Winter 12-3-2021

Information Security and Firms' Market Value: The Preliminary Analysis

Runbo Ye

Xiong Zhang

Ye, R. & Zhang, X. (2021). Information security and firms' market value: The preliminary analysis. In *Proceedings of The International Conference on Electronic Business, Volume 21* (pp. 236-243). ICEB'21, Nanjing, China, December 3-7, 2021.

Information Security and Firms' Market Value: The Preliminary Analysis

Runbo Ye [1]
Xiong Zhang [2,*]

*Corresponding author
[1] Master Student, Imperial College London, U.K, runbo.ye21@imperial.ac.uk
[2] Associate Professor, Beijing Jiao Tong University, Beijing, China, xiongzhang@bjtu.edu.cn

ABSTRACT

In the era of information and big data, security events have caused serious impacts on companies' business operations. The paper aims to investigate the impact of information system security events on firms' market value. To do so, this study collects security events data from Chinese mainstream media platforms and newspapers. The event study approach and regression analysis are used to show that the involved companies associated with the events will suffer the loss on its market value. Moreover, the involved companies' characteristics and the events' attributes can also affect the loss caused by these information security events. The findings of the study provide managerial insights for enterprise managers and help them formulate suitable coping strategies for potential events.

Keywords: Enterprise Information Systems, Security Event, Event Study Approach, Stock Price, Regression Analysis

INTRODUCTION

With the advent of the information age and the era of big data, enterprise information systems are playing important roles in companies' business operations. Enterprise information systems can help enterprises greatly improve the efficiency of data and internal resource management, the integrity of data and information, making it easier for enterprises to make objective decisions based on the overall situation. However, security issues with information systems, the widespread application of enterprise information systems have also brought the negative impact on enterprises under spotlights. This is the research focus of this study.

Once an information system security event occurs, the upgrade of the enterprise requires a large amount of time and financial consumption. The enterprise also suffers from the loss of commercial value and potential users. Rahul and Sunil found that some software vendors' stock price and market value will account for about 0.6% after the release of software vulnerability announcement (Telang & Wattal, 2007). Given the complicated nature of listed companies, e.g., volume, industries, product diversity among others, and characteristics of security events, e.g., risk level, type, what loss will information security events cause is not immediately clear. Under certain scenarios, whether this influence will be constrained and affected?

To this end, this study chooses listed companies in China as the research objects, uses a keyword to search for event data from China's mainstream media platforms and news channels. We plan to answer the following two research questions: (1) whether the enterprise information system security event will have a negative impact on the market value of the involved enterprises and cause losses in the short term? (2) Whether event attributes, market characteristics, and the characteristics of the involved companies will restrict this loss and impact?

This study uses the event study approach to observe the fluctuations in the market value of the involved companies after the event. This study also establishes a regression model to further discuss the results of the event analysis and discuss how characteristics of companies and security events would influence such negative impacts. After that, we provide theoretical guidance and suggestions for enterprises to solve the events of enterprise information system security vulnerabilities.

LITERATURE REVIEW

The event analysis method was first proposed by Dolley in 1933. Dolley used the 95 common stock splitting events from 1921 to 1931 as the research object to observe the fluctuations in stock value before and after the stock split to verify whether the stock split event would be affected. The stock value has an impact. Then at the end of the 20th century, the event analysis method was mainly used to study the performance of mergers and acquisitions and to measure the success of corporate mergers and acquisitions by observing the fluctuations in stock value after the merger. In recent years, the event analysis method has become more widely used. For example, He et al. (2020) used event analysis in COVID-19's Impact on Stock Prices Across Different Sectors-An Even Study Based on the Chinese Stock Market Law studied the impact of the new crown epidemic on China's stock market (He et al., 2020). Rahul and Sunil used the event analysis method in An Empirical Analysis of the Impact of Software Vulnerability Announcements on Firm Stock Price to study the impact of software vulnerability announcements on software vendors' stock prices and concluded that software vulnerability announcements would approximately affect vendors. The market value has an impact of 0.6% (Telang & Wattal, 2007). Similarly, Steven and Burcu also used the event analysis method in Effect of Qatar diplomatic and economic isolation on GCC stock markets: An event study approach to

study the impact of Qatar's diplomatic and economic isolation events on GCC stock prices and explain the economic isolation events. GCC will face a capital outflow of US$35.4 billion and a decline of US$21 billion in foreign exchange reserves (Buigut & Kapar, 2020). In general, the event research method has a reliable performance in the research of the stock market, and there are many successful cases, and the event objects tend to be diversified. This provides a lot of practice and experience for the research of this article.

DATA COLLECTION AND DATA PROCESSING

In this research, 84 events of enterprise information system security reported on China's mainstream media platforms and news channels are selected, involving 18 listed companies in China. We use the official databases and keywords of various media platforms to retrieve events. After the event data retrieval is completed, we further process the event data according to the criteria of event study and the need for data analysis and further summarize the enterprise information system security event category, enterprise information system security event risk level, enterprise response, and attitude to the event. Finally, we need to collect financial data about the involved enterprise and the stock price of the various window periods of the event to observe the impact of the enterprise information system security event on the company's stock price.

Information System Security Event Data

Drawing on Rahul and Sunil's research on software vulnerability notifications, we tried to use keyword retrieval to collect the event records from the mainstream media and newspapers: Sina, People's Daily, Guangming Daily, Xinhua, and CCTV. The event data includes articles and reports from Sina, Xinhua, and other media platforms, as well as daily reports from popular newspapers such as People's Daily and Guangming Daily. It also includes graphic data provided by CCTV and CCTV. In order to ensure the timeliness and consistency of the data, we selected the largest media data retention cycle (the length of time each media platform saves data and news) for three years, as the research unit selected the enterprise information system security events from 2018 to 2021 as the research object. In Rahul and Sunil's study, they used "vulnerability and disclosure," "software and vulnerability," "software and flaw," "virus and vulnerability, "vulnerability and patch" to search in the New York Times, Washington Daily News, and Wall Street Journal (Telang & Wattal, 2007). In conjunction with the above research, we use the following terms as search indexes, "system and vulnerability," "platform and vulnerability," "information and vulnerability," "system and problem," "system and defect," "information and leak."

Stock Price and Financial Position

We also collect the event-related business share prices and basic financial situation to supplement the research. For the corporate stock price, we use the Python interface in the WIND database quantification tool to count the closing prices of each stock code on each specific date. For financial data on the enterprise, we query from the annual financial statements disclosed by each listed company on the stock exchange.

Record Labeling

When we have completed the first round of data retrieval and collection, we will be exposed to a large amount of event data. We must determine two points, 1) all event data is in our controlled and understandable context 2) All events meet the requirements for event analysis and ensure complete and consistent data, so we need to further classify and process the data (Holzmann, 2001).

Regarding the risk assessment of each event, we assume that the coverage of events is objective on the premise that all news reporters are rational. So based on the texts used by event reporters in the description of the event, we can simply categorize and judge the level of risk of the event: if there are words such as "very serious," "very dangerous," and "extremely serious" in the report, we consider the event to be very serious. If no similar adverbs appear in the report, or if words such as "Minor severe" or even "not severe" are used, we consider the event to be generally serious. In our collection of events, a total of 47 events are very serious information system security events, and the remaining 37 events are generally critical.

We found that when words such as "operational issue" and "service interruption" are included, usually the event is an enterprise information system security event caused by a design problem. Words such as "injection" usually code injection events. Words such as "information disclosure," "sensitive information," and "privilege" are often information disclosure events.

When the enterprise information system security event occurs, the enterprise will often respond after a period, explain the event to mitigate the value impairment of the event to the involved enterprise. However, in some special cases, it is also very likely that the involved enterprises will not make any response or explanation of the event. Therefore, we need to distinguish and identify the different response attitudes of enterprises. If we see "alarm," "confirmation," "explanation," "response," "transfer to a third party," and other acts, we think that the enterprise involved in the event has a response. Conversely, if the feedback from the media platform is "unreachable," "unanswered," "unexplained," and "ignored," we think that the involved enterprise has ignored the events.

Some security events may cause serious impacts on people's lives and property, and such events violate the rules of the relevant state agencies, so national regulators, such as the China Securities Regulatory Commission (CSRC) or the China Banking Regulatory Commission (CBRC), will deal with the event. The national regulators may disclose the involved company in the violation, and then national regulators may impose penalties. For example, on March 26, 2021, the China

Securities Regulatory Commission issued an administrative supervision notice for the Haitong Asset Management Trading System for its schedule machine event and pointed out that Haitong Securities did not comply with the relevant prudential principles to prevent risks. Therefore, the security event of Haitong Securities is deeply involved by the national regulatory agency.

Data Processing and Cleaning

We first delete duplicated event data. For some enterprise information system security events, multiple media platforms may repeatedly report them in a time period. In this case, we only select the report of this event appearing in the streaming media for the very first time. Secondly, we also need to ensure that the "purity" of the event. According to the event study analysis, we need to ensure that the species involved firms are not "polluted" by other events, e.g., the merge or acquisition. Finally, in order to ensure that the whole process of event analysis and regression analysis is in a controlled and unified external environment, we only selected listed companies in China as the research object in this study. Moreover, we only selected the security events directly related to the enterprise information systems, regardless of the chain reaction caused by other management problems and financial problems.

EVENT STUDY ANALYSIS

Model Construction

Event study can illustrate the impact of emergencies on financial markets in the short term. Its premise is that the market is rational, so the financial market will give feedback on some abnormal events in the short term. This study adopts an event study approach to study whether information system security events will have a short-term negative impact on companies' stock returns (Mackinlay, 1997). In the analysis of event study, event collections, event announcement dates, event window will be determined, and abnormal return during this period will be estimated to observe events' impact. Regression analysis will be conducted between the market index and firms' actual returns.

In this study, events of interest are information system security events in firms. The time period during which we observe events is the event window. The shortest event window is one day. The first day of the event window is the day of the event, called day 0. Similarly, day *t* is the *t*-th day after the event, and day *-t* is the *t*-th day before the event. This study sets the one-day event window for two reasons: (1) A shorter event window can exclude other possible contamination events; (2) A shorter event window would lead to more convincing statistical test results (Buigut & Kapar, 2020). We also need to define the post-event window (from day *0* to day *n*) to demonstrate the events' continuous impact. This study will observe the abnormal returns of the nine trading days after the event. In order to avoid the pre-event leakage, it is necessary to set the pre-event window (from day *-1* today *-m*). When calculating the expected return, we will exclude the data in the pre-event window to ensure the stability of the results (Mackinlay, 1997). This study sets $m = 16$. In addition to these three windows, we also need to determine the estimated window to calculate the relationship between the company's stock returns and the market index.

Expected Returns

The expected return of the involved company can be predicted based on the performance of the involved company's stock price gains within the estimation window. Expected income is also called normal income and is the income of involved enterprises under normal circumstances or in the absence of an enterprise information system security event. In order to clarify this normal state, a linear regression method is used to establish a linear relationship with the market index by using the historical return of the company's stock in the estimation window. Using this linear model, we can relatively accurately estimate the expected income of the involved enterprise within the event window. Therefore, the length of the estimation window determines the accuracy of the expected return calculation. Regarding the estimated window length, the window period should not be too long, which will include other events in the estimated window that may affect the stock price of the involved company. The estimation window should not be too short, which may lead to the problem of the small size of data collection (Hendricks & Singhal, 1996).

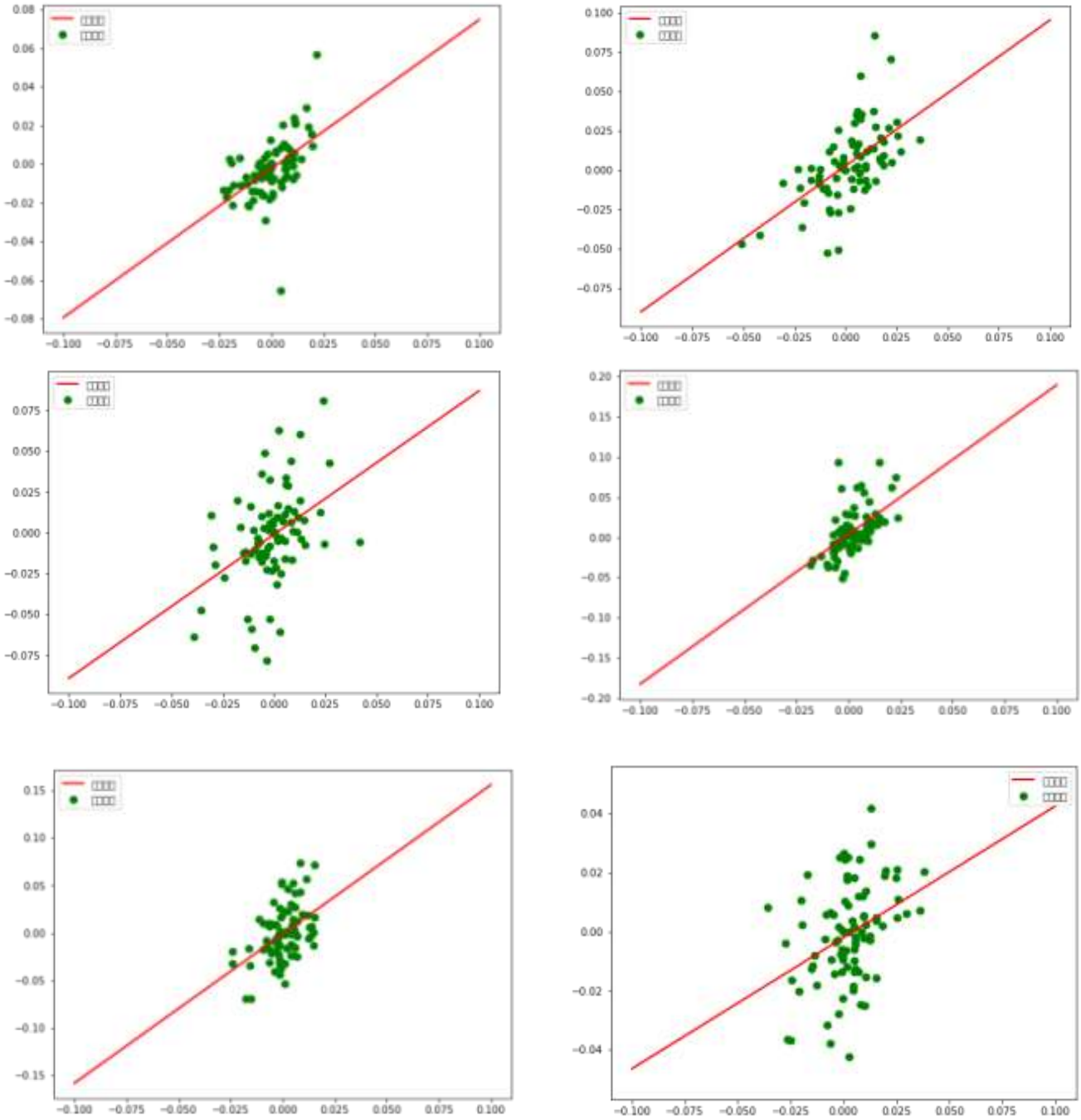
Market Model

To estimate the expected benefits, this research adopts the Market Model. The important assumption of the market model is that there is a stable linear relationship between the market index and the company's stock returns. The market model can exclude external factors from market returns. These external factors are more sensitive to the stock price of a specific company and can also enhance the convincing power of statistical test results (Benninga, 2014). When there are historical data references for the corresponding survey indicators, the market model can establish a more reliable expected return calculation framework. In the following, we will first introduce how to use the market model to estimate expected returns and use the expected returns to calculate the extraordinary returns of the event window. Then, we also conduct a hypothesis test and a sign test for the cumulative abnormal return (CAR).

In the market model, we must first establish the linear relationship between the market index and the actual income of the company in the estimation window. This linear relationship is as follows:

$$R_{k,t} = \alpha_k + \beta_k R_{m,t} + \varepsilon_k \quad (1)$$

where *k* is the event ID of the research subject, *t* is the trade date. $R_{k,t}$ is the actual stock return of the involved company in event *k* at day *t*. $R_{m,t}$ is the market index on day *t*. α_k and β_k are the parameters. Figure 1 demonstrates the linear fitting results in some event estimation windows.



Source: This study.

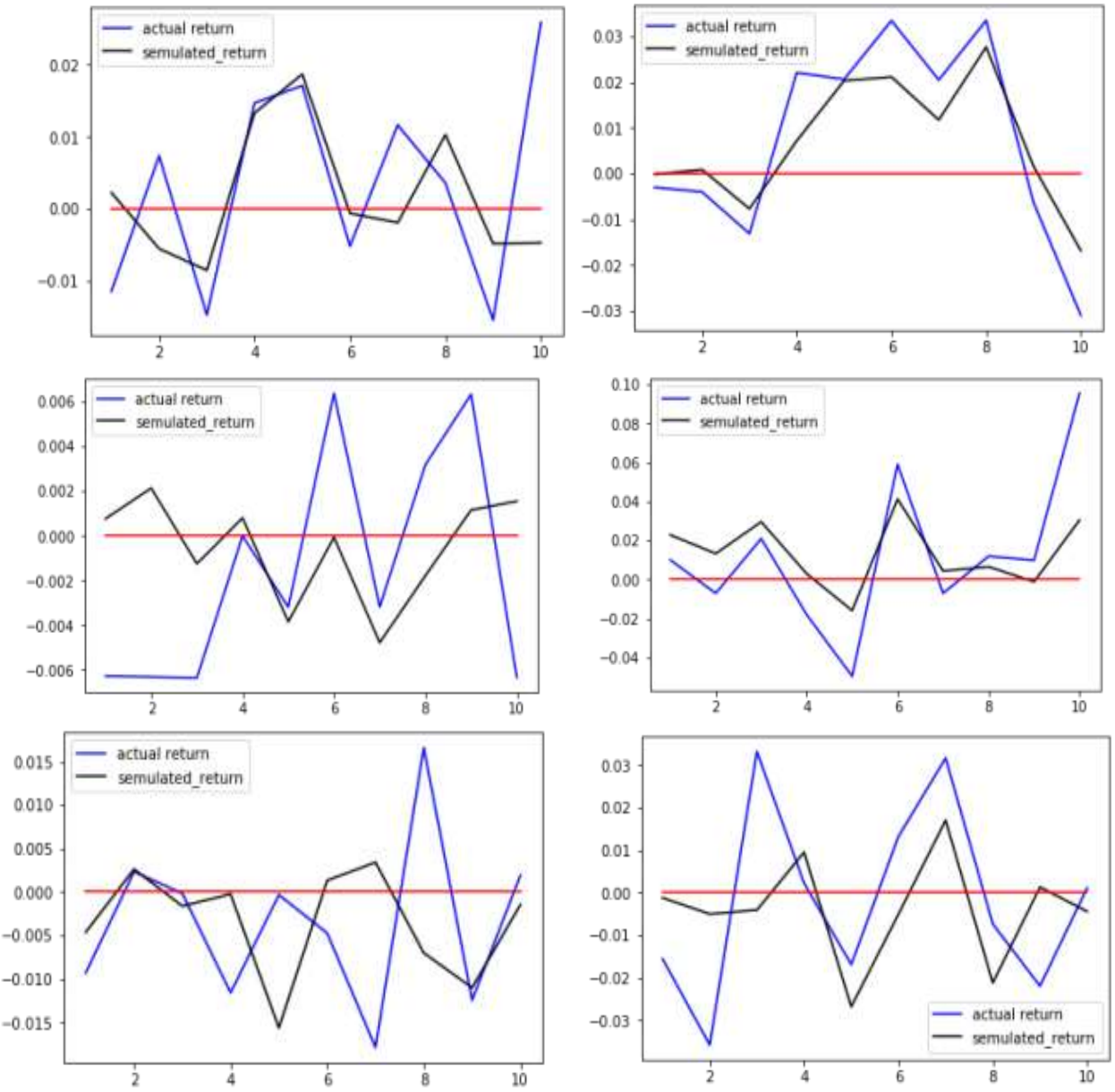
Figure 1： Linear fitting results in the event estimation window

Then we can use the estimation event window to calculate the expected return in the post-event window using Equation (2).

$$E(R_{k,t}) = \widehat{\alpha_k} + \widehat{\beta_k} R_{m,t} \tag{2}$$

In the equation, $\widehat{\alpha_k}$ and $\widehat{\beta_k}$ represent the parameters obtained by OLS. $E(R_{k,t})$ Represents the expected income or normal income of the involved company in event *k* at day *t*. Abnormal return is the difference between actual return and expected return as in equation (3).

$$AR_{k,t} = R_{k,t} - E(R_{k,t}) \tag{3}$$



Source: This study.

Figure 2: Event excess return and expected return

To evaluate the total impact of information security events on the stock price of the involved company, we also calculated the Cumulative Abnormal Return for event *k* and all events, as in equation (4).

$$CAR_{k,t} = \sum_t AR \tag{4}$$

where $CAR_{k,t}$ represents the total abnormal return from day *0* to day *t* for event *k*.

$$CAR_t = \sum_N \sum_{day\ t} AR \tag{5}$$

We use the probability distribution of the residual in equation (1) to represent the probability distribution of the cumulative abnormal return *CAR*, so the probability distribution of *CAR* can be formulated as:

$$CAR_t \sim N(0, \sigma_{\varepsilon_t}^2) \tag{6}$$

Thus, the test statistics *t_statistics* used for hypothesis testing is:

$$\text{t\_statistics} = {}^{\text{CAR}_t}\Big/_{\widehat{\sigma_{\varepsilon_t}}} \tag{7}$$

Then, we present the result of the *t*-test and abnormal returns in the following table.

Table 1: AR and CAR Descriptive Analysis

Day	0	0 to 1	0 to 2	0 to 3	0 to 4	0 to 5	0 to 9
CAR	-0.43	-0.59	-0.51	-0.52	-0.45	-0.36	-0.63
t_statitic	-7.4***	-8.0***	-5.2**	-4.4**	-3.81**	-2.63*	-2.12*

Source: This study.

In the null hypothesis, the test statistic is 0. The large enough t-statistic or the small enough p-value can reject the null hypothesis. We noticed that *CAR* from day *0* to day *nine* is negative. After day 1, *CAR* began to weaken, but this is not a stable trend. For example, on day 9, the cumulative abnormal return is even larger than day 0 and day 1. From a statistical point of view, on day 0 and day 1, the cumulative abnormal return was obviously negative, and it was significant at the level of $p<0.05$. On days 2, 3, and 4, the cumulative abnormal return is still statistically significant at the level of $p<0.1$, but the significance has begun to decrease compared with that on days 0 and day 1. After day 5, although the cumulative abnormal returns are still less than 0, they are not statistically significant. We also use the Wilcoxon signed-rank test to test the sign of the cumulative abnormal return CAR without considering the absolute value of the cumulative abnormal return. We found that the proportion of cumulative abnormal returns less than 0 in the event window is about 63%, which is greater than 50% which is required in the sign test. Therefore, we believe that the sign of cumulative abnormal returns is statistically significantly negative (Fagerland & Sandvik, 2009).

REGRESSION ANALYSIS

This paper defines the regression model as:

$$AR_k = \alpha X_{i,1} + \beta X_{i,2} + \cdots\cdots \gamma X_{i,n} + \varepsilon_i \quad (8)$$

AR_k represents the abnormal return caused by event *k*. $X_{i,n}$ represents independent variables, which can represent *n* factors related to enterprise information system security events. α, β, γ represent the coefficients that needed to be determined in the regression analysis. Independent variables are shown in Table 2.

Table 2: Description of Independent Variables

Variables Type	Variable Name	Variable Description
Independent Variables	*Com_Size*	The volume of the company refers to the size of the company involved.
	Com_Div	This indicator can evaluate the degree of diversification of the company involved.
	Com_Comp	Market competition environment
	Com_GR	Revenue growth rate
	Com_Response	Companies' Response to events. When enterprise information system security events are publicly released, the involved companies may respond to these events, and of course, they may not respond and ignore these events.
	Event_Type	Types of security events in enterprise information systems
	Event_Security	The severity of security events in enterprise information systems
	Event_Dispose	Involvement of national regulatory agencies
Control Variables	*Channel*	Media platform and data source for an event release
	Year	The time span for the event to be published
	Industry	The industry classification for the events

Source: This study.

Regression Analysis Result

In the regression analysis, we calculated the correlation coefficient between each variable and the abnormal return and verified its statistical significance. We also calculated the R^2 and p-values of the entire regression model. The R^2 of the regression model is 37%, which is sufficient to explain the abnormal returns of the regression model. The p-value (0.0008) of the whole regression model is low enough (Gabaix & Ibragimov, 2011). It can be seen from Table 3 that enterprise characteristics, enterprise response, and event attributes can adjust the losses caused by information system security events.

Regarding the nature of the event, we found that the disposal of the national regulatory authority has the largest negative impact on the market value of relevant companies. When the national regulatory authorities take some punitive measures, the market value of the involved company will lose 1.4% more. We also found that the type of event and the severity of the event will also cause greater losses after the event, but the correlation coefficient of these two factors is not very significant in our model. We retain our views on the relevance of these two factors and excess returns. Our preliminary analysis suggests that the possible reason is that domestic streaming media platforms still have doubts about the accuracy and objectivity of corporate information system security event reports.

Regarding the response of the company, we found that if the involved company can make a positive response in a timely manner, the loss of its market value can be reduced. We found that the correlation coefficient of Response is 0.014, which means that companies that have not responded to the event or even ignored the event will suffer from an additional 1.4% market value less than those that have responded positively.

Table 3: Regression Analysis Result

Classification	Variables Simple Description	Variables Name	Coefficient
Involved Companies' Characteristics	Market Competitive Environment	*Com_Comp*	-0.087**
	Revenue Growth Rate	*Com_GR*	-0.010
	Diversification	*Com_Div*	-0.007
	Asset volume	*Com_Size*	-0.005***
	Response	*Com_Response*	0.014***
Information Security Events' Attributes	Event Type	*Event_Type*	-0.002**
	Event Security	*Event_Severity*	-0.001*
	National Regulatory Agencies' Involvement	*Event_Dispose*	-0.014**
Control variables	Medial Platform and News Channels	*Channel_Sina*	-0.002
		Channel_People Daily	-0.012*
		Channel_Guang MingDaily	-0.008
		Channel_Xinhua	-0.007
		Channel _CCTV	-0.028**
	Industry Classification	*Industry_Finance*	-0.039*
		Industry_Internet	0.003
		Industry_Other	-0.006
	Year	*Year_2018*	0.005
		Year_2019	-0.002
		Year_2020	-0.006**
		Year_2021	-0.012***
P_VALUE	0.0008		
R^2	0.37		

Source: This study.

For the control variables, we found that the absolute value of the Year correlation coefficient showed an upward trend from 2018 to 2021. The level of statistical significance is also increasing. This shows that investors, markets, and customers are more sensitive to changes in corporate information system security events over time. From the perspective of the industry characteristics, in the financial industry, information system security events will cause greater losses, and the significance level of *Industry_Finance* is also significantly better than the other two in Industry. This shows that the financial industry has an impact on information system security events.

CONCLUSION

This research finds enterprise information security events can cause serious negative impacts on involved firms: a loss of 1.93% of its market value or a loss of $69 million, which are equivalent to the revenue from a certain product line for some enterprises. Thus, it is extremely necessary for companies to pay much attention to their information security investment.

First, large companies in financial service with large volumes need to pay such special attention. In our event data collection, we find that security events in enterprise information systems often bring greater blows to financial service companies. Financial service companies often have relatively bigger asset volumes which will amplify this negative impact. The possible reason is that users and customers of financial service companies are often very sensitive to information security, and their tolerance for such security events is relatively low. Besides, the financial service is not a must for most people. Therefore, once such events occur, users will terminate or abandon the corresponding financial products and services in a very short time.

Secondly, companies need to always pay attention to the corresponding industry dynamics and market operations, and they need to analyze the company's user profile in a timely manner. The switching cost and the user stickiness will greatly affect the losses caused by enterprise information system security events. When user stickiness and switching costs are lower, users will have more choices, and it is easier for them to switch to other companies due to information system security events. Therefore, when an enterprise is in a more competitive market, or its market share has increased substantially in a short period of time, this may mean weaker user stickiness, and the enterprise needs to be more sensitive to information security.

Finally, we find the security state of enterprise information systems is gradually increasing the impact of events. This may be because data and data-related services carry greater commercial value. Often information data is linked to assets, value, and

personal credit. Therefore, with the improvement of information development, especially in some special periods (social emergencies), users will increase their attention to information security, and enterprises should also increase investment in information security.

If the enterprise can provide timely feedback on the enterprise information system security incident, associated firms' loss will be alleviated. On the contrary, if the involved company does not give a reasonable explanation or violates the relevant regulations of the national regulatory agency, it is very likely to cause more serious and bad consequences. Firms are encouraged to explain the incident in a timely manner considering the actual situation after the incident occurs. We believe that it is preferable for the enterprise to self-check the internal process first. If the cause of the incident is the loopholes in the internal control process and the defect of the management model or for problems leftover from system design, companies should acknowledge their mistakes in a timely manner, release patches as soon as possible, minimize user losses, and avoid violating national laws and regulations and causing worse impacts. If, after investigation, it is found that the cause of the incident is an external factor, such as the system supplier's version update is not timely, hacker attacks, etc., the company should also actively respond. After completing the public relations, contact the police in time for filing and forward the vulnerability to CNNVD. Companies are also encouraged to establish a professional, independent information system security emergency response team.

ACKNOWLEDGMENT

This research is supported by grants from the National Natural Science Foundation of China (Grant 71801014), Beijing Social Science Foundation (Grant 17GLC069).

REFERENCES

Benninga, S. (2014). Financial modeling, fourth edition. *ProQuest Ebook Central* https://ebookcentral.proquest.com

Buigut, S., & Kapar, B. (2020). Effect of qatar diplomatic and economic isolation on GCC stock markets: An event study approach. *Finance Research Letters*, 37, 101352. https://doi.org/10.1016/j.frl.2019.101352

Fagerland, M. W., & Sandvik, L. (2009). The Wilcoxon–Mann–Whitney test under scrutiny. *Statistics in Medicine*, 28(10), 1487-1497. https://doi.org/10.1002/sim.3561

Gabaix, X., & Ibragimov, R. (2011). Rank− 1/2: A simple way to improve the OLS estimation of tail exponents. *Journal of Business & Economic Statistics*, 29(1), 24-39.

He, P., Sun, Y., Zhang, Y., & Li, T. (2020). COVID–19's impact on stock prices across different sectors—An event study based on the Chinese stock market. *Emerging Markets Finance and Trade*, 56(10), 2198-2212.

Hendricks, K. B., & Singhal, V. R. (1996). Quality awards and the market value of the firm: An empirical investigation. *Management Science*, 42(3), 415-436. https://doi.org/10.1287/mnsc.42.3.415

Holzmann, G. (2001). Economics of software verification. In Proceedings of the 2001 ACM SIGPLAN-SIGSOFT workshop on Program analysis for software tools and engineering (pp 80-89). https://doi.org/10.1145/379605.379681

MacKinlay, A. C. (1997). Event studies in economics and finance. *Journal of Economic Literature*, 35(1), 13-39.

Shishkov, B., & SpringerLink (Online service). (2020). Designing enterprise information systems: Merging enterprise modeling and software specification (1st 2020. ed.). *Springer International Publishing*.

Telang, R., & Wattal, S. (2007). An empirical analysis of the impact of software vulnerability announcements on firm stock price. *IEEE Transactions on Software Engineering*, 33(8), 544-557. https://doi.org/10.1109/TSE.2007.70712