Winter 12-11-2022

Cybersecurity risk of interfirm cooperation: Alliance or joint venture?

Hüseyin Tanriverdi
University of Texas at Austin

Ghiyoung Im
University of Louisville, ghiyoung.im@louisville.edu

Cybersecurity Risk of Interfirm Cooperation: Alliance or Joint Venture?

Hüseyin Tanriverdi
University of Texas at Austin
McCombs School of Business
Austin, TX 78712, USA

Ghiyoung Im[1]
University of Louisville
College of Business
Louisville, KY 40208, USA

ABSTRACT

Interfirm cooperation between two or more firms is undertaken to create value jointly. However, interfirm cooperation also entails risks. We focus on cybersecurity risks of interfirm cooperation. Two prominent governance modes for interfirm cooperation are: (i) non-equity alliances and (ii) equity alliances such as joint ventures (JVs). We explain why non-equity alliances are likely to increase cybersecurity risks of collaborators whereas JVs are likely to reduce them. We test these ideas in the context of hospital–physician group collaborations in the U.S. Hospital Industry during 2009-2017. The results indicate that hospitals using non-equity alliances for physician group collaborations are more likely to experience cybersecurity breaches. Hospitals that use JVs to govern physician group collaborations are less likely to experience cybersecurity breaches. We discuss the implications of these findings for IS research and practice.

Keywords: cybersecurity breaches, interfirm cooperation, alliance, joint venture

[1] Corresponding author. ghiyoung.im@louisville.edu +1-770-286-3301

INTRODUCTION

Firms enter into interfirm collaborations to gain access to complementary resources and jointly create value. There are challenges in governing such cooperation (Das and Teng 2016). For instance, cybersecurity risks increase when collaborators open up their resources for each other's use: e.g., IT, business processes, sensitive data, etc. Firms have to govern and control not only their own technologies, processes, and data, but also those of the collaborators that are involved in the interfaces of the interfirm cooperation. Collaborators face dilemmas in how much to trust each other and share confidential data to achieve the goals of the cooperation (Ghondaghsaz et al. 2022). They also face tensions in how much to protect their confidential data and restrict sharing so that the firm's intellectual property does not leak to the collaborators (Jarvenpaa and Majchrzak 2016).

Generally, cybersecurity risks of IT-enabled inter-organizational relationships are well recognized in operations, supply chains (Bandyopadhyay et al. 2010; Massimino et al. 2018; Shafiu et al. 2016) and outsourcing relationships (Bhatti et al. 2021). In the market-hierarchy continuum of governance modes, such relationships are closer to the market mode of governance. Relatively well-understood and standardized operational, supply chain, and outsourcing services can be managed with transactional purchasing contracts in the market. In comparison, strategic interfirm cooperation formed to address poorly understood problems and opportunities do not lend themselves well to transactions in the market. Collaborators often seek to use intermediate or hybrid governance modes, such as strategic alliances, in between the market and hierarchy modes of governance. Those are relational governance modes under which the collaborators seek to bring their complementary resources to bear in addressing the poorly understood problems and opportunities. Cybersecurity risks posed by such relational governance modes have received little or no attention. This study begins to address this gap by studying how different relational governance modes affect cybersecurity risks of cooperating firms.

Two prominent relational governance modes used in strategic interfirm cooperation are: (i) non-equity alliances and (ii) joint ventures (JVs) which require equity investments. We hypothesize non-equity alliances present much higher cybersecurity risks than the JVs. Our empirical context is the hospital–physician group affiliations in the U.S hospital industry during 2009-2017. Physicians are strategic resources of hospitals. Some hospitals use a staff model to employ and internalize the governance of physicians (i.e., the hierarchy mode of governance). Other hospitals enter into either non-equity alliances with physician groups or they set up JVs to which both the hospital and the physician groups put equity (Casalino and Robinson 2003). We find that hospitals that choose non-equity alliance for governing physician group cooperation are significantly more likely to experience cybersecurity breaches. In contrast, hospitals that use JV to govern physician group cooperation are significantly less likely to experience cybersecurity breaches.

BACKGROUND

Strategic alliances are cooperative arrangements aimed at achieving strategic objectives of two or more firms by combining the firms' complementary resources in the course of jointly developing and offering products, services, and technologies (Das 2019; Gulati 1998). They can be grouped into: (i) non-equity alliances and (ii) and joint ventures which require equity investments (Das and Teng 2016). In a non-equity alliance, collaborators manage the cooperation directly through contracts and relational governance without making equity investments or creating an independent firm (Barney 2014). In a joint venture, collaborators create a legally independent firm in which they invest equity. Profits generated by the JV compensate the collaborators for their investments (Barney 2014).

Non-equity alliance has higher cybersecurity risks as it requires the establishment of organic, fluid IT connections between the collaborators whose access to each other's IT systems and sensitive data can change dynamically over time. The non-equity alliance extends the boundaries of the collaborators' respective enterprise IT environments, and subjects the firms to larger cybersecurity attack surfaces (Theisen et al. 2018). This can enable external attackers to target weak links in any of the collaborators and exploit them to gain access to sensitive assets of the other collaborators as well. Internally, threats can also come from the collaborators as they may have incentives to expropriate each other's sensitive data and intellectual property (Jarvenpaa and Majchrzak 2016).

In comparison, JV is a legally independent firm. It clearly separates the boundaries of the JV and the collaborators. Thus, the attack surfaces of the collaborators stay the same relative to their pre-JV attack surfaces. The JV can even shrink the attack surfaces of the collaborators somewhat if they contribute some sensitive data and intellectual property to the JV in addition to equity. Thus, external hackers would target the JV rather than the collaborators for such sensitive data, which can reduce the attack surface and cybersecurity risks of the collaborators. Economically, JV aligns the incentives of collaborators better. As equity holders in the JV, collaborators have incentives to behave in ways to increase returns and reduce risks of the JV including cybersecurity risks.

HYPOTHESES

Non-equity alliance and cybersecurity breaches

Non-equity alliances extend the boundaries of collaborators' enterprise IT environments (Park et al. 2017). An alliance adds a new external IT node and a new IT connection to a collaborator's enterprise IT environment (Karlsson et al. 2016). Cybersecurity becomes a function of not just the collaborator's own IT environment but also the collaborators' IT environments (Park et al. 2017). If external attackers can breach one of the collaborators' weak links, they can laterally move to the interfirm IT interfaces to gain access to the other collaborators' IT environments and sensitive data as well (Karlsson et al. 2016). Thus, an alliance can increase collaborators' cybersecurity breach risks. Mitigating the risks would require the institution of new IT security controls at the interfirm interface points with the collaborators (Park et al. 2017; Ponemon 2016; Star 2016). However, when multiple stakeholders from different firms need to agree on the IT controls of the alliance, the likelihood of successfully designing and operating the IT controls is low (Tanriverdi and Du 2020).

There are often incompatibilities in the collaborators' control objectives (Jarvenpaa and Majchrzak 2016). Some collaborators might prioritize the sharing of sensitive data to foster cooperation and achieve the goals of the alliance. Others might prioritize the protection of their own sensitive data and restrict access to the data in order to reduce the leakage of the sensitive data to collaborators. Moreover, such priorities of the collaborators can change over time. Under such circumstances, cooperation among the collaborations cannot be taken for granted (Das and Teng 2016). Establishing and effectively operating joint governance and controls over the shared resources of the alliance becomes highly important but also highly challenging (Tanriverdi and Du 2020). Despite heavy dependence on third-party collaborators, however, many firms do not have centralized control over third-party risk management (Park et al. 2017). They may not be able to sense and respond to the dynamically evolving security control needs of the alliance. In summary, the increased risks and the weakened controls lead us to expect the non-equity alliance to increase the cooperating firms' likelihood of experiencing cybersecurity breaches.

> **H1**: Using a non-equity alliance to govern interfirm cooperation is likely to increase a firm's cybersecurity breaches.

Joint venture and cybersecurity breaches

As a distinct legal entity, JV does not have to have organic IT ties to the collaborators. The collaborators do not interconnect and open up their internal resources for each other's use. Thus, each collaborator manages its own set of information technologies, business processes, and sensitive data. There is no integration. Instead, collaborators invest equity in the JV. The JV has its own set of technologies, business processes, and sensitive data. If JV is formed for R&D purposes, collaborators can provide some sensitive knowledge to the JV in addition to equity. However, the JV would be responsible for securing such sensitive assets. If hackers are interested in stealing the intellectual property, they would have to target the JV to gain access to it. There is a clear, legally separated boundary between the JV and the collaborators. This separation allows the collaborators to isolate their respective cybersecurity risks rather than developing dependencies and becoming subject to correlated cybersecurity risks. Thus, JV is likely to reduce collaborating firm's cybersecurity breach in an interfirm cooperation. In summary, the improvements in economic incentive alignment and the reduction in operational risk management challenges lead us to expect the joint ventures to reduce the cooperating firms' likelihood of experiencing cybersecurity breaches.

> **H2**: Using an equity-based joint venture to govern interfirm cooperation is likely to reduce a firm's cybersecurity breaches.

METHODS

We choose the hospital–physician cooperation in the U.S hospital industry as the empirical context for testing our hypotheses. Hospitals have several motivations to cooperate with physician groups: e.g., coordinate care services for patients, gain leverage with health plans, bring in more patient referrals to the hospital, and share the costs and benefits of providing care services to patients (Casalino and Robinson 2003). Physician groups also share some of these motivations. In addition, physician groups seek to gain access to advanced technologies, facilities, and expertise of hospitals. As the healthcare industry has gone through various eras of regulation, and innovations in technology and business models, the industry has tried various governance modes for governing hospital-physician group cooperation (Casalino and Robinson 2003). Among the various governance modes used for hospital-physician group cooperation, we focus on non-equity alliance and equity-based joint venture. In non-equity cooperation, for instance, a physician group consistently refers a specific type of patient to a specific specialty hospital for further treatment and care (McConnell 2020). In joint venture, hospital and physician group creates a new organizational entity such as an integrated delivery system (IDS) of physicians and hospitals. Each collaborator has ownership stake in IDS and it provides specific services to support the IDS (McConnell 2020). Hospitals exhibit variance in their choice of non-equity alliance versus joint ventures for physician cooperation. This variance creates an opportunity for us to test our hypotheses.

Sample and Data Collection

We construct our sample by merging data from four data sources. The primary data source is a database of annual surveys of hospitals in U.S. The American Hospital Association (AHA) conducts yearly surveys of all hospitals registered in the United States to examine the industry with respect to governance, facilities and services, and staffing. We also include data from the

AHA's Annual Information Technology Supplement Survey, which collects information about the characteristics of IT applications and information sharing practices of hospitals. To obtain additional information about the characteristics of IT applications of hospitals, we also use data from the Healthcare Information and Management Systems Society (HIMSS) Analytics Database. Finally, we collect data on data breaches of hospitals from two sources: (i) the U.S. Department of Health and Human Services (HHS) which publishes data breaches reported by healthcare organizations; and (ii) the Privacy Rights Clearinghouse (PRC), a website which tracks publicly announced data breaches. We cross-validate the hospital data breaches by checking both HHS and PRC datasets. After merging the four datasets and losing some observations due to missing data in each data sources, the final, effective sample retained for data analysis contains a total of 19,648 observations from 4,256 hospitals during 2009-2017.

Measures

Dependent variable

Our dependent variable is a data *breach* in a hospital. It is defined as the leakage of hospital's sensitive patient data to unauthorized parties in a given year (Verizon 2019).

Independent variables

Non-equity alliance. The AHA survey lists eight different types of hospital-physician arrangements, which range from an arm's-length relationship to an integrated organizational form (Kapoor and Lee 2013). We identify four of these arrangements as non-equity alliances. In the first one, a hospital cooperates with an Independent Practice Association (IPA), which is a legal entity that helps physicians obtain managed care contracts. In the second one, a hospital cooperates with a Group Practice without Walls (GPW), an entity which helps physicians form a quasi-group for sharing administrative expenses. In IPA and GPW, physicians receive management services from hospitals and remain independent. In the third one, a hospital cooperates with a Closed Physician-hospital Organization (CPHO), an entity in which qualified physicians can make exclusive contracts to the hospitals to coordinate patient care. The scope of CPHO is broader than the previous two. In the fourth one, a hospital cooperate with a Foundation, which purchases assets for medical practice on behalf of physicians. Physicians remain independent and make a service contract with the foundation. We use the four arrangements to compute the total number of hospital-physician non-equity alliances (*Physician alliance*) a hospital maintained in a given year.

Joint venture is measured with an AHA survey item capturing whether a hospital participated in an equity-based joint venture with physicians or physician groups in a given year [1], or not [0]. In the hospital industry, examples of joint ventures include limited service hospital (for cardiac, orthopedic, surgical), ambulatory surgical centers, and imaging centers. Ambulatory surgical centers are one of the most popular areas of joint venture activities between hospitals and physicians. These centers are formed when hospitals and physicians agree on creating unincorporated businesses (Zasa 2011). Also, hospitals with surgical centers may invite physicians to join them as partners and vice versa. Unlike in the non-equity alliance arrangements, the AHA survey does not inquire about the further details of joint ventures such as the percentage of equity owned or how many different JVs a hospital maintained in a given year. Thus, we are able to measure only if a hospital used the JV mode of governance in a given year or not.

Controls

To rule out alternative explanations to our findings and address potential endogeneity concerns, we include several controls on hospital characteristics that might influence hospital's data breaches. *Network participation* is an indicator that capture whether a hospital is a participant in a network. *Core-based statistical area (CBSA) type* captures whether the hospital is located in a metro, micro, or rural area according to the definition of the Office of Management and Budget. *Facility* is the number of facilities and services that the hospital or its subsidiaries owns and provides. *Hospital revenue* is included as a measure of hospital's size.

Table 1. Summary of Archival Data Sources

Data Source	Variables		Measure
	Name	Type	
PRC & HHS	Breach	DV	If hospital had a breach [1] or not [0] in a year.
AHA	Physician alliance	IV	The total number of non-equity physician alliances of hospital in a year (IPA, GPW, CPHO, and Foundation).
	Joint venture	IV	If hospital used a JV in a given year [1] or not [0].
	Network participation	Control	If hospital was part of a network in a year [1] or not [0].
	CBSA type	Control	Dummy variables capturing if a hospital was located in a metro, micro, or rural area.
	Facility	Control	The number of the facilities and services of a hospital or its subsidiaries in a year.
	Hospital revenue	Control	Annual revenue of hospital.
	Accredited	Control	Accredited for graduate medical education [1] or not [0].
	Teaching	Control	Member of teaching hospital association [1] or not [0].
	Non-government	Control	Had for-profit status [1] or not [0].
AHA IT	HIE	Control	Participated in a HIE or RHIO [1], or not [0].
	Information sharing	Control	Number of different types of patient data electronically exchanged with other hospitals.
HIMSS	Electronic medical record (EMR)	Control	Number of EMR applications.
	Security	Control	Number of IT security applications.
	Decision support system (DSS)	Control	Number of DSS applications.

We also included controls for whether a hospital is *accredited* (accreditation for graduate medical education), whether it is a *teaching* hospital (member of teaching hospital association), and whether it is a *non-government,* for-profit hospital or not. We also control for *information sharing* pattern of a hospital by controlling for the count of different types of patient data the hospital electronic exchanges with other hospitals. The AHA surveys asks about whether a hospital electronically exchanges patient demographics, laboratory results, medication history, radiology reports, and clinical/summary care record with other hospitals. In addition, we include controls for *Health information exchange* (HIE), i.e., a hospital's participation in at least one HIE or a regional health information organization (RHIO). Finally, we include controls for *Electronic medical record* (EMR), *security*, and *decision support system* (DSS) usage of a hospital by controlling the number of IT applications in each of those categories. Table 1 summarizes the data sources, variables, and measures of the study.

DATA ANALYSIS AND RESULTS

Descriptive Statistics and Correlations

The descriptive statistics and correlations are presented in Table 2. Table 2 is constructed based on the effective sample that is used in data analysis. Security breach is observed 346 times in the sample of 19,648 observations. The total number of physician alliances is 3,929 cases over nine years while joint venture participation is observed 6583 times.

Table 2. Descriptive Statistics and Correlations

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
1. Breach	1.00														
2. Alliance	0.05	1.00													
3. JV	0.03	0.13	1.00												
4. Info share	0.03	0.03	0.11	1.00											
5. Facility	0.16	0.14	0.38	0.26	1.00										
6. Non-gov	0.01	0.02	0.18	0.17	0.19	1.00									
7. CBSA	-0.08	-0.10	-0.30	-0.20	-0.50	-0.29	1.00								
8. Accredited	0.12	0.10	0.22	0.23	0.57	0.14	-0.41	1.00							
9. Teaching	0.18	0.13	0.11	0.12	0.52	0.00	-0.23	0.45	1.00						
10. Revenue	0.10	0.11	0.32	0.18	0.60	0.22	-0.50	0.39	0.31	1.00					
11. Network	0.02	0.04	0.08	0.15	0.14	0.10	-0.04	0.09	0.08	0.07	1.00				
12. HIE	0.02	0.01	0.08	0.43	0.17	0.12	-0.12	0.15	0.07	0.13	0.11	1.00			
13. EMR	0.05	0.00	0.18	0.46	0.35	0.18	-0.27	0.25	0.13	0.27	0.13	0.38	1.00		
14. Security	0.05	0.00	0.13	0.21	0.27	0.15	-0.21	0.15	0.12	0.20	0.10	0.15	0.43	1.00	
15. DSS	0.06	0.00	0.20	0.31	0.38	0.23	-0.35	0.24	0.16	0.38	0.09	0.23	0.52	0.41	1.00
Mean	0.02	0.20	0.33	5.10	59.63	1.78	1.59	0.30	0.09	16.51	0.43	0.46	7.05	4.25	4.56
S.D.	0.13	0.47	0.47	3.78	26.13	0.41	0.81	0.46	0.29	2.65	0.49	0.50	2.48	2.74	2.17

N=19,648; The correlation above 0.002 is significant at $p < .05$.

Analysis

The dataset was constructed after consolidating the data from four different data sources. Each data source carried missing values and hence the consolidated data ended up having more missing values than each individual data source. We used Stata for data analysis and the statistical package uses listwise deletion to handle missing values, leaving 19,648 observations as the effective sample size for data analyses.

In our panel data, the dependent variable is a binary indicator about the occurrence of security breaches in a given year. Therefore, we selected the logit panel data model. We tested a random-effects model to fit to the data. We conducted a likelihood-ratio test of $\rho=0$ to examine the hypothesis that the variance of the time-invariant component of the error is zero (i.e., $\sigma^2_u=0$). The null hypothesis is rejected at $p < .05$. This means that the panel model needs to take characteristics of entities into account and the random-effects model is better than the pooled regression model. Model 1 in Table 3 shows the result of the random-effects logistic regression.

Selection bias

Endogeneity is a serious concern in non-experimental research. In our model, it is likely that a hospital's decision to use a non-equity alliance or a JV may be endogenously determined. We used the Heckman model (Heckman 1979) test for endogenous sample selection. We followed the procedure suggested by Hsieh (2011). First, we tested for the selection equation with the probit panel data model after setting each of the indicator variables for physician alliances and joint ventures as the dependent variable. In constructing the selection equations, we included additional covariates (e.g., governance structure) as controls. After running each of the selection equations, we manually calculated the lambda (the coefficient of inverse Mills ratio). Second, we added the lambda from the selection equation to the regression equation as an additional explanatory variable. Models 2 and 3 in Table 3 shows the results of the two-step Heckman model. The testing of the lambda coefficients indicates that each of the coefficients is not significantly different from zero. Therefore, we conclude that selection bias is not a serious concern in our panel data model.

Table 3. Results of Random-effects Logistic Regression

DV	**Breach**	**Breach**	**Breach**
	Model 1	Model 2	Model 3
Governance mode			
Alliance	0.2154*	0.2879*	0.2923*
	(0.0991)	(0.1215)	(0.1210)
Joint venture	-0.2640*	-0.3843*	-0.4162**
	(0.1243)	(0.1571)	(0.1559)
Controls			
Information sharing	-0.0472*	-0.0373	-0.0360
	(0.0189)	(0.0253)	(0.0253)
Facility	0.0269**	0.0353**	0.0259**
	(0.0038)	(0.0081)	(0.0088)
Non-government	0.0573	-0.4105^{+}	-0.3552
	(0.1638)	(0.2328)	(0.2422)
CBSA type 1	0.7836*	0.8325	0.5063
	(0.3789)	(0.5382)	(0.6351)
CBSA type 2	0.5257	-0.1754	-0.1721
	(0.4039)	(0.5870)	(0.6754)
Accredited	0.4009*	0.3314^{+}	0.3323^{+}
	(0.1630)	(0.2003)	(0.2010)
Teaching	0.7873**	0.7279**	0.7520**
	(0.1686)	(0.2080)	(0.2131)
Revenue	0.0538	0.0521	0.0589
	(0.0385)	(0.0464)	(0.0475)
Network	-0.1360	-0.1457	-0.2014
	(0.1207)	(0.1550)	(0.1513)
HIE	0.0270	0.0420	0.0495
	(0.1316)	(0.1630)	(0.1628)
EMR	0.0084	0.0269	0.0257
	(0.0426)	(0.0548)	(0.0548)
Security	0.0025	0.0146	0.0124
	(0.0253)	(0.0316)	(0.0314)
DSS	0.0233	-0.0083	-0.0055
	(0.0370)	(0.0483)	(0.0484)
Year dummies	Yes, sig.	Yes, sig.	Yes, sig.
(constant)	-8.9039**	-11.3244**	-8.1490**
	(0.6862)	(2.5691)	(1.8507)
Lambda1		0.6745	
		(0.5752)	
Lambda1			-0.0531
			(0.2448)
N	19,648	11,568	11,568

Standard errors in parentheses. $^{+}$ $p < 0.10$, * $p < 0.05$, ** $p < 0.01$

Results

Table 3 presents the results of random-effects logistic regression. Alliance has a positive and significant effect on data breach (β = 0.2154, p<0.05). Thus, H1 is supported. Joint venture has a negative and significant effect on data breach (β = -0.2640, p<0.05). Thus, H2 is also supported.

DISCUSSIONS AND CONCLUSION

This study generates new knowledge on cybersecurity implications of interfirm cooperation.

Contributions to research

A taken-for-granted assumption in information security literature has been that third-party relationships present additional cybersecurity risks for firms (Bhatti et al. 2021; Ghondaghsaz et al. 2022; Karlsson et al. 2016). However, this assumption has not been validated with empirical studies on the plethora of third-party relationships being used in practice. To our knowledge, this is the first empirical study on cybersecurity implications of strategic interfirm cooperation. Our findings present a more nuanced view of the cybersecurity implications of strategic interfirm cooperation than currently assumed. Specifically, in the context of strategic cooperation with third parties, joint venture mode of governance reduces cybersecurity risks significantly. This finding requires a modification in our taken-for-granted assumptions about the cybersecurity risks of third-party relationships. Specifically, some third-party relationships such as joint ventures might reduce the cybersecurity risks of collaborators. Other types of third-party relationships, such as non-equity alliances, might increase the cybersecurity risks of collaborators significantly as we find in this study. Together, these findings highlight the importance of theorizing and testing the cybersecurity implications of each of the many different governance modes being used in practice for third-party relationships.

Contributions to practice

Despite decades of experience with different governance modes for hospital-physician group cooperation, hospitals still struggle to decide which governance mode might be appropriate for a given physician group (Casalino and Robinson 2003; McConnell 2020). Although our study does not directly study this question, our theory and findings inform executives that the cybersecurity risk governance abilities of non-equity alliances and JVs are different. If cooperation with a physician group entails high cybersecurity risks around shared resources such as patient data, hospital-specific devices, procedures, technologies, and medical expertise, the JV mode of governance can significantly reduce the cybersecurity risks of sharing such resources with physician groups. Using non-equity alliance would make it highly challenging to secure those resources and increase the likelihood of cybersecurity breaches.

Boundary Conditions, Limitations, and Future Work

A boundary condition and limitation of the proposed theory is that we only focused on strategic interfirm cooperation. Whether the theory and findings would generalize to operational, transactional interfirm cooperation in manufacturing, supply chains, and outsourcing contracts should be tested in future research. A second boundary condition and limitation of our theory is that we studied alliances and JV at an aggregated level, at the hospital level of analysis. We did not have access to finer-grained data on the specifics of each alliance or JV. Future research can collect data at the level of each interfirm cooperation to test how the characteristics of each cooperation affect the cybersecurity risks. Finally, we tested our theory in one industry. Further research is required to test if the theory and findings of this study would generalize to other industries.

REFERENCES

Bandyopadhyay, T., Jacob, V., and Raghunathan, S. 2010. "Information Security in Networked Supply Chains: Impact of Network Vulnerability and Supply Chain Integration on Incentives to Invest," *Information Technology & Management* (11:1), pp. 7-23.

Barney, J. B. 2014. "Gaining and Sustaining Competitive Advantage."

Bhatti, B. M., Mubarak, S., and Nagalingam, S. 2021. "Information Security Risk Management in IT Outsourcing - a Quarter-Century Systematic Literature Review," *Journal of Global Information Technology Management* (24:4), pp. 259-298.

Casalino, L., and Robinson, J. C. 2003. "Alternative Models of Hospital-Physician Affiliation as the United States Moves Away from Tight Managed Care," *Milbank Quarterly* (81:2), pp. 331-+.

Das, T. K. 2019. *Managing Interpartner Risks in Strategic Alliances*.

Das, T. K., and Teng, B. S. 2016. *Risk Types and Interfirm Alliance Structures*. Charlotte: Information Age Publishing-Iap.

Ghondaghsaz, N., Chokparova, Z., Engesser, S., and Urbas, L. 2022. "Managing the Tension between Trust and Confidentiality in Mobile Supply Chains," *Sustainability* (14:4), p. 25.

Gulati, R. 1998. "Alliances and Networks," *Strategic Management Journal* (19:4), pp. 293-317.

Heckman, J. J. 1979. "Sample Selection Bias as a Specification Error," *Econometrica: Journal of the econometric society*), pp. 153-161.

Hsieh, J. P.-A., Rai, A., and Xu, S. X. 2011. "Extracting Business Value from IT: A Sensemaking Perspective of Post-Adoptive Use," *Management science* (57:11), pp. 2018-2039.

Jarvenpaa, S. L., and Majchrzak, A. 2016. "Interactive Self-Regulatory Theory for Sharing and Protecting in Interorganizational Collaborations," *Academy of Management Review* (41:1), pp. 9-27.

Kapoor, R., and Lee, J. M. 2013. "Coordinating and Competing in Ecosystems: How Organizational Forms Shape New Technology Investments," *Strategic management journal* (34:3), pp. 274-296.

Karlsson, F., Kolkowska, E., and Prenkert, F. 2016. "Inter-Organisational Information Security: A Systematic Literature Review," *Information and Computer Security* (24:5), pp. 418-451.

Massimino, B., Gray, J. V., and Lan, Y. C. 2018. "On the Inattention to Digital Confidentiality in Operations and Supply Chain Research," *Production and Operations Management* (27:8), pp. 1492-1515.

McConnell, C. R. 2020. *Hospitals and Health Systems: What They and How They Work*. Burlington, MA: Jones & Bartlett Learning.

Park, K., Corstens, J., Griffiths, D., and Sen, S. 2017. "Overcoming the Threats and Uncertainty; Third-Party Governance and Risk Management; Extended Enterprise Risk Management Global Survey 2017," Deloitte Touche Tohmatsu Limited, London, United Kingdom.

Ponemon. 2016. "Data Risk in the Third-Party Ecosystem," Ponemon Institute LLC, Traverse City, Michigan.

Shafiu, I., Wang, W. Y. C., and Singh, H. 2016. "Information Security Compliance Behaviour of Supply Chain Stakeholders: Influences and Differences," *International Journal of Information Systems and Supply Chain Management* (9:1), pp. 1-16.

Star, J. R. 2016. *The Cybersecurity Due Diligence Handbook: A Plain English Guide for Corporations Contemplating Mergers, Acquisitions, Partnerships, Vendors or Other Strategic Alliances and Relationships*. Amazon Kindle: BookBaby.

Tanriverdi, H., and Du, K. 2020. "Corporate Strategy and Information Technology Control Effectiveness," *MIS Quarterly* (44:4).

Theisen, C., Munaiah, N., Al-Zyoud, M., Carver, J. C., Meneely, A., and Williams, L. 2018. "Attack Surface Definitions: A Systematic Literature Review," *Information and Software Technology* (104), pp. 94-103.

Verizon. 2019. "2019 Data Breach Investigations Report," Verizon Trademark Services LLC.

Zasa, R. J. 2011. "Physician-Hospital Joint Ventures." Retrieved May 2, 2022