Communications of the Association for Information Systems

Volume 39 Article 12

9-2016

Impact of Information Technology (IT) Security Information Sharing among Competing IT Firms on Firm's Financial Performance: An Empirical Investigation

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

Dinko Bačić
University of Southern Indiana

Recommended Citation
Appan, Radha and Bačić, Dinko (2016) "Impact of Information Technology (IT) Security Information Sharing among Competing IT Firms on Firm's Financial Performance: An Empirical Investigation," *Communications of the Association for Information Systems*: Vol. 39 , Article 12.
DOI: 10.17705/1CAIS.03912
Available at: http://aisel.aisnet.org/cais/vol39/iss1/12

Communications of the Association for Information Systems

Research Paper ISSN: 1529-3181

Impact of Information Technology (IT) Security Information Sharing among Competing IT Firms on Firm's Financial Performance: An Empirical Investigation

Radha Appan
Information Systems
Monte Ahuja College of Business
Cleveland State University
r.appan@csuohio.edu

Dinko Bačić
Management and Information Sciences
Romain College of Business
University of Southern Indiana

Abstract:

Traditionally, IT firms closely guard the management and control of critical information assets. A group of IT firms, however, adopted a different approach and formed an organization with the goal of sharing critical IT security information with industry peers (firms in the same industry that do not directly compete) and competitors to more effectively manage IT security. The inherent vulnerability in sharing critical information with other (potentially competing) firms presents an interesting, coopetition paradox for firms. Drawing from the theoretical foundations of the relational view of the firm that resolves the coopetition paradox, we conducted an empirical test to determine whether security information sharing impacts firm's financial performance. Our findings suggest that IT firms engaged in interfirm security information sharing outperform their industry peers in terms of operational costs and overall profitability.

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

This manuscript underwent peer review. It was received 09/20/2015 and was with the authors for 3 months for 2 revisions. Harvey Enns served as Associate Editor.

1 Introduction

The impact of information technology (IT) on firm's financial performance is of great interest for both practice and research. In fact, due to increases in cybercrime occurrences and the resulting impact on firms' operations, customers, and brands, managing IT security information and its impact on financial performance is of particular importance to this research. Since critical information resources such as IT security information are sources of competitive advantage, firms have traditionally closely guarded the management and control of such resources in their boundaries. However, the exponentially increasing rate of IT security-related crimes has had a crippling effect on many businesses (Wilshusen, 2012) and forced IT firms to consider crossing firm boundaries to more efficiently and effectively manage IT security information. Therefore, and not surprisingly, 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 IT security information with industry peers and competitors. Recognizing the firms' inherent vulnerability while sharing critical information with competing firms (coopetition paradox), we focus on the following research question:

RQ: Does IT security-information sharing among competing IT firms impact their financial performance?

Although prior IS literature has evaluated the role and impact of information sharing in organizations and acknowledged the role of IT security information, our research question remains relevant for the following reasons. Despite calls to empirically evaluate the benefits of IT security-related information sharing (ENISA, 2010) and numerous quantifications of individual and industry-wide costs of specific security breaches (Cavusoglu, Cavusoglu, & Raghunathan, 2004a; Cavusoglu, Mishra, & Raghunathan, 2004b, 2004b, 2005) no research has investigated the impact of IT security information sharing on firm's financial performance. In addition, the existing literature fails to provide a theoretical foundation that can explain why firms' engagement in IT security information would impact firm's financial performance or act as potential motivation to engage in sharing IT security information. To close these gaps, based on the theoretical foundations of the relational view of the firm, we empirically tested the impact of IT security information sharing on financial performance of IT firms. Before delving into our study's specifics, however, we consider the extent and scope of the IT security issue that motivates this research.

Specifically, some evidence suggests that IT security breaches have a strong negative impact on firm performance. For example, an annual benchmarking survey of companies in 15 industries that assesses the impact of security breaches on a broad range of business costs has reported that the average cost of a data breach has increased from US$6.65 million in 2008 to US$6.75 million in 2009 and US$7.2 million in 2010 (Ponemon Institute, 2010, 2011). The same study for 2012 included 12 countries and suggests the average costs of a data breach range from US$1.4 million (India) to US$5.4 million (United States) per incident (Ponemon Institute, 2013a). These studies conclude that information theft and costs associated with business disruption represent significant external costs to the firm (43% of total external costs). Specifically, external costs to the firm include business disruption (22% of total external costs), equipment damage, and revenue loss due to customer churn (13% of total external costs) (Ponemon Institute, 2013a). At the same time, recovering from and detecting security breaches are the most costly internal activities. In fact, the insurance industry has reported that the costs of cyber-crimes now exceeding those of weather, fire, and social unrest because cyber-crimes disrupt the supply chain (Carpenter, 2013).

One could draw analogous conclusions evaluating the magnitude of specific instances of firms' suffering from information security breaches, such as when 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). Similarly, the well-publicized Anthem data breach potentially exposed personal information for up to 80 million people (Huddleston, 2015). These types of IT security-related crimes have taken a significant financial and performance toll on firms. For example, Global Payments, a credit card processor, saw its shares tumble 9 percent following a discovery that hackers stole account numbers and other key information from up to 1.5 million accounts in North America. Further, this event resulted in their halting their stock from trading (Sidel, 2012). Given the growing rate of IT security breaches and their financial impact on businesses, firms' economic success depends greatly on whether they effectively manage their IT security (Cavusoglu et al., 2004a). Consequently, IT security management has emerged as one of the top concerns facing organizations in the last decade (Gal-Or & Ghose, 2005; Pfleeger & Pfleeger, 2010). Not surprisingly, security concerns are a top concern for CIOs. According to a recent CIO

survey, security was the top spending priority with 75 percent of CIOs expecting to increase spending in 2015 (PiperJaffray. 2015).

Amid the increase in the number of security breaches and the documented benefits of information sharing as a backdrop, the U.S. Government promoted the creation of industry-based trade associations called information sharing and analysis centers (ISACs). As we note above, IT-ISAC is one such ISAC with the goal of cooperating on IT security issues in the private sector. IT-ISAC gathers and disseminates relevant IT security information on system vulnerabilities, threats, and incidents to its members. It also shares the best practices related to IT security management and solutions. In IT-ISAC, competing firms such as Oracle and IBM share security information and help each other and, thus, engage in coopetition; that is, simultaneously behaving cooperatively and competitively. Indeed, both academicians and practitioners have recognized the importance of within-industry IT security-related information sharing (GAO, 2004a, 2004b, 2010). In addressing IT security threats facing organizations, researchers had already suggested that the road to better information security passes through information sharing (Lohrmann, 2007). More specifically, the key to improving IT security lies in gathering, analyzing, and sharing information related to successful and unsuccessful attempts at breaching firms' IT security (Gal-Or & Ghose, 2005).

In this research, we explore the coopetitive behaviors exhibited by firms participating in information-sharing organizations such as IT-ISAC and resolve the apparent coopetition paradox (situations where firms belonging to information sharing organization need to share sensitive and potentially competitive intelligence with their direct competitors) by viewing IT security information sharing through the lens of the relational view of the firm (Dyer & Singh, 1998). Furthermore, we empirically test how information-sharing behavior impacts firms' financial performance in both the short and longer term.

This paper proceeds as follows. In Section 2, we discuss the background of IT-ISAC and information-sharing organizations in general. In Section 3, consistent with Bharadwaj (2000), Martin and Mykytyn (2009), and Santhanam and Hartono (2003), we detail the theoretical background that helps resolve security-information exchange's coopetitive paradox and present formal research hypotheses. In Section 4, we describe the methodology and analyses and present the results. In Section 5, we discuss the results and offer implications for practice and research. Finally, in Section 6, we conclude the paper by discussing the study's limitations and future research opportunities.

2 IT-ISAC: Background

Academic studies often discuss ISACs through the trade association (TA) perspective (Gordon, Loeb, & Lucyshyn, 2003). Accordingly, we need to understand the existing literature on TAs and information sharing, the research focused specifically on ISACs and IT security-related information sharing, and the corresponding paradox that arises when competitors agree to share critical information.

2.1 Trade Associations and Information Sharing

Trade associations are mechanisms for exchanging or sharing information in an industry (Kirby, 1988). TAs pool information from its members, organize it, and disseminate it to member firms (Vives, 1990). The semiconductor, trucking, and cement industries in North America leverage TAs' information-sharing role (Vives, 1990). Furthermore, trade associations participate in business and social activities via political influence, public relations, and specific regulation or rule enforcement.

Studies of TA phenomenon mostly focus on understanding the benefits and costs of the membership relative to firms, larger marketplace such as the association itself, and/or social welfare. The majority of the TA-related literature on information sharing adopts an oligopolistic-market perspective (Clarke, 1983; Gal-Or, 1985, 1986; Kirby, 1988; Li, 1985; Novshek & Sonnenschein, 1982; Ponssard, 1979; Raith, 1996; Sakai & Yamato, 1989; Shapiro, 1986; Vives, 1984); however, studies have also explored other market contexts (Vives, 1989; Vives, 1990). In addition, research on TAs includes topics such as incentives to share information and membership motivation (Bennett, 2000; Hirschman, 1970, 1982; Vives, 1990), the impact of disclosure rules (Vives, 1990), the economic impact of information sharing (Gordon et al., 2003), and the free rider concept (Bennett, 2000; Gordon et al., 2003).

While these research efforts offer many unique findings and suggestions, they offer several findings particularly relevant to our research: 1) there are economic benefits to information sharing among firms stemming from better-informed decisions (Gordon et al., 2003; Vives, 1990); 2) one can capture information sharing's benefits at the firm level (Vives, 1990), association members and/or aggregate

industry levels (Clarke, 1983), and the 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). Given that the benefits related to information sharing are context dependent, we need to take a closer look at ISACs in general and IT-ISAC in particular and their role in security-related information sharing.

2.2 ISAC and Information Sharing

Recognizing the criticality of information to its national and economic security, the U.S. Government played a central role in creating ISACs (GAO, 2010). ISACs are a form of security-based information-sharing organizations (SBISOs) including organizations such as US-CERT (Computer Emergency Response Team)[1], INFRAGARD[2], Secret Service Electronic Crime Task Force[3], and Chief Security Officers Round Tables (CSORTs)[4] (Gordon et al., 2003). More specifically, ISACs are information-sharing organizations "that serve as mechanisms for gathering, analyzing, and disseminating information on cyber infrastructure threats and vulnerabilities to and from owners and operators of the sectors and the federal government" (GAO, 2010, p. 8.). ISACs arose because firms and the government recognized that the private sector owns and operates much of the critical infrastructure of the U.S. economy. This recognition resulted in the Presidential Decision Directive 63 (PDD-63)[5] in May, 1998, that established the protection of the critical infrastructure as a national goal by calling for public and private cooperation through, among others, creating voluntary ISAC organizations.

ISACs assume that coordination and sharing aligns the goals between the public and private sector and, therefore, improves the security of strategically critical assets (Gal-Or & Ghose, 2005). As of 2016, there are currently 18 sector-aligned ISACs (see Table A1) that coordinate their activities under the National Council of ISACS[6]. Although ISACs share a common mission, the organizations form them design and establish their "rules of engagement", which results in ISACs based on the unique characteristics and needs of their individual sectors. Consequently, each ISAC can differ from the other in terms of its business model (legal structure, level of government involvement, staffing level), funding (fee structure, budgets, and government grants), and sharing mechanisms (email, Web access, conferences, etc.) (GAO, 2004a). While each ISAC organization is unique, three sets of activities are common to all of them:

> *establishing baseline statistics and patterns on the various infrastructures; serving as a clearinghouse for information within and among various sectors; providing a library of historical data for use by the private sector and government, and reporting private-sector-incidents to National Infrastructure Protection Center (NIPC)*[7]. (GAO, 2004a, p. 5)

2.2.1 Information Technology Information Sharing and Analysis Center (IT-ISAC)

In January 2001, 19 leading high-tech companies announced (U.S. Department of Commerce, 2001) sector-wide cooperation on cyber security issues through forming IT-ISAC. Using shared IT security information, IT-ISAC disseminates relevant information about system vulnerabilities, threats, and incidents to its members. It also shares the best practices and solutions among its members. As of 2004, the membership covered significant majority of North American and the world's IT goods and services: 90 percent of desktop operating systems, 85 percent of all databases, 50 percent of all desktop computers,

[1] The Department of Homeland Security in September 2003 created the United States Computer Emergency Readiness Team (US-CERT) to protect U.S. Internet infrastructure by coordinating defense against and response to cyber-attacks. US-CERT is responsible for analyzing and reducing cyber threats and vulnerabilities, disseminating cyber threat warning information, and coordinating incident response activities. More information on US-CERT available at www.us-cert.gov.

[2] InfraGard is an association of businesses, academic institutions, state and local law enforcement agencies, and other participants dedicated to sharing information and intelligence to prevent hostile acts against the United States. More information on InfraGard available at www.infragard.org.

[3] The Electronic Crime Task Force (ECTF) network brings together federal, state and local law enforcement, prosecutors, private industry, and academia to prevent, detect, mitigate, and aggressively investigate attacks on the nation's financial and critical infrastructures. More information on ECTF available at http://ectaskforce.org.

[4] See example at http://fcw.com/articles/2009/11/16/feat-ciso-roundtable.aspx.

[5] Presidential Decision Directive 63 resulted from effort across agencies to create a framework for protecting critical infrastructure. More information available at http://www.fas.org/irp/offdocs/pdd-63.htm.

[6] Only 15 ISACs are members of National Council of ISACS. For more information, see http://www.isaccouncil.org/memberisacs.html.

[7] A federal agency based in Washington, DC, the National Infrastructure Protection Center (NIPC) is the primary governmental organization charged with safeguarding the infrastructure networks and systems of the United States from attack, including computer-generated attacks such as hacking and viruses. For more information, see http://www.dhs.gov/national-infrastructure-coordinating-center.

85 percent of all routers, and 65 percent of security software (GAO, 2004b; ISAC Council, 2004). In the last 10 years, even though its membership structure has changed, the relative size of IT-ISAC's coverage of critical IT goods and services has remained significant. As a result of IT-ISAC membership and involvement in sharing and analyzing cyber information, member companies achieve benefits through trusted collaboration, analysis, and coordination and are in a position to "drive decision making by policy makers on cybersecurity, incident response, and information sharing issues" (IT-ISAC, n.d.b).

IT-ISAC is funded through a tiered membership fee structure (foundation platinum, foundation gold, premium silver and participant bronze) (IT-ISAC, n.d.c) and covers both cyber and physical hazards. As of May 2016, IT-ISAC comprises 42 member companies (see Appendix A2). The organization operates 24x7 by analyzing cyber alerts and advisories and reporting physical issues. Its information-sharing mechanisms include encrypted emails, SSL-protected websites, cellular phones, VoIP telephony, the Government Emergency Telecommunications Service (GETS) system[8] for priority calls, and the Critical Infrastructure Warning Network (CWIN)[9] (GAO, 2004b).

IT-ISAC members receive several benefits. The IT-ISAC website describes the benefits of membership as helping member firms to "manage risks through trusted analysis, collaboration and coordination and drive informed decision making by policy makers on cybersecurity, incident response and information sharing issues (IT-ISAC, n.d.a). Members have access and the ability to anonymously share security expertise on both cyber and non-cyber threats and events. Further, firms who share such information have access to cyber security experts' often non-public information. Information about non-cyber threats and events involves information on human and natural disasters with potential implications for member firms' IT departments. Operations centers in each member company and the IT-ISAC's operations center coordinates the information sharing.

2.2.2 IT Security-related Information Sharing in Information Systems (IS) Research

Researchers have conducted little IS-related research in the context of inter-firm information sharing such as IT-ISAC, but such research is gaining attention due to recent growth in security breaches requiring intra and inter-firm information sharing. The existing research builds on the TA literature and focuses on why firms share information and its implications. For example, using modeling approaches, research has suggested that a firm that shares more information or invests more in security technology motivates other firms in its industry to share more information and invest in security technology and that industry competitiveness positively impacts this motivation (Gal-Or & Ghose, 2005). The model also explains the impact of sharing information and investing in security technology on expanding demand in the product market ("direct effect") and on alleviating price competition ("strategic effect") (Gal-Or & Ghose, 2005). Other research has focused on efficiency of information sharing in the context of computer systems security and suggested that the economic analysis of information sharing requires understanding: 1) the information type, 2) the potential value associated with sharing information, 3) competition type, 4) the nature of the products produced, and 5) the firm's market share of those products (Gordon et al., 2003). While acknowledging the possibility that sharing security information will lower the overall costs of obtaining any level of information on security, research has criticized the current lack of effective incentives to reward information sharing in ISAC organizations. Namely, research has claimed that, in the absence of appropriate incentive mechanisms, firms will engage in "free-riding" that can ultimately lead to their underinvesting in information security (Gordon et al., 2003).

From the economic perspective, IS literature has focused on positive economic effects stemming from sharing IT security information. Research has discussed these effects in the context of the reduction of security breaches (Schechter & Smith, 2003) and security costs (Gordon et al., 2003), spillover-based improved product demand (Gal-Or & Ghose, 2005), consumers' comfort level with perceived security risks (Schenk & Schenk, 2002), and through improvements in operational benefits (Lohrmann, 2007). Related IS research has assessed the impact of inter-firm strategic information sharing in the context of buyer-supplier logistic relationships and found that the flow of strategic information yields performance gains for

[8] The Government Emergency Telecommunications Service (GETS) is an emergency phone service provided by the National Communications System (NCS) to be used in an emergency or crisis situation when the ability of completing a call over normal telecommunication means has significantly decreased. For more information, see http://www.dhs.gov/government-emergency-telecommunications-service.

[9] Operational since 2003, CWIN is the survivable link in the Homeland Security Information Network (HSIN), connecting DHS with the vital sectors that restore the Nation's infrastructure during emergencies. For more information, see http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cwin.pdf.

both parties and added additional conditions that promote the flow of information: party interdependence, asset specific investments in IT to promote information exchange mechanisms, and the role of trusting beliefs (Klein & Rai, 2009).

Despite the attention and calls for quantifying the benefits of security information sharing (ENISA, 2010), IS research has not empirically investigated the net impact of sharing IT security-related information through established organizations. Consistent with research investigating firm performance (e.g., Bharadwaj, 2000; Martin & Mykytyn, 2009; Santhanam & Hartono, 2003), we do not explicitly test how constructs from a theory influence firm performance. That is, we do not test the nomological network of relationships involving the constructs of a particular theory. Rather, based on Bharadwaj (2000), Martin and Mykytyn (2009), and Santhanam and Hartono (2003), we use the theoretical background that is important for understanding the benefits of security information sharing and that purports to realistically assess the impact of security information sharing. Accordingly, based on robust theoretical foundations, we empirically tested whether firm performance is better or worse based on membership in IT-ISAC. In Section 3, we discuss the theoretical background that can help resolve the paradox of sharing critical IT security information with competitors and present formal hypotheses.

3 Theoretical Background

3.1 Security Information Sharing Paradox

Simultaneous cooperative and competitive behavior among rival firms is called coopetition. The literature on coopetition provides a useful starting point to explore why firms participate in trade associations such as IT-ISAC. Coopetition involves sharing knowledge among competitors (Tsai, 2002) and is a model in which a network of stakeholders that cooperate and compete to create maximum value. Research has called coopetition one of the most important business perspectives of recent years (Bowser, 2010). For Khanna, Gulati, and Nohria (1998), while the cooperative aspect of coopetition is the use of shared knowledge to pursue common interests, the competitive aspect is the use of shared knowledge to outperform the competition. That is, while competing with each other, business players also cooperate among themselves to acquire new knowledge from each other. This behavior of using alliances to obtain new technology skills is not deceitful but rather suggests "the commitment and capacity of each partner to absorb the skill of the other" (Hamel, Doz, & Prahalad, 1989, p. 134).

Despite the acceptance of coopetition as a strategic management approach, several observers approached the announcement of IT-ISAC deployment with skepticism. Why would Oracle share its own security shortcomings with Microsoft or IBM? Why would EDS assist Computer Sciences in patching its security hole (Hurley, 2001)? What would steer these organizations into a cooperative/competitive mode rather than the traditional competition-only mode that worked so well for them in the past? These questions are even more relevant given some publicly reported disputes between information-sharing associations and their members over handling shared information. In one instance, a company shared security information with CERT, which CERT forwarded to third parties. Given that CERT shared information with information provider's competitors (CERT members), the company discontinued its ties with CERT (Roberts, 2003). Such real-world examples highlight the potential negative implications of sharing proprietary IT security information and raises questions about the motivations behind sharing IS security-related information.

Therefore, sharing information, especially security-based information, presents an interesting paradox. To achieve the benefits of being IT-ISAC members, such members need to share sensitive and potentially competitive intelligence with their direct competitors. Why would a firm then resort to a critical information-sharing strategy? In Section 3.2, we discuss this question via the relational view of the firm.

3.2 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 & Singh, 1998). Relational research argues that competitiveness arises not from the firm but rather from inter-firm sources of advantage. This view of the firm suggests that firms engaged in relational-based behaviors, such as knowledge sharing, achieve relational rents in the form of performance gains. Specifically, relational rents are 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 & Singh, 1998, p. 662). According to the

relational view of the firm, four potential sources of competitive advantage 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 & Singh, 1998). In Sections 3.2.1 to 3.2.4, we discuss each of these sources of competitive advantage and link them to behaviors and outcomes resulting from IT-ISAC firms' sharing security information between themselves.

3.2.1 Idiosyncratic Resources and IT-ISAC

Dyer and Singh's (1998) concept of idiosyncratic resources builds on the idea that strategic assets are specialized by their nature and that specializing resources is necessary for rent to occur (Amit & Schoemaker, 1993). Firms may create specialized resources through alliances/relationships with other firms (Teece, 1987), which results in relation-specific resources. Specifically, the nature of firms' investments, publicized efficiencies, changes in approaches to information gathering with time, dynamism, frequency of transactions, and long-lasting relationships strongly suggest that IT-ISAC membership exhibits characteristics of idiosyncratic asset creation. As such, one can expect it to be a source of competitive advantage and relational rents (Dyer & Singh 1998), which motivates firms to engage in sharing information with other firms.

According to relational-based view, entities can develop idiosyncratic resources when they accumulate know-how through relationships. For example, IT firms often invest in human assets in the form of time, resources, and available expertise to contribute to IT-ISAC partnerships. This investment is evident through member firms' investments in 1) their own operation center teams, 2) their providing access to their own security experts to share and exchange ideas, information, and the know-how with other member firms' experts, and 3) their own processes and policies to use the shared information. This investment could lead to partners' gaining experience and know-how, reacting to a change in the security environment that leads to process improvements, and developing resources idiosyncratic to the relationships specific to IT-ISAC.

3.2.2 Interfirm Knowledge Sharing and IT-ISAC

Beyond creating idiosyncratic assets, Dyer and Singh (1998) suggest and provide examples in which interfirm knowledge sharing is a source of relational rents as well. Interfirm knowledge-sharing routines are regular patterns of interfirm interactions that permit one to transfer, recombine, or create specialized knowledge (Grant, 1996). Research has described these routines as institutionalized processes designed to enable and support knowledge sharing. In the case of IT-ISAC, members have access to a confidential forum with 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 postings, and historical alerts.

IT security-related knowledge is distributed across the members of IT-ISAC. Sharing such information often involves pooling and transferring distributed, complex, and specialized knowledge. Prior research has shown that networks (rather than individual firms) are more effective in transferring such knowledge (Dyer & Nobeoka, 2000; Powell, Koput, & 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". For example, IT-ISAC activities often involve anonymous information sharing, activities focused around meetings, discussions with security experts, the set-up of operations centers, and discussions/briefings with government agencies. Non-members cannot easily imitate the insights and capabilities generated through these know-how sharing activities that arise from the Web of relationships owing to IT-ISAC membership. The governance and processes necessitated by IT-ISAC membership means members can quickly reach one another's critical expertise. In general, the member firms appear to have the ability to absorb and implement innovative and complex knowledge into their operational and overall business routines. Therefore, the interfirm knowledge-sharing routines that IT-ISAC provides to help firms share 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 given the coopetition paradox.

3.2.3 Complementary Resources and IT-ISAC

Complementary resources are another potential source of competitive advantage. Such resources are "distinctive resources of alliance partners that collectively generate greater rents than the sum of those

obtained individual endowments of each partner" (Dyer & Singh, 1998, p. 666-667). These complementary resources realized through IT-ISAC are not currently attainable through known alternate relationships or for purchase via the marketplace, and individual firms cannot develop these resources on their own without significant investments. Consequently, in the context of information security, the alliance appears to produce stronger competitive positions than firms that operate individually can achieve (Dyer & Singh, 1998; Shan & Walker, 1994). Similarly, the relational view suggests that certain organizations are in better position to recognize the complementary potential of shared resources. Firms' size and expertise in the information security field makes IT-ISAC members well positioned to assess the complementary potential of security information. Member firms have access to the IT security-related resource stacks that are not available to non-members. For instance, IT-ISAC is a founding member of the National Council of ISACs (NCI) and a member of its executive committee and operations committee. This governance structure enables members to benefit from more direct access to the Department of Homeland Security by "hosting a private sector liaison at the Department of Homeland Security (DHS) and National Infrastructure Coordinating Center (NICC) during incidents of national significance, emergency classified briefings, and real-time sector threat level reporting" (National Council of ISACs, n.d.). Other structures that enable potential complementary-resource creation include member postings, presentation materials, and the exchange of information during technical and special/affinity groups' meetings/events. Membership in IT-ISAC creates access to a forum of security specialists who are experts in their fields and have access and understand non-public details about vulnerabilities and threats. None of these complementary resources and resulting capabilities are available to non-members (National Council of ISACs, n.d.). Therefore, as per the relational view, complementary resources can be a source of relational rents. As such, the attractiveness of complementary resources is an important motivating factor for firms to engage in coopetition.

3.2.4 Effective Governance and IT-ISAC

The relational view suggests that effective governance is a key ingredient in relational rent creation because it minimizes transaction costs while positively impacting alliance/partnership willingness to engage. Specifically, it posits that the greater the ability to align transactions with governance structures in discriminating (cost reducing) manner, the greater the potential for relational rent (Dyer & Singh, 1998). IT-ISAC deploys the structure and the mechanisms used for information sharing to minimize transaction costs while maximizing the value of the shared information. Furthermore, research has suggested that self-enforcing safeguards exhibit a higher potential of relational rents due to lower contracting costs, monitoring costs, adaptation costs and re-contracting costs and superior incentives for value-creation initiatives (Dyer & Singh, 1998). Research has suggested that dynamic, highly complex and specialized knowledge such as the one found in IT-ISAC requires self-enforcing governance because "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 & Singh, 1998, p. 671). In line with relational view, our analysis of IT-ISAC suggests that IT-ISAC governance exhibits primarily self-governance safeguards rather than third party safeguards and, as such, better aligns governance with transactions. As a result, they have the potential to minimize transaction costs (efficiency) and promote information sharing (effectiveness), which lead to relational rents.

The governance of IT security related information-sharing process is a key service that IT-ISAC provides. For example, to incentivize members to share discovered weaknesses, IT-ISAC deploys non-disclosure agreements that enable members to freely and anonymously "share and understand non-public details of threats, incidents, effective practices and vulnerabilities" (IT-ISAC, n.d.a). It also requires members to use encrypted emails, SSL-protected websites, and the Government Emergency Telecommunications Service (GETS) system for priority calls (GAO, 2004b) to ensure information security and confidentiality. This governance came as a direct response to needing to ensure the flow of information and protect member firms from unwanted reputation risks. Using IT-ISAC's communication protocols, the partners achieve lower transaction costs than competitors who attempt to invest independently in the specialized assets. IT-ISAC communication protocols and information-sharing incentives are an example of transactions' being aligned with governance structures that leads to the greater potential for relational rent as advocated by the relational view.

In conclusion, we recognize that Dyer and Singh's (1998) relational view provides evidence that IT-ISAC members are privy to 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. Therefore,

we posit that the potential for relational sources of competitive advantage effectively eliminates the paradox and acts as an incentive to join and participate. In Section 3.3, we turn our attention to whether the sharing security information impacts firm performance. Accordingly, we develop hypotheses and empirically examine the impact of membership in IT-ISAC on financial performance.

3.3 Hypotheses

In Section 3.2, we suggest that the economic goals of relational rents/super-profits incentivize member companies to share and fully participate. Others have also addressed the topic of economic incentives to sharing information. For Schechter and Smith (2003), sharing security-related information can deter hackers and, in turn, can lead to the higher effectiveness of security technologies. The effectiveness of security technologies could have a spillover effect on the product demand and, thus, result in positive implications for the information-sharing organization's financial (profitability) performance. Specifically, Gal-Or and Ghose (2005) offer an example of the implications of IT security-related information sharing: customers (such as Procter and Gamble) of firms (such as Microsoft and Oracle) that are members of IT-ISAC are likely to have greater confidence in the product offerings when they perceive an increase in the effectiveness of the security technologies offered to them. The increased confidence will result in an increased demand for a firm's products. Furthermore, in the context of trade associations, Vives (1990, p. 413) states "in general, the increased precision of the information for a firm has a positive effect on its expected profits".

Collaboration in IT-ISAC increases the technological effectiveness of IT security products. The increase in the product's effectiveness will result in an increase in the firm's reputation and a greater demand for the firm's products and services and, hence, superior financial performance (Cavusoglu et al., 2004a; Gal-Or & Ghose, 2005). One can find evidence of information sharing's impacting financial performance in IS research on supply chains. For example, Klein and Rai (2009) found that strategically sharing information between firms improves the profitability dimensions of financial performance in areas of asset management and productivity. They also suggest that information sharing could result in improvements in capabilities such as production planning, resource control, and process flexibility, which ceteris paribus would lead to greater profitability. Given that reputation and the loss of customer loyalty in the context of data breaches do the most damage to firms' bottom line (Ponemon Institute, 2014), firms that are not part of IT-ISAC could suffer. Therefore:

> **Hypothesis 1:** Firms that participate in sharing IT security-related information have higher profitability than non-participating IT firms.

In addition to overall profitability, available research has repeatedly documented that IT security threats increase both direct and indirect costs for IT firms (Ettredge & Richardson, 2003; Garg, Curtis, & Halper, 2003). Direct costs include the loss of productivity (Klein & Rai, 2009; Wang, Rees, & Kannan, 2007), and indirect costs include the loss of future transactions (Wang et al., 2007). Research has quantified the impact of security threats and breaches on costs incurred by IT firms. For example, Corbin (2013) has estimated that the costs of cyber-crime to the U.S. economy has reached US$100 billion and 500,000 jobs. At the firm level, the average cost of a security breach in 2010 amounted to US$7.2 million (Ponemon Institute, 2011). More recent data suggests the range of average costs of data breach from US$1.4 million (India) to US$5.4 million (United States) per incident (Ponemon Institute, 2013a). Reports have stated the average annualized estimate of cyber-crime costs for each firm in the US in 2013 was US$11.6 million (Ponemon Institute, 2013b) and that the average cost of a data breach to a company in 2014 was US$3.5 million, which represents an increase of 15 percent over previous year (Ponemon, 2014). The insurance market has also confirmed cyber-crime's and security breaches' high costs: one longitudinal study found sufficient evidence that information security management has a significant economic impact on firms (Camp, 2006). In fact, the costs of cyber-crimes now exceed those of weather, fire, and social unrest events as they relate to disrupting firms' supply chain (Carpenter, 2013).

Given the magnitude of the impact of security threats and breaches on costs, we argue that any meaningful strategy to mitigate, prevent, avoid, and manage them, such as sharing security information, will impact the costs that firms incur. Available literature supports our view and suggests that sharing information will reduce firms' costs and the number of security breaches they incur (Schechter & Smith, 2003). Specifically, when firms share information with one another, they tend to lower their costs intended to support information-security activities (Gordon et al., 2003). Further, firms engaged in sharing IT security-related information can use the information they receive from other IT firms to build better products and more effectively guard against security threats, which should lead to reduced costs and

better resource management (Gal-Or & Ghose, 2005). Furthermore, IS research in the context of strategic information sharing in buyer-supplier relationship has found positive implications of information sharing in areas of operational costs and capabilities such as resource control that impacts firms' cost ratios (Klein & Rai, 2009). Therefore:

Hypothesis 2: Firms that participate in sharing IT-security related information have lower costs than non-participating IT firms.

According to the relational view of the firm, a firm can gain and sustain superior firm performance by accessing key resources that span its boundaries (Dyer & Singh, 1998). Since we establish in Section 3.2 that IT security-related information sharing is a key resource that spans firms' boundaries, that it builds on trust, and that its impact can only strengthen with time and frequency of interaction (Dyer & Singh 1998), we posit that the positive impact of sharing IT security-related information on firm performance (profitability and cost) will continue during subsequent time periods.

This expectation is in line with prior research on the long-term impact of IS-related capabilities on firms' financial performance (Bharadwaj, 2000; Santhanam & Hartono, 2003). Therefore, we hypothesize that IT-ISAC members (i.e., firms engaged in sharing IT-security related information sharing) will experience greater profitability and lower costs than non-members in the long run.

Hypothesis 3: In the long run, firms that participate in sharing IT-security related information have higher profitability than non-participating IT firms.

Hypothesis 4: In the long run, firms that participate in sharing IT-security related information have lower costs than non-participating IT firms.

4 Method and Results

4.1 Scope

In operationalizing the concept of sharing IT-security information, we limit our scope to IT firms for two reasons. Rooted in relational view of the firm, IT security-based information sharing is a source of superior performance and competitive advantage for firms whose business model, strategies, and offerings link closely to IT security. In IT security-based information sharing context, engaging and investing in coopetition appears to be most appropriate for IT firms because the benefits they accrue from sharing information are more closely related to their core value proposition. Second, since we focus on IT security-related information sharing, we believe that focusing on IT firms will lend significance to the statistical findings. That is, for IT firms, managing IT security is an integral part of their business, and any degradation of technology can impact firm performance.

4.2 Matched Sample Comparison

To test our hypotheses, we employ a matched sample comparison test by creating two groups of companies: a treatment group and a control group. Research has used this approach to empirically test differences in firm performance in fields such as accounting (e.g., Balakrishnan & Linsmeier, 1996) and marketing (e.g., Kalwani & Narayandas, 1995). IS research has also used the approach (Bharadwaj, 2000; Martin & Mykytyn, 2009; Morris, 2011; Santhanam & Hartono, 2003).

4.2.1 Treatment Group

Since IT-ISAC was the first industry-wide information-sharing association that specifically asked and encouraged its members to disclose private/company specific information that other members (possibly competitors) could directly use to potentially gain competitive advantages, it presents an appropriate setting for our investigation. Further, IT-ISAC has presented evidence about how its successful information-sharing practices and behaviors have resulted in positive outcomes. Therefore, we treated IT-ISAC's original members (i.e., when the organization announced its creation) as the members of the treatment group as long as: 1) firms belonged to the IT sector (scope) and 2) firms were publicly listed (financial data availability) (See Table 1).

The official announcement of IT-ISAC's formation listed 19 firms. Of that 19, 11 met our two conditions and formed the treatment group. We excluded AT&T since it is not an IT firm, and we excluded the remaining seven w because they are private companies.

Table 1. IT-ISAC Original Members*

Treatment group firms			
	Firm	**Firm type**	**GICS economic sector**
1	Computer Associates International Inc.	Publicly listed	Information technology
2	Cisco Systems Inc.	Publicly listed	Information technology
3	Computer Sciences Corp.	Publicly listed	Information technology
4	Hewlett-Packard Co.	Publicly listed	Information technology
5	Intel Corp.	Publicly listed	Information technology
6	IBM Corp.	Publicly listed	Information technology
7	Microsoft Corp.	Publicly listed	Information technology
8	Nortel Networks Ltd.	Publicly listed	Information technology
9	Oracle Corp.	Publicly listed	Information technology
10	Symantec Corp.	Publicly listed	Information technology
11	VeriSign Inc.	Publicly listed	Information technology
Firms excluded from the treatment group			
	Firm	**Firm type**	**GICS economic sector**
12	AT&T[1]	Publicly listed	Telecommunications services
13	RSA Security Inc.[2]	Private	N/A
14	Electronic Data Systems Corp.[2]	Private	N/A
15	Entrust Technologies Inc.[2]	Private	N/A
16	KPMG Consulting LLC [1] [2]	Private	N/A
17	Securify Inc.[2]	Private	N/A
18	Titan Systems Corp.[2]	Private	N/A
19	Veridian[2]	Private	N/A

*Source: https://fcw.com/articles/2001/01/21/it-firms-join-to-share-security-information.aspx
[1] Excluded from the treatment group due to economic sector (non-IT firms)
[2] Excluded from the treatment group due to firm type (non-publicly listed companies)

4.2.2 Control Group

In analyzing IT capability's impact on firm performance, Bharadwaj (2000) used the single-firm benchmark approach. This approach matches each treatment firm to a single comparison (control) firm. However, while matching allows for a strong statistical test due to subjectivity in selection, it limits the robustness of the results (Santhanam & Hartono, 2003). Since we focus on comparing select firms relative to the performance of the rest of their industry, we adopt Santhanam and Hartono's (2003) approach to benchmarking and creating control groups. Martin and Mykytyn (2009) successfully adopted this methodology to analyze the impact of business-method patents on firm performance. We found this method appropriate for several reasons: 1) since IT-ISAC membership is voluntary to any organization in the IT industry, it would be consistent to use the industry approach to evaluate the treatment groups' performance relative to all other firms in the industry and 2) an industry-wide basket of firms can serve as a statistically more accurate indicator of relative industry/market conditions versus potential variations stemming from selecting a single or smaller group of firms as the benchmark (Santhanam & Hartono, 2003). Furthermore, using standard industry classifications as basis for benchmarking allows for flexibility in the "industry" definition. By leveraging generally accepted classification systems, we can "roll up" company groups to industries and sectors to better measure the robustness of the results. Santhanam and Hartono (2003) also note that adopting this approach to comparing groups allows one to replicate the results for generalizability (Tsang & Kai-Man, 1999). Hence, we adopted an approach in which we

matched all the firms identified as the treatment group to other publicly traded companies in the same industry grouping, which resulted in a pool of companies used as a control group.

To pool together firms as a control group, we used the Global Industry Classification Standard (GICS) company-classification structure[10]. The GICS classification structure comprises 10 broad economic sectors aggregated from 23 industry groups, 59 industries, and 122 sub-industries. We selected GISC over other available classification mechanisms such as SIC and NAIC because it outperforms others in explaining financial ratios and lowering valuation errors (Bhojraj, Lee, & Oler, 2003; Weiner, 2005). Given we focus on financial performance ratios and their use in IS research (Chang, Jackson, & Grover, 2003; Du, Huai, & Liu, 2006; Martin & Mykytyn, 2009; Mojsilovic, Ray, Lawrence, & Takriti, 2007; Schumaker & Chen, 2010; Shu, 2010), adopting GISC seems appropriate.

Table 2. Control Group(s) Formation

Level 1: GICS industry group		Level 2: GICS Sub-industry		Basis for control group
Code	Description	Code	Description	IT-ISAC firms
4510	Software & services	45101010	Internet software & services	VeriSign Inc.
		45102010	IT consulting & other services	IBM Corp.
		45102020	Data processing & outsourced services	Computer Sciences Corp.
		45103020	Systems software	Microsoft Corp, Oracle Corp., Symantec Corp, Computer Associates International Inc
4520	Technology hardware & equipment	45201020	Communications equipment	Cisco Systems Inc., Nortel Networks Ltd.
		45202010	Computer hardware	Hewlett-Packard Co.
4530	Semiconductors & semiconductor equipment	45301020	Semiconductors	Intel Corp.

While we chose GICS over SIC (Bhojraj et al., 2003; Martin & Mykytyn, 2009; Weiner, 2005) and, therefore, differ from Santhanam and Hartono (2003), we did adopt the general approach of both Santhanam and Hartono (2003) and Martin and Mykytn (2009) in testing our hypotheses at two levels of the classification system (sub-industry and industry group) to strengthen the findings. Table 2 shows the final list of GICS sub-industries and industry groups whose firm members we included as control firms in testing our multi-level hypotheses based on the mapping of IT-ISAC firms to the most granular classification category (GICS sub-industries). In creating the control groups, we omitted the firms from the treatment group. In other words, we excluded a firm appearing as a member of the treatment group from the list of control group for the same industry and/or sub-industry.

4.3 Dependent Variable: Firm Performance

Firm performance can be viewed through the prism of profit and cost ratios. Within the IS context, a number of studies focus on these ratios (Alpar & Kim, 1990; Bharadwaj, 2000; Brown, Gatian, & Hicks, 1995; Brynjolfsson & Hitt, 1996; Cron & Sobol, 1983; Li & Richard, 1999; Mahmood & Mann, 1993; Martin & Mykytyn, 2009; Ravinchandran & Lertwongsatien, 2005; Santhanam & Hartono, 2003). In this research, we adopt the eight ratios from Bharadwaj (2000) which were later replicated in Santhanam and Hartono (2003) and Martin and Mykytyn (2009) as the operationalization of firm performance (Table 3).

Based on prior research on IS capabilities' influence on firm performance, we scaled two forms of income (net income and operating income) based on sales (return on sales (ROS) and operating income to sales (OI/S)), assets (return on assets (ROA) and operating income to assets (OI/A)), and employees (operating income to employees (OI/E)) and adopted them as firm's profitability indicators. While ROA represents a measure of a firm's income for each dollar of its assets, ROS captures a firm's income for each dollar of its sales. ROS as a measure of profitability is particularly useful because it avoids the effects of potential differences in asset-valuation methods across firms (Li & Richard, 1999). Other measures of profitability,

[10] Standard & Poor and MCSI/Barra created GICS in 1999 to establish a global standard for categorizing companies into sectors and industries.

such as OI/A and OI/S, effectively capture a firm's profit potential without relying on non-operating/extra sources of income (interest income, extraordinary income, etc.). Mckeen and Smith (1993) list these two measures as particularly appropriate for measuring IT value to the firm. Lastly, OI/E measures income level potential per employee. Combined, these five measures offer a parsimonious, accepted, and well-rounded picture of a firm's financial performance.

Table 3. Measures of Firm Performance (Bharadwaj, 2000)

Ratio type	Description	Acronyms
Profit ratios	Average return on sales	ROS
	Average return on assets	ROA
	Average operating income to assets	OI/A
	Average operating income to sales	OI/S
	Average operating income to employee	OI/E
Cost ratios	Average cost of goods sold to sales	COG/S
	Average selling and general administration expenses to Sales	SGA/S
	Average operating expenses to sales	OPEX/S

In addition to the profit focus, cost-focused measures offer another way to measure the effect of IS capabilities on firm performance. These measures include operating expenses to sales (OPEX/S), cost of goods sold to sales (COG/S), and selling and general administration expenses to sales (SGA/S). Since profit measure comprises both revenues and costs, focusing on only profit measures could "hide" the impact of IS investment in security-based information sharing. OPEX/S captures the total operating costs one needs to incur to obtain the measured profitability and is calculated as the sum of COG/S and SGA, which are "the generally accepted accounting measures for the production and overhead costs of a firm" (Bharadwaj, 2000), p. 181) [11].

In capturing more immediate/short term benefits of security-based information sharing, we extracted the financial performance measure information for the year-end results of the announcement year (2001), the results of which we used to test H1 and H2. Based on the theoretical support of relational view and resulting expectation of superior firm performance in the long run (H3 and H4), we also captured two more years of financial performance information (2002 and 2003) well. Other relevant IS research used the same methodology of capturing both the immediate and the sustained period (three years) (Bharadwaj, 2000; Martin & Mykytyn, 2009; Santhanam & Hartono, 2003) [12].

4.4 Data Analyses

We analyzed the data with SAS and used the Wilcoxon rank sum test and the two-sample t-test. An accepted way to test the impact of IS capability on firm performance is to compare the firm-performance means for the treatment and control groups using the two-sample t-test and to compare the respective median levels via the Wilcoxon rank sum test (Bharadwaj, 2000; Martin & Mykytyn, 2009; Santhanam & Hartono, 2003). Researchers have acknowledged the Wilcoxon rank sum test as appropriate (Bharadwaj, 2000) in the context of non-normality (Conover 1980). Furthermore, because our data for every measure exhibited unequal variances (using folded F test), we deemed a two-sample unequal variance test appropriate (using the Satterthwaite method).

We also employed the logistic regression analysis to assess the impact of prior years' financial performance. As financial performance is strongly influenced by prior years' performance (Santhanam & Hartono, 2003; Fama & French, 2000), researchers recommend this approach to control the halo effect (Bharadwaj, 2000). Since we used a three-year period to test a pair of hypotheses related to medium-term performance, we used the same three year period (1998-2000) in logistic regression to assess the impact of prior years' financial performance. Bharadwaj (2000) used five-year period in her halo effect test, but,

[11] We used COMPUSTAT to obtain all financial performance information and GISC codes associated with the firms. As other researchers have recognized (Martin & Mykytyn, 2009; Santhanam & Hartono, 2003), in some instances, financial performance information was missing from COMPUSTAT. In those instances and for a particular year and measure, we omitted the firms with missing information from further analysis.

[12] IT-ISAC was actually formed in December, 2000, and the official announcement was released on January 18, 2001. By capturing the results of 2001, 2002, and 2003, we effectively captured three years of performance following the event.

since a firm's immediate history generally has a stronger impact on current performance, a three-year period is a more conservative approach (Santhanam & Hartono, 2003).

Aligned with standard practices when using logistic regression, we coded the dependent variable as a binary variable (Y = 1 for the treatment group and Y = 0 for control firms), which resulted in the full model:

$$Y = ß_0 + ß_1 (ROS) + ß_2 (ROA) + ß_3 (OI/A) + ß_4 (OI/S) + ß_5 (OI/E) + ß_6 (COG/S) + ß_7 (SGA/S) + ß_8 (OPEX/S) + e \quad (1)$$

Additionally, since we did not achieve convergence while using logistic regression as Equation 1 outlines, we created separate logistic regression models and tested them for profit and cost measures using the following equations:

$$Y = ß_0 + ß_1 (ROS) + ß_2 (ROA) + ß_3 (OI/A) + ß_4 (OI/S) + ß_5 (OI/E) + e \quad (2)$$

$$Y = ß\ 0 + ß_1 (COG/S) + ß_2 (SGA/S) + ß_3 (OPEX/S) + e \quad (3)$$

4.5 Results

Table 4 summarizes the results. We found support for all four hypotheses. However, the strength of the support varies because some measures did not show statistical robustness when compared to others.

Table 4. Results Summary

H1	Firms that participate in sharing IT security-related information have higher profitability than non-participating IT firms.	Supported
H2	Firms that participate in sharing IT-security related information have lower costs than non-participating IT firms.	Supported
H3	In the long run, firms that participate in sharing IT security-related information have higher profitability than non-participating IT firms.	Strongly supported
H4	In the long run, firms that participate in sharing IT-security related information have lower costs than non-participating IT firms.	Strongly supported

Overall, out of 96 different tests, over 85 percent (83 out of 96) of them showed superior financial performance of the treatment group over the control group at the 10 percent significance level or below[13]. Furthermore, in the remaining 13 cases, all ratios showed better financial performance for the treatment group relative to the control group. For the same 13 tests outside of the 10 percent significance cut-off, four approached the 10 percent significance level. Lastly, similar statistical strength of the results is exhibited for both t-tests and z-statistics.

Table 5 and Table 6 show the specific results for all tests conducted. Each table provides performance data across eight financial ratios for both the treatment (original IT-ISAC members) and control (remaining firms in the industry) groups. The tables provide sample counts, respective mean values, t-statistics (t-test), and respective median values and their z-statistics (Wilcoxon test) across groups, years, and two-levels of industry definitions. We followed the convention used in similar studies and placed the negative sign before the t and z test statistic if the financial performance ratio of the treatment group was better than the control group's performance ratio. With regards to profit ratios, higher values represent better performance, and, for cost ratios, lower values represent better financial performance.

We originally intended to test the hypotheses at sub-industry, industry, and sector group level of the GISC firm classification system. However, since our treatment group members came from all three industry groups in the IT economic sector, our tests for industry group level represent results for the whole sector as well. In Sections 4.5.1 to 4.5.2, we present the results for each hypothesis separately.

[13] Given the similarity in hypotheses development, methodology, context, identical performance measures, and statistical tests, we reported the levels of significance thresholds at 0.1, 0.05, and 0.01. This approach is consistent with prior research on IS's impact on firm performance (e.g., Bharadwaj 2000; Santhanam & Hartono, 2003). The findings do not change in any meaningful way if we adopt a $p < 0.05$ significance level as all but 7 out of 83 statistically significant tests were significant at $p<0.5$ or below.

4.5.1 Current/Short-term Firm Performance (Hypotheses 1 and 2)

Table 5 summarizes the results based on t-tests and Wilcoxon tests of firms' financial performance for 2001 (the year IT-ISAC formed). We used these results to assess support for H1 and H2.

Table 5 shows that treatment group performed significantly better than the control group for all five profit ratios and across both levels of the control group. Out of 20 tests conducted for 2001 data, 16 (80%) were significant at the 10 percent significance level or below. Additionally, for every profit ratio test, the z-statistic was significant at or below the 5 percent significance level. Therefore, supporting H1, we conclude that, with regards to profitability-based financial performance, the members of the original IT-ISAC outperformed other firms in the industry.

Table 5 also shows the performance of the groups with reference to cost ratios. Data for all three cost ratios exhibited the treatment group's superiority (lower ratio values), while the difference between groups for two out of three cost ratios was significant at the 10 percent significance level or below. The cost of goods sold over sales (COG/S) ratio failed to meet the level of significance for three out of four tests. However, the t-test for sub-industry level approached significance (it was significant at below 11 percent significance). Furthermore, when combined with SGA costs in the OPEX ratio, the difference between the

Table 5. Summary of Short-term Financial Performance (2001): H1 and H2

		Subindustry level					Industry/sector level				
		N	Mean	Median	t	Z	N	Mean	Median	t	Z
Profitability ratios											
ROA	Treatment	11	-0.226	0.029	-2.04**	-2.19**	11	-0.226	0.028	-1.69*	-1.92*
	Control	504	-2.666	-0.179			940	-6.932	-0.131		
ROS	Treatment	11	-1.324	0.022	-1.36	-1.99**	11	-1.324	0.022	-1.21	-1.80*
	Control	482	-5.056	-0.234			907	-3.519	-0.140		
OI/A	Treatment	11	-0.009	0.062	-2.35**	-2.55**	11	-0.009	0.062	-1.98**	-2.20**
	Control	504	-1.901	-0.139			940	-4.279	-0.084		
OI/S	Treatment	11	-0.274	0.062	-1.94*	-2.26**	11	-0.274	0.062	-2.48**	-2.07**
	Control	482	-3.935	-0.176			907	-2.912	-0.088		
OI/E	Treatment	11	-0.076	0.024	-0.14	-2.17**	11	-0.076	0.024	0.02	-1.97**
	Control	472	-0.091	-0.029			871	-0.074	-0.016		
Cost ratios											
COG/S	Treatment	11	0.487	0.450	-1.59	-1.06	11	0.487	0.450	-2.03**	-1.14
	Control	482	3.355	0.586			907	2.470	0.590		
SGA/S[1]	Treatment	10	0.372	0.397	-3.30***	-1.81*	10	0.372	0.397	-4.65***	-1.34
	Control	432	1.368	0.514			827	1.259	0.460		
OPEX/S[1]	Treatment	10	0.811	0.811	-3.75***	-3.31***	10	0.811	0.811	-5.24***	-3.25***
	Control	432	1.968	1.044			827	1.853	0.991		

* Significant at p < 0.10, ** Significant at p < 0.05, *** Significant at p < 0.001
[1] We did not include CA Inc. because its 2001 data for SGA was missing from COMPUSTAT.

treatment and control groups become significant at the 1 percent level of significance. These findings support H2.

4.5.2 Superior Firm Performance in the Long Run (Hypotheses 3 and 4)

Table 6 summarizes the results of the financial performance of the firms for the second and third year following IT-ISAC's formation. We used these results to assess support for H3 and H4.

Table 6. Summary of Longer-term Financial Performance (2002-2003): H3 and H4

2002		Sub-industry Level					Industry/sector level				
		N	Mean	Median	t	Z	N	Mean	Median	t	Z
Profitability ratios											
ROA	Treatment	11	-0.170	0.039	-1.51	-2.41**	11	-0.170	0.039	-1.79*	-2.22**
	Control	522	-4.466	-0.161			975	-2.922	-0.138		
ROS	Treatment	11	-0.362	0.030	-1.98**	-2.13**	11	-0.362	0.030	-2.29**	-2.00**
	Control	497	-11.467	-0.199			946	-7.180	-0.133		
OI/A	Treatment	11	0.064	0.074	-1.53	-3.03***	11	0.064	0.074	-1.82*	-2.82***
	Control	523	-4.242	-0.095			975	-2.706	-0.063		
OI/S	Treatment	11	0.074	0.056	-2.75***	-2.79***	11	0.074	0.056	-3.41***	-2.70***
	Control	497	-6.938	-0.108			946	-4.624	-0.075		
OI/E	Treatment	11	0.037	0.017	-4.26***	-2.89***	11	0.037	0.017	-4.02***	-2.76***
	Control	482	-0.083	-0.020			903	-0.078	-0.012		
Cost ratios											
COG/S	Treatment	11	0.414	0.353	-2.11**	-1.99**	11	0.414	0.353	-2.59***	-2.14**
	Control	497	5.095	0.589			946	3.519	0.596		
SGA/S	Treatment	11	0.392	0.382	-1.86*	-1.74*	11	0.392	0.382	-2.38**	-1.39
	Control	444	2.743	0.503			855	2.009	0.470		
OPEX/S	Treatment	11	0.806	0.765	-1.97**	-3.33***	11	0.806	0.765	-2.60***	-3.31***
OPEX/S[1]	Control	444	3.305	1.012	-3.75***	-3.31***	855	2.580	0.991	-5.24***	-3.25***
2003		**Industry/sector level**					**Sub-industry level**				
		N	Mean	Median	t	Z	N	Mean	Median	t	Z
Profitability ratios											
ROA	Treatment	11	0.058	0.073	-3.32***	-3.09***	11	0.058	0.073	-4.11***	-2.94***
	Control	552	-2.002	-0.067			1015	-1.350	-0.041		
ROS	Treatment	11	0.088	0.085	-3.32***	-3.01***	11	0.088	0.085	-4.30***	-3.02***
	Control	529	-3.667	-0.075			983	-3.455	-0.042		
OI/A	Treatment	11	0.103	0.102	-3.55***	-3.30***	11	0.103	0.102	-4.34***	-3.11***
	Control	552	-1.719	-0.047			1014	-1.131	-0.018		
OI/S	Treatment	11	0.164	0.119	-3.20***	-3.32***	11	0.164	0.119	-4.19***	-3.26***
	Control	529	-3.395	-0.049			982	-3.115	-0.013		
OI/E	Treatment	11	0.067	0.033	-4.71***	-3.58***	11	0.067	0.033	-4.71***	-3.46***
	Control	507	-0.065	-0.010			943	-0.058	-0.003		
Cost ratios											
COG/S	Treatment	11	0.385	0.307	-2.13**	-2.18**	11	0.385	0.307	-3.12***	-2.27**
	Control	530	2.240	0.564			983	2.595	0.569		
SGA/S	Treatment	11	0.366	0.381	-3.42***	-1.46	11	0.366	0.381	-4.19***	-1.29
	Control	483	1.888	0.439			911	1.405	0.432		
OPEX/S	Treatment	11	0.751	0.712	-3.74***	-3.58***	11	0.751	0.712	-4.80***	-3.64***
	Control	483	2.503	0.975			911	2.003	0.959		

* Significant at p < 0.1, ** Significant at p < 0.05 , *** Significant at p < 0.001

Table 6 shows that the treatment group performed significantly better than the control group for all five profit ratios and across both levels of the control group. Out of 40 tests conducted for 2002-2003 data, 38 (95%) were significant at the 10 percent significance level. Additionally, for every profit ratio test, the z-statistic was significant at or below the 5 percent significance level. In 2003, all profitability ratios were significant at the 1 percent significance level for both t-test and z-statistics. Combined with the results for 2001, these results show that, with regards to profitability-based financial performance, the original IT-ISAC members sustained better performance than the industry as a whole and, thus, strongly support H3.

Similarly, the information about cost ratio in Table 6 offers strong evidence of the treatment group's superior firm performance over the rest of the industry. The table shows that the treatment group performed significant better (20 out of 24 tests) than the remaining firms from the industry for all three cost ratios and across both levels of the control group. Combined with the results for 2001, these results strongly support H4.

4.5.3 Controlling for Prior Firm Performance

To control for the halo effect associated with prior financial performance, we ran a logistic regression analyses using three-year historical data (1988-2000) to see if one could explain our firm groupings (at the sub-industry level) though historical performance. Our full model (all eight ratios—Equation 1) failed to converge, which made the model fit questionable. As such, our interpretation of the results could be misleading. We proceeded with two separate logistic regressions—one associated with profit ratios (Equation 2) and one with cost ratios (Equation 3). While the cost model failed to converge, the profit model converged successfully. Score and Wald tests showed that the profit model was not statistically significant (score p-value was 0.53 and Wald p-value was 0.17); hence, prior profit-related financial-firm performance failed to explain our grouping the companies we identified into the treatment and control groups (Table 7). The finding, while not conclusive because the full and cost models failed to converge, partially supports this research's significance[14].

Table 7. Controlling for Prior Performance

Profitability model (converged)				**Cost model (failed to converge)**			
Test	Significance	Variable	Significance	Test	Significance	Variable	Significance
Score	0.53	ROA	0.5626	Score	0.92	COSS	0.8923
Wald	0.17	ROS	0.9572	Wald	0.04	SGAS	0.9292
		OIA	0.3112			OPEX	0.6330
		OIS	0.9492				
		OIE	0.6974				

5 Discussion

In this paper, we explore whether sharing security information impacts firms' financial performance. The empirical results confirm that firms that shared IT security-related information performed better than peer firms. We observed their superior performance 1) in both cost and profitability ratios, 2) at both the sub-industry and industry levels, and 3) across the short and longer term. The robustness our findings suggest that inter-firm IT security-information sharing occurring in IT-ISAC results in relational rents for participants.

Second, the results are in line with a Delphi study by the European Network and Information Agency (ENISA, 2010) that suggests that two top incentives influence firms to share IT-security information: 1) economic incentives stemming from cost savings and 2) effectiveness incentives stemming from the quality, value, and use of shared information. While our results indicate the expected direction of results for both profitability and cost measures, note that IT sharing security-related information appears to have greater influence on profitability measures than cost measures (as measured by differences in ratios between our two groups). Although we did not hypothesize the relative size of the impact between our two dimensions of financial performance, other studies suggest that sharing IT security-related information

[14] While one customarily reports the probabilities, odds, and odds ratios when analyzing logistic regression results, the value of reporting these results and their interpretations is limited in our context because the models and corresponding financial measures/ratios were not significant.

might improve product demand (Gal-Or & Ghose, 2005) and consumers' comfort level with how secure they perceive a firm's products (Schenk & Schenk, 2002), which lead to improved revenues. Since profitability measures comprise both cost and revenue dimensions, reducing costs and increasing revenues could explain why sharing IT security-related information has such a significant effect on firms' profitability. Moreover, the treatment firms' superiority relative to both sub-industry and industry level peers further support to our findings.

Lastly, we found similar results for both one- and three-year periods, which indicates that one can maintain the benefits of sharing IT security-related information over time. However, the gap between IT-ISAC and non-IT-ISAC members relative to total operating cost ratio (OPEX/S) widened over time. The percent difference in median values between the two groups in 2001 was 18 percent (industry), and, in 2003, the difference was over 24% respectively. Furthermore and as expected, our empirical findings reflect that superior performance in COG/S was the most significant contributor to OPEX/S gap; the difference in median values for COG/S between the treatment and control group increased from 14 percent in 2001 to 26 percent in 2003. One might explain this widening gap with fact that, with time and frequency of transactions, partner trust increases (Dyer & Singh, 1998), which results in more advantages from information sharing.

5.1 Implications for Practice

Our research offers relevant implications to IT firms and security-based information-sharing organizations. From an IT firm perspective, this research offers three important implications. First, this research indicates that firms gain financial advantage if they engage in sharing IT security information with other firms. Specifically, security-based information sharing has positive profitability impact both in the short and longer terms. We found that sharing IT security-related information not only helps lower costs but also impacts revenues. This finding highlights that IT security-based information-sharing leadership practices have the potential for improved demand through improved consumer comfort levels with perceived security risk of firm's products. These effects on profitability appear to increase in statistical significance over time, which suggests that firms should be patient to realize the effectiveness and efficiency benefits of information-sharing practices. Executives could leverage these results as evidence of sharing IT security information's positive ROI and promote investments and initiatives to support it not as a low return, regulatory/"keeping-the-lights-on" investments but rather as cost reducing-/revenue-supporting initiatives. Indeed, a firm needs to integrate sharing IT security information into its overall business strategy.

Second, IT firms should not treat IT security management as an exclusively, internally focused activity anymore. Our study shows that IT security information is dynamic, complex, distributed, and too costly for firms to manage in isolation. We show that investing into inter-firm assets through sharing IT security information creates more effective and efficient transactions. This approach may require a firm to reorganize itself and change its culture, which further reinforces the case for an enterprise-level approach to managing internal IT security information.

Third, IT firms' executives and the management need to pay attention to how they manage and communicate the sharing of IT security-related information. Our research suggests that one needs to know "how" knowledge is shared; therefore, firms needs to address questions around governance, procedures, tacit knowledge transfer, and absorptive capacity to realize the benefits of sharing IT security information. IT firms need to ensure they not only share and receive information with others but also have the absorptive capacity to integrate new information and know-how quickly and deeply throughout themselves. Consequently, company-wide coordination, the total and deep integration of shared information, the magnitude of costs and spill-over product effects, and the frequency of incidents makes sharing IT security information's impact evident at all levels/units of the business. Firms need to elevate sharing IT security-related information as an enterprise-wide priority that receives visibility and attention from cross-functional leaders.

Our research also has implications for security-based information-sharing organizations (SBISOs), such as IT-ISAC, other ISACs, and equivalent global organizations. First, one could use findings from our research to educate and inform current and potential members on the financial implications of sharing IT security information between firms. Second, effective governance is paramount to promote trust and, in turn, information sharing among firms. Effective governance can foster more information-sharing transactions and, over time, allow organizations to go from simply exchanging information to exchanging know-how that can ensure the efficiency and effectiveness impact of the collaboration over competition.

Third, given that "how" information is shared is extremely important in the context of the relational view of the firm, SBISOs and member firms need to be careful in accepting new members. New members have to be willing be commit resources to share information and have the absorptive capacity to implement newly acquired information and know-how. Changes in membership without understanding those critical elements may have unintended consequences on underlying factors such as trust, "free-riding", and incentives.

The current practitioner literature stresses the importance of addressing IT security management through enterprise-wide governance that is strategic and elevated to the C and/or board level[15]. Further, practitioners recognized that IT and data security is something that IT firms should not manage only in their borders. In fact, some practitioner studies suggest outsourcing to third parties (managed security-service providers) as way of dealing with IT security[16]. Due to large supply chain disruption risks, the insurance industry has suggested (in line with our recommendations) that firms manage cyber risks across company borders (Carpenter, 2013).

5.2 Implications for Research

This is the first study, to the best of our knowledge, to provide empirical evidence that sharing IT security information among firms positively impacts their financial performance. While others have 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, this research is the first to provide empirical evidence.

This research builds on the theoretical foundations of the relational view of the firm. However, in this research, we do not explicitly link the different constructs from the relational view to firm performance, and future research could look into this aspect. In addition, future research could also investigate employee-level (e.g., role conflict, esprit de corps, organizational commitment) and client-level (e.g., loyalty, satisfaction) consequences.

In the context of resolving the security information-sharing paradox, we did not explore specific firm and managerial motivations for joining the IT-ISAC. That is, we did not evaluate and interview individual firms, assess their unique situations beyond IT-ISAC membership, or talk to firm executives or managers about their motivations**.** 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. Therefore, we welcome further conceptual scrutiny on the arguments we present. In doing so, future research could explore alternative and/or rival theoretical explanations and subject them to conceptual and empirical scrutiny as well.

In addition, this research offers a promising theoretical lens for analyzing additional IS activities that span organizational boundaries and are dynamic and complex in nature. In an environment where significant components of products and services are distributed and collaborative in the IT context, the importance of cross-organizational, boundary-spanning IS activities will most likely increase. Accordingly, our research's theoretical foundations provide fertile ground for future research that examines complex IS activities, such as IS-enabled supply chain management, customer-relationship management, credit/risk management, and regulatory compliance.

6 Limitations and Corresponding Future Research

This paper has several limitations. First, we focused on IT and publicly listed companies; as such, we did not capture the performance of other firms that are similar to the treatment firms. As such, future research should consider ways of incorporating non-IT and smaller firms with significant IT implications on firms' business strategy and value proposition. Further, the methodology we adopted resulted in a pool of large, U.S.-centric firms. For the purposes of generalizability, we need to replicate this study with a more diverse basket of firms in terms of size and geography.

[15] https://buildsecurityin.us-cert.gov/articles/best-practices/governance-and-management/security-is-not-just-a-technical-issue
[16] http://www.gartner.com/it-glossary/mssp-managed-security-service-provider

In this study, the conceptualization of financial performance included a basket of ratios that might not have completely captured firms' cost and profitability performance. Although this conceptualization concurs with the peer-validated methodology of cost and profitability conceptualization, we need to explore other indicators of cost and profitability. Further, we focused on only officially published accounting data. Other studies should consider adding more perceptual measures of firm performance from experts, customers, and other informants to further validate their and our results and potentially offer new insights.

We adopted a three-year period to evaluate the implications of sharing IT security-related information. By selecting this period, this study remains aligned with other IS studies that have examined the impact of IS on firm performance (Li & Richard, 1999; Martin & Mykytyn, 2009; Ravinchandran & Lertwongsatien, 2005; Santhanam & Hartono, 2003). We chose a shorter period to guard against spurious associations (often a risk with longer periods) and to mitigate halo effects (Bharadwaj, 2000; Kettinger, Grover, Guha, & Segars, 1994; Martin & Mykytyn, 2009; Santhanam & Hartono, 2003). Our choice of methodology, however, limits the results since we do not know if the results would hold for longer periods. Future research should explore longer-term implications of sharing IT security-related information and our results' generalizability.

In conclusion, our research explores a critical research questions in the IT-ISAC context: does sharing security information impact firms' financial performance? Based on the relational view of the firms as a theoretical foundation that resolves the coopetition paradox, our empirical analyses provide robust results that support the assertion that sharing security information positively impacts firm's financial performance. Acknowledging our research as a starting point, we invite further conceptual and empirical research in this important research domain.

Acknowledgments

We thank Scott Algeier, the executive director of IT-ISAC, for his help with this research. In addition, we thank the Associate Editor and the Editor-in-Chief for their invaluable feedback, guidance, and insights on streamlining this manuscript.

References

Alpar, P., & Kim, M. (1990). A microeconomic approach to the measurement of information technology value. *Journal of Management Information Systems, 7*(2), 55-69.

Amit, R., & Schoemaker, P. J. H. (1993). Strategic assets and organizational rent. *Strategic Management Journal, 14*(1), 33-46.

Balakrishnan, R., & Linsmeier, T. J. (1996). Financial benefits from jit adoption: Effects of customer concentration and cost structure. *Accounting Review, 71*(2), 183-205.

Bennett, R. J. (2000). The logic of membership of sectoral business associations. *Review of Social Economy, 58*(1), 17-42.

Bharadwaj, A. S. (2000). A resource-based perspective on information technology capability and firm performance: An empirical investigation. *MIS Quarterly, 24*(1), 169-196.

Bhojraj, S., Lee, C. M. C., & Oler, D. K. (2003). What's my line? A comparison of industry classification schemes for capital market research. *Journal of Accounting Research, 41*(5), 745-774.

Bowser, J. (2010). Strategic co-opetition: The value of relationships in the networked economy *IBM Executive Strategy Report.* Retrieved from http://www-935.ibm.com/services/uk/index.wss/multipage/igs/ibvstudy/a1008082/2?cntxt=a1006870

Brading, A. (2013). Adobe breach thirteen times worse than thought, 38 million users affected.Retrieved from http://nakedsecurity.sophos.com/2013/10/30/adobe-breach-thirteen-times-worse-than-thought-38-million-users-affected/

Brown, R. M., Gatian, A. W., & Hicks, J. O., Jr, (1995). Strategic information systems and financial performance. *Journal of Management Information Systems, 11(4)*, 215-248.

Brynjolfsson, E., & Hitt, L. (1996). Paradox lost? Firm-level evidence on the returns to information systems spending. *Management Science, 42*(4), 541-558.

Camp, J.L. (2006). The state of economics of information security. *I/S: A Journal Of Law And Policy, 2*(2), 189-205.

Carpenter, G. (2013). *Emerging risk report*. Retrieved from http://www.biztositasiszemle.hu/files/201309/emerging-risks-report-2013.pdf

Cavusoglu, H, Mishra, B., & Raghunathan, S. (2004b). The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers. *International Journal of Electronic Commerce, 9*(1), 69-104.

Cavusoglu, H., Cavusoglu, H., & Raghunathan, S. (2004a). Economics of IT security management: Four improvements to current security practices. *Communications of AIS*, *14*, 65-75.

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004c). A model for evaluating IT security investments. *Communications of the ACM, 47*(7), 87-92.

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2005). The value of intrusion detection systems in information technology security architecture. *Information Systems Research, 16*(1), 28-46.

Chang, K., Jackson, J., & Grover, V. (2003). E-commerce and corporate strategy: An executive perspective. *Information & Management, 40*(7), 663-675.

Clarke, R. N. (1983). Collusion and the incentives for information sharing. *The Bell Journal of Economics, 14*(2), 383-394.

Corbin, K. (2013). Cybercrime costs U.S economy $100 billion and 500,000 jobs. *CIO.* Retrieved from http://www.cio.com/article/736824/Cybercrime_Costs_U.S_Economy_100_Billion_and_500_000_Jobs

Cron, W. L., & Sobol, M. G. (1983). The relationship between computerization and performance: A strategy for maximizing the economic benefits of computerization. *Information & Management, 6*(3), 171-181.

Du, Z., Huai, J., & Liu, Y.. (2006). Ad-UDDI: An active and distributed service registry technologies for e-services. In C. Bussler & M.-C. Shan (Eds.), *Lecture Notes in Computer Science* (vol. 3811, pp. 58-71). Heidelberg, Berlin: Springer.

Dyer, J. H., & Nobeoka, K.. (2000). Creating and managing a high-performance knowledge-sharing network: The Toyota case. *Strategic Management Journal, 21*(3), 345-367.

Dyer, J. H., & Singh, H. (1998). The relational view: Cooperative strategy and sources of interorganizational competitive advantage. *Academy of Management Review, 23*(4), 660-679.

ENISA. (2010). *Incentives and challenges for information sharing in the context of network and information security.* Retrieved from http://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/information-sharing-exchange/incentives-and-barriers-to-information-sharing

Ettredge, M. L., & Richardson, V. J. (2003). Information transfer among internet firms: The case of hacker attacks. *Journal of Information Systems, 17*(2), 71-82.

Fama, E. F., & French, K. R. (2000). Forecasting probability and earnings. *The Journal of Business, 73*(2), 702-728.

Gal-Or, E. (1985). Information sharing in oligopoly. *Econometrica, 53*(2), 329-343.

Gal-Or, E. (1986). Information transmission—Cournot and Bertrand equilibria. *Review of Economic Studies, 53*(172), 85.

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

GAO. (2004a). *Critical infrastructure protection: Establishing effective information sharing with infrastructure sectors* (Publication No. GAO-04-699T). Retrieved from www.gao.gov/cgi-bin/getrpt?GAO-04-699T

GAO. (2004b). *Critical infrastructure protection: Improving information sharing with infrastructure sectors* (Publication No. GAO-04-780). Retrieved from www.gao.gov/cgi-bin/getrpt?GAO-04-780

GAO. (2010). *Critical infrastructure protection; key private and public cyber expectations need to be consistently addressed* (Publication No. GAO-10-628T). Retrieved from www.gao.gov/cgi-bin/getrpt?GAO-10-628

Garg, A., Curtis, J., & Halper, H. (2003). Quantifying the financial impact of IT security breaches. *Information Management & Computer Security*, *11*(2), 74-83.

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

Grant, R. M. (1996). Prospering in dynamically-competitive environments: Organizational capability as knowledge integration. *Organization Science, 7*(4), 375-387.

Hamel, G., Doz, Y. L., & Prahalad, C. K. (1989). Collaborate with your competitors—and win. *Harvard Business Review, 67*(1), 133-139.

Hirschman, A.O. (1970). *Exit, voice and loyalty*. Cambridge, Mass: Harvard University Press.

Hirschman, A.O. (1982). *Shifting involvements: Private interest and public action*. Oxford: Basil Blackwell.

Huddleston, T. (2015). Anthem's big data breach is already sparking lawsuits. *Fortune.* Retrived from http://fortune.com/2015/02/06/anthems-big-data-breach-is-already-sparking-lawsuits/

Hurley, E. (2001). IT-ISAC: *A matter of trust.* Retrieved from http://searchsecurity.techtarget.com/news/517824/IT-ISAC-A-matter-of-trust

ISAC Council. (2004). *Reach of the major ISACs.* Retrieved from http://www.isaccouncil.org/images/Reach_of_the_Major_ISACs_013104.pdf

IT-ISAC. (n.d.a). *Member benefits*. Retrieved from http://www.it-isac.org/#!SERVICES/ch6q

IT-ISAC. (n.d.b). *Sharing cybersecurity threats and insights*. Retrieved from http://www.it-isac.org/

IT-ISAC. (n.d.c). *IT-ISAC membership*. Retrieved from http://www.it-isac.org/#!members/c1tsl

Kalwani, M. U., & Narayandas, N. (1995). Long-term manufacturer-supplier relationships: Do they pay off for supplier firms? *Journal of Marketing, 59*(1), 1-16.

Kettinger, W. J., Grover, V., Guha, S., & Segars, A. H. (1994). Strategic information systems revisited: A Study in Sustainability and Performance. *MIS Quarterly*, 18(1), 31-58.

Khanna, T., Gulati, R., & Nohria, N. (1998). The dynamics of learning alliances: Competition, cooperation, and relative scope. *Strategic Management Journal, 19*(3), 193-210.

Kirby, A. J. (1988). Trade associations as information exchange mechanisms. *RAND Journal of Economics, 19*(1), 138-146.

Klein, R., & Rai, A.. (2009). Interfirm strategic information flows in logistics supply chain relationships. *MIS Quarertly, 33*(4), 735-762.

Li, L.. (1985). Cournot oligopoly with information sharing. *RAND Journal of Economics, 16*(4), 521-536.

Li, M., & Richard Y. L. (1999). Information technology and firm performance: Linking with environmental, strategic and managerial contexts. *Information & Management, 35*(1), 43-51.

Lohrmann, D. (2007). Sharing with ISAC. *Public CIO, 5*(6), 56.

Mahmood, M. A., & Mann, G. J. (1993). Measuring the organizational impact of information technology investment: An exploratory study. *Journal of Management Information Systems, 10*(1), 97-122.

Martin, N. L., & Mykytyn, P. P. (2009). Evaluating the financial performance of business method patent owners. *Information Systems Management, 26*(3), 285-301.

Mckeen, J. D., & Smith, H. A. (1993). The relationship between information technology use and organisational performance. In R. D. Banker, R. J. Kauffman, & M. A. Mahmood (Ed.), *Strategic information technology management: Perspectives on organisational growth and competitive advantage*. Harrisburg, PA: Idea Group Publishing.

Mojsilovic, A., Ray, B., Lawrence, R., & Takriti, S. (2007). A logistic regression framework for information technology outsourcing lifecycle management. *Computers and Operations Research, 34*(12), 3609-3627.

Morris, J. J. (2011). The impact of enterprise resource planning (ERP) systems on the effectiveness of internal controls over financial reporting. *Journal of Information Systems, 25*(1), 129-157.

National Council of ISACs. (n.d.). *About us*. Retrieved from http://www.isaccouncil.net/aboutus.html

Novshek, W., & Sonnenschein, H. (1982). Fulfilled expectations Cournot duopoly with information acquisition and release. *The Bell Journal of Economics, 13*(1), 214-218.

Pfleeger, C. P., & Pfleeger, S. L. (2010). *Security in computing* (4th ed.). Westford, MA: Prentice Hall.

PiperJaffray. (2015). *CIO survey.* Retrieved from https://piper2.bluematrix.com/sellside/EmailDocViewer?encrypt=7856c68e-3f1a-4ce9-a7e7-99fe25145cd9&mime=pdf&co=Piper&id=jyarow@businessinsider.com&source=mail

Ponemon Institute. (2011). *2010 annual study: US cost of data breach*. Retrieved from http://www.symantec.com/content/en/us/about/media/pdfs/symantec_ponemon_data_breach_costs_report.pdf?om_ext_cid=biz_socmed_twitter_facebook_marketwire_linkedin_2011Mar_worldwide_costofdatabreach

Ponemon Institute. (2013a). *2013 cost of data breach: Global analysis.* Retrieved from http://www.ponemon.org/library/2013-cost-of-data-breach-global-analysis

Ponemon Institute. (2013b). *2013 cost of cyber crime study: United states*. Retrieved from http://www.hpenterprisesecurity.com/ponemon-2013-cost-of-cyber-crime-study-reports

Ponemon Institute. (2014). *2013 cost of data breach: Global analysis.* Retrieved from http://www.ponemon.org/blog/ponemon-institute-releases-2014-cost-of-data-breach-global-analysis

Ponemon. (2010). *2009 annual study: US cost of data breach*. Retrieved from http://www.ponemon.org/local/upload/fckjail/generalcontent/18/file/US_Ponemon_CODB_09_012209_sec.pdf

Ponssard, J. (1979). The strategic role of information on the demand function in an oligopolistic market. *Management Science, 25*(3), 243-250.

Powell, W. W., Koput, K. W., & Smith-Doerr, LI. (1996). Interorganizational collaboration and the locus of innovation: Networks of learning in biotechnology. *Administrative Science Quarterly, 41*(1), 116-145.

Raith, M. (1996). A general model of information sharing in oligopoly. *Journal of Economic Theory, 71*(1), 260-288.

Ravinchandran, T., & Lertwongsatien, C.. (2005). Effect of information systems resources and capabilities on firm performance: A resource-based perspective. *Journal of Management Information Systems, 21*(4), 237-276.

Roberts, P. (2003). Security company breaks with CERT over disclosure. *Computerworld.* Retrieved from http://www.computerworld.com.au/article/63089/security_company_breaks_cert_over_disclosure/

Sakai, Y., & Yamato, T. (1989). Information sharing and welfare. *Journal of Economics, Zeitenschrift fur Nationaloknonomie, 49*, 3-24.

Santhanam, R., & Hartono, E. (2003). Issues iin linking information technology capability to firm performance. *MIS Quarterly, 27*(1), 125-165.

Schechter, S., & Smith, M. (2003). *How much security is enough to stop a thief?* Paper presented at the Financial Cryptography Conference Le Gosier, Guadeloupe.

Schenk, M., & Schenk, M. (2002). Defining the value of strategic security. *Secure Business Quarterly, 1*(1), 1-6.

Schumaker, R. P., & Chen, H. (2010). A discrete stock price prediction engine based on financial news. *Computer, 43*(1), 51-56.

Shan, W., & Walker, G. (1994). Interfirm cooperation and startup innovation in the biotechnology industry. *Strategic Management Journal, 15*(5), 387-394.

Shapiro, C. (1986). Exchange of cost information in oligopoly. *Review of Economic Studies, 53*(174), 433-446.

Shu, H. (2010). Competing through services: Service migration of information technology product vendors. In *Proceedings of the Hawaii International Conference on System Sciences*.

Sidel, R. (2012). Card processor: Hackers stole account numbers. *The Wall Street Journal.* Retrieved from http://online.wsj.com/article/SB10001424052702304750404577318083097652936.html

Teece, D. J. (1987). Profiting from technological innovation: Implications for integration, collaboration, licensing and public policy. In D. J. Teece (Ed.), *The competitive challenge: Strategies for industrial innovation and renewal*. Cambridge, MA: Ballinger.

Tsai, W. (2002). Social structure of "coopetition" within a multiunit organization: Coordination, competition, and intraorganizational knowledge sharing. *Organization Science, 13*(2), 179-190.

Tsang, E. W. K., & Kai-Man, K. (1999). Replication and theory development in organizational science: A critical realist perspective. *Academy of Management Review, 24*(4), 759-780.

U.S. Department of Commerce. (2001). *Commerce Secretary Mineta Announces New Information Technology (IT) Information Sharing and Analysis Center (ISAC).* Retrieved from https://www.ntia.doc.gov/legacy/ntiahome/press/2001/itsac011601.htm

Vives, X. (1984). Duopoly information equilibrium: Cournot and bertrand. *Journal of Economic Theory, 34*(1), 71-94.

Vives, X. (1989). Technological competition, uncertainty, and oligopoly. *Journal of Economic Theory, 48*(2), 386-415.

Vives, X. (1990). Trade association disclosure rules, incentives to share information, and welfare. *RAND Journal of Economics, 21*(3), 409-430.

Wang, T. , Rees, J., & Kannan, K. (2007). *Reading the disclosures with new eyes: Bridging the gap between information security disclosures and incidents*. Retrieved from http://www.krannert.purdue.edu/academics/mis/workshop/wr_113007.pdf

Weiner, C. (2005). *The impact of industry classification schemes on financial research* (SFB 649 Discussion Paper 2005-062). School of Business and Economics, Humbroldt-Universitat zu Berlin.

Wilshusen, G. C. (2012). Threats impacting the nation. *United States Government Accountability Office*. Retrieved from http://www.gao.gov/assets/600/590367.pdf

Appendix A: ISACs

Table A1. ISACs by Sector

Sector	ISAC	Established	Administration
Banking and Finance	Financial Services	October 1999	FS-ISAC
Chemical and Hazardous Materials	Chemical[17]	April 2002	CHEMTREC
Emergency Services	Emergency Fire	October 2000	FEMA
Energy	Electric	October 2000	ES-ISAC
	Energy[24]	November 2001	
	Nuclear	1994	Nuclear Energy Institute (NEI)
Food	Food[18]	February 2002	Discontinued
Government	Multi-State	January 2001	MS-ISAC
Information Technology & Telecommunications	IT	December 2000	IT-ISAC
	Telecom/Communications	January 2000	NCC
	Research & Education Network	February 2003	REN-ISAC
Transportation	Public Transit	January 2003	American Public Transportation Association
	Surface Transportation	May 2002	ST-ISAC
	Highway[24]	March 2003	American Trucking Associations (ATA)
	Maritime	1988	Maritime Security Council
Drinking Water & Water Treatment Systems	Water	December 2002	WaterISAC
Health and Public Health	Healthcare	2010	NH-ISAC
Other	Real Estate	April 2003	RE-ISAC
	Supply Chain	June 2006	SC-ISAC

Sources: GAO (2004b) and http://www.isaccouncil.org/memberisacs.html

[17] Not a member of the Council of ISACs but has been recognized as the ISAC in GAO documents.
[18] Discontinued due to lack of activity.

Table A2. Current IT-ISAC Members

Foundation members	Silver members	Bronze members	Foundation members
BAE Systems	Afilias USA, Inc.	AT&T	BAE Systems
Cargill	Cisco Systems	Commvault	Cargill
eBay	CSC	Box.com	eBay
HP	Juniper Networks	EMC Corporation	HP
Intel Corporation	Neustar	Acquia	Intel Corporation
Oracle Corporation	Symantec Corporation	IBM	Oracle Corporation
	Fire Eye	BrandProtect, Inc.	
	Monsanto	Bricata	MS-ISAC
	Trend Micro, US	Lockheed Martin Corporation	IT-ISAC
	Netflix	Microsoft, Inc.	NCC
		Mischel Kwon and Associates	REN-ISAC
		Prescient Solutions	American Public Transportation Association
		Sony Corporation of America	ST-ISAC

Source: http://www.it-isac.org/#!members/c1tsl

About the Authors

Radha Appan is an Associate Professor of Information Systems at Cleveland State University. She received her PhD in information systems from Texas Tech University. Her research interests include information requirements determination, systems analysis and design, online auction markets, human decision making, and e-commerce related trust issues. She has taught courses such as IT for managers, knowledge management, database management, systems analysis and production and operations management. She has papers published in refereed journals such as *MIS Quarterly*, *Journal of the Association of Information Systems*, *Decision Support Systems*, and *Information and Management*. She has also published her work in several conferences.

Dinko Bačić is an Assistant Professor in the Department of Management and Information Sciences at Romain College of Business at the University of Southern Indiana. He holds an MBA degree in Finance from Miami University (Ohio) and a DBA degree in Information Systems from the Cleveland State University. His research interests include the impact of IS on firm performance, information visualization, decision making, cognitive effort, eye-tracking, and BI (business intelligence). Dr. Bačić has over fifteen years of experience in BI, finance, and HR. He provides consulting services to firms in banking and clinical research industry.