Security Related Information Sharing among Firms: Potential Theoretical Explanations

Completed Research

Radha Appan  
Cleveland State University  
r.appan@csuohio.edu

Dinko Bačić  
University of Southern Indiana  
dbacic@usi.edu

Sreedhar Madhavaram  
Cleveland State University  
s.madhavaram@csuohio.edu

Abstract

Information technology (IT) related security crimes are on the rise, and are beginning to have a critical impact on firms. Considering the potential financial impact of IT security breaches on firms, effective IT security becomes the cornerstone of firm performance. In exploring effective ways to guard against IT security crimes, a small group of IT firms came together to form Information Technology-Information Sharing and Analysis Center (IT-ISAC), an information sharing organization with the goal of sharing critical information with industry peers and competitors. In the context of IT-ISAC, member firms have to engage cooperative and competitive behaviors. Such simultaneous cooperation and competition among rival firms is called coopetition. However, there is no research that explores why IT firms engage in security information sharing with other firms including competitors. In exploring the coopetitive behaviors exhibited by firms participating in the sharing of IT security related information, this research analyzes existing literature streams to see if they can resolve this particular coopetition paradox. Specifically, this research (i) analyzes research streams on transaction cost theory (TCT), resource based view (RBV), competence based view (CBV), and relational view of the firm (RVF), and (ii) finds that, while TCT, RBV, and CBV fail to resolve the IT-ISAC information sharing paradox, RVF provides appropriate theoretical foundations for the resolution of the paradox. We conclude with a discussion of the implications of our paper for future research.

Keywords

IT Security, Information Sharing, Coopetition, Relational View of the Firm, RVF, Firm Performance, ISAC, IT-ISAC

Introduction

Information technology (IT) related security crimes are on the rise, and are beginning to have a critical impact on firms. For example, an annual benchmarking survey of 277 firms in 15 industries that assesses the impact of security breaches on a broad range of business costs, reports that the range of average costs of data breach from $1.4 million (India) to $5.4 million (United States) per incident (Ponemon 2013). In fact, the “information theft and costs associated with business disruption represent significant external
costs to the firm” (Appan and Bacic 2016, p. 215). Sometimes, firms can suffer potentially irreparable damages to their business credibility. A couple of examples of firms suffering from security breaches are: (i) hackers obtained unauthorized access to user ids and encrypted passwords of over 38 million users of Adobe Reader, Acrobat, ColdFusion, and Photoshop products (Brading 2013) and (ii) Global Payments Inc., a credit card processor, saw its shares tumble 9% following a discovery that hackers stole account numbers and other key information from up to 1.5 million accounts in North America (Sidell 2012). Accordingly, considering the potential financial impact of IT security breaches on firms, effective IT security becomes the cornerstone of firm performance. Accordingly, IT security has emerged as one of the top concerns facing firms (Pfleeger and Lawrence Pfleeger 2010, Ismail 2017, Srebnick 2003).

Given how the exponentially increasing rate of IT related security crimes can cripple businesses, firms are continuously looking for ways to strengthen IT security. In exploring effective ways to guard against IT security crimes, a small group of IT firms came together to form Information Technology-Information Sharing and Analysis Center (IT-ISAC), an information sharing organization with the goal of sharing critical information with industry peers and competitor (Appan and Bacic 2016). In fact, this is a result of the efforts of the U.S. federal government to promote the creation of industry-based trade associations called Information Sharing and Analysis Centers (ISACs). The goal of IT-ISAC is to get firms to cooperate on IT security issues in the private sector. IT-ISAC (i) gathers and disseminates relevant IT security information on system vulnerabilities, threats, and incidents to its members and (ii) shares the best practices related to IT security management and solutions. Therefore, in IT-ISAC, competing firms such as Oracle and IBM share security information and help each other. Therefore, membership in IT-ISAC requires effective competition and cooperation (i.e., coopetition) to take place simultaneously.

While there is research that documents the impact of IT security breaches on various aspects of the firm (Cavusoglu, Cavusoglu, and Raghunathan 2004, Cavusoglu, Mishra, and Raghunathan 2004a, b, 2005), there is no research that explores why firms engage in IT security information sharing with competitors. Similarly, despite the calls to empirically evaluate the benefits of IT security related information sharing (ENISA 2010), with the exception of Appan and Bačić (2016), no research examines the impact of IT security information sharing on firm’s financial performance. According to Appan and Bačić (2016, p. 214), “IT firms engaged in interfirm security information sharing outperform their industry peers in terms of operational costs and overall profitability.” However, there is no research that explores why IT firms engage in security information sharing with other firms including competitors. In fact, even Appan and Bačić (2016), while basing their empirical investigation on the theoretical foundations of the relational view of the firm, do not provide any theoretical or empirical explanations as to why firms engage in IT security information sharing with competitors.

Both academics and practitioners recognize the importance of within-industry IT security related information sharing (GAO 2010). For Lohrmann (2007), the road to better information security passes through information sharing among firms that face, manage, and/or mitigate IT security threats. That is, the key to improving IT security is the gathering, analysis, and sharing of information related to successful, as well as unsuccessful, attempts at IT security breaches (Gal-Or and Ghose 2005). In exploring the coopetitive behaviors exhibited by firms participating in the sharing of IT security related information, we look for and analyze existing literature streams to see if they can resolve this particular coopetition paradox.

The remainder of the paper is organized as follows. First, we provide a brief discussion of the background of IT-ISAC. Second, we provide an analysis of relevant literature to identify existing theoretical perspective that helps resolve security information exchange coopetitive paradox. Third, we discuss the implications of for theory and practice. We conclude with a discussion of limitations and corresponding future research.
ISACs and IT-ISACs - Background

ISACs are often viewed, approached, and discussed through the Trade Association (TA) lens (Gordon, Loeb, and Lucyshyn 2003). As TAs are mechanisms for exchanging or sharing information within an industry (Kirby 1988), they pool information from members, organize it, and disseminate it to member firms (Vives 1990). Most research concerning TAs is motivated by the benefits and costs of the membership, and explores issues such as incentives to share information and membership motivation (Bennett 2000, Hirschman 1970, 1982, Vives 1990), the impact of disclosure rules (Vives 1990), economic impact of information sharing (Gordon, Loeb, and Lucyshyn 2003), and analysis of the free rider concept (Bennett 2000, Gordon, Loeb, and Lucyshyn 2003). Overall, according to Appan and Bačić (2016, p. 216-217), the following conclusions can be drawn: “(1) there are economic benefits to information sharing among firms stemming from better-informed decisions (Gordon, Loeb, and Lucyshyn 2003, Vives 1990), (2) benefits of information sharing can be captured at firm level (Vives 1990), association members level and/or aggregate industry (Clarke 1983), and social level (Bennett 2000), and (3) economic incentives and benefits related to information sharing are context dependent (type of competition, nature of the products, market conditions (Kirby 1988, Vives 1984)).

Responding to their needs and noting the benefits of ISACs, in 2001, 19 leading high tech companies came together for sector-wide cooperation on cyber security issues through the formation of IT-ISAC (Appan and Bacic 2016). Using shared IT security information, IT-ISAC (i) disseminates relevant information about system vulnerabilities, threats and incidents to its members, and (ii) shares the best practices and solutions among its members. Therefore, it has become important to understand the existing literature on TAs and information sharing, along with the research focused specifically on ISACs and IT security related information sharing. Accordingly, it can be noted that IS related research in the context of inter-firm information sharing such as IT-ISAC is still sparse but is gaining attention due to recent growth in security breaches requiring intra- and inter-firm information sharing. The existing research is based on the TA literature and is primarily focused on information sharing motivation and implications (Appan and Bacic 2016). However, why would firms be willing to share critical IT security related information with other industry firms and potential competition in the first place? In an attempt to address this paradox, in the next section, we explore literature on coopetition and a number of extant theories that could potentially resolve the paradox.

Why do firms engage in coopetition in the context of security information exchange?

IT-ISAC Information Sharing Paradox

In the context of IT-ISAC, member firms have to engage cooperative and competitive behaviors. Such simultaneous cooperation and competition among rival firms is called coopetition. Coopetition, one of the most important business perspectives of recent years (Bowser 2010), involves knowledge sharing among competitors (Tsai 2002) and is a model in which a network of stakeholders cooperate and compete to maximize value. While cooperation involves the use of shared knowledge to pursue common interests, competition involves the use of shared knowledge to outperform the competition (Khanna, Gulati, and Nohria 1998). In spite of the widespread acceptance of coopetition as a strategic management approach, the announcement of IT-ISAC deployment was received with skepticism (Appan and Bacic 2016). Why would firms share their security shortcomings with competitors? Why would firms help competitors with their security issues? What would steer these organizations into a cooperative/competitive mode rather than the traditional competition-only mode (Bowser 2010) that worked so well for them in the past? These questions are even more relevant in the context of potential negative implications of sharing proprietary IT security information and the motivations behind sharing IS security related information.
Therefore, sharing of information, especially security-based information presents an interesting paradox (Appan and Bacic 2016). In order to achieve the benefits of being members of the ITISAC, members of IT-ISAC are required to share sensitive and potentially competitive intelligence with their direct competitors. Why would a firm then resort to critical information sharing strategy? There are a number of theories that attempt to explain firm’s motivations for existence, competitive advantage and, therefore, its resulting strategies and behaviors: transactional cost theory, resource-based view and competence-based view. Next few paragraphs will provide a brief overview of these three approaches as evidence of paradox and assess their ability to explain it.

**Transaction Cost Theory**

Transaction cost theory (TCT) originated with an attempt to theoretically explain the existence of firms relative to a marketplace by introducing the cost of transactions as the basic unit of economic analysis (Commons 1931). Furthermore, TCT approach proposes that we can identify governance structures that result in simple and smooth transactions and those that result in ‘friction’ (Williamson 1981). A firm, as a type of governance structure, exists because transaction costs of coordination in the market exchange exceed those of same costs within firm. In other words, in the context of complicated market structure, firms offer more directed, efficient and effective way for conducting certain activities (Coase 1937). This has been described as a middle level theory as it defines the efficient boundaries of where certain activities should occur and why (Williamson 1981) and is of particular interest to our paradox discussion. TCT approach suggests that in situation of asymmetric information and asset specificity (Coase 1937, Williamson 1981), the transaction cost in the market exchange would be high due to behavioral aspects of human entities involved, namely bounded rationality and opportunism (Williamson 1981). With regards to bounded rationality (Simon 1957), all economic exchanges are governed through contracts, where complicated exchanges tend to be inefficiently contractualized. However, inefficient or incomplete contracting would not be detrimental if all of the agents are immune to opportunism (Williamson 1981).

TCT would not only fail to explain security information sharing between potential competitors but would most likely suggest that the cost of coordination of security information outside of a firm is high given the asymmetric nature of the security information ‘production’ (about cyber-attacks, for instance). Additionally, given the nature of, often anonymous, information sharing in IT-ISAC, ‘contracting’ would be attempted but difficult and costly to enforce given the potential for opportunism by some members. Hence, through the TCT lens, cyber security information sharing between IT firms and competitors is a paradox that is difficult to explain.

**Resource Based Theory**

Resource-based view (RBV) of the firm deals with resources controlled by a firm (Barney 1986b, a, 1991, Penrose 1959, Teece, Pisano, and Shuen 1997, Wernerfelt 1984) and suggests that the application of resources that are valuable, rare, inimitable, and non-substitutable, could result in competitive advantages. That is, firm performance is due to heterogeneity in resources rather than industry structure and sources of competitive advantage are couched in resources. Accordingly, firms will attempt to protect resources that are valuable, rare, inimitable, and non-substitutable (Crook et al. 2008).

Participation in an organization such as IT-ISAC and ensuing information sharing would result in a state where critical security information is not controlled anymore by a single firm and therefore the information and related potential actions would become less rare and more imitable. While shared resources could accrue rent to firm in an alliance, such rent accruals are especially problematic when competitors are involved (Lavie 2006). Hence, firm’s sharing of critical security-based information (resource) with potential competitors would minimize firm’s potential competitive advantages. As a result, RBV theoretical lens fails to explain the coopetition paradox as well.
Competence Based Theory

Competence based view (CBV) of the firm shares a number of similarities with RBV, however, it is more deliberate in addressing causality between key resources and superior firm performance by focusing on developing competencies to actually deploy those resources (Dierickx and Cool 1989). Although CBV of the firms tends to be more ‘holistic’ and open to outside factors (market, partners, customers) in building firm competencies, it still assumes that assets supporting the performance of key resources and competencies need to be controlled by the firm (Freiling 2004).

Similar to RBV, while CBV suggests the importance of ‘organization-addressable resources’ that lie beyond the boundaries of the organization, those boundaries tend not to include competitors. Due to its view on competency control and tendency not to include potential competitors ‘within boundaries’, CBV also fails to provide a mechanism that explains the coopetition paradox.

In summary, TCT, RBV and CBV fail to effectively explain the motivation behind voluntarily information sharing between potentially competing firms. Not surprisingly, research over the last decade has sufficiently documented that inter-firm relations have not been sufficiently addressed within the resource- and competence-based literature (Das and Teng 2000, Foss 1999). Hence, the existence of this paradox in the context of IT-ISAC members sharing security related information, advocates that traditional, single entity (firm) focused theories do not provide appropriate theoretical foundation for explaining this coopetition paradox.

Instead, the paradox suggests the need for an alternative view which goes beyond single-entity focus, but rather is focused on explaining behavior based on multiple entities or network relations. More specifically, an alternative lens that describes resources that are deeply entrenched in interfirm relations as suggested by the relational view of firm (Dyer and Singh 1998). Furthermore, as we explore through theoretical lens of relational view of the firm it is critical that we evaluate whether the phenomenon of security information sharing exhibits relational-based behaviors and outcomes (“sources”) that would lead to competitive advantage and therefore serve as incentives for information sharing.

Relational View of the Firm and IT Security Information Sharing

The relational view of the firm posits that a firm’s critical resources may be embedded in inter-firm resources and routines (Dyer and Singh 1998). As per relational research, competitiveness does not arise from the firm, as suggested by some theories (e.g., TCT, RBT, and CBT), but rather arises from inter-firm sources of advantage. This view of the firm suggests that firms engaged in knowledge sharing through strong relationships, achieve relational rents in the form of performance gains. Specifically, relational rents are defined as a “supernormal profit jointly generated in an exchange relationship that cannot be generated by either firm in isolation and can only be created through the joint idiosyncratic contributions of the specific alliance partners” (Dyer and Singh 1998, p. 662). According to the relational view of the firm, there are four potential sources of competitive advantage that can arise from inter-firm relationships and lead to superior firm performance: idiosyncratic (relationship specific) resources, knowledge sharing routines, complementary resources/capabilities, and effective governance (Dyer and Singh 1998, Appan and Bacic 2016). Next, we discuss each of these sources of competitive advantage and link them to behaviors and outcomes resulting from security information sharing between IT firms within IT-ISAC.

Idiosyncratic Resources and IT-ISAC

Membership in IT-ISAC creates relationships among industry firms, who are often competitors, based on an agreement to share IT security related information that the members are privy to. While some of the information may be available to non-members, comprehensive information about cyber-attacks, threats or vulnerabilities is gathered from all the members and is made available to members only. As a result, critical and comprehensive information is available to the members of IT-ISAC. Such idiosyncratic information (asset) is dynamic in nature, as IT security information keeps changing and knowledge of prior threats does not guarantee the prevention of the next breach. This dynamic idiosyncratic nature makes it valuable and
therefore capable of positively impacting firm performance. The nature of firms’ investments, publicized efficiencies, changes in approaches to information gathering with time, dynamism, frequency of transactions and long lasting relationship strongly suggest that IT-ISAC membership exhibits characteristics of idiosyncratic asset creation. As such, it is expected to be a source of competitive advantage and relational rents as described by Dyer and Singh (1998) and a motivating factor for firms to be engaged in information sharing with other firms.

**Interfirm Knowledge sharing and IT-ISAC**

For Dyer and Singh (1998), interfirm knowledge sharing is a source of relational rents as well. Interfirm knowledge sharing routines are regular patterns of interfirm interactions that permit the transfer, recombination or creation of specialized knowledge (Grant 1996). These routines have been described as institutionalized processes that are purposefully designed to enable and support knowledge sharing. In the case of IT-ISAC, members are provided confidential forum with access to the latest vulnerability/virus information and to member only presentation materials and podcasts. Members also have the ability to post alerts and notifications, view member-submitted materials, and historical alerts. Email system is also used by communicating ad-hoc, weekly roll-up assessment emails, urgent alert emails, and technical emails. Lastly, twice-a-week technical conference calls, special interest and affinity groups are deployed for additional information and know-how exchange.

In addition to the act of communication and sharing, ‘how’ knowledge is shared is important in knowledge sharing actually yielding relational rent (Dyer and Singh 1998). Namely, the relational view suggests the importance of (i) know-how sharing (vs. only information), (ii) partner absorptive capacity, and (iii) enablement mechanisms that reduce ‘free-riding’ (Appan and Bacic 2016). As IT security related knowledge is distributed across the members of IT-ISAC. Sharing of such information often involves the pooling and transfer of distributed, complex, and specialized knowledge. Prior research has shown that networks (rather than individual firms) are more effective in the transfer of such knowledge (Dyer and Nobeoka 2000, Powell, Koput, and Smith-Doerr 1996). IT-ISAC inter-firm knowledge appears to exhibit the necessary characteristics of ‘how’ knowledge is shared, namely know-how sharing, partner absorptive capacity, and governance and incentives to limit ‘free-riding’. Therefore, the interfirm knowledge sharing routines provided by IT-ISAC to facilitate sharing of valuable information can be a potential source of competitive advantage. As such, they can also serve as an important reason why firms would consider being engaged in the IT-ISAC in the context of the coopetition paradox.

**Complementary resources and IT-ISAC**

Complementary resources, defined as “distinctive resources of alliance partners that collectively generate greater rents than the sum of those obtained individual endowments of each partner” (Dyer and Singh 1998, p.666-667), are another potential source of competitive advantage. Furthermore, these complementary resources cannot be purchased on secondary market and should be indivisible where alliances allow partners to obtain resources and capabilities not readily available in competitive marketplace, especially specialized expertise (Oliver 1997). The power and relational rent potential of complementary resources resides in the synergetic effect where ‘the combined resource endowments were more valuable, rare, difficult to imitate than they had been before they were combined’ (Dyer and Singh 1998, p.667). Member firms of IT-ISAC have access to the IT security related resource stacks that are not available to members outside of the association. For instance, IT-ISAC was recently reorganized to better leverage subject matter experts from member companies to share threat indicators and techniques from specific incidents. Furthermore, IT-ISAC provides structure for more direct access to important stakeholders in cyber security. Specifically, through structures enabling potential complementary resource creation, membership in IT-ISAC creates access to and understanding of non-public details about vulnerabilities and threats. None of these resources and resulting capabilities are available to individual firms and non-members. Complementary resources created through IT-ISAC appear to produce stronger competitive positions than those achievable by the firms operating individually (Dyer and Singh 1998, Shan and Walker 1994). Lastly, relational view also suggests that certain organizations are in better position to recognize complementary potential of shared resources.
Therefore, as per the relational view, complementary resources can be sources of competitive advantages. Therefore, complementary resources act as an important motivating factor for firms to engage in coope-
tion.

Effective Governance and IT-ISAC

Effective governance is key to relational rent creation because it minimizes transaction costs while posi-
tively impacting alliance/partnership willingness to engage. The governance of IT security related infor-
mation sharing process is a key service provided by IT-ISAC. The organization deploys the structure and
the mechanisms used for information sharing in order to minimize transaction costs while at the same time
maximizing the value of the shared information. For example, to incentivize sharing of discovered weak-
nesses, IT-ISAC deploys non-disclosure agreements that can enable members to freely and anonymously
share, and develop a thorough understanding threats, incidents, effective practices and vulnerabilities
(Appan and Bacic 2016). Furthermore, the use of encrypted emails, SSL-protected websites, and Govern-
ment Emergency Telecommunications Service (GETS) system for priority calls (GAO 2004) by IT-ISAC can
ensure information security and confidentiality. This governance is a direct response to needing to ensure
the flow of information while at the same time protecting member firms from unwanted risks. The usage of
IT-ISAC’s communication protocols results in members achieving lower transaction costs than competitors.

Beyond efficiency gains achieved through lower transaction costs, relational view posits that relational rent
potential of governance also resides in its effectiveness based on partners’ trust. Trust is an important ele-
ment of ensuring that partners make investments in idiosyncratic assets, interfim knowledge and comple-
mentary resources. More specifically, self-enforcing governance is expected to be more effective than third
party enforcements mechanisms in promoting information sharing, while lowering transaction costs (Dyer
and Singh 1998). IT-ISAC’s primarily self-enforcing governance structure appears to recognize the value of
trust. Furthermore, the monetary fee to participate in the organization and investment in human assets
such as operations centers are examples of self-enforcing safeguards described in relational view. Further-
more, self-enforcing safeguards are suggested to exhibit higher potential of relational rents due to lower
contracting costs, monitoring costs, lower adaptation costs, lower re-contracting costs, and superior incen-
tives for value creation initiatives (Dyer and Singh 1998). Research suggests that dynamic, highly complex
and specialized knowledge such as the one found in IT-ISAC, requires self-enforcing governance as “it is
difficult (if not impossible) to explicitly contract for value creation initiatives, such as sharing fine-grained
tacit knowledge, exchanging resources that are difficult to price” (Dyer and Singh 1998, p. 671).

Overall, we recognize that many theoretical approaches and views are unable to resolve the coopetition par-
adox occurring in IT-ISAC. However, Dyer and Singh’s (1998) relational view provides evidence that IT-
ISAC members have four potential sources of competitive advantage that can arise from inter-firm relation-
ships and lead to superior firm performance: idiosyncratic (relationship specific) resources, knowledge
sharing routines, complementary resources/capabilities, and effective governance (Appan and Bacic 2016).
Accordingly, given that relational resources and associated benefits have the potential to effectively elimi-
nate the paradox, the relational view provides theoretical foundations for the resolution of the IT-ISAC
information sharing paradox.

Discussion

Given that the IT-ISAC provides a coopetition context to participating firms, we first explored if any of the
existing theories resolve the coopetition paradox. Our analyses of TCT, RBV, and CBV research streams
reveal that they fail to support the resolution of the paradox. However, the relational view whose origins
can be traced to the work of Dyer & Singh (1998) provides an appropriate theoretical foundation for the
resolution of the paradox. Specifically, the relational view of the firm suggests that through idiosyncratic
resources, knowledge sharing routines, complementary resources/capabilities, and effective governance,
firms can achieve relational rents in the form of performance gains. However, we do not claim that the
relational view does not share affinities with the RBV or CBV research streams. In fact, RBV and CBV
Security Information Sharing among Firms: Potential Theoretical Explanations

As our search for theoretical underpinnings to resolve the coopetition paradox in the context of IT security related information exchange reveals interesting insights, there are a number of implications for practice and research. To our knowledge, our research is the first to explore theoretical foundations that can resolve the coopetition paradox in the context of IT security information exchange. While our analysis of extant research reveals relational view as the foundation for the resolution of the paradox, we have not explored specific firm and managerial motivations for joining the IT-ISAC. Therefore, based on the theoretical foundations discussed in this research, future research could explore firm and managerial motivations in joining IT-ISACs. According to the relational view based explanation discussed in this paper, because of idiosyncratic (relationship specific) resources, knowledge sharing routines, complementary resources/capabilities, and effective governance, firms achieve relational rents in the form of performance gains. Accordingly, we welcome further conceptual scrutiny on the arguments presented in this research. In doing so, future research could explore alternative and/or rival theoretical explanations and subject them to empirical scrutiny as well.

Second, to the best of our knowledge, with the exception of Appan and Bacic (Appan and Bacic 2016), there is no empirical research on the impact of interfirm IT security information sharing on firm performance. While others suggested a need to conduct such research, offered indications of cost implications, and/or provided modeling proof of positive impact of information sharing on costs or profitability, no research has explicitly linked the theoretical foundations to firm performance, and future research could consider this aspect. In addition, future research could also explore employee level and client level consequences such as organization comment, client satisfaction, employee role conflict, and so on. Third, while this research offers a promising theoretical lens for analyzing IS activities, it requires scrutiny with reference to foundational premises, nomological structures, critical evaluation of concepts and constructs, and formalization through empirical verification.

The use of relational based view offers fertile grounds for understanding IS strategy, technology and activities that involve and enable inter-firm relationships. As companies continue to engage in various forms of cooperation, alliances and coopetition, our research community will be challenged to provide theory-based empirical research to explain the results of such relationships as well as provide thought leadership in this context. ERP II, SCM technologies, and CRM are relevant examples of technologies and related business processes where IS can serve an important role in activities that span outside firm boundaries and offer significant potential for further research.

In conclusion, our research explores, in the context of IT-ISAC context, why IT firms engage in security information sharing with other firms including competitors. While the analyses of extant literatures reveals the relational view of the firms as providing theoretical foundations that resolves the coopetition paradox, further conceptual and empirical research in this important research domain is clearly required.

References


GAO, United States. 2010. Critical infrastructure protection; key private and public cyber expectations need to be consistently addressed.


Twenty-fourth Americas Conference on Information Systems, New Orleans, 2018 9