (2017). *McGraw-hill series in psychology, Psychometric theory* (third ed.). New York, USA: McGraw-Hill, ISBN: 978-0-07-047849-7.

Park, Byunga Il (2011). Knowledge transfer capacity of multinational enterprises and technology acquisition in international joint ventures. *International Business Review*, *20*(1), 75–87.

Parsons, Kathryn, et al. (2014). Determining employee awareness using the human aspects of information security questionnaire (HAIS-q). *Computers & Security*, *42*, 165–176.

Peri, Giovanni (2005). Determinants of knowledge flows and their effect on innovation. *The Review of Economics and Statistics*, *87*(2), 308–322.

Petty, Richard E., & Cacioppo, John T. (1986). The elaboration likelihood model of persuasion. In *Communication and Persuasion* (pp. 1–24). Springer, ISBN: 978-1-4612-4964-1.

Phelan, Steven E., & Lewin, Peter (2000). Arriving at a strategic theory of the firm. *International Journal of Management Reviews*, *2*(4), 305–323.

Pi, Shih-Ming, Chou, Chen-Huei, & Liao, Hsiu-Li (2013). A study of facebook groups members' knowledge sharing. *Computers in Human Behavior*, *29*(5), 1971–1979.

Podsakoff, Philip M., MacKenzie, Scott B., et al. (2003). Common method biases in behavioral research: a critical review of the literature and recommended remedies. *Journal of Applied Psychology*, *88*(5), 879–903.

Podsakoff, Philip M., & Organ, Dennis W. (1986). Self-reports in organizational research: Problems and prospects. *Journal of Management*, *12*(4), 531–544.

Polanyi, Michael (1962). Tacit knowing: Its bearing on some problems of philosophy. *Reviews of Modern Physics*, *34*(4), 601–616.

Powner, David A (2005). *Critical infrastructure protection department of homeland security faces challenges in fulfilling cybersecurity responsibilities: Report to congressional requesters*. DIANE Publishing.

Ransbotham, Sam, Kane, Gerald C., & Lurie, Nicholas H. (2012). Network characteristics and the value of collaborative user-generated content. *Marketing Science*, *31*(3), 369–547.

Reinholt, Mia, Pedersen, Torben, & Foss, Nicolai J. (2011). Why a central network position isn't enough: The role of motivation and ability for knowledge sharing in employee networks. *Academy of Management Journal*, *54*(6), 1277–1297.

Ryan, Richard M., & Deci, Edwarda L. (2000). Intrinsic and extrinsic motivations: Classic definitions and new directions. *Contemporary Educational Psychology*, *25*(1), 54–67.

Safa, Nadera Sohrabi, & Von Solms, Rossouw (2016). An information security knowledge sharing model in organizations. *Computers in Human Behavior*, *57*, 442–451.

Sait, Saada Y., et al. (2015). Multi-level anomaly detection: Relevance of big data analytics in networks. *Sadhana*, *40*(6), 1737–1767.

Scarbrough, Harry (2003). Knowledge management, HRM and the innovation process. *International Journal of Manpower*, *24*(5), 501–516.

Schilling, Melissa A. (2010). *Strategic management of technological innovation* (third ed.). New York, USA: McGraw-Hill Education, ISBN: 978-0-07-128957-3.

Schmidt, Tobias (2010). Absorptive capacity—one size fits all? A firm level analysis of absorptive capacity for different kinds of knowledge. *Managerial and Decision Economics*, *31*(1), 1–18.

Sedenberg, Elaine M., & Dempsey, James X. (2018). Cybersecurity information sharing governance structures: An ecosystem of diversity, trust, and tradeoffs. *Computing Research Repository*.

Shiva, Sajjan, Roy, Sankardas, & Dasgupta, Dipankar (2010). Game theory for cyber security. In *Proceedings of the sixth annual workshop on cyber security and information intelligence research* (pp. 34–37). Oak Ridge, USA: ACM Press, ISBN: 978-1-4503-0017-9.

Siesfeld, Tony, Cefola, Jacquelyn, & Neef, Dale (2009). *The economic impact of knowledge*. Routledge.

Simon, Herbert A. (1991). Bounded rationality and organizational learning. *Organization Science*, *2*(1), 125–134.

Singh, Kavita (2005). *Organisation change and development*. New Delhi, India: Excel Books, ISBN: 978-81-7446-442-2, (Google-Books-ID: rQLjYrAcKWkC).

Singh, Jayveer, & Nene, Manisha J (2013). A survey on machine learning techniques for intrusion detection systems. *International Journal of Advanced Research in Computer and Communication Engineering*, *2*(11), 4349–4355.

Skopik, Florian, Settanni, Giuseppe, & Fiedler, Roman (2016). A problem shared is a problem halved: a survey on the dimensions of collective cyber defense through security information sharing. *Computers & Security*, *60*(10), 154–176.

Solms, Rossouw von, & Niekerk, Johan van (2013). From information security to cyber security. *Computers & Security*, *38*, 97–102.

Spender, J.-C. (1996). Making knowledge the basis of a dynamic theory of the firm: Making knowledge. *Strategic Management Journal*, *17*, 45–62.

Tamjidyamcholo, Alireza, et al. (2014). Evaluation model for knowledge sharing in information security professional virtual community. *Computers & Security*, *43*, 19–34.

Teece, David J. (1977). Technology transfer by multinational firms: the resource costs of transferring technological know-how. *The Economic Journal*, *87*(346), 242–261.

Teece, D. (1983). The growth of international business. In *Technological and organizational factors in the theory of the multinational enterprise, Vol. 1* (Mark Casson). (pp. 51–62). London, UK: George Allen & Unwin.

Ter Wal, Anne LJ., Criscuolo, Paola, & Salter, Ammon (2017). Making a marriage of materials: The role of gatekeepers and shepherds in the absorption of external knowledge and innovation performance. *Research Policy*, *46*(5), 1039–1054.

Terzi, Duygua Sinanc, Terzi, Ramazan, & Sagiroglu, Seref (2017). Big data analytics for network anomaly detection from netflow data. In *International conference on computer science and engineering* (pp. 592–597). IEEE.

Tether, Bruce S., & Tajar, Abdelouahid (2008). Beyond industry-university links: Sourcing knowledge for innovation from consultants, private research organisations and the public science-base. *Research Policy*, *37*(6), 1079–1095.

Tosh, Deepak K., et al. (2017). Risk management using cyber-threat information sharing and cyber-insurance. In *International conference on game theory for networks* (pp. 154–164). Cham, Switzerland: Springer, ISBN: 978-3-319-67540-4.

Tounsi, Wiem, & Rais, Helmi (2018). A survey on technical threat intelligence in the age of sophisticated cyber attacks. *Computers & Security*, *72*, 212–233.

Trevor, Charlie O., & Nyberg, Anthony J. (2008). Keeping your headcount when all about you are losing theirs: Downsizing, voluntary turnover rates, and the moderating role of HR practices. *Academy of Management Journal*, *51*(2), 259–276.

Tricomi, Elisabeth, et al. (2010). Neural evidence for inequality-averse social preferences. *Nature*, *463*(7284), 1089–1091.

Tsai, Wenpin (2001). Knowledge transfer in intraorganizational networks: Effects of network position and absorptive Capacity on business unit innovation and performance. *Academy of Management Journal*, *44*(5), 996–1004.

Vázquez, Diego Fernández, et al. (2012). Conceptual framework for cyber defense information sharing within trust relationships. In *2012 4th international conference on cyber conflict* (pp. 1–17). IEEE.

Wagner, Thomas D., et al. (2018). A novel trust taxonomy for shared cyber threat intelligence. *Security and Communication Networks*, *2018*, 1–11.

Wang, Wei-Tsong, & Hou, Ya-Pei (2015). Motivations of employees' knowledge sharing behaviors: A self-determination perspective. *Information and Organization*, *25*(1), 1–26.

Wang, Sheng, & Noe, Raymond A. (2010). Knowledge sharing: a review and directions for future research. *Human Resource Management Review*, *20*(2), 115–131.

Wang, Jessie Hui, et al. (2011). A study on key strategies in P2P file sharing systems and ISPp2p traffic management. *Peer-to-Peer Networking and Applications*, *4*(4), 410–419.

Wang, Yuan, et al. (2014). A network gene-based framework for detecting advanced persistent threats. In *Ninth international conference on P2P, parallel, grid, cloud and internet computing* (pp. 97–102). IEEE.

Weiss, N. Eric (2014). Legislation to facilitate cybersecurity information sharing: Economic analysis. Washington, USA: Congressional Research Service.

Williamson, Olivera E. (1981). The economics of organization: The transaction cost approach. *American Journal of Sociology*, *87*(3), 548–577.

Xiong, Li, & Liu, Liang (2004). Peertrust: Supporting reputation-based trust for peer-to-peer electronic communities. *IEEE Transactions on Knowledge and Data Engineering*, *16*(7), 843–857.

Yan, Zhijun, et al. (2016). Knowledge sharing in online health communities: a social exchange theory perspective. *Information & Management*, *53*(5), 643–653.

Zibak, Adam, & Simpson, Andrew (2019). Cyber threat information sharing: Perceived benefits and barriers. In *Proceedings of the 14th international conference on availability, reliability and security* (p. 85). ACM.