The impact of information sharing legislation on cybersecurity industry

Agnes Yang
Carlson School of Management, University of Minnesota, Minneapolis, Minnesota, USA, and
Young Jin Kwon and Sang-Yong Tom Lee
School of Business, Hanyang University, Seoul, South Korea

Received 11 October 2019
Revised 11 February 2020
25 June 2020
23 July 2020
Accepted 2 August 2020

Abstract

Purpose – The objective of this paper is to investigate how firms react to cybersecurity information sharing environment where government organizations disseminate cybersecurity threat information gathered by individual firms to the private entities. The overall impact of information sharing on firms' cybersecurity investment decision has only been game-theoretically explored, not giving practical implication. The authors therefore leverage the Cybersecurity Information Sharing Act of 2015 (CISA) to observe firms' attitudinal changes toward investing in cybersecurity.

Design/methodology/approach – The authors design a quasi-experiment where they set US cybersecurity firms as an experimental group (a proxy for total investment in cybersecurity) and nonsecurity firms as a control group to measure the net effect of CISA on overall cybersecurity investment. To enhance the robustness of the authors' difference-in-difference estimation, the authors employed propensity score matched sample test and reduced sample test as well.

Findings – For the full sample, the authors' empirical findings suggest that US security firms' overall performance (i.e. Tobin's Q) improved following the legislation, which indicates that more investment in cybersecurity was followed by the formation of information sharing environment. Interestingly, big cybersecurity firms are beneficiaries of the CISA when the full samples are divided into small and large group. Both Tobin's Q and sales growth rate increased for big firms after CISA.

Research limitations/implications – The authors' findings shed more light on the research stream of cybersecurity and information sharing, a research area only explored by game-theoretical approaches. Given that the US government has tried to enforce cybersecurity defensive measures by building cooperative architecture such as CISA 2015, the policy implication of this study is far-reaching.

Originality/value – The authors' study contributes to the research on the economic benefits of sharing cybersecurity information by finding the missing link (i.e. empirical evidence) between "sharing" and "economic impact." This paper confirms that CISA affects the cybersecurity industry unevenly by firm size, a previously unidentified relationship.

Keywords Cybersecurity information sharing, Cybersecurity industry, Economic impact, Real option theory, Quasi-experiment, Difference-in-difference

Paper type Research paper

1. Introduction

The importance of protecting firm data has been emphasized ever than before. Many empirical studies have proven that security breaches cause enormous economic damages to firms, in terms of decreased market value of breached firms (Campbell *et al.*, 2003; Cavusoglu *et al.*, 2004; Acquisti *et al.*, 2006; Kannan *et al.*, 2007). On the contrary, a cybersecurity investment announcement by a firm increases its market value (Chai *et al.*, 2011). For example, the Marriot's recent cybersecurity incident [1] exposed 500m personal data, dealing a devastating blow to both the firm and its users, along with creating socially undesirable costs. It is often stated that

This work was supported by the Ministry of Education of the Republic of Korea and the National Research Foundation of Korea (NRF-2017S1A3A2066740)

Industrial Management & Data Systems

0263-5577
DOI 10.1108/IMDS-10-2019-0536

a breached firm usually experiences damaged reputation. In a nutshell, keeping an adequate security level is crucial for firms to protect both tangible and intangible assets.

While cybersecurity has traditionally been fortified at the firm level, there has been a change in recent years due to the active involvement of the US government. The Cybersecurity Information Sharing Act of 2015 (CISA), passed by the US Senate on October 27, 2015, was introduced for timely sharing of classified cyber threats indicators (CTIs) and defensive measures (DMs) with private entities, federal agencies (DHS, FBI, etc.) and Information Sharing and Analysis Center (ISAC) members. Section 103 [2] of the bill states that, "It requires the Director of National Intelligence (DNI) and the Departments of Homeland Security (DHS), Defense (DoD), and Justice (DoJ) to develop and promulgate procedures to promote the sharing of: (1) classified and declassified cyber threat indicators in possession of the federal government with private entities, nonfederal government agencies, or state, tribal, or local governments; (2) unclassified indicators with the public; (3) information with entities under cybersecurity threats to prevent or mitigate adverse effects; and (4) cybersecurity best practices with attention to the challenges faced by small businesses."

Despite the ardent support of the US government for sharing cybersecurity information, there is a debate on whether the legislation can be effectively implemented, as US firms are not forced to share cybersecurity information. Contrary to these concerns, the DHS reports that they have shared 210,087 unclassified CTIs with private sector partners and 33 federal entities since March 2016 and shared 2,290 classified CTIs, from October 2015 to April 2017. Private entities have shared 181,307 CTIs with the DHS since November 2016 (DHS 2017 [3]). A recent survey by Chief Information Security Officer (CISO) and cybersecurity officers reveals that large firms share information and are more engaged, whereas smaller firms tend not to share (Koepke, 2017).

The introduction of this law is a huge step forward for the whole industry and the cybersecurity industry in particular as it is the first strong step to combat cybersecurity threats – bringing them within an information sharing strategy – and is different from previous attempts to merely establish information sharing organizations (ISACs). The Obama administration stated on several occasions that it would encourage information sharing and reduce the antitrust scrutiny of sharing firms (e.g. Presidential Policy Directive 41 of 2016), which illustrates the government's keenness regarding the legislation.

Meanwhile, CISA is part of a larger bill – the Cybersecurity Act of 2015. Therefore, a question arises how only the impact of CISA can be measured, as other parts of the bill can interfere with the measurement. Even though CISA does not affect all industries, it is of great interest to most private sector entities (Sullivan and Cromwell, 2015 [4]). For example, many of the provisions of the National Cybersecurity Protection Advancement Act of 2015 (NCPAA) aim to facilitate the implementation of the information sharing mechanism set forth in CISA (Sullivan and Cromwell, 2015). Hence, we argue that the impact of CISA on the cybersecurity industry is worth examining.

Many economists have examined the mechanisms of information sharing in nonsecurity areas (Fried, 1984; Shapiro, 1986; Kirby, 1988). However, there are no empirical studies that examine the impact of information sharing on the cybersecurity industry, especially in economic terms, except the ones on the consequences of breach information disclosure (Arora *et al.*, 2006; Wang *et al.*, 2013), software vulnerability announcements (Telang and Wattal, 2007; Arora *et al.*, 2010), strategic disclosure of incident information (Moore and Clayton, 2011; Gay, 2017).

In comparison, some researchers argue that cybersecurity information sharing increases social welfare (Gordon *et al.*, 2003b; Gal-Or and Ghose, 2005) and encourages firms to invest in cybersecurity-related activities. However, there is no empirical evidence to corroborate this stand. Therefore, we design a quasi-experiment and empirically investigate the impact of CISA implementation on the cybersecurity industry. We collected firm-level panel data of

US and global firms to conduct difference-in-difference (hereafter DID) and propensity score matching (PSM) analyses. Key implications of this study are as follows:

(1) To our understanding, this study is the first attempt to identify causal relationship between formation of cybersecurity information sharing environment and its subsequent impact on overall firm performance of cybersecurity industry. We tried to figure out this relationship by taking advantage of CISA as an exogenous shock to the industry.

(2) We bridge the gap between theory and practice in terms of how general firms would react to an environment where cybersecurity threat information is shared by each firm. Two pioneering papers, Gordon *et al.* (2003b) and Gal-Or and Ghose (2005), have solely approached this phenomenon by theories due to the absence of real-world event, such as CISA in our case.

(3) Multiple DID estimation analyses and accordingly robustness check by PSM analyses also reveal that, in general, firm performance of cybersecurity industry increased after CISA 2015 relative to the period before the initiation. Surprisingly, the impact is differential by firm size; we interpret this phenomenon as a result of CISA playing a role that contributes to make cybersecurity industry an oligopolistic market to a certain extent.

Further descriptions about the estimation results are elaborated on the Empirical Results and Robustness Check sections.

2. Theoretical background and literature review

2.1 Real options theory – investing firms' point of view

A real option is a type of right to adjust capital budgeting decisions, such as a project's size, timing, abandonment and so on (Myers, 1977; Black and Scholes, 1973). For example, a deferment option is the right to choose when to start a project. This option confers flexibility to the management to choose the investment timing until market conditions are favorable. The expected value of a real option to defer an investment rises as the uncertainty of the investment opportunity increases (McDonald and Siegel, 1986; Dixit and Pindyck, 1994).

Gordon *et al.* (2003a) took the real option approach to explain cybersecurity investment decisions. To the best of our knowledge, they were the first researchers to explicitly apply real options theory to cybersecurity investment. Many other studies that took real option approach on cybersecurity were followed (Benaroch, 2018; Demetz and Bechlechner, 2013; Herath and Herath, 2008; Tatsumi and Goto, 2010). Firms are unsure of the adequate amount of investment in cybersecurity, as the return on security investment (ROSI) is difficult to estimate (Cavusoglu *et al.*, 2008). In other words, the uncertainty of the investment decision plays a part in increasing the value of the option to delay investments in cybersecurity (Gordon *et al.*, 2003a).

Later, Gordon *et al.* (2015) re-examined their earlier analysis (Gordon *et al.*, 2003) to shed light on the efficacy of information sharing organizations (ISACs). They find that information sharing among firms decreases the uncertainty over cybersecurity investment decisions and thereby reduces the value of the real option to defer the investments, which encourages firms to invest in overall cybersecurity sooner. The ability to measure the expected value of the shared information could be an incentive for firms to share their information in exchange for information received from other firms. They can invest more cost-effectively with accurate information from information sharing organizations by reducing the uncertainty over cybersecurity investment decisions, leading to enhanced social welfare.

2.2 Externality and demand spillover effect – cybersecurity vendors' point of view

A positive externality refers to the benefit given to a third party that did not make the decision (Buchanan and Stubblebine, 1962). According to Gal-Or and Ghose (2005), firms' cybersecurity information sharing behavior leads to an increased demand for cybersecurity products, as their behavior convinces consumers that there is an increased utility in using cybersecurity products. Thus, cybersecurity information sharing can cause a demand-side spillover effect, leading to positive externalities for the cybersecurity industry. Moreover, the researchers argue that a higher demand-side spillover effect promotes both information sharing and technology investment. This increased spillover effect shifts the demand curve outward, enabling cybersecurity vendors to increase their product prices and, ultimately, profits.

2.3 Prior studies on cybersecurity information sharing

In a broad sense, the term Cyber Threat Intelligence (CTI) refers to information about cybersecurity threats and players that helps mitigate malign incidents in cyberspace (Bank of England, 2016), which is a part of a concept of cybersecurity information. In recent years following the legislation of CISA 2015, there have been attempts to identify which factors contribute to realize sound environment where CTI sharing is actively engaged by private entities and public entities. Wanger *et al.* (2016) suggested a platform aiming to help in setting up counter measures and proactive actions used against cyberattacks. Qamar *et al.* (2017) performed a comprehensive and conceptual evaluation of cyber threats sharing platform and presented that the suggested framework outperforms existing evaluation approaches in terms of effectiveness and efficiency. Sillaber *et al.* (2016) argued that data quality in CTI platform is extremely important factor sharing CTIs, especially for the data source integration and scalability of data shared. Likewise, existing literature has focused on CTI sharing in terms of platform design and its evaluation, though little attention has been paid to the formation of cybersecurity information sharing and its economic impact on our society or cybersecurity industry.

In terms of the value of information sharing, most of the studies that examined the impact of cybersecurity information sharing use a game theoretic approach to highlight the difference in the stance of an individual firm and a social planner (Gordon *et al.*, 2003b; Gal-Or and Ghose, 2005; Hausken, 2007; Liu *et al.*, 2011; Laube and Böhme, 2015). Cybersecurity information sharing has both advantages and disadvantages. The disadvantages are the opportunity costs of monitoring by external organizations (He *et al.*, 2018) and damage to reputation (Skopik *et al.*, 2016). Also, the true value of information sharing is only realized when the sender and receiver share integral information (Wong *et al.*, 2019; Yu and Cao, 2019). On the other hand, the advantages are defense against terrorist threats (Swire, 2006), faster detection of security breaches (Fleming and Goldstein, 2012) and expected reduction in losses (Gordon and Loeb, 2003). Given that information is one of the vital resources for firms (Li *et al.*, 2019), obtaining adequate level of information through information sharing is therefore critical for the firms to remain competitive.

Taken together, prior studies speculated that cybersecurity investment is beneficial for investing firms (Gal-Or and Ghose, 2005), and information sharing ultimately maximizes social welfare by lowering excess costs incurred by undesirable amount of investment in cybersecurity (Liu *et al.*, 2011; Gal-Or and Ghose, 2005). In addition, the functional importance of a social planner (i.e. government organizations such as DHS or ISAC) has been emphasized (Hausken, 2007; Liu *et al.*, 2011; Gal-Or and Ghose, 2005). However, there has been a research gap between those theoretically examined studies and empirical findings based on real-world example. We expect our study to fill the gap by exploiting CISA as an exogenous shock and by measuring the subsequent impact on firms' investment in cybersecurity.

3. Hypotheses development

3.1 Real option theory and positive externalities

As discussed in the previous section, researchers have long argued that a cybersecurity information sharing regime plays a crucial role in enhancing social welfare. To verify their proposition, we divide the related entities into two: firms directly affected by CISA (i.e. firms investing in cybersecurity) and firms indirectly affected by CISA due to demand-side spillover effect (i.e. cybersecurity vendors).

Figure 1 illustrates the projected cybersecurity investment and firm performance that conceptually integrates two different theories into one. The first stage starts with the perspective of investing firms (Gordon *et al.*, 2003a, 2015), who purchase cybersecurity vendors' products or services. CISA lowers the uncertainty of cybersecurity investment decisions, which, in turn, lowers the value of the option to defer investment in cybersecurity. The reduced uncertainty itself does not directly lead to increased cybersecurity investment; the information sharing is more likely to reduce the common tendency of firms to wait for a cybersecurity breach before investing in related activities (Gordon *et al.*, 2015). The second stage starts with the demand-side spillover from increased cybersecurity investments, which enhances the firm-level performance of the cybersecurity industry (Gal-Or and Ghose, 2005). If we extract the essential logic from the two-stage model, we arrive at the assumption that the introduction of CISA 2015 would positively influence the US cybersecurity industry. With this assumption, we describe our research hypotheses in detail.

3.2 Firm performance measurements: Tobin's Q and sales growth rate

Numerous previous studies, including the well-known Bharadwaj *et al.* (1999) study, have used Tobin's Q as a dependent variable that is forward-looking, less susceptible to changes and a risk-adjusted measure of firm performance (Montgomery and Wernerfelt, 1988). This measure is widely used in empirical studies (Bose and Leung, 2019; Mithas and Rust, 2016; Jacobs *et al.*, 2016; Ak and Patatoukas, 2016) that try to measure firm performance in terms of market value. Therefore, we used Tobin's Q ratio as the firm performance-measuring variable.

H1a. CISA 2015 positively affects US cybersecurity firms' overall performance (Tobin's Q).

Another common variable for measuring firm performance is the sales growth rate (e.g. Xue *et al.*, 2012). This measure intuitively and explicitly captures firm performance change compared with the past and future.

H1b. CISA 2015 positively affects US cybersecurity firms' overall performance (sales growth rate).

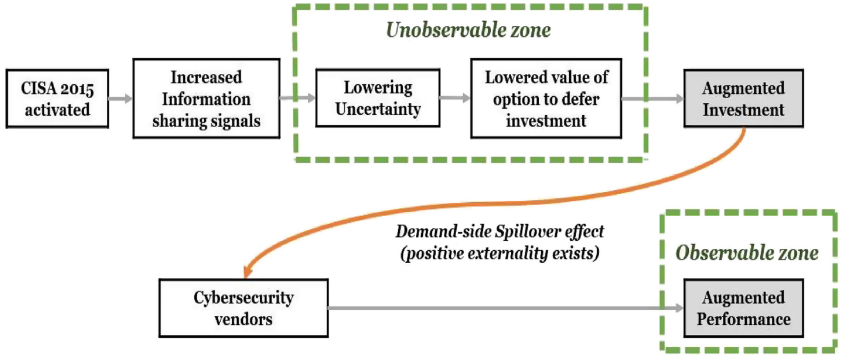

Figure 1. Projected cybersecurity investment and firm performance stream

3.3 Firm size division and subsample analysis

Gal-Or and Ghose (2005) also point out that cybersecurity information sharing and investment have "complementary relations," meaning information sharing and cybersecurity investments by one firm induce other firms to mimic that behavior, increasing the total volume of information sharing and security investment. They suggest two effects in their model: the so-called "direct effect," which increases the demand for security products, and the "strategic effect," which alleviates price competition among cybersecurity vendors. They state that these two effects increase with an increase in the size of the firm. Thus, we divide firm size into two (big and small). Following are the subhypotheses that check the effect of firm size.

H2a. The overall performance (Tobin's Q) enhancement of US cybersecurity firms is concentrated in big firms after CISA 2015.

H2b. The overall performance (sales growth rate) enhancement of US cybersecurity firms is concentrated in big firms after CISA 2015.

4. Method

4.1 Difference-in-differences (DID)

As CISA 2015 provides a quasi-experimental setting, we analyze the variation in firm performance before and after the enactment of CISA. Since our control group is the most innovative and fastest-growing firms, including overseas markets, it is reasonable to assume that if it were not for CISA, there would not have been significant a difference in firm performance. Due to its power on causal inference, DID estimation has long been employed by researchers and practitioners as favored identification strategy, in the field of business such as Information Systems (Burtch *et al.*, 2018; Greenwood and Wattal, 2017; Hui and Png, 2015), Operation and Production Management (Dhanorkar, 2018; Tang and Whinston, 2019) and Marketing (Israeli, 2018; Fedorenko, 2018).

To measure the effect of CISA, we use a DID method. The basic idea of DID is to identify a specific treatment effect (i.e. often the passage of the law). A simple way to identify the impact of CISA on cybersecurity firm is to evaluate the difference in performance of cybersecurity firm around CISA while controlling for firm-level characteristics. However, this method fails to control for total changes in performance caused by macroeconomic trends. A well-used solution to this problem is to exploit a control group; we can compare the change in performance of firms directly affected by CISA to that of firms whose performance is irrelevant to CISA. DID method is believed to control for macroeconomic trends and industry-specific or firm-specific patterns. More specifically, we evaluate the impact of CISA by estimating the following equation using firm-level data:

$$Y_{it} = \beta_0 + \beta_1 \cdot \text{US\_Security}_i + \beta_2 \cdot \text{CISA}_t + \beta_3 \cdot (\text{US\_Security}_i * \text{CISA}_t) + X_{it}^{'}\gamma_1 + \varepsilon_{it} \quad (1)$$

where Y_{it} denotes firm performance, defined as Tobin's Q and sales growth rate; US_Security is a dummy variable equal to 1 for US cybersecurity firms and 0 for others; CISA is a dummy variable equal to 1 for the period post-2015 and 0 for the period before 2015; X is firm control variable including industry dummy variables. The main coefficient of interest, β_3, measures how the performance gap is different between US cybersecurity firms and other fast-growing firms after CISA. Under the null that CISA does not affect US security firm's performance, $\beta_3 = 0$, we expect β_3 to be positive because CISA would have a positive effect on their performance. Note that we exclude 2015, a baseline year, from our data to highlight the time difference. And, we do not take both the firm fixed effects and time fixed effects into account in our DID analyses.

5. Data

5.1 Sample selection

We carefully consider which listed firms are to be designated as experimental and control groups before implementing DID analyses. Fundamentally, we define cybersecurity firm as "a private-entity engaged in protecting against harm that may be done via network access, malicious data, and code injection," following Schatz *et al.* (2017).

Table 1 illustrates the composition of samples used, separating location, size and lists. We select "*the world's hottest and most innovative 500 cybersecurity companies to watch in 2017*," listed on Cybersecurity Ventures' recent report, as qualified candidates for being experimental group. Unfortunately, only 75 of the total 500 firms were listed on US stock markets, whereas most of the firms on the list were private firms. And only 57 of the 75 listed firms remain on final samples. The reasons for omitting 18 firms are as follows: firms listed on the stock market after 2016 (5/18); firms that we cannot extract essential data from the Compustat database (8/18) and so forth. The reason we use samples listed on 2017 instead of 2015, the baseline year, is the number of publicly traded firms we only consider; presumably, there is no significant compositional difference between the list of 2015 and of 2017 in terms of the number of firms publicly traded. Next, we collect samples for control group based on Forbes' "*The 100 World's Most Innovative Companies 2015*" and Fortune's "*100 Fastest-Growing Companies in the World 2015*," which explicitly distinguishes the difference between the treatment and control group, as these two sources (Forbes and Fortune lists) are ranked by firm performance thus representing the world's most outstanding firms. Of the total 200 firms, only 168 (84×2) remain due to similar reasons we explained earlier.

The firm location is where the headquarter is located, bisecting into inside and outside of US, thus we can check whether a firm was under the influence of CISA. We classify firm size based on total sales of 2014, a year just prior to the passage of CISA. A firm that has under 1bn dollars sales is categorized as a small firm, reversely, over 3bn dollars sales is categorized as a big firm. The criterion for this amount is to obtain the corresponding volume of samples; big firms ($n = 80 = 17 + 17+46$) versus small firms ($n = 80 = 29 + 48+3$). At the result section, we will show DID analysis results in accordance with these firm size classifications.

5.2 Data extraction and variables

We gather firm-level panel data from the Compustat database, covering the 2013–2017 period. Our analyses exclude the baseline year 2015, which accentuates the time difference. Data from US listed firms were collected from Compustat North America and those from overseas exchanges were collected from Compustat Global.

Dependent variables are Tobin's Q and sales growth rate. The definition of those variables is summarized in Table 2. The level variables such as total sales and market capitalization

	Treatment group	Control groups			
	US security	Non-US security	Fortune's 100	Forbes' 100	Total
Location					
US	57	0	73	41	171
Non-US	0	22	11	43	76
Size					
Big	17	8	17	46	88
Small	29	14	48	3	94
Medium	11	0	19	35	65

Table 1.
Description of samples

were converted into US dollars by reflecting the average exchange rate of foreign currencies during the sampling period. Control variables are also summarized in Table 2. In order to prevent the listing period of a firm from becoming 0, as some sample firms went public in 2013 and 2014, we calculated firm age as the natural logarithm of current year minus Initial Public Offering (IPO) year plus 1, following the method used in a prior study (Loderer and Waelchli, 2010). Then, we control firm size by controlling the number of employees. The industry sector was separated into five segments, following NAICS' industry classification, and also controlled when implementing DID.

6. Empirical results

Table 3 reports summary statistics for the two years prior to and after of CISA. Then, each period is classified into two separate groups: US security firm, designated as an experimental group, and otherwise. On average, the control group outperforms the experimental group (e.g. sales growth rate, market value) and also outnumbers the experimental group in the average number of employee and firm age. That is, those groups are comparable because the experimental group was not readily defeating the control group in firm performance before 2015.

6.1 Primary analysis 1 – results with the full sample (H1a and H1b)

We employ a DID to evaluate the effect of CISA on US cybersecurity firm performances. The results are shown in Table 4.

The first three columns with Tobin's Q are provided as a benchmark. The coefficients on US security*CISA are positive and statistically significant at the 5% level, and the point estimate of the effect of CISA is an increment in Tobin's Q by 0.630 with a complete set of controls. Therefore, H1a is supported. The coefficient corresponds with about 18% of average Tobin's Q (and 22% of a standard deviation), which presents economically significant evidence. In other words, after CISA, the performance is higher for US cybersecurity firm, compared to other promising firms. Our findings support the argument of Gordon *et al.* (2015) in that the cybersecurity firms' Tobin's Q significantly increases after CISA. Also, it can be interpreted that the increased Tobin's Q is partially generated by demand-side spillover effect, arising from CISA.

In column 4 through 6, we also consider sales growth rate as a performance-measuring variable. While Tobin's Q captures market expectations of future firm performance, the sales growth rate is a measure of current growth rates of firms. Therefore, it's more appropriate to consider using both as indicators of firm performance, but the impact of CISA is smaller and insignificant than Tobin's Q. That is, H1b is not supported. With the same logic as in the case of Tobin's Q, while we expect the sales growth rate of US cybersecurity firms will also be higher than that of other firms, our results are mixed. Our hypothesis tests for H1a and H1b

Table 2.
Variable description

Variable	Definition
Tobin's Q	$\frac{\text{total assets} + \text{market value} - \frac{\text{common}}{\text{ordinary}} \text{ equity}}{\text{total assets}}$
Sales growth rate	$\frac{\text{current year total sales} - \text{previous year total sales}}{\text{previous year total sales}}$
Employees	ln (numb. of employees)
Firm age	ln (current year – IPO year +1)
Industry classification	-manufacturing: NAICS code starting from 31–33 -information: NAICS code starting from 51/54 -financials: NAICS code starting from 52–53 -trade: NAICS code starting from 42/44–45/48–49

	Tobin's Q	Sales growth rate	Market value	Assets	Sales	Employee	Age
Mean	3.443	0.191	19145.14	9579.94	5627.82	20182.48	17.03
Median	2.673	0.116	6751.76	3877.31	2504.52	6825	16
SD	2.818	0.455	38388.08	17214.53	8932.33	40800.36	11.85
N	817	635	817	860	860	803	860
2013–2014							
Mean (US security)	3.021	0.260	12815.95	10003.47	6503.58	16189.26	13.89
Mean (other)	4.079	0.322	19071.37	6919.50	4304.95	18227.4	16.17
2016–2017							
Mean (US security)	2.765	0.142	15798.64	12448.78	7006.40	20816.21	17.11
Mean (other)	3.121	0.122	22713.76	11392.57	6301.69	23714.14	19.07

Table 3.
Summary statistics

	Tobin's Q			Sales growth rate		
Dependent var.	(1)	(2)	(3)	(4)	(5)	(6)
US security	−1.057***	−1.134***	−1.574***	−0.062	−0.114	−0.125
	(0.264)	(0.265)	(0.310)	(0.115)	(0.101)	(0.096)
CISA	−0.958***	−0.837***	−0.791***	−0.200***	−0.176***	−0.175***
	(0.242)	(0.248)	(0.242)	(0.050)	(0.055)	(0.055)
US security*CISA	0.701**	0.631**	0.630**	0.082	0.095	0.095
	(0.328)	(0.321)	(0.312)	(0.121)	(0.114)	(0.113)
ln_employee		−0.015	−0.048		−0.031*	−0.031
		(0.067)	(0.072)		(0.018)	(0.019)
ln_firm age		−0.263**	−0.345**		−0.084***	−0.089***
		(0.127)	(0.136)		(0.024)	(0.026)
Dummy_Manu			1.488***			0.009
			(0.302)			(0.054)
Dummy_Info			1.302***			−0.014
			(0.332)			(0.044)
Dummy_Fin			−0.063			−0.038
			(0.315)			(0.068)
Dummy_trade			0.063			−0.061
			(0.353)			(0.054)
Constant	4.079***	4.836***	4.414***	0.323***	0.809***	0.834***
	(0.204)	(0.432)	(0.428)	(0.049)	(0.180)	(0.206)
adj.*R* squared	0.031	0.033	0.075	0.032	0.068	0.064
N	817	773	773	635	590	590

Note(s): Note that we report heteroskedasticity-robust standard errors in parentheses. *, ** and *** represent significance at the 10%, 5% and 1% level, respectively.

Table 4.
DID results with the full sample

demonstrate that market expectation for the cybersecurity industry increases after the CISA, whereas no evidence of firms' short-term expenditure on cybersecurity was captured by sales growth rate.

6.2 Primary analysis 2 – results with the subsample (H2a and H2b)

Table 5 shows the subsample results. The regressions are different in the samples according to whether the total sales in 2014 were below (as small) 1bn dollars or above (as big) 3bn dollars.

Table 5.
DID results based on firm size

	Tobin's Q				Sales growth rate			
	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
Dependent var.	Big	Small	Big	Small	Big	Small	Big	Small
US security * CISA	0.809**	0.256	0.744**	0.311	0.279***	−0.076	0.278***	−0.046
	(0.368)	(0.561)	(0.362)	(0.543)	(0.101)	(0.212)	(0.102)	(0.202)
ln_firm age			−0.199	−0.217			−0.01	−0.099**
			(0.168)	(0.167)			(0.018)	(0.048)
Industry dummies	X	X	√	√	X	X	√	√
adj.*R* squared	0.085	0.0113	0.103	0.066	0.050	0.037	0.035	0.043
N	280	291	280	291	231	217	231	217

Note(s): Note that we report heteroskedasticity-robust standard errors in parentheses. *, ** and *** represent significance at the 10%, 5% and 1% level, respectively

For the subsample of big firms, the coefficients for the interaction term (US security*CISA) are higher and more significant than for the rest of the entire subsamples (i.e. the "small" columns). In other words, big firms mostly seem to be affected by CISA more than small firms when analyzed by the market expectation measurement (Tobin's Q). Thus, H2a is supported. In the last four columns where sales growth rates are the dependent variable, the difference in the degree of influence of CISA is further widened between samples. The coefficient of the large firm sample is significant at the 1% level, while for small firms, the coefficient is not significant and even negative values are observed. Therefore, H2b is supported. In sum, big-size security firm receives the influence of CISA immediately, from the result of the respective analyses for big and small firm samples. Especially, this appears evident in the 1% significance of the key coefficient when the sales growth rate is a dependent variable in the big firm sample regression.

There are two possible explanations for this result. First, though controversial, the cybersecurity industry might belong to an oligopoly market. In that case, the rising demand and investment to cybersecurity congregate to some large cybersecurity firms. Gal-Or and Ghose (2005) also show that the immediate effects related to information sharing begin in large firms due to the "direct effects," that is, characteristics of oligopoly market. Second, it could be reasonable for firms to contract with the same vendor when they share information. Generally, firms in common system want to use the same vendors; thus, a few big cybersecurity firms might benefit from CISA in terms of market value and sales.

7. Robustness check

7.1 An estimate using propensity score matching (PSM)

As our research design is fundamentally not based on a randomized experimental setting, the selection bias problem can appear when setting both experimental group and control group (Heckman, 1990). Thus, we employ PSM to support DID identification assumptions, enabling us to check the robustness of our empirical findings.

More specifically, from the various matching options, we adopt the one-to-one nearest neighbor matching approach, the most common matching criterion (Austin, 2011). After the matching procedure, we implement the covariate balance test for the matched samples to verify whether there is a difference between treated and untreated groups (Atanasov and Black, 2016).

Essentially, the intuition behind matching experimental group sample with that of control group is as follows: the more similar treated and untreated firms are in their pretreatment observations (i.e. the covariates used in PSM setting), the less likely they are to differ in unobserved ways (Zervas *et al.*, 2017). Having balanced groups, matched by observable characteristics, we can mitigate the endogeneity concerns by making the treated and untreated groups more homogeneous and comparable (Heckman and Navarro-Lozano, 2004). Thus, the causal interpretation for estimates resulting from DID analysis would be more assured.

To implement PSM procedure, we first select a set of covariates by which the samples are newly matched in accordance with the criterion of one-to-one nearest neighbor matching. In our case, we used "leverage ratio" and "capital expenditure divided by total asset" as covariates. We replicate the analyses presented in Tables 4 and 5, regrouping the control groups. The results are shown in Tables 6 and 7, respectively.

As shown in column 1 through 3 of Table 6, we find that the effect of CISA on US security firms is robust to PSM, attaining a magnitude ($\beta_3 = 0.781$ in column 3 and 0.715 in column 1) that is highly comparable to our initial estimate ($\beta_3 = 0.630$) reported in column 3 of Table 4.

Table 7 indicates group comparison depending on size classification, replicating Table 5. When the firm performance is measured by Tobin's Q, the results are inconsistent with what

Dependent var.	Tobin's Q (1)	(2)	(3)	Sales growth rate (4)	(5)	(6)
DID results combined with propensity score matched samples (1:1 nearest neighbor matching)						
US security	−0.551**	−0.734***	−1.715***	0.029	−0.046	−0.146*
	(0.270)	(0.252)	(0.384)	(0.110)	(0.081)	(0.076)
CISA	−0.947***	−0.829***	−0.811***	−0.143***	−0.119***	−0.111***
	(0.273)	(0.288)	(0.273)	(0.038)	(0.037)	(0.039)
US security*CISA	0.715***	0.760**	0.781**	0.026	0.066	0.058
	(0.353)	(0.343)	(0.331)	(0.116)	(0.097)	(0.096)
ln_employee		−0.136**	−0.208***		−0.059**	−0.064**
		(0.055)	(0.057)		(0.026)	(0.030)
ln_firm age		−0.410***	−0.413***		−0.105***	−0.100***
		(0.104)	(0.102)		(0.032)	(0.031)
Dummy_Manu			1.086**			−0.088
			(0.445)			(0.076)
Dummy_Info			1.571***			0.056
			(0.506)			(0.091)
Dummy_Fin			−0.435			−0.084
			(0.469)			(0.101)
Dummy_trade			0.379			0.038
			(0.716)			(0.141)
Constant	3.560***	5.725***	5.725***	0.231***	1.017***	1.085***
	(0.211)	(0.477)	(0.539)	(0.033)	(0.292)	(0.345)
adj.R squared	0.032	0.108	0.182	0.014	0.154	0.150
N	389	377	377	290	275	275

Table 6.
Robustness check with matched samples

Note(s): Note that we report heteroskedasticity-robust standard errors in parentheses. *, ** and *** represent significance at the 10%, 5% and 1% level, respectively

is shown in Table 5, making our interpretation about the results intermingled. In settings where the US security firms and respective counterparts are matched by observed characteristics, there is no statistical evidence that big-sized US security firms' market value defeats the others after the introduction of CISA. So, the H2a is no longer believed to be supported. However, when it comes to measuring the firms' performance as sales growth rate, all the β_3s maintain their statistical significance in this constrained model regardless of how the control group samples are regrouped. So, the H2b is still supported. We can interpret the result that CISA directly and promptly affects the big-sized US cybersecurity firms, enhancing firm performance with respect to market sales and hence making them beneficiaries of information sharing regime.

8. Conclusions

There has long been debate on the role of cybersecurity information sharing in preventing future breaches and reducing the uncertainty of cybersecurity investment. The importance of information sharing stems from a change in recent years due to the active involvement of the US government. Despite the argument (Gordon *et al.*, 2003a, 2015; Gal-Or and Ghose, 2005) that information sharing can save the cost of cybersecurity investment, empirical evidence is rare.

Our study designs a quasi-experiment to investigate the causal effect of information sharing legislation on firms' cybersecurity investment decisions. We employ the DID approach to estimate the impact of CISA on the overall cybersecurity industry. The

Table 7. Robustness check with matched samples based on size classification

	Tobin's Q				Sales growth rate			
	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)
Dependent var.	Big	Small	Big	Small	Big	Small	Big	Small
DID results combined with propensity score matched samples (1:1 nearest neighbor matching)								
US security * CISA	0.501	1.456**	0.323	2.152**	0.341***	−0.036	0.337***	−0.036
	(0.543)	(0.674)	(0.517)	(0.843)	(0.127)	(0.205)	(0.129)	(0.217)
ln_firm age	−0.331*	−0.264	−0.229	−0.368*	−0.018	−0.146***	−0.013	−0.157***
	(0.182)	(0.209)	(0.164)	(0.191)	(0.024)	(0.057)	(0.027)	(0.061)
Industry dummies	X	X	√	√	X	X	√	√
adj.*R* squared	0.189	0.068	0.305	0.151	0.188	0.066	0.254	0.042
N	143	192	143	192	111	138	111	138

Note(s): Note that we report heteroskedasticity-robust standard errors in parentheses. *, ** and *** represent significance at the 10%, 5% and 1% level, respectively

methodology allows us to isolate the effect of CISA from other exogenous factors that could affect cybersecurity investment.

The DID estimates show a positive effect of CISA on overall firm performance in the cybersecurity industry in the US. The increment in firms' cybersecurity investments after CISA is reflected in the sharp increase in Tobin's Q or market participants' expectations of US cybersecurity firms. Indeed, the impact of CISA is noticeable considering the characteristics of the control group – the best firms in the world in terms of firm performance, according to Forbes and Fortune. If we combine the real options theory (Gordon *et al.*, 2015) and the game theoretic approach (Hausken, 2007; Liu *et al.*, 2011), firms are likely to defer their cybersecurity investment decision in the absence of a social planner, as there is significant uncertainty over the decision. Therefore, the introduction of CISA plays an important role in reducing the uncertainty and thus, decreases the value of an option to defer. Therefore, increased investment in cybersecurity enhances future firm value and the present market sales of cybersecurity firms. One interesting finding is that, as Gal-Or and Ghose (2005) had demonstrated, the impact of the information sharing regime is especially concentrated in large-sized firms. The results of all analyses consistently show that large US cybersecurity firms are the primary beneficiaries of CISA, as they are the focal subjects of demand-side spillover effect from firms' investments in cybersecurity.

9. Discussion

9.1 Limitation

Despite the consistency of our empirical results with theory, this study has some limitations. First, we cannot completely rule out the possibility that the effect that we capture in our analyses could be partly driven by other exogenous factors. Owing to the lack of microdata – the individual firm's cybersecurity investment – we estimate it indirectly using the vendor's market sales information. In fact, 2015 was said to be an eventful year for cybersecurity industry; simultaneous developments including GDPR enforcement and massive healthcare breaches (Anthem, UCLA health, etc.). Second, we only considered publicly traded firms in our study. Small and private firms are not included in our sample, which might cause selection bias. We employ PSM to alleviate the problem related to sample selection. Nevertheless, a more extended study should be conducted to mimic a randomized experiment. Third, there is ambiguity over the jurisdiction. In our research, we classify the nationality of an individual firm based on the location of its headquarters. However, like the recent case of GDPR, laws often have influence across national borders. Despite our effort (e.g. PSM) to mitigate and examine this issue, we have not been able to eliminate it completely. The fourth limitation concerns the presence of an information sharing entity in the private domain. A platform like the Threat Exchange of Facebook could dilute the only effect of CISA we want to measure. That is, the Splunk add-on to the platform could generate profit not created by CISA.

9.2 Implication

Nevertheless, our research makes several academic contributions. First, this study is the first empirical research to demonstrate a causal relationship between information sharing and an increase in cybersecurity investment. This was possible due to the introduction federal information sharing law in 2015, enabling us to exploit this milestone as a natural experiment. Second, this study conceptually integrates two theories into a single model – the real options theory that measures the relationship between information sharing and cybersecurity investment (Gordon *et al.*, 2015) and a theory of the existence of demand-side spillover effects on the cybersecurity industry (Gal-Or and Ghose, 2005). Third, this study confirms that CISA

affects the cybersecurity industry unevenly by firm size, a previously unknown fact. We believe this is because CISA contributes to making the cybersecurity industry an oligopolistic market to a certain extent. In the process of sharing cybersecurity information within the sharing group, the customer reviews of cybersecurity vendors could be shared by one firm with the others, making big cybersecurity vendors even bigger.

Our findings also have managerial implications for the cybersecurity firms. It is important for cybersecurity firms to understand the impact and dynamics of government involvement in the industry, especially in terms of economic benefits or costs. However, there was no empirical evidence to distinguish the "before" and "after" effect of CISA 2015 on cybersecurity industry. Thus, we shed light on the previously unknown impact of a cybersecurity information sharing regime on the cybersecurity industry, which gives the cybersecurity industry an action plan for the government's next move.

Notes

1. The stock price of Marriot decreased about 5% after the breach announcement. Although the market return should be considered, a size of the drop seems huge (CNBC, November 30, 2018, please see: https://www.cnbc.com/2018/11/30/marriott-hack-raises-questions-about-merger-diligence-tools-in-use.html).
2. "Cybersecurity Information Sharing Act of 2015," S. 754, 114th Congress. U.S. Senate, 2015. available at: https://www.congress.gov/bill/114th-congress/senate-bill/754 (last visited: March 29, 2018).
3. "Biennial Report on DHS's Implementation of the Cybersecurity Act of 2015," Department of Homeland Security; Office of Inspector General, November 2017.
4. "The Cybersecurity Act of 2015," Sullivan & Cromwell, December 2015.

References

Acquisti, A., Friedman, A. and Telang, R. (2006), "Is there a cost to privacy breaches? An event study", *Proceedings of International Conference on Information Systems (ICIS)*.

Ak, B.K. and Patatoukas, P.N. (2016), "Customer-base concentration and inventory efficiencies: evidence from the manufacturing sector", *Production and Operations Management*, Vol. 25 No. 2, pp. 258-272.

Arora, A., Nandkumar, A. and Telang, R. (2006), "Does information security attack frequency increase with vulnerability disclosure? An empirical analysis", *Information Systems Frontiers*, Vol. 8 No. 5, pp. 350-362.

Arora, A., Krishnan, R., Telang, R. and Yang, Y. (2010), "An empirical analysis of software vendors patch release behavior: impact of vulnerability disclosure", *Information Systems Research*, Vol. 21 No. 1, pp. 115-132.

Atanasov, V. and Black, B. (2016), "Shock-based causal inference in corporate finance and accounting research", *Critical Finance Review*, Vol. 5, pp. 207-304.

Austin, P.C. (2011), "An introduction to propensity score methods for reducing the effects of confounding in observational studies", *Multivariate Behavioral Research*, Vol. 46 No. 3, pp. 399-424.

Bank of England (2016), *CBEST Intelligence-Led Testing: Understanding Cyber Threat Intelligence Operations*, Bank of England.

Benaroch, M. (2018), "Real options models for proactive uncertainty-reducing mitigations and applications in cybersecurity investment decision making", *Information Systems Research*, Vol. 29 No. 2, pp. 315-340.

Bharadwaj, A.S., Bharadwaj, S.G. and Konsynski, B.R. (1999), "Information technology effects on firm performance as measured by Tobins q", *Management Science*, Vol. 45 No. 7, pp. 1008-1024.

Black, F. and Scholes, M. (1973), "The pricing of options and corporate liabilities", *Journal of Political Economy*, Vol. 81 No. 3, pp. 637-654.

Bose, I. and Leung, A.C.M. (2019), "Adoption of identity theft countermeasures and its short-and long-term impact on firm value", *MIS Quarterly*, Vol. 43 No. 1, pp. 313-327.

Buchanan, J.M. and Stubblebine, W.C. (1962), "Externality", in *Classic Papers in Natural Resource Economics*, pp. 138-154.

Burtch, G., Carnahan, S. and Greenwood, B.N. (2018), "Can you gig it? An empirical examination of the gig economy and entrepreneurial activity", *Management Science*, Vol. 64 No. 12, pp. 5497-5520.

Campbell, K., Gordon, L.A., Loeb, M.P. and Zhou, L. (2003), "The economic cost of publicly announced information security breaches: empirical evidence from the stock market", *Journal of Computer Security*, Vol. 11 No. 3, pp. 431-448.

Cavusoglu, H., Mishra, B. and Raghunathan, S. (2004), "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*, Vol. 9 No. 1, pp. 70-104.

Cavusoglu, H., Raghunathan, S. and Yue, W.T. (2008), "Decision-theoretic and game-theoretic approaches to IT security investment", *Journal of Management Information Systems*, Vol. 25 No. 2, pp. 281-304.

Chai, S., Kim, M. and Rao, H.R. (2011), "Firms information security investment decisions: stock market evidence of investors behavior", *Decision Support Systems*, Vol. 50 No. 4, pp. 651-661.

Demetz, L. and Bachlechner, D. (2013), "To invest or not to invest? Assessing the economic viability of a policy and security configuration management tool", in *The Economics of Information Security and Privacy*, Springer, Berlin, Heidelberg, pp. 25-47.

Dhanorkar, S. (2018), "Environmental benefits of internet-enabled C2C closed-loop supply chains: a quasi-experimental study of craigslist", *Management Science*, Vol. 65 No. 2, pp. 660-680.

Dixit, A.K. and Pindyck, R.S. (1994), *Investment Under Uncertainty*, Princeton University Press, Princeton, New Jersey.

Fedorenko, I. (2018), "Marketing secrets: a conceptual model and quasi-experimental study: an abstract,"in *Academy of Marketing Science Annual Conference*, Springer, Cham, pp. 189-190.

Fleming, M.H. and Goldstein, E. (2012), "Metrics for measuring the efficacy of critical-infrastructure-centric cybersecurity information sharing efforts", available at: https://ssrn.com/abstract=2201033 (accessed 5 May 2018).

Fried, D. (1984), "Incentives for information production and disclosure in a duopolistic environment", *Quarterly Journal of Economics*, Vol. 99 No. 2, pp. 367-381.

Gal-Or, E. and Ghose, A. (2005), "The economic incentives for sharing security information", *Information Systems Research*, Vol. 16 No. 2, pp. 186-208.

Gay, S. (2017), "Strategic news bundling and privacy breach disclosures", *Journal of Cybersecurity*, Vol. 3 No. 2, pp. 91-108.

Gordon, L.A. and Loeb, M.P. (2003), "Expenditures on competitor analysis and information security", *Management Accounting in the Digital Economy*, Vol. 95, pp. 95-111.

Gordon, L.A., Loeb, M.P. and Lucyshyn, W. (2003a), "Information security expenditures and real options: a wait-and-see approach", *Computer Security Journal*, Vol. 19 No. 2, pp. 1-7.

Gordon, L.A., Loeb, M.P. and Lucyshyn, W. (2003b), "Sharing information on computer systems security: an economic analysis", *Journal of Accounting and Public Policy*, Vol. 22 No. 6, pp. 461-485.

Gordon, L.A., Loeb, M.P., Lucyshyn, W. and Zhou, L. (2015), "The impact of information sharing on cybersecurity underinvestment: a real options perspective", *Journal of Accounting and Public Policy*, Vol. 34 No. 5, pp. 509-519.

Greenwood, B.N. and Wattal, S. (2017), "Show me the way to go home: an empirical investigation of ride-sharing and alcohol related motor vehicle fatalities", *MIS Quarterly*, Vol. 41 No. 1, pp. 163-187.

Hausken, K. (2007), "Information sharing among firms and cyberattacks", *Journal of Accounting and Public Policy*, Vol. 26 No. 6, pp. 639-688.

He, M., Devine, L. and Zhuang, J. (2018), "Perspectives on cybersecurity information sharing among Multiple stakeholders using a decision-theoretic approach", *Risk Analysis*, Vol. 38 No. 2, pp. 215-225.

Heckman, J. (1990), "Varieties of selection bias", *The American Economic Review*, Vol. 80 No. 2, pp. 313-318.

Heckman, J. and Navarro-Lozano, S. (2004), "Using matching, instrumental variables, and control functions to estimate economic choice models", The *Review of Economics and Statistics*, Vol. 86 No. 1, pp. 30-57.

Herath, H.S. and Herath, T.C. (2008), "Investments in information security: a real options perspective with bayesian post audit", *Journal of Management Information Systems*, Vol. 25 No. 3, pp. 337-375.

Hui, K.L. and Png, I.P. (2015), "Research note—migration of service to the internet: evidence from a federal natural experiment", *Information Systems Research*, Vol. 26 No. 3, pp. 606-618.

Israeli, A. (2018), "Online MAP enforcement: evidence from a quasi-experiment", *Marketing Science*, Vol. 37 No. 5, pp. 710-732.

Jacobs, B.W., Kraude, R. and Narayanan, S. (2016), "Operational productivity, corporate social performance, financial performance, and risk in manufacturing firms", *Production and Operations Management*, Vol. 25 No. 12, pp. 2065-2085.

Kannan, K., Rees, J. and Sridhar, S. (2007), "Market reactions to information security breach announcements: an empirical analysis", *International Journal of Electronic Commerce*, Vol. 12 No. 1, pp. 69-91.

Kirby, A.J. (1988), "Trade associations as information exchange mechanisms", *The Rand Journal of Economics*, Vol. 19 No. 1, pp. 138-146.

Koepke, P. (2017), "*Cybersecurity information sharing incentives and barriers*", Working Paper, MIT Sloan Business School.

Laube, S. and Böhme, R. (2015), "Mandatory security information sharing with authorities: implications on investments in internal controls," in *Proceedings of the 2nd ACM Workshop on Information Sharing and Collaborative Security*, pp. 31-42.

Li, S., Cui, X., Huo, B. and Zhao, X. (2019), "Information sharing, coordination and supply chain performance: the moderating effect of demand uncertainty", *Industrial Management and Data Systems*, Vol. 119 No. 5, pp. 1046-1071.

Liu, D., Ji, Y. and Mookerjee, V. (2011), "Knowledge sharing and investment decisions in information security", *Decision Support Systems*, Vol. 52 No. 1, pp. 95-107.

Loderer, C. and Waelchli, U. (2010), "Firm age and performance", available at: https://ssrn.com/abstract=1342248 (accessed 13 February 2018).

McDonald, R. and Siegel, D. (1986), "The value of waiting to invest", *Quarterly Journal of Economics*, Vol. 101 No. 4, pp. 707-727.

Mithas, S. and Rust, R.T. (2016), "How information technology strategy and investments influence firm performance: conjecture and empirical evidence", *MIS Quarterly*, Vol. 40 No. 1, pp. 223-245.

Montgomery, C.A. and Wernerfelt, B. (1988), "Diversification, ricardian rents, and Tobins q", *The RAND Journal of Economics*, Vol. 19 No. 4, pp. 623-632.

Moore, T. and Clayton, R. (2011), "The impact of public information on phishing attack and defense", *Communications and Strategies*, Vol. 81, pp. 45-68.

Myers, S.C. (1977), "Determinants of corporate borrowing", *Journal of Financial Economics*, Vol. 5 No. 2, pp. 147-175.

Qamar, S., Anwar, Z., Rahman, M.A., Al-Shaer, E. and Chu, B.T. (2017), "Data-driven analytics for cyber-threat intelligence and information sharing", *Computers and Security*, Vol. 67, pp. 35-58.

Schatz, D., Bashroush, R. and Wall, J. (2017), "Towards a more representative definition of cyber security", *Journal of Digital Forensics, Security and Law*, Vol. 12 No. 2, pp. 53-74.

Shapiro, C. (1986), "Exchange of cost information in oligopoly", *The Review of Economic Studies*, Vol. 53 No. 3, pp. 433-446.

Sillaber, C., Sauerwein, C., Mussmann, A. and Breu, R. (2016), "Data quality challenges and future research directions in threat intelligence sharing practice", in *Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security*, pp. 65-70.

Skopik, F., Settanni, G. and Fiedler, R. (2016), "A problem shared is a problem halved: a survey on the dimensions of collective cyber defense through security information sharing", *Computers and Security*, Vol. 60, pp. 154-176.

Swire, P.P. (2006), "Privacy and information sharing in the war on terrorism", *Villanova Law Review*, Vol. 51 No. 4, pp. 1-30.

Tang, Q. and Whinston, A.B. (2019), "Do reputational sanctions deter negligence in information security management? A field quasi-experiment", *Production and Operations Management*, Vol. 29 No. 2, pp. 410-427.

Tatsumi, K. and Goto, M. (2010), "Optimal timing of information security investment: a real options approach", *Economics of Information Security and Privacy*, Springer, Boston, pp. 211-228.

Telang, R. and Wattal, S. (2007), "An empirical analysis of the impact of software vulnerability announcements on firm stock price", *IEEE Transactions on Software Engineering*, Vol. 33 No. 8, pp. 544-557.

Wagner, C., Dulaunoy, A., Wagener, G. and Iklody, A. (2016), "Misp: the design and implementation of a collaborative threat intelligence sharing platform", *Proceedings of the 2016 ACM on Workshop on Information Sharing and Collaborative Security*, pp. 49-56.

Wang, T., Kannan, K.N. and Ulmer, J.R. (2013), "The association between the disclosure and the realization of information security risk factors", *Information Systems Research*, Vol. 24 No. 2, pp. 201-218.

Wong, W.P., Tan, H.C., Tan, K.H. and Tseng, M.L. (2019), "Human factors in information leakage: mitigation strategies for information sharing integrity", *Industrial Management and Data Systems*, Vol. 119 No. 6, pp. 1242-1267.

Xue, L., Ray, G. and Sambamurthy, V. (2012), "Efficiency or innovation: how do industry environments moderate the effects of firms IT asset portfolios?", *MIS Quarterly*, Vol. 36 No. 2, pp. 509-528.

Yu, M. and Cao, E. (2019), "Strategic information sharing and competition under cap-and-trade regulation", *Industrial Management and Data Systems*, Vol. 119 No. 3, pp. 639-655.

Zervas, G., Proserpio, D. and Byers, J.W. (2017), "The rise of the sharing economy: estimating the impact of airbnb on the hotel industry", *Journal of Marketing Research*, Vol. 54 No. 5, pp. 687-705.

About the authors

Agnes Yang got her Master's degree from the School of Business at Yonsei University. She is currently a Ph.D. student at the Carlson School of Management at the University of Minnesota. University of Minnesota, 321 19th Ave. S., Minneapolis, MN, USA.

Young Jin Kwon got his Master's degree from the School of Business at Hanyang University. School of Business, Hanyang University, 222 Wangsimni-ro, Seongdong-gu, Seoul 133-791, Korea.

Sang-Yong Tom Lee is a professor at the School of Business at Hanyang University. He previously worked at the National University of Singapore. His research interests include economics of information systems, online information privacy, and value of IT. His publications have appeared in *MIS Quarterly,*

Management Science, Journal of Management Information Systems, Information & Management, the IEEE Transactions on Engineering Management and others. School of Business, Hanyang University, 222 Wangsimni-ro, Seongdong-gu, Seoul 133-791, Korea. Sang-Yong Tom Lee is the corresponding author and can be contacted at: tomlee@hanyang.ac.kr