Niu, X.M., Li, W.H., Zhang, J.F., Zhang, X., Chen, J.L. & Xu, H.J. (2022). The impact of information systems vulnerability announcements on firms' market value. In Li, E.Y. *et al.* (Eds.) *Proceedings of The International Conference on Electronic Business, Volume 22* (pp. 694-700). ICEB'22, Bangkok, Thailand, October 13-17, 2022



# The impact of information systems vulnerability announcements on firms' market value

*(Work-in-Progress)*

Xueming Niu [1]
Weihua Li [2]
Jinfeng Zhang [3]
Xiong Zhang [4,*]
Jianlong Chen [5]
Haijie Xu [6]

*Corresponding author
[1] Graduate student, Beijing Jiao Tong University, Beijing, China, 20120609@bjtu.edu.cn
[2] Lecturer, Beijing Daxing District No. 1 Vocational School, Beijing, China, li_weihua0814@163.com
[3] Bachelor student, Nankai University, Tianjin, China, 1911304@mail.nankai.edu.cn
[4] Associate Professor, Beijing Jiao Tong University, Beijing, China, xiongzhang@bjtu.edu.cn,
[5] Bachelor student, Beijing Jiao Tong University (Weihai), Weihai, China, 19711001@bjtu.edu.cn
[6] Bachelor student, Beijing Jiao Tong University (Weihai), Weihai, China, 19711033@bjtu.edu.cn

## ABSTRACT

With the increasing deployment of IT systems, information systems vulnerabilities have led to a severe negative impact on firms and businesses. This paper aims to examine the impact of information system vulnerability announcements on the market value of Chinese firms. Using the collected security incidents in Chinese firms from 2015 to 2021, we study how characteristics of enterprises and vulnerabilities affect enterprises' market value through event study and regression analysis. In particular, we find that state-owned enterprises suffer larger negative effects than other types of firms. This study also provides companies and managers with insights in decision-making and recommendations from a managerial perspective.

*Keywords*: Information Security Announcements, Event Study, Abnormal Return, Regression Analysis.

## INTRODUCTION

According to the latest data released by the International Telecommunication Union (ITU), the growth in internet usage between 2019 and 2021 was the largest in the past decade. As of 2021, the number of active Internet users worldwide has reached 4.66 billion, accounting for 59.5 percent of the total population(Number of Internet Users 2021 | Statista, 2021). China is one of the countries with the largest internet population. 1.011 billion people have used the internet in 2021, and the internet penetration rate reaches 71.6% (China Internet Network Information Center, 2021). The rapid development of the Internet and related information technologies have greatly changed the people's daily life. However, with the vigorous development of the Internet, more information security incidents occur, causing huge economic losses. There were 1,896 data breaches in 2021, an increase of 23 percent from 2020. IBM's 2021 Cost of Data Breach Report stated that in 2021, each data breach will cost companies an average of $4.24 million (IBM Security, 2021). For instance, it is reported that a ransomware breach would cost an average of $4.62 million to affiliated firms.

Thus, the impact of information security incidents on firms is an important topic to investigate. This study aims to answer this question in a Chinese context by investigating following issues: (1) How the market value of Chinese firms will change due to the information security incidents? (2) How the firm's characteristics and attributes of information systems vulnerabilities will impact this change?

This study adopts the event study method. According to our preliminary analysis, we find that the average market value of firms will lose 0.5% on the day when information systems vulnerabilities were announced. In addition, we also confirm that the firm's characteristics and attributes of a company's information systems vulnerabilities will play an important role in the fluctuation of market value caused by information system vulnerabilities.

## LITERATURE REVIEW

Researchers had investigated the security issues of information systems from various perspectives. (Zhang et al., 2015) adopted a machine learning approach to analyze hackers' behavior from the knowledge sharing perspective. (Zhang, Shao, et al., 2020) analyzed the patterns and modes of vulnerabilities in firms' information systems by applying the LDA topic modeling method. (Zhang, Xie, et al., 2020) established a common framework to gain a deeper understanding about the characteristics of vulnerabilities and their solutions to ensure the security of enterprise information systems.

Besides, there exist various empirical studies focusing on the impacts of news disclosure on enterprise management decisions. However, compared with vulnerability disclosure, the impacts of information security incidents on enterprises' market value is not well understood, and the existing related research in academia is limited. Some scholars summarized that studies related to impacts of information security on stock prices, and found about 37 related articles (Spanos & Angelis, 2016).

(Aytes et al., 2006) studied the impacts of potential security bugs on the market value of listed companies by examining the impacts of information security bugs announcements on shareholders' value from an economic perspective. It was found that after the announcement of security bugs, the market value of the competitors increases, and the magnitude of this increment depends on the nature of the security bugs. The increase in competitor value is higher when security bugs involve unclassified company and customer information. The impacts are significantly negative when security bugs involve confidential data. (Cavusoglu et al., 2004) analyzed the reaction of capital markets to companies involved and security developers after the incident, and found that the impact of security incident disclosure is not limited to the companies involved, but also to the market value of Internet developers. (Yang et al., 2021) examined the companies' responses to network vulnerabilities after security incidents, and found that factors such as sentiment in the vulnerability repair plan, vulnerability report anonymity, vulnerability type, vulnerability risk level, and the industry sector to which companies belong have significant impacts on the companies' response. Using event study and regression analysis, (Ye & Zhang, 2021) found that the enterprises related to such events will suffer from a market value loss. They also investigated the moderating effect of companies' characteristics and attributes of security events on this effect. Using event study approach, (Wang & Zhang, 2022) compared and analyzed impacts of non-information security events and information security incidents on enterprises and identified various factors adjusting such impacts. (Das et al., 2012) proposed to identify factors which could modulate cumulative abnormal returns (CAR). They found that company type, company size, and the risk level of attacks can independently regulate CAR.

## HYPOTHESES DEVELOPMENT

How the stock market responds to the information security breach announcements depends on the attitude of people to the incidents. Generally, when a security incident happens, people's property or information will suffer loss. Therefore, most people will maintain negative views on the incidents though other factors may influence their view. This is consistent with previous studies. Thus, we have:

**Hypothesis 1:** Information security vulnerability announcement negatively affect the market value of firms.

### *Firm Type*

State-owned enterprises (SOEs) play a critical role in Chinese economy and even the global economy (Lin et al., 2020). The number of SOEs in Fortune Global 500 (FG500) has increased from 27 in 2000 to 102 in 2017, and the revenue of FG500 SOEs reached 22% of all FG500 companies (Lin et al. 2019). In particular, China's SOEs are an essential component of global SOEs. Chinese SOEs have advantages in maintaining social stability and maximizing resource mobility. Thus, they draw better attention from social and investors. When there is an information security vulnerability announcement covered by the media, it may have a higher negative impact on the SOEs. It leads to our second hypothesis:

**Hypothesis 2:** When facing the announcement of information security vulnerability, the market value of SOEs will be negatively affected in a higher level than that of non-SOEs.

### *Firm Assets*

The impact of the information systems vulnerabilities may be related to firms' intangible assets. In the stock market, investors usually evaluate the information security investment of a firm by its intangible assets. When information security incidents occur, a firm owning more intangible assets may lose more trust from investors, who may be skeptical about the effectiveness of information security investments. Thus, we propose the following hypothesis:

**Hypothesis 3:** When facing information vulnerability announcements, firms with more intangible assets will suffer higher negative impacts than those with less tangible assets.

### *Time Effect*

As time goes by, both the number and diversity of information security breaches increase. All kinds of news about the vulnerabilities stimulate the nervous nerves of people, who have become more sensitive to privacy and safety. Therefore, when a new information system breach is announced, people have less tolerance for it compared to the past, leading to more losses in a firm. Thus, we put forward the following hypothesis:

**Hypothesis 4:** Information systems vulnerabilities will have a greater negative impact on the firm's market value than those in the past.

## DATA AND METHODOLOGY

### *Data Collection*

To collect information security incidents, we searched in domestic high-impact portals with specific keywords. We use the combination of two groups of keywords, one group includes "system", "security", "information", and "platform" and the other group includes "vulnerability", "breach", "privacy" and "incident" respectively. We limit the search period between 2015 and 2021. Initial data is preprocessed according to the following criteria: (1) The listed company must be listed for at least three months; (2) The historical stock data of the listed company should be available from 5 days before the announcement day to 5

days after the announcement day; (3) If the event is reported multiple times, the event date should be selected as the earliest announcement.

Finally, we conducted 54 observations on the information security vulnerability announcements of 34 companies. In general, associated enterprises are distributed in various industries, with over 70% of enterprises belong to the financial industry and high-technology industry.

***Event Study Methodology***

We use the event study methodology to estimate the impact of information security vulnerability announcements on the market value of firms. This methodology has been widely used in economic and finance research (MacKinlay, 1997). Based on the market rationality, changes in the stock values can immediately reflect the impact of one certain event in the market on firms. Thus, the impact of the information security vulnerability announcement on the market value of firms can be investigated by the change of stock value on the event date via event study methodology.

The first step is to calculate the return of the stock using the Capital Asset Pricing Model (CAPM) in our study. CAPM assumes that a linear relationship exists between the market return and the return of a stock. The model is as follows:

$$R_{it} = \alpha_i + \beta_i R_{mt} + \varepsilon_{it} \quad (1)$$

which is the return of the stock *i* on day *t*; $R_{mt}$ is the return of the market on day *t*; $\alpha_i$ and $\beta_i$ represent the intercept and the slope parameter of the stock *i* respectively; $\varepsilon_{it}$ is the disturbance term of the market model.

The stocks of the companies we selected are from three markets. Thus, we use the NASDAQ, HKEX, SZSE market index return as the proxy of the market return respectively, depending on which market the stock i in. The period of the event window is important, and a shorter event window is preferred in event study (McWilliams & Siegel, 2017). Previous studies used a 2-day event window, the day of the announcement and the day after the announcement, to capture the impact of an announcement made after the stock market close (Cavusoglu et al., 2014). Others chose a 3-day event window, starting on the day before the announcement and ending on the day after the announcement (Das et al., 2012). They avoided the effect of information leakage before the announcement. However, in our study, we choose a 1-day event window. It not only increases the power of the statistical test but also reduces the effect of the cofounding events. We need to set an estimation window to estimate the parameter $\alpha_i$ and $\beta_i$. Generally, the estimation window, between 120 days and 200 days, is a period that is prior to the event window. In our study, we choose the period from 170 days to 10 days before the event day as our estimation window.

Next, the abnormal return (AR) of the stock i on day t can be concluded by:

$$AR_{it} = R_{it} - \left(\hat{\alpha}_i + \hat{\beta}_i R_{mt} + \varepsilon_{it}\right) \quad (2)$$

The abnormal return measures the difference between the actual return and the expected return of the stock *i* on day *t*. The cumulative abnormal return (CAR) of the stock *i* can be calculated over the event window by:

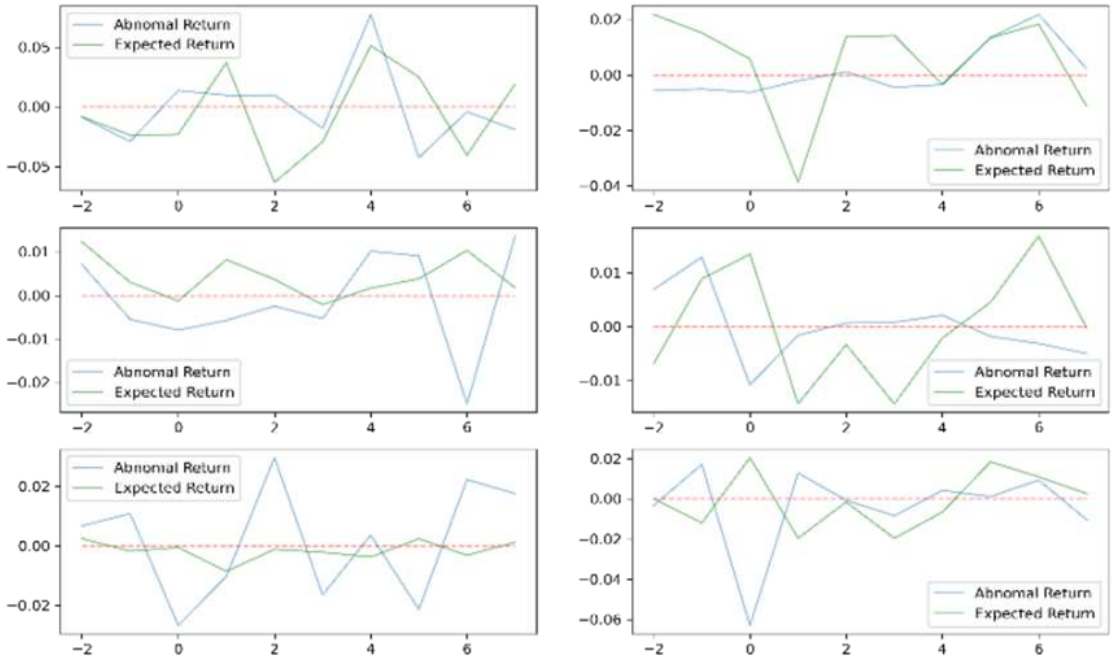
$$CAR_i = \sum_{t_1}^{t_2} AR_{it} \quad (3)$$

where $t_1$ and $t_2$ represent the starting date and the ending date of the event window.

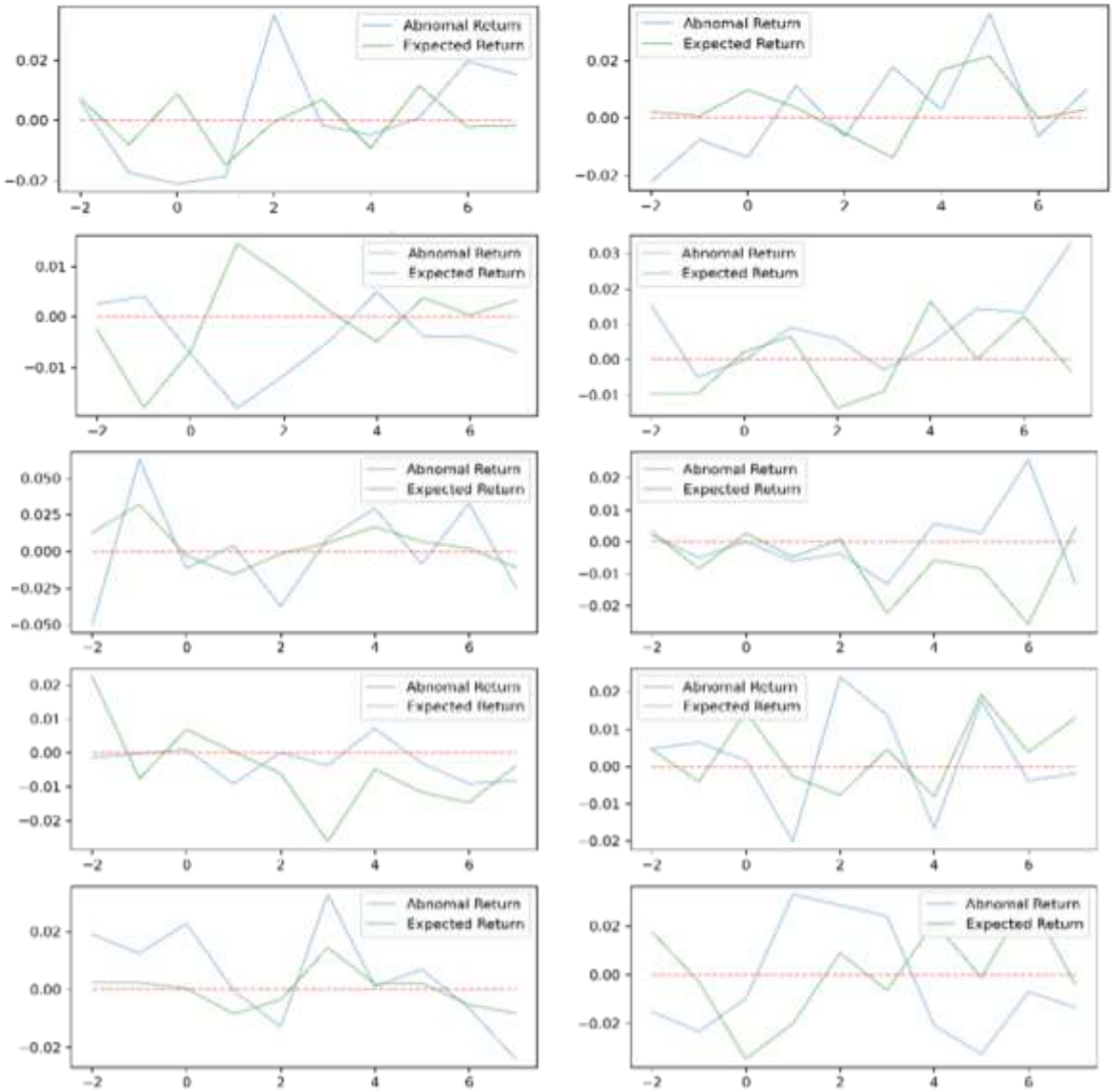
The mean of cumulative abnormal return of all *N* events can be calculated by:

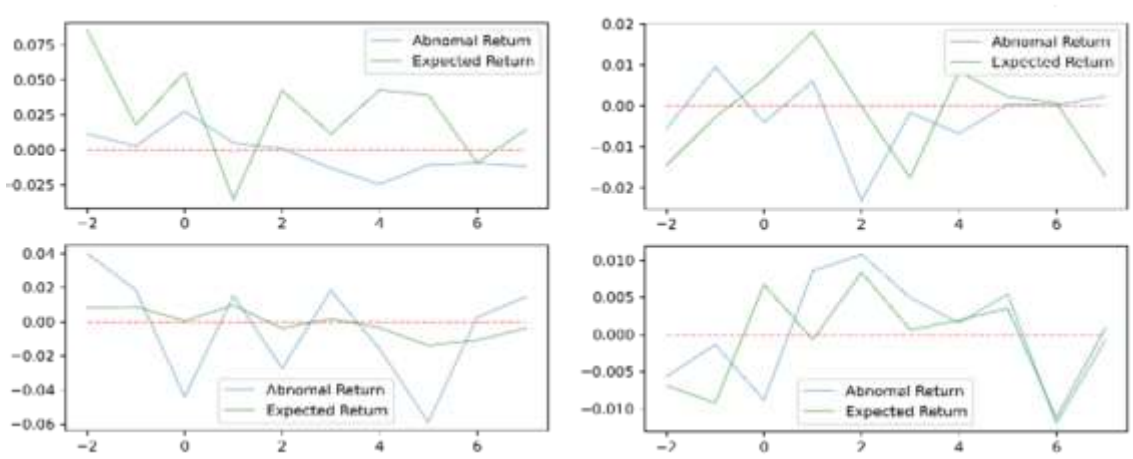
$$CAR = \frac{1}{N}\sum_{i=1}^{N} CAR_i \quad (4)$$

Table 1 summarizes the results produced by the event study methodology. In the table, the mean cumulative abnormal returns and *p* values from the t-test are represented. The mean cumulative abnormal return on event day (day 0) is negative and statistically significant, which suggests that the market value of the firms suffers a negative effect on the announcement day of. The mean cumulative abnormal return on the day before the event day (day -1) is positive and not significant, showing that there is little effect of news leakage. The mean cumulative abnormal return on the day after the event day (day 1) is negative but not statistically significant, suggesting that the impact of the announcement lasts for a short time. All *p* values are one-tailed.

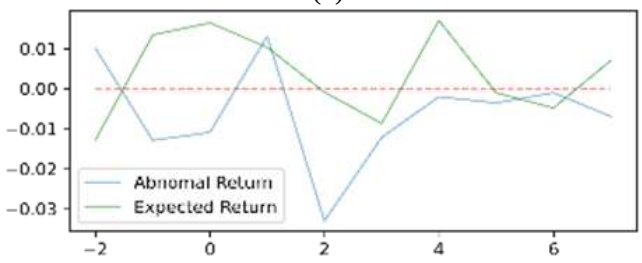

Abnormal Return
Expected Return

(a)


Abnormal Return
Expected Return




(b)




(d)

Figure 1: Abnormal Return and Expected Return of Some Incidents

Table 1: Mean Abnormal Return

| **Day** | -2 | -1 | 0 | 1 | 2 |
|---|---|---|---|---|---|
| **Mean abnormal return** | 0.005 (0.05) | 0.000 (0.44) | -0.005 (0.03) | -0.003 (0.13) | -0.003 (0.19) |

## DATA ANALYSIS AND RESULTS

**Regression Analysis**

To verify our hypotheses, we develop a multiple linear regression model as follows:

$$AR_{it} = \alpha + \beta_1 Tangible\ Asset + \beta_2 Intangible\ Asset + \beta_3 Growth + \beta_4 Opertions + \beta_5 Finance + \beta_6 SOEs + \beta_7 Time + \beta_8 Severity + \beta_9 Response + \beta_{10} Type + \beta_{11} Source \quad (5)$$

The description of independent variables is as follows. Tangible asset and intangible asset represented by the variable *Tangible Asset* and *Intangible Asset* are calculated by the natural logarithm of the tangible asset and intangible asset of the firm. The growth rate of the firm will influence the reaction of market to the vulnerability. It is measured by the variable *Growth* = $\frac{Assel_{current} - Assel_{previous}}{Asset_{previous}}$. The operation of the firm can be measured by basic earnings per share, which is represented by the variable *Operation*. To define type of the firm, we use *Finance* = 1 if the firm is in finance and *Finance* = 0 otherwise. In a similar way, *SOEs* = 1 if the firm is a stated-owned enterprise and *SOEs* = 0 otherwise. In order to measure the time effect, we denote the initial year (2015 year) as 0, the second year as 1, the third year as 2, etc. For vulnerability, *Severity* = 1 if the vulnerability is severe, and *Severity* = 0 otherwise.

Additionally, we have the following control variables. First, we use the variable *Response* to control the firm's action or response to the announcement, which is a dummy variable. When the firm has an active response and takes appropriate action to the vulnerability, like providing a patch or paying compensation for stakeholders, *Response* = 1. When the firm admits the incident, *Response* = 0. Importantly, if the firm doesn't take action to the incident and denies it, *Response* = -1, Second, the type of vulnerabilities is measured by the variable *Type. Type* = 1 if the vulnerability is related to confidential information and *Type* = 0 if not. Third, we also control the source of the news. *Source* = 1 if the news is form official media and *Source* = 0 if not. Table 2 shows the descriptive statistics of all variables.

Table 2: Descriptive Statistics of the Variables

| **Variables** | **Mean** | **Max** | **Min** |
|---|---|---|---|
| Tangible Asset | 18.13 | 21.72 | 12.41 |
| Intangible Asset | 13.36 | 16.71 | 8.20 |
| Growth | 0.17 | 0.76 | -0.64 |
| Operation | 4.89 | 32.95 | -8.71 |
| Finance | 0.24 | 1 | 0 |
| SOEs | 0.5 | 1 | 0 |
| Time | 3.5 | 6 | 0 |
| Severity | 0.43 | 1 | 0 |
| Response | 0.31 | 1 | -1 |
| Type | 0.41 | 1 | 0 |
| Source | 0.3 | 1 | 0 |

***Results***

The results are listed in Table 3. The $R^2$ of the model is 31.6%, and the adjusted $R^2$ is 13.7%. They are sufficient enough to explain the abnormal stock return. Furthermore, the variance inflation factors (VIF) for our model is below the recommended level of 10. Some interesting phenomena are observed from our model. First, the coefficient of *Tangible Asset* variable is negative, while the coefficient of *Intangible Asset* is positive, both of which are significant (t = -3.186, p = 0.003; t = 2.280, p = 0.028). It suggests that firms which have more tangible assets will suffer more negative effects, while the firms which have more intangible assets will be less negatively impacted. On average, the market value of firms will lose by 0.79 percent if the tangible asset of firms increases by 1 percent, while the market value of firms will increase by 0.5 percent if the intangible asset of firms increases by 1 percent. Second, the coefficient of the finance is positive and significant (t = 2.386, p = 0.023), indicating that the financial industries suffer more negative effect. Third, the coefficient of *SOEs* variable is positive and significant (t = 3.439, p = 0.001), showing that the Sate-owned enterprises suffer more negative effects. Besides, the variable *Time* has a positive and significant (t = 2.089, p = 0.043) coefficient. Information security incidents in recent years have greater negative impact on enterprises than those in the past. However, the coefficient of variable *Severity* is positive but not significant, indicating that there is no significant difference in abnormal returns in terms of vulnerability severity.

Table 3 Regression Results

| Variables | Coefficient | t-statistic | p-value |
|---|---|---|---|
| Tangible Asset | -0.0079*** | -3.014 | 0.004 |
| Intangible Asset | 0.0050** | 2.146 | 0.038 |
| Growth | -0.0065 | -0.336 | 0.739 |
| Operations | 0.0007* | 1.753 | 0.087 |
| Finance | 0.0233** | 2.202 | 0.033 |
| SOEs | 0.0253*** | 3.332 | 0.002 |
| Time | 0.0027** | 2.043 | 0.047 |
| Severity | 0.0097 | 1.445 | 0.156 |
| Response | -0.0018 | -0.540 | 0.592 |
| Type | -0.0010 | -0.153 | 0.880 |
| Source | -0.0065 | -1.081 | 0.286 |

Note: *** denotes significance at the 1 percent level, ** denotes significance at the 5 percent level, * denotes significance at the 10 percent level

## CONCLUSION AND DISCUSSION

This study uses the event study methodology to explore the impact of information systems vulnerabilities announcement on firms' market value. We focus on Chinese companies and study the behavior of SOEs in the face of the information systems vulnerabilities.

We find that there exists a statistically significant negative correlation between the information systems vulnerabilities announcements and the market value of firms. Information security incidents will cause more negative influence on firms owning more intangible assets. In addition, we also observe the financial firms and SOEs will suffer more losses than others. What's more, information security incidents will cause more harms to the companies than in the past.

Based on the above results, some implications are summarized as follows. First, companies need to increase the information security investment to reduce risks because investors and customers have less tolerance for vulnerabilities. For example, they

can invest more cost on inspection and maintenance. Second, financial firms pay more attention to customers' privacy and improve their confidence in the companies. It can reduce customer losses after security incidents happen. Third, companies need to be more cautious when choosing the vendors of systems and establish a more professional information security team to deal with emergencies.

Finally, due to its special social status, state-owned enterprises will suffer more losses under the same conditions. They should pay more attention to the occurrence of information security incidents, especially when the country advocates new digital infrastructure and information security.

## ACKNOWLEDGEMENT

This research is supported by grants from the National Natural Science Foundation of China (Grant 71801014) and Beijing Social Science Foundation (Grant 17GLC069). Xiong Zhang (xiongzhang@bjtu.edu.cn) is the corresponding author.

## REFERENCES

Aytes, K., Byers, S., & Santhanakrishnan, M. (2006). The Economic Impact of Information SecurityBreaches: Firm Value and Intra-industry Effects. In AMCIS. http://aisel.aisnet.org/amcis2006/399

Cavusoglu, H., Mishra, B., & 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, 9(1), 70–104. https://doi.org/10.1080/10864415.2004.11044320

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2014). The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers. Https://Doi.Org/10.1080/10864415.2004.11044320, 9(1), 70–104. https://doi.org/10.1080/10864415.2004.11044320

China Internet Network Information Center. (2021). The 48th Statistical Report on China's Invest Internet Development. http://www.cnnic.net.cn/hlwfzyj/hlwxzbg/hlwtjbg/202109/P020210915523670981527.pdf

Das, S., Mukhopadhyay, A., & Anand, M. (2012). Stock Market Response to Information Security Breach: A Study Using Firm and Attack Characteristics. Journal of Information Privacy and Security, 8(4), 27–55. https://doi.org/10.1080/15536548.2012.10845665

IBM Security. (2021). Cost of a Data Breach Report 2021. https://www.ibm.com/downloads/cas/OJDVQGRY

Lin, K. J., Lu, X., Zhang, J., & Zheng, Y. (2020). State-owned enterprises in China: A review of 40 years of research and practice. China Journal of Accounting Research, 13(1), 31–55. https://doi.org/10.1016/J.CJAR.2019.12.001

MacKinlay, A. C. (1997). Event Studies in Economics and Finance. Journal of Economic Literature, 35(1), 13–39. https://ideas.repec.org/a/aea/jeclit/v35y1997i1p13-39.html

McWilliams, A., & Siegel, D. (2017). Event Studies In Management Research: Theoretical And Empirical Issues. Https://Doi.Org/10.5465/257056, 40(3), 626–657. https://doi.org/10.5465/257056

Number of internet users 2021 | Statista. (2021). https://www.statista.com/statistics/273018/number-of-internet-users-worldwide/

Spanos, G., & Angelis, L. (2016). The impact of information security events to the stock market: A systematic literature review. In Computers and Security (Vol. 58, pp. 216–229). Elsevier Ltd. https://doi.org/10.1016/j.cose.2015.12.006

Yang, H., Zhang, J., & Zhang, X. (2021). Network Vulnerability and Enterprises' Response: The Preliminary Analysis. AMCIS 2021 Proceedings. https://aisel.aisnet.org/amcis2021/info_security/info_security/22

Ye, R., & Zhang, X. (2021). Information Security and Firms' Market Value: The Preliminary Analysis. ICEB 2021 Proceedings (Nanjing, China). https://aisel.aisnet.org/iceb2021/11

Wang, H., & Zhang, X. (2022, August 19). The Impact of Information Security Events on Stock Value of Firms. The 7th International Conference on Smart Finance.

Zhang, X., Shao, H., Zhu, M., & Zhang, R. (2020). The Towards Understanding Vulnerability in Information Systems: The Topic Modeling Perspective. Twenty-Fourth Pacific Asia Conference on Information Systems (PACIS 2020), 6–22. https://aisel.aisnet.org/pacis2020

Zhang, X., Tsang, A., Yue, W. T., & Chau, M. (2015). The classification of hackers by knowledge exchange behaviors. Information Systems Frontiers, 17(6), 1239–1251. https://doi.org/10.1007/s10796-015-9567-0

Zhang, X., Xie, H., Yang, H., Shao, H., & Zhu, M. (2020). A General Framework to Understand Vulnerabilities in Information Systems. IEEE Access, 8, 121858–121873. https://doi.org/10.1109/ACCESS.2020.3006361