

Article

A Pilot Study to Assess the Effects of News Coverage Articles about Security Incidents on Stock Prices in Korea

Se-Hyeon Han 

School of Media Communication, Hanyang University, Seoul 04763, Republic of Korea; han382@gmail.com

Abstract: This study was conducted to assess the effects of security incidents on the stock prices of firms in Korea. A content analysis of news coverage articles about security incidents was performed. The research questions (RQs) of the current study were as follows: RQ1: this study evaluated whether the news coverage of a security incident can influence an investor's decision to buy or sell a stock; and RQ2: the study also analyzed whether the type of industry, the amount of damage caused by the incident, and the specific security incident itself would affect how investors assessed a stock's value. The results of the study indicate the following: (1) news coverage articles about security incidents have a significant effect on stock prices; and (2) the degree of such an effect varies depending on the tone, theme, and category of the news coverage. A more negative tone was associated with a decrease in stock prices. Less negative and neutral tones were associated with an increase in stock prices. In particular, a neutral tone was associated with an increase in stock prices, which was commonly seen in most of the firms experiencing security incidents. Furthermore, the number of news coverage articles about security incidents had no relationship to variations in stock prices. In firms experiencing security incidents, variations in stock prices varied depending on the types of industry, the types of damages, and the type of incident. In conclusion, the current study used an event study and a content analysis of news coverage articles about security incidents to assess their effects on the stock prices of firms. Further studies are warranted to establish the feasibility of this approach in a real-world setting.



Citation: Han, Se-Hyeon. 2023. A Pilot Study to Assess the Effects of News Coverage Articles about Security Incidents on Stock Prices in Korea. *Journal of Risk and Financial Management* 16: 425. <https://doi.org/10.3390/jrfm16100425>

Academic Editor: Thanasis Stengos

Received: 21 June 2023

Revised: 5 September 2023

Accepted: 14 September 2023

Published: 25 September 2023



Copyright: © 2023 by the author. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

Keywords: information and communication technology; firm; stock price; security incidents; damages

1. Introduction

To date, information and communication technology (ICT) has an integral role in the management of firms. ICT has provided benefits to society, although it has become vulnerable to failures and attacks. The increasing dependency of a firm on ICT has greatly increased its vulnerability to threats made to ICT (Dias Canedo et al. 2020; Sadiq et al. 2022; Masip-Bruin et al. 2021; Karaman Aksentijević et al. 2021). According to Ahmad et al. (2012), at some stage, a firm will suffer security incidents that may result in multiple negative impacts such as the loss of a company's reputation and customer confidence, legal issues, a loss of productivity, and direct financial loss. With the prevalence of ICT-based business operations, the frequency and severity of corporate cyber-attacks and security breaches has increased; therefore, information security has become a crucial concern for firms (Kankanhalli et al. 2003). Appropriate measures can be taken against the possible occurrence of security incidents, although the complete protection and safety of ICT systems is not economically feasible. Moreover, it is known that the cost to establish the right security measures at the outset is far lower compared with that required to recover from a security incident (Grigaliūnas et al. 2023).

In cases of potential threats to a firm's operations due to security incidents and the resulting damages, such as legal costs and negative effects on its reputation, it is mandatory that investors understand the mechanisms by which such incidents could affect a firm's

future performance; this is essential for making well-informed investment decisions (Perera et al. 2022; Kitsios et al. 2022; Chang et al. 2020).

Media coverage about security incidents or breach announcements that are typically found in major media outlets or blog posts serve as the primary information sources for investors. Differences in terminology and other characteristics between news coverage articles about security incidents may affect investors' perceptions of the impact of the breach. That is, such articles may contain either specific or ambiguous terminologies, which may cause different reactions in investors. Moreover, diverse types of security incidents may have diverse implications for the affected firm (Wang et al. 2013).

To date, financial studies have focused on the role of media coverage on security incidents in capital markets, including on stock prices in particular (Dyck et al. 2008; Joe et al. 2009).

Given the above background, this study was conducted to assess the effects of security incidents on the stock prices of firms. An event study and a content analysis of news coverage articles about security incidents were performed. The research questions (RQs) of the current study are as follows:

RQ1: This study evaluates whether the news coverage of a security incident can influence an investor's decision to buy or sell a stock.

RQ2: The study also analyzes whether the type of industry, the amount of damage caused by the incident, and the specific security incident itself can all affect how investors assess a stock's value.

The current study is composed of five chapters: Section 1, Introduction; Section 2, Literature review; Section 3, Materials and methods; Section 4, Results; and Section 5, Discussion and conclusions.

2. Literature Review

2.1. A Content Analysis

A content analysis is a methodology used to collect and analyze data using diverse tools; it is useful when analyzing the text information from an interview, a questionnaire survey, and the news (Kondracki et al. 2002). According to Kassarjian (1977), content analysis can be performed to reconfigure the content collected for particular purposes and to establish criteria for minimizing a bias between authors. Moreover, it is useful for easily addressing questions that cannot be resolved using a quantitative analysis (Holdford 2008).

A content analysis can be applied for diverse purposes. Kolbe and Burnett (1991) reported that it is useful for not only obtaining a definite understanding of specific events but also for grasping follow-up news coverage articles, which is essential for identifying the causes of a security incident and thereby estimating the degree of its seriousness. Moreover, it is also useful for drawing conclusions through an analysis of the text of news coverage articles and statistics reports (Bos and Tarnai 1999). An and Gower (2009) noted that news coverage articles about incidental crises had a tendency to emphasize the effects of the spread of economic damage, the social crisis of a firm, and its delinquency due to a lack of accountability. According to these authors, it is mandatory for a firm to be prepared for the prevention of an incident, risk management, and a follow-up plan (An and Gower 2009). News coverage articles about security incidents focus on the delinquency of firm. It is highly probable that security incidents caused by the employees of a firm might directly impair its reputation. An and Gower (2009) reported that a content analysis of news coverage articles about a security incident is useful for not only identifying its causes but also for determining the scope of the resulting damages and its causal relationship with the stock prices of a firm.

The current study used a content analysis of news coverage articles about security incidents, as proposed by Holdford (2008).

2.2. An Event Study

An event study is a popular methodology that is advantageous for analyzing variations in stock prices from various aspects, measuring alterations in market reactions, and estimating the scale of future damages (Maqsood et al. 2022; Škrinjarić 2019). It is therefore useful for resolving limitations in collecting data about security incidents (Chang et al. 2020; Kim et al. 2020). Moreover, event studies have also been used to objectively measure damages due to security incidents resulting in alterations in the stock prices of a firm (Chang et al. 2020; Ali et al. 2021; Hung 2019; Ban et al. 2023; Moreno et al. 2020; Andrade et al. 2022). Thus, it can be used to perform a quantitative analysis of the negative effects of security incidents on the stock prices of a firm, although there is a limitation in its applicability in identifying the definite causes of decreased stock prices. To overcome its limited applicability, previous studies have been conducted to measure the degree of interaction between the negative content of news media coverage and the decreased stock prices of a firm (Tetlock 2007; Tetlock et al. 2008; Aman 2013).

An event study is rooted in the financial theory that is used to assess the effects of disclosure on the stock prices of a firm, such as dividends, capital increases with consideration, mergers and acquisitions, and earnings announcements. It is applied to areas such as finance, economics, organization, strategy and marketing. It is therefore widely used to measure the degree of the effects of an unpredictable event on variations in the expected profitability of a firm (Brown and Warner 1980) It is also a methodology based on an efficient market hypothesis proposed by Fama et al. (1969) stating that an unpredictable event will have a direct effect on stock prices if it affects the present or future profits of a firm. As shown in previous studies measuring the effects of security incidents on the stock prices of a firm (Bharadwaj et al. 2009; Konchitchki and O’Leary 2011; Cavusoglu et al. 2004; Hovav and D’Arcy 2005; Kannan et al. 2007; Bose and Leung 2013), an event study is a useful methodology to measure variations in the market price of a firm. Moreover, it is also useful when analyzing the effects of security incidents on the stock prices of a firm depending on the type of security incident and the scale of a firm. In more detail, Campbell et al. (2003) reported that there was a 1.9% decrease in the stock prices of a firm whose secret information was leaked. Cavusoglu et al. (2004) reported that smaller firms were more vulnerable to decreased stock prices as compared with larger ones. It has also been reported, however, that security incidents, such as system paralysis due to a distributed denial of service (DDoS), had no effects on the stock prices of a firm (Campbell et al. 2003; Hovav and D’Arcy 2003). Table 1 summarizes the previous studies analyzing variations in the stock prices due to security incidents based on the duration and incidence of security incidents and cumulative abnormal returns (CAR).

Table 1. Quantitative studies on security incidents.

Year	Authors	Period	N	Events Window (Day)	CAR
2002	Cavusoglu et al.	1998–2000	66	[0, 1]	−2.10%
2003	Campbell et al.	1995–2000	43	[−1, 1]	−1.90%
2005	Hovav & D’Arcy	1998–2002	186	[0, 25]	−0.1~−0.01%
2006	Ko & Dorantes	1997–2001	19	[−365, 365]	N/A
2007	Kannan et al.	1997–2003	41	[−1, 1]	−5.00%
2009	Bharadwaj et al.	1990–2000	213	[−1, 0]	−2.00%
2009	Goel & Shawky	2004–2008	168	[−2, 1]	−1.00%
2013	Bose & Leung	1996–2012	87	[0, 1]	−0.63%
2014	Pirounias et al.	2008–2011	105	[−1, 1]	N/A

Note: N, the number of events; N/A, non-applicable. Abbreviation: CAR, cumulative abnormal return.

2.3. Usefulness of News Coverage Articles about Security Incidents

News coverage plays a role in promptly providing top news stories of a specific industry for stakeholders, thus serving as an information source (Luyckx and Paulussen 2022). The widespread use of Internet news media and activated social network media has prompted the generation, progression, and transmission of information (Pabian and Pabian 2023; de la Garza Montemayor and Pineda Rasgado 2023). Negative news coverage articles about security incidents provide overall information about its actual causes and the social responsibility of a firm to the public (An and Gower 2009). Therefore, the results of the interpretation of psychological alterations of an investor based on news articles are applied to the identification of causes of variations in stock prices (Tetlock 2007).

There are also reports that the stock prices of a firm vary depending on the news coverage articles about security incidents. It has also been argued that qualitative contents of news coverage articles are not sufficient for explaining variations in stock prices that are subject to macro-economic events (Cutler et al. 1989). Negative news coverage articles are classified as 3 tones: ‘Pessimistic’, ‘Negative’ and ‘Weak’. Thus, it has been shown that pessimistic news coverage articles had a significant effect on stock prices (Tetlock 2007; Tetlock et al. 2008). In addition, Aman (2013) also reported that positive news coverage articles had no significant effects on stock prices but showed that negative coverage had a significant effect on lowering stock prices. Until recently, there has been no widespread recognition of the actual effects of news coverage articles about security incidents on the stock prices of firms. Moreover, little is known about the definite causes affecting stock prices. Therefore, the current study used both a content analysis of news coverage articles about security incidents and an event study, thus attempting to identify the factors involved in variations in stock prices.

3. Materials and Methods

3.1. Study Design

In the current study, three methodologies were used to assess the effects of news coverage articles about security incidents on variations in stock prices (Figure 1).

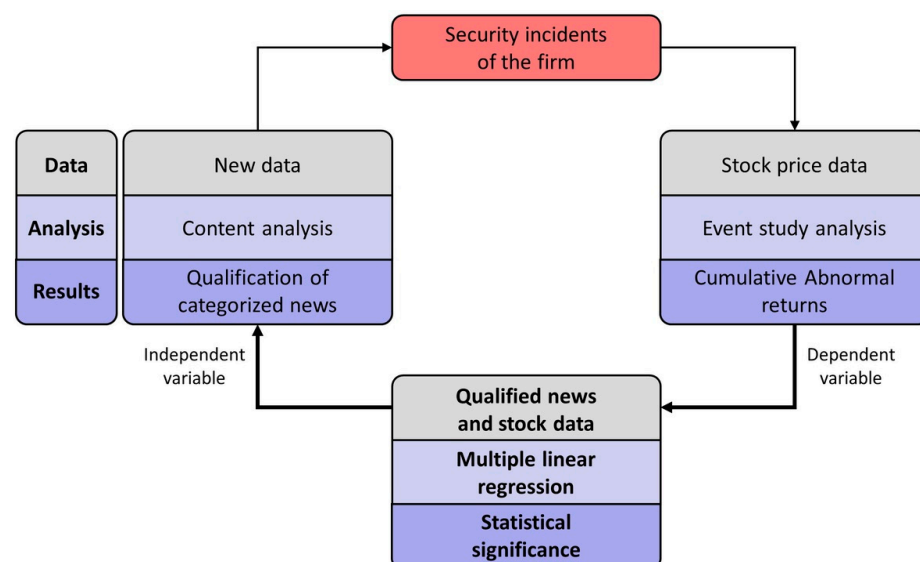


Figure 1. Study flowchart.

First, both a content analysis and a quantitative analysis were performed to evaluate news coverage articles about security incidents. Second, an event study was conducted to estimate the CAR of a firm and to measure variations in its stock prices. Then, the results of a content analysis of news coverage articles and those of an event analysis of stock prices served as an independent variable and a dependent variable, respectively. This was

followed by a multiple linear regression analysis to test the statistical significance of the effects of news coverage articles about security incidents on stock prices.

3.2. Data Collection

To make an accurate definition of the term security incident, the current study used criteria for determining the definition based on the types of threat factors classified by Loch et al. (1992) and Jouini et al. (2014), such as internal/external threat and incidental/deliberate threat.

News coverage articles about security incidents were searched using a news search engine, BIGKINDS (News Bigdata and Analysis, www.bigkinds.or.kr (accessed on 3 May 2023)), hosted by a reliable news service provider for a variety of media, the Korea Press Foundation. Thus, one representative news coverage article about a security incident was collected. Keywords for searching news coverage articles about security incidents included ‘Hacking’, ‘Cyber attack’, ‘Internet infringement’, ‘Breach’, ‘Privacy’, ‘Industrial technology leakage’, ‘Phishing’, ‘Malicious code’ and ‘DDoS’.

If there was a multitude of news coverage articles about a security incident, an article with the known date of the first publication was selected. Moreover, if a single security incident occurred in a multitude of firms, all of them were included in the analysis. Thus, attempts were made to evaluate their effects on stock prices of each firm. If there were damages to a multitude of firms due to the occurrence of a security incident, all the events were considered as independent not only because there was a variability in the degree of damages but also because variations in stock prices were measured for each firm.

News coverage articles about security incidents were used to finally screen firms, as summarized in Table 2.

Table 2. Inclusion and exclusion criteria.

Table Cont.	N1	N2
An initial set of news coverage articles about breach or attack of firm’s information security	251	184
Public organizations or multi-national firms	153 (−98)	89 (−95)
Non-listed or merged firms	57 (−96)	74 (−15)

Note: N1, the number of excluded news coverage articles; N2, the number of excluded firms.

The duration of the occurrence of the security incidents in each firm ranged between 2013 and 2021. Of a total of news coverage articles about individual cases of security incidents published in the media during this period, 98 (47 with unidentified and unknown firms and 51 with an obscure time point of occurrence and scope of damages) and 77 (51 public organizations and 26 multi-national firms that are not listed on the Korean stock market) were excluded. Non-listed firms (16) and merged firms (3) were also excluded. Thus, 74 listed firms that corresponded to 57 news coverage articles about security incidents were analyzed. In news coverage articles about a single security incident, a multitude of firms experiencing damages were included. Therefore, the number of firms was larger by 17 as compared with that of news coverage articles.

A total of 54 news coverage articles of 74 firms were searched from the BIGKINDS. By a single security incident, the first reported news coverage articles were selected. To collect follow-up news coverage articles by each security incident, searching was performed for the NAVER (<http://www.naver.com> (accessed on 3 May 2023)), one of the biggest portal sites in Korea. Thus, a total of 1016 news coverage articles were collected. That is, BIGKINDS selected representative news coverage articles that are appropriate for criteria of security incidents in the current study. In the NAVER news, representative news coverage articles were enlarged or followed up. Thus, news coverage articles were collected and then identified. Duplicate news coverage articles were excluded. This two-stage collection of news coverage articles is a useful method for filtering unconfirmed news coverage articles

about security incidents among Internet news media. The period of news publications ranged between Day + 0 (the first date of the publication of news coverage articles about the security incident) and Day + 5, during which the relevant articles were collected. After the date of the first date of the publication of news coverage articles, there was a pattern of smooth decrease in stock prices until Day + 1. This period was determined to be that of a multiple regression analysis. During a period ranging from Day + 3 to Day + 5, the trend of changes in news coverage articles about security incidents was analyzed. New coverage articles collected based on these criteria are summarized in Table 3. Listed firms were registered with the Korea Composite Stock Price Index (KOSPI) and Korea Securities Dealers Automated Quotations (KOSDAQ), whose information was collected using the Korea Exchange (KRX).

Table 3. Inclusion and exclusion criteria for selecting news coverage articles.

Inclusion and Exclusion Criteria	N1	
	N2	N3
Collected news coverage articles about security incidents	N/A	1016
Collected news coverage articles whose publication date was five days after the first article	106	910
News coverage articles about multiple cases of security incidents rather than a specific one, particularly including editorials or columns and short ones with less than two paragraphs, those with a single news media. In these cases, the possibility of selection bias cannot be completely ruled out	69	841
News coverage articles, where a total of two days had elapsed since the date of its first publication, determined to be eligible for a statistical analysis of data	136	705

Note: N1, the number of eligible news coverage articles; N2, the number of excluded news coverage articles; N3, the number of eligible news coverage articles; N/A, non-applicable.

3.3. Methods of Analysis

3.3.1. Content Analysis of News Coverage Articles about Security Incidents

With regards to criteria for collecting data, keywords *as well as* online keyword search tools were defined for the collection of news coverage articles. To clarify the above criteria, the relevant keywords were applied to the selection of news coverage articles that were appropriate to them. Thus, attempts were made to minimize errors and burdens when collecting the news coverage articles. News coverage articles are composed of a paragraph consisting of several sentences combined with another several ones. For a content analysis, the content should be reconfigured by setting a minimal unit for an analytical procedure. Therefore, unit of analysis was defined based on a paragraph and then coded. The title, running head and the images embedded in its text are major expressions that were already included in its main body; these were therefore excluded from the analysis.

Based on the contents of the news coverage articles collected, the information for the analytical procedure was composed of the name of firm experiencing the security incident, the unique ID for the identification of the firm experiencing the incident, the date of the news publications, their contents and their uniform resource locators (URL). Upon completion of the coding based on the above information, a relevant category was determined. Each category was combined using a single category. In addition, each theme was provided with a tone that best matched it. To describe the results of the content analysis performed in the current study, 12 categories were created with four theme subcategories that included the delinquency of the firm, additional damages and resulting losses, AIR and the mentioning of damages. Each theme was further classified into three tones: ‘More negative’, ‘Less negative’ and ‘Neutral’. Table 4 provides a detailed description of the meaning of each variable.

Table 4. The analysis of tone, theme, and categories from news coverage articles about security incidents.

Theme	Tone Coverage	Category	N
A. Firm Fault	More negative	A1 Occurrence of security incident due to an insufficiency in firm’s security management	145
		A2 Recurrence of security incident	62
		A3 Inappropriate follow-up measures against security incident	35
B. Additional Damages and Loss		B1 Concerns for direct or indirect damages due to security incident	155
		B2 Statement about potential damages (e.g., concerns for additional damages)	56
		B3 Statement about the possibility of the enlargement of the scale of damages	23
C. Damage Mention	Less negative	C1 Statement about a leakage of personal information, the corresponding firm, and the scale of the resulting damages	664
		C2 Statement about damages and losses incurred by clients	215
		C3 Hacking and exploration technologies used for security incident	123
D. Aggressive Incident Re-sponse	Neutral	D1 Statement about the facts related damages and the progression of follow-up measures against it	287
		D2 Statement about formal apology, follow-up measures against security incident, and compensation plans	151
		D3 Statement about the methods for confirming damages and preventing them	19
Total			1935

Note: N, the number of analysis units.

Keywords and online keyword search tools, and news coverage articles about a firm experiencing a security incident were collected based on a unit of analysis. Then, news coverage articles about security incidents were coded based on the relevant category. A coding of collected news coverage articles is a process where the theme and category are persistently created or combined. With regards to a single security incident, a multitude of news coverage articles were identified. Considering an event study based on time-series data and the convenience of analysis, coding was performed in the order ranging from the first news coverage articles about each security incident to the latest one.

Reliability testing was the method used for securing the consistency and objectivity of the results in the coding of news coverage articles about security incidents. Of the total news coverage articles, 10% were selected as a sample. There should be a more than an 80% match between the results of the coding, performed by two investigators. It was determined that reliability can be secured using this method (Lacy et al. 2015). Two investigators were therefore appointed as secondary coders and then trained for approximately two hours. This was followed by the preparation of the coding sheet. Holsti’s reliability coefficient was used, as proposed by An and Gower (2009). Until the overall average agreement rate exceeded 80%, criteria were established in a stepwise manner, and reconfiguration of the news coverage articles, and collection and coding of the sample data were repetitively performed, as previously proposed (Lacy et al. 2015). The current study showed an overall average agreement rate of 86%; this corresponds to a good level of agreement.

After the coding of the results of the content analysis, the number of paragraphs, serving as the minimal unit of analysis of news coverage articles about security incidents, was summed and then quantified for a regression analysis in comparison with the results

of the event study. The paragraph forming the main body of a single news coverage article was assigned with a 1 if it corresponded to the category, a single news coverage article was assigned with a 1 based on a multitude of the relevant categories. In two paragraphs sharing the same theme, duplicate sharing was permitted for the category. For a single security incident, a regression analysis was performed in comparison with the information about stock prices seen on an event study in such a manner that a value of 1 assigned to a multitude of news coverage articles was set as a sum of those of each category.

3.3.2. An Event Study of a Security Incident

In the current study, abnormal variations in stock prices due to security incidents were estimated using an event study. An earnings ratio of the daily stock prices for the estimation of the abnormal variation was used, based on the market model established by Fama et al. (1969). In the market model, after the estimation of the sensitivity of the corresponding item to the market earnings ratio, the normal one was calculated during the event period. In addition, the market model assumed that the current value of a firm is based on its assets and the flow of future predictable cash; this pretense was based on an efficient market hypothesis that the stock prices of a firm are directly reflected in the market.

The abnormal return (AR) was calculated by subtracting the daily normal earnings ratio, estimated based on the market model, from the actual earnings ratio during the event period. Moreover, it also estimated the CAR, a cumulative sum of AR, in each firm. Thus, it measured the effects of a specific incident on variations in stock prices serving as the value of the stock market prices of the corresponding firm. In an event study where the earnings ratio to the market factor ($R_{m,t}$) serves as an independent variable, the stock prices earnings ratio due to the unique factors of the corresponding firm ($R_{i,t}$) is reflected. $\beta_{i,t}$ is referred to as a sensitivity to the stock price earnings ratio of the corresponding firm. In addition, $\alpha_{i,t}$ is referred to as an earnings ratio of the corresponding item that can be expected at a market earnings ratio of 0. Furthermore, $\varepsilon_{i,t}$ is referred to as variations in stock prices due to unique factors. The normal earnings ratio before and after the occurrence of the security incident for the estimation of the abnormal one can be calculated as follows:

$$R_{i,t} = \alpha_i + \beta_i R_{m,t} + \varepsilon_{i,t} \quad (1)$$

$R_{i,t}$: Stock return of firm i on day t

$R_{m,t}$: Rate of return the market index on day t

α_i : Intercept for firm i

β_i : Slope for firm i

$\varepsilon_{i,t}$: Disturbance term for stock i on day t

$\beta_i R_{m,t}$ represents changes in the earnings ratio of stock i depending on those in the index of the total market. The error term is used to describe changes in the earnings ratio of a certain firm, i , which cannot be explained based on those in the total stock market, at the time of t . In addition, $\alpha_i + \beta_i R_{m,t}$ is referred to as an expected return that can be obtained when there is a persistent presence of the past performance before the occurrence of a certain security incident. The market portfolio earnings ratio, $R_{m,t}$, represents KOSPI or KOSDAQ, thus corresponding to the earnings ratio of a listed firm. The abnormal earnings ratio, AR, represents the degree of deviation from the range of errors of the predicted earnings ratio of a certain firm in the market model. The AR is used to calculate the profit that is deviated from the expectation due to the occurrence of a certain event based on the predicted variables in the market model (Campbell et al. 2003).

The estimation period for the determination of difference in the actual stock prices after the prediction of AR is commonly set at 100–300 days. In the current study, it was set at 200 days, as this is most commonly used. Thus, the estimation period prior to the occurrence of the security incident was estimated. To ensure that there were no effects related to the security incident, a total of –230 days, extending from –200 to –30 days before the date of the news publication, were determined to be the estimation period (Bose and Leung 2013). AR, serving as the prediction of errors, and CAR, the cumulative sum of

the event window of AR, and the mean CAR of a total of 74 events were then individually expressed, as previously described (Pandey and Kumari 2021):

The event window used for the analysis of the event is [0, 1]. Therefore, the date of the initiation of a CAR corresponds to 0 days before the date of the news publication (Day + 0). The date of the completion of a CAR corresponds to the following day of the date of the news publication (1 day) (Day + 1). Thus, the market reaction was analyzed during this period. The period of analysis is sensitive to the results. According to a review of the literature on event studies, as summarized in Table 1, the date of the initiation and completion were determined as the period of analysis (Bose and Leung 2013; Campbell et al. 2003).

3.3.3. A Multiple Linear Regression Analysis of the Effects of News Coverage Articles on the Stock Prices

To identify the correlation between a content analysis of news coverage articles about security incidents and an event study, the following regression analysis was performed. Quantitative results of a content analysis for news coverage articles about security incidents are based on 4 themes and 3 categories under each theme, whose meanings are described in detail in Table 4. Four themes include damage mention (DM), additional damage and loss (ADL), firm fault (FF) and aggressive incident response (AIR), each of which underwent regression analysis using 12 regression coefficients corresponding to 3 categories under each theme. The regression analysis formula is as follows:

$$CAR_i^t = \beta_0 + \beta_1 DM_{i1}^t + \beta_2 DM_{i2}^t + \beta_3 DM_{i3}^t + \beta_4 ADL_{i1}^t + \beta_5 ADL_{i2}^t + \beta_6 ADL_{i3}^t + \beta_7 FF_{i1}^t + \beta_8 FF_{i2}^t + \beta_9 FF_{i3}^t + \beta_{10} AIR_{i1}^t + \beta_{11} AIR_{i2}^t + \beta_{12} AIR_{i3}^t \tag{2}$$

DM_{ij}^t : j subcategory variables of DM theme on t in a firm i (j = 1–3)

ADL_{ij}^t : j subcategory variables of ADL theme on t in a firm i (j = 1–3)

FF_{ij}^t : j subcategory variables of FF theme on t in a firm i (j = 1–3)

AIR_{ij}^t : j subcategory variables of AIR theme on t in a firm i (j = 1–3)

If the security incident has a negative effect on the CAR, the results of an event analysis, β_0 (coefficient of interest), would have a negative value. DM refers to details of damages due to the security incident. ADL refers to a concern for additional losses. FF refers to content about the delinquency of a firm. Finally, AIR is referred to as AIR. Of the news coverage articles about security incidents of a firm i, published on the first date of publication, the first is (C1) and the second is (C2) with a DM theme.

If there is a paragraph that corresponds to a category, $\beta_1 DM_{0i1}$ and $\beta_2 DM_{0i2}$, serving as DM values of a firm i, were given a value of 1 each. Thus, contents of news coverage articles were quantified. After a content analysis of the news coverage articles, a multiple regression analysis of the CAR was performed, corresponding to 0 days of a firm i, in comparison with the results of a quantitative analysis. Thus, the statistical significance was confirmed.

To analyze the statistical significance of the proposed regression model, a p-value of the regression coefficient was measured using a stepwise regression with a robust standard error where the variables of 12 categories were calculated in a fixed order during the regression analysis with the use of the SPSS software package for windows version 26.0 (SPSS Inc., Chicago, IL, USA). A stepwise regression is referred to as a regression analysis of variables after the removal of those with a higher degree of correlation or multiple collinearity. With regards to the level of statistical significance, results of the analysis were described for values with a p-value of ≤ 0.05 .

4. Results

4.1. A Content Analysis of News Coverage Articles

As shown in Table 4, the paragraphs of all the news coverage articles about security incidents were classified into relevant categories. Common categories were constructed into a single theme. Thus, the results were summarized by representative tone coverage. Themes

were defined based on whether the content was classified as more negative when the news coverage articles stated that the firm deserved blame or had problems, or according to positive components (praise, satisfaction, and inspiration) and negative components (blame, hardship and denial), as previously described (Laskin and Mikhailovna Nesova 2022). In addition, any content about stakeholders’ opinions and behaviors upon the announcement of the occurrence of a security incident and the resulting damages were classified as ‘Less negative’. Furthermore, the firm explained the reasons for the occurrence of the security incident and the resulting damages. While mentioning the progress of measures taken against the resulting damages, the firm made a formal apology and proposed the methods for resolving the issue. Thus, efforts to achieve a normal recovery from the security incident were classified as neutral.

The criteria for applying tone coverage are as follows:

The FF theme (242) and the ADL theme (234) correspond to blame for problems due to the lack of security management by the firm and the further extending direct damages, and was therefore defined as a ‘More negative’ tone. The DM theme (1002) is not direct damage; it corresponds to the progression of the causes of, and losses due to, security incidents and the overall information about the resulting damages. Thus, the DM theme corresponds to the sharing of information about the resulting damages and was therefore defined as a ‘Less negative’ tone. The AIR theme (234) corresponds to active content about efforts to achieve a normal recovery by making a formal apology, taking measures against future possible occurrences and compensating victims, and was therefore defined as a ‘Neutral’ tone. Security incidents have been generally recognized as having a negative tone. After the application of detailed classifications, as defined in the current study, news coverage articles were confirmed to be ‘More negative’ (476 cases, 24.6%), ‘Less negative’ (1002 cases, 52.8%) and ‘Neutral’ (457 cases, 23.6%).

4.2. Correlations between Security Incidents and News Stats

With regards to news coverage articles about security incidents, after the first publication, there was a gradual decrease in their significance because of concerns for the enlargement of the scope of damages or the possibility of enlargement and position statements of the corresponding firm. This is well illustrated in Figure 2.

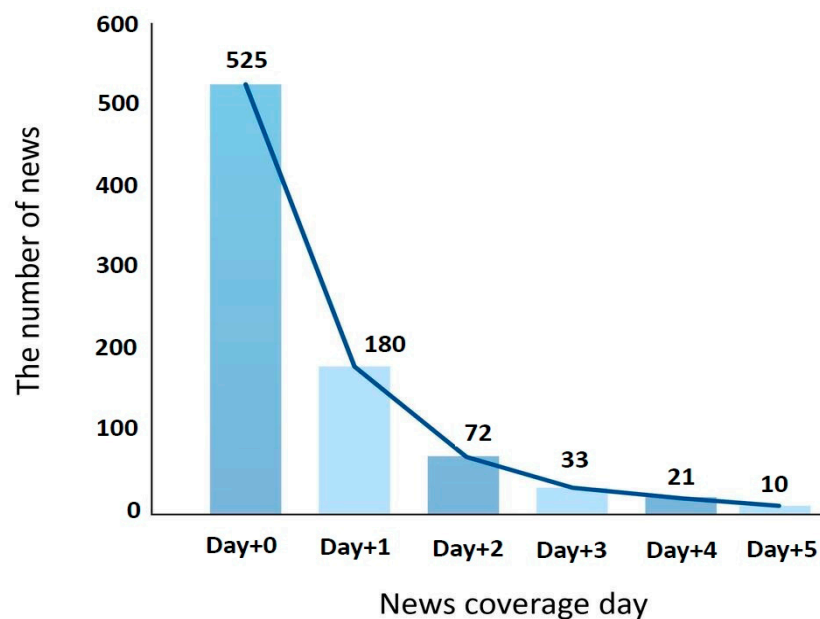


Figure 2. Changes in the number of news coverage articles about security incidents by the date of publication.

In particular, since Day + 2 after the first publication of news coverage articles about security incidents, there were few topics or additional information. Therefore, there is an abrupt decrease in the number of news coverage articles after this period. In the current study, there was an abrupt decrease in news coverage articles, but this showed a gradual decrease at a certain point. Thus, this point was included in the analysis. In other words, news coverage articles published until Day + 1, corresponding to CAR + 1 serving as a dependent variable of the event study, were analyzed. However, news coverage articles published after Day + 2 were excluded from the analysis.

From the collected news coverage articles, firms experiencing security incidents were categorized based on the type of industry, the year of the occurrence, the distribution of the type of incident and the distribution of news coverage articles by date. This was followed by the presentation of the results of an analysis of 705 news coverage articles of 74 firms experiencing security incidents in Korea, all of which were published during a period ranging from January of 2013 to December of 2021. Table 5 summarizes the distribution of security incidents by the type of industry.

Table 5. The types of security incident by industries.

Industries (2-Digit SIC Code)	N	%
Manufacturing (10–33)	20	26.3%
Electricity, gas, steam and water supply (35–36)	1	1.3%
Wholesale and retail trade (45–47)	2	2.6%
Transportation (49–52)	2	2.6%
Information and communications (58–63)	26	34.2%
Financial and insurance activities (64–66)	22	28.9%
Professional, scientific and technical activities (70–73)	2	2.6%
Business facilities management and business support services (74–75)	1	1.3%
Total	74	100%

Note: N, the number of security incidents. Abbreviations: SIC, standard industrial code.

Industries experiencing security incidents mainly included information and communications with a high degree of dependence on ICT. In addition, both the finance and manufacturing industries had a similar level of dependence on ICT. The occurrence of security incidents in these two industry sectors accounted for approximately 90% of security incidents. This is because they have a higher degree of dependence on ICT compared with other types of industries. Figure 2 illustrates the occurrence of security incidents in three groups of industries that are vulnerable to security incidents such as ICT, Financial and Manufacturing industries.

As shown in Figure 3, security incidents, such as a leakage of customer information and secret information related to the firm in an ICT industry prevalently occurred during a period ranging from 2013 to 2019. Since 2020, there has been an increasing trend in the leakage of customer information in financial industries such as insurance firms. In 2021, when security incidents occurred the most prevalently, there was an abrupt increase in such incidents in the financial industry. In association with this, it was reported that an increased occurrence of leakages of financial customer information due to direct extortion as a result of impersonations of financial organizations, such as phishing or pharming (the direction of users to a wrong website through a modification of domain name server) were a major cause. It is presumed that such incidents have also affected the Korean financial industry.

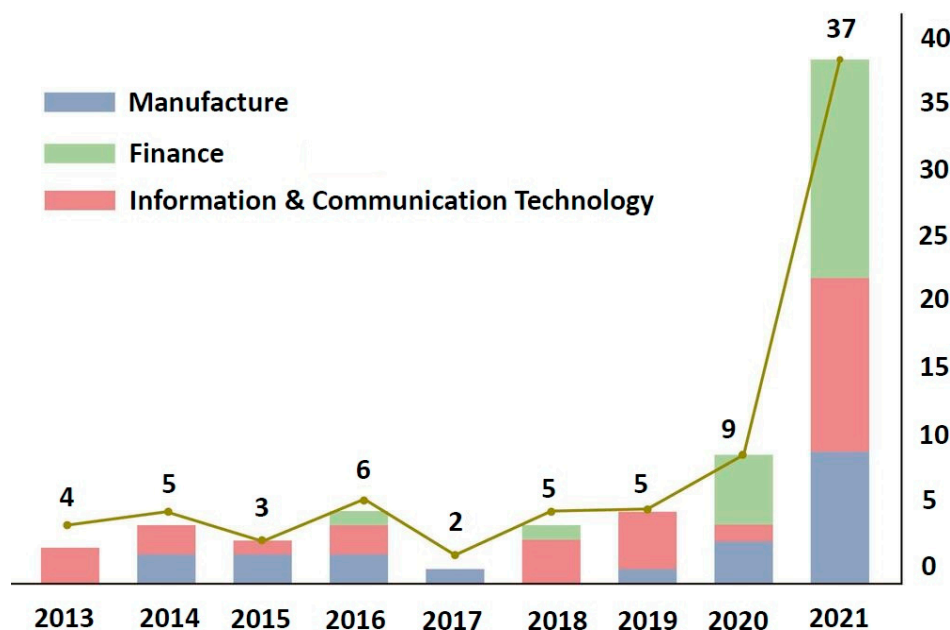


Figure 3. Annual changes in the number of security incidents by the type of industry in each year. Abbreviation: ICT, information and communication technology.

As shown in Table 6, cases of security incidents in news coverage articles were classified according to criteria proposed by Loch et al. (1992) and Jouini et al. (2014). In addition, as shown in Table 6, sources were used to classify security incidents as originating internally, within an organization, or externally, from outside of the organization.

Table 6. Classification of security incidents.

Involvement	Intention	Origin	Consequences	N
Human	Intentional	Internal	Theft, loss of information and illegal use	23
			Theft, loss of information only	14
		External	Theft, loss of information and illegal use	6
			Theft, loss of information only	25
			Denial of use	8
Total			74	

Note: N, the number of security incidents.

Perpetrators were used to determine whether any security incident occurred as a result of human behavior due to the direct involvement of humans or by non-human factors such as a computer virus specifically prepared for hacking. Intent was used to determine whether any security incident was a deliberate attempt or an unpredictable one. Consequences were applied to the analytical procedure performed in the current study, based on criteria proposed by Jouini et al. (2014) modified from those of Loch et al. (1992). Of the total cases of security incidents, 25 cases of ‘Theft, loss of information only’ due to an external attempt occurred and were the most prevalent cases, and 23 cases of ‘Theft, loss of information and illegal usage’ occurred due to an internal cause.

4.3. Analysis of the Effect of News Coverage Articles on Stock Prices

The CAR represents the information about stock prices of a firm experiencing a security incident, and it served as a dependent variable in this study. In addition, the results of a content analysis of news coverage articles served as an independent variable. Thus, attempts were made to evaluate the effects of news coverage articles, classified as a specific

type, on the stock prices. Security incident categories, serving as an independent variable, were used for a stepwise regression analysis.

Figure 4 illustrates the results of an analysis of CAR, the mean value of overall data, thus showing that it was decreased on CAR + 1, one day after the announcement of the security incident, but the effects of the security incident were generally weakened and then a recovery was achieved due to efforts by the firm.

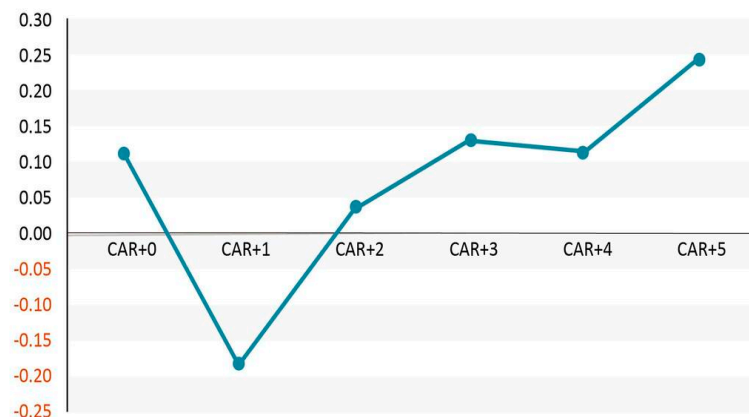


Figure 4. Daily changes in the mean cumulative abnormal return due to the occurrence of security incidents. Abbreviation: CAR, cumulative abnormal return.

The results of the content analysis were classified into categories, themes and tones (Birz and Lott 2011). In addition, after the detailed classification of data corresponding to a specific type from the overall data, the results were also classified depending on the type of industry, the type of security incident and the situations of the firm for the purposes of identifying characteristics from news coverage articles. This was followed by the appropriate analysis (Cahan et al. 2015). These approaches are effective in identifying a pattern that has not been observed from overall data due to a lack of peculiarity and in discovering a variety of characteristics from a limited amount of data. Therefore, all the cases of security incidents were equivalently analyzed depending on the type of industry, the type of incident and the situations of the firms. Thus, attempts were made to examine the contents of news coverage articles on stock prices.

4.3.1. Analysis of All Security Incidents and Major Industry-Specific Security Incidents

Table 7 shows the results of the stepwise regression performed by entering 12 independent variables for the purposes of analyzing the results of a content analysis of news coverage articles about all the firms experiencing security incidents. As a result, the D2 category of the AIR theme, using a neutral tone, (formal apology, measures against security incidents and compensation plan) had a significant positive (+) effect on stock prices. This indicates that if β is a positive value, the effects of security incidents on the stock prices would be increased (+). By contrast, if β is a negative value, the effects of security incidents on the stock prices would be decreased.

Table 7. An analysis of the effects of news coverage articles about all firms experiencing security incidents on the stock prices.

N1	N2	Dependent Variable	Independent Variable	β	t	p-Value
74	705	CAR + 1	D2 category with AIR theme	0.352	3.231	0.002 *

Note: N1, the number of firms; N2, the number of news coverage articles. Abbreviation: CAR, cumulative abnormal return; AIR, aggressive incident response. * Statistical significance at $p < 0.05$.

AIR statements included a formal apology, plans for compensation and instructions for the prevention of damages, all of which corresponded to a neutral tone. News coverage articles about these matters had a positive (+) correlation with stock prices, which could be confirmed with a β value. Following an analysis of all the cases of security incidents, there were no news coverage articles with negative effects. By contrast, D2 with an AIR theme (formal apology, plans for compensation and instructions for the prevention of damages) had a positive effect on stock prices. Efforts to take appropriate measures against security incidents both promptly and actively on the date of the publication of news coverage articles (Day + 0) and the date following it (Day + 1) led to a positive assessment by investors. Thus, the stock prices achieved a recovery. In addition, this confirmed the validity of RQ1 about the possible effects of news coverage articles about security incidents on stock prices.

From this section, the collected data were divided and examined as to whether there is variability in investors’ assessments of stock prices depending on the types of industry, the type of damages and the type of security incident, as mentioned in RQ2. In the current study, industries such as manufacturing (20 firms and 193 news coverage articles), ICT (25 firms and 293 news coverage articles) and finance (22 firms and 200 news coverage articles), accounting for approximately 90% of total cases of security incidents, were analyzed. Results are presented in Table 8. From the A3 category (inappropriate measures against security incidents) with the FF theme, to the D2 category (formal apology, measures against security incidents and plans for compensation) with the AIR theme, variables having a significant effect on stock prices were identified.

Table 8. A comparative analysis of security incidents by the type of industry.

	N1	N2	Dependent Variable	Independent Variables	β	t	p-Value
Manufacturing	20	193	CAR + 1	N/A	N/A	N/A	N/A
ICT	25	293		A3 category with FF theme	-0.392	-2.259	0.034 *
				D2 category with AIR theme	0.724	4.166	0.000 *
Finance	22	200	N/A	N/A	N/A	N/A	

Note: N1, the number of firms; N2, the number of news coverage articles; N/A, non-applicable. Abbreviations: CAR, cumulative abnormal return; FF, firm fault; AIR, aggressive incident response. * Statistical significance at $p < 0.05$.

Following an analysis of the effects of news coverage articles about security incidents on the CAR by the type of industry, manufacturing and financial firms had no categories with a significant effect on stock prices. In ICT firms, however, A3 (inappropriate measures against security incidents) corresponding to the FF theme, with a ‘More negative tone’, did. Based on a (-) β value, news coverage articles with an FF theme were associated with a decrease in stock prices. By contrast, the D2 (formal apology, measures against security incident and plans for compensation) category with an AIR theme corresponded to a neutral tone. Based on a (+) β value, it can be stated that news coverage articles in which an AIR theme was featured had a significant correlation with increased stock prices.

4.3.2. Analysis by Type of Security Incident

According to the criteria for classifying security incidents shown in Table 6, it was classified into a leakage of personal information by internal employees of the firm and that due to an external hacking. As shown in Table 9, there were variables that had an effect on stock prices in the A1 (the occurrence of security incidents due to an insufficient security management of firm) category with an FF theme and the D2 (formal apology, measures against security incidents and plans for compensation) category with the AIR theme in internal cases and C1 (information about a leakage of personal information, the firm experiencing it and the scope of damages) category with a DM theme in external cases.

Table 9. A comparative analysis of internal and external security incidents.

	N1	N2	Dependent Variable	Independent Variables	β	t	p-Value
Internal security incident	37	395	CAR + 1	A1 category with FF theme	-0.471	-3.180	0.003 *
				D2 category with AIR theme	0.334	2.256	0.031 *
External security incident	31	387		C1 category with DM theme	0.421	2.499	0.018 *

Note: N1, the number of firms; N2, the number of news coverage articles. Abbreviations: CAR, cumulative abnormal return; FF, firm fault; AIR, aggressive incident response; DM, damage mention. * Statistical significance at $p < 0.05$.

In association with security incidents due to a deliberate act or insufficient security management by employees of a firm, the amount of news coverage articles in A1 (the occurrence of security incident due to insufficient security management by the firm) category with the FF theme had a negative effect on stock prices, which was confirmed based on a negative (-) β value. These results are in agreement with a study published by Campbell et al. (2003) that stock prices were lowered by 1.9% in firms whose employees were involved in a leakage of secret information as compared with those whose employees were not (Campbell et al. 2003) By contrast, the D2 (formal apology, measures against security incidents and plans for compensation) category with the AIR theme had a positive (+) effect on stock prices, which is in agreement with the results of an analysis of data shown in Section 4.3.1. On the other hand, in association with security incidents due to external hacking, the C1 (information about a leakage of personal information, the firm experiencing it and the scope of damages) category with the DM theme, corresponding to a ‘Less negative tone’, had a positive (+) β had a positive effect on the stock prices. The reasons for this might be that a non-serious security incident induced investors to purchase stock because it had a high possibility of achieving a recovery and thereby was promoted by the degree of their expectations. As compared with other variables, A1 C1 had an abundant presence of analysis units. This indicates that there was variability in the results of the analysis with no respect to the number of analysis units.

Table 10 represents the results of a comparison of the security incident involving the unauthorized use of personal information after a leakage of it with a single occurrence of a leakage of personal information, as shown in Table 6. In the case of a security incident accompanied by a single occurrence of a leakage of personal information, the C2 (statements about customer damage and loss due to the occurrence of incident) category with the DM theme, corresponding to a ‘Less negative tone’, there were variables that had an effect on stock prices. In the case of a security incident accompanied by the illegal use of personal information after a leakage of it, the A3 (inappropriate measures against security incidents) category with the FF theme, corresponding to a ‘More negative tone’, and D2 (formal apology, measures against security incidents and plans for compensation) category, corresponding to a neutral tone, had variables that had an effect on stock prices.

Table 10. A comparative analysis of security incidents including a leakage of information or its illegal use.

	N1	N2	Dependent Variable	Independent Variables	β	t	p-Value
Leakage of information	37	425	CAR + 1	C2 category of DM theme	0.428	2.878	0.007 *
				A3 category of FF theme	-0.583	-3.504	0.002 *
Leakage of information and its illegal use	29	325		D2 category of AIR theme	0.395	2.374	0.025 *

Note: N1, the number of firms; N2, the number of news coverage articles. Abbreviations: CAR, cumulative abnormal return; DM, damage mention; FF, firm fault; AIR, aggressive incident response. * Statistical significance at $p < 0.05$.

In the case of security incidents accompanied by an illegal use of personal information after a leakage of it, the A3 (inappropriate measures against security incidents) category with the FF theme, corresponding to ‘More negative tone’, was associated with decreased stock prices. However, D2 (formal apology, measures against security incidents and plans for compensation) with an AIR theme, corresponding to a neutral tone, had a positive effect on stock prices, and stock prices increased accordingly. This is in agreement with the results of an analysis of the total data. By contrast, in the case of a security incident accompanied by a single occurrence of a leakage of personal information, C2 (seriousness of incident and customer damages/emphasis on loss) with a DM theme had variables that had an effect on the stock prices. If the damages that occurred as a result of the security incident were not serious, DM had no effect in decreasing stock prices. It can therefore be inferred that the stock prices were increased as a result of the involvement of other external factors. DDoS security incidents had no malicious effects on the value of a firm, as previously described (Joe et al. 2009).

4.3.3. Analysis of the Types of Damage by Firms

Following a comparison between a firm experiencing a security incident only once and that of a firm experiencing incidents more than twice, the former was characterized by the involvement of variables that had an effect in decreasing the stock prices in the A3 (inappropriate measures against security incidents) category with an FF theme, corresponding to a ‘More negative tone’. By contrast, the D2 (formal apology, measures against security incidents and plans for compensation) category with the AIR theme, corresponding to a neutral tone, had variables associated with increased stock prices, as shown in Table 11. D2 had a positive effect on stock prices, which is also shown in the results of an analysis of the total data.

Table 11. A comparative analysis of firm experiencing a single or multiple security incidents.

	N1	N2	Dependent Variable	Independent Variables	β	t	p-Value
Initial occurrence	45	355	CAR + 1	A3 category of FF theme	-0.273	-3.017	0.003 *
				D2 category of AIR theme	0.310	3.125	0.002 *
Recurrence	29	411			0.505	3.092	0.004 *

Note: N1, the number of firms; N2, the number of news coverage articles. Abbreviations: CAR, cumulative abnormal return; FF, firm fault; AIR, aggressive incident response. * Statistical significance at $p < 0.05$.

Following a comparison between a security incident occurring in a single firm and that occurring in multiple firms, the results are presented in Table 12.

Table 12. A comparative analysis of firms experiencing a single or multiple security incidents.

	N1	N2	Dependent Variable	Independent Variables	β	t	p-Value
Single firm	40	588	CAR + 1	D2 category of AIR theme	0.408	2.827	0.007 *
				B2 category of ADL theme	-0.653	-2.424	0.021 *
Multiple firms	34	178		D3 category of AIR theme	0.893	3.315	0.002 *

Note: N1, the number of firms; N2, the number of news coverage articles. Abbreviations: CAR, cumulative abnormal return; AIR, aggressive incident response; ADL, additional damages and loss. * Statistical significance at $p < 0.05$.

In news coverage articles about security incidents occurring in a single firm, the D2 (formal apology, measures against security incidents and plans for compensation) category with the AIR theme, corresponding to a neutral tone, had variables that had an effect on stock prices. By contrast, in the case of security incidents occurring in more than two firms, the B2 (statement about potential damages such as concerns for additional occurrences of security incidents) category with the ADL theme, corresponding to a ‘More negative

tone’, had a negative effect on stock prices. In the case of a security incident occurring in multiple firms, the scope of damages is generally large. Due to the contents of news coverage articles with a high degree of damages and seriousness, there were negative effects on stock prices. Based on the D3 (instructions for customers on the confirmation of damages and the prevention of potential ones) category with the AIR theme, corresponding to a neutral tone, the relevant guidance had a positive effect on stock prices even in the case of a security incident occurring in multiple firms.

Based on the total data and three types of measures for comparison, the effects of news coverage articles on stock prices were analyzed. Following an analysis, the relationship between news coverage articles based on each measure for comparison and stock prices was analyzed in various ways. Thus, statistical significance was identified. The results of the content analysis confirmed that news coverage articles had an effect on stock prices. Approaches to the analysis depended on the measures for comparison, such as the types of industry, the type of damage, and the type of incident, thus confirming that there was variability in the pattern of variations in stock prices due to security incidents, thereby answering RQ2. Moreover, results of the analysis were also useful in identifying definite causes and the degree of the effects. The results of an analysis of all the measures for comparison described above are presented in Table 13. By expressing categories with (+) and (−) β as ‘+β’ and ‘−β’, respectively, the categories of news coverage articles about security incidents associated with increases or decreases in stock prices were described.

Table 13. Analysis of security incidents depending on their types.

A Content Analysis of News Coverage Articles Depending on Tone, Theme and Category												
	More Negative						Less Negative			Neutral		
	FF		ADL				DM			AIR		
	A1	A2	A3	B1	B2	B3	C1	C2	C3	D1	D2	D3
All data											+β	
The type of industry												
Manufacturing												
ICT	−β									+β		
Finance												
The type of security incidents												
Internal	−β									+β		
External							+β					
Leakage of information only										+β		
Leakage of information and its illegal use	−β									+β		
The type of damages												
Initial occurrence	−β									+β		
Recurrence										+β		
Single firm										+β		
Multiple firms							−β			+β		

Abbreviations: FF, firm fault; ADL, additional damages and loss; DM, damage mention; AIR, aggressive incident response; ICT, information and communication technology.

5. Discussion and Conclusions

With the increased number of firms operating e-businesses, there has been an increase in the frequency of security incidents, particularly data breaches. This has led to substantial financial damages, which has raised concerns (Chang et al. 2020).

Vulnerability to security incidents may cause a wide range of damages. Such damages may entail a decrease in revenue and intangible losses. Inadequate protection from security incidents may lead to leakages of customers' credit card information, which could result in the collapse of customer confidence and trust (Hung 2019).

A firm may pay little attention to the importance of information security out of concern for the cost. This may consequently result in periodic recurrences of security incidents (Hung 2019). It is therefore valuable to assess the effects of news coverage articles about security incidents on the stock prices of a firm, which will also be essential for establishing a reliable, safe platform for the users of a firm's business.

The current study used an event study to assess the effects of news coverage articles about security incidents on stock prices using financial market data. The study was based on the premise that the stock prices of a firm are directly dependent on the consequences of a specific event, and also that time-dependent changes in responses to them can be used to take measures against the effects of such events (MacKinlay 1997). The current study also performed a content analysis of news coverage articles about security incidents on the stock prices of a firm.

The current results indicate the following: first, news coverage articles about security incidents had a significant effect on stock prices. Second, the degree of such an effect varied depending on the tone, theme and category of the articles. Specifically, a 'More negative' tone was associated with a decrease in stock prices. 'Less negative' and 'Neutral' tones were associated with an increase in stock prices. In particular, the 'Neutral tone' was associated with increases in stock prices, which was commonly seen in most of the firms experiencing security incidents. Third, the number of news coverage articles about a security incident had no relationship with variations in stock prices. Fourth, for firms experiencing security incidents, the variations in stock prices varied depending on the type of industry, the type of damage, and the type of incident.

However, the above results cannot be generalized because there are three limitations of the current study, as follows: first, the current study failed to determine whether the current approaches are applicable in real-world cases. Second, the current study failed to consider the possibility that fluctuations in stock prices might affect news coverage articles. Two controversial opinions exist regarding the effects of media coverage on stock returns. According to the risk compensation theory, media coverage has a negative effect on stock returns (Fang and Peress 2009; Merton 1987). That is, stocks with no, or less, media coverage should provide a risk premium because they have a lower level of transparency and a higher risk of recognition caused by asymmetric information. There is also a contradicting opinion that media coverage has a positive short-term effect on stock returns; it is difficult for real-world investors to make fully rational choices on the stock market (Barber and Odean 2008). Third, the current study failed to rule out market-driven variables in assessing the effects of news coverage articles about security incidents on the stock prices of a firm. Stock prices are indicators of information on the efficient financial market, thus are termed as market variables derived from trading information; there is variability in the effects of market variables depending on the types of markets, possibly due to the different efficiency levels of different markets (Zhou 2015; Zhou et al. 2015).

In conclusion, the current study used both an event study and content analysis of news coverage articles about security incidents to assess their effects on the stock prices of a firm. However, further studies are warranted to establish the feasibility of our approach in a real-world setting.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: No new data were created or analyzed in this study. Data sharing is not applicable to this article.

Conflicts of Interest: The authors declare no conflict of interest.

References

- Ahmad, Atif, Justin Hadgkiss, and A. B. Ruighaver. 2012. Incident Response Teams—Challenges in Supporting the Organisational Security Function. *Computers & Security* 31: 643–52.
- Ali, Syed E. A., Fong-Woon Lai, Rohail Hassan, and Muhammad K. Shad. 2021. The Long-Run Impact of Information Security Breach Announcements on Investors' Confidence: The Context of Efficient Market Hypothesis. *Sustainability* 13: 1066. [\[CrossRef\]](#)
- Aman, Hiroyuki. 2013. An analysis of the impact of media coverage on stock price crashes and jumps: Evidence from Japan. *Pacific-Basin Finance Journal* 24: 22–38. [\[CrossRef\]](#)
- An, Seon-Kyoung, and Karla K. Gower. 2009. How do the news media frame crises? A content analysis of crisis news coverage. *Public Relations Review* 35: 107–12. [\[CrossRef\]](#)
- Andrade, Roberto, Iván Ortiz-Garcés, Xavier Tintin, and Gabriel Llumiquinga. 2022. Factors of Risk Analysis for IoT Systems. *Risks* 10: 162. [\[CrossRef\]](#)
- Ban, Tao, Takeshi Takahashi, Samuel Ndichu, and Daisuke Inoue. 2023. Breaking Alert Fatigue: AI-Assisted SIEM Framework for Effective Incident Response. *Applied Sciences* 13: 6610. [\[CrossRef\]](#)
- Barber, Brad M., and Terrance Odean. 2008. All that glitters: The effect of attention and news on the buying behavior of individual and institutional investors. *The Review of Financial Studies* 21: 785–818. [\[CrossRef\]](#)
- Bharadwaj, Anandhi, Mark Keil, and Magnus Mähring. 2009. Effects of information technology failures on the market value of firms. *The Journal of Strategic Information Systems* 18: 66–79. [\[CrossRef\]](#)
- Birz, Gene, and John R. Lott. 2011. The effect of macroeconomic news on stock returns: New evidence from newspaper coverage. *Journal of Banking & Finance* 35: 2791–800.
- Bos, Wilfried, and Christian Tarnai. 1999. Content analysis in empirical social research. *International Journal of Educational Research* 31: 659–71. [\[CrossRef\]](#)
- Bose, Indranil, and Alvin C. Leung. 2013. The impact of adoption of identity theft countermeasures on firm value. *Decision Support Systems* 55: 753–63. [\[CrossRef\]](#)
- Brown, Stephen J., and Jerold B. Warner. 1980. Measuring security price performance. *Journal of Financial Economics* 8: 205–58. [\[CrossRef\]](#)
- Cahan, Steven F., Chen Chen, Li Chen, and Nhut H. Nguyen. 2015. Corporate social responsibility and media coverage. *Journal of Banking & Finance* 59: 409–22.
- Campbell, Katherine, Lawrence A. Gordon, Martin P. Loeb, and Lei Zhou. 2003. The economic cost of publicly announced information security breaches: Empirical evidence from the stock market. *Journal of Computer Security* 11: 431–48. [\[CrossRef\]](#)
- Cavusoglu, Huseyin, Birendra Mishra, and Srinivasan Raghunathan. 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: 70–104. [\[CrossRef\]](#)
- Chang, Kuo-Chung, Yu-Kai Gao, and Shih-Cheng Lee. 2020. The Effect of Data Theft on a Firm's Short-Term and Long-Term Market Value. *Mathematics* 8: 808. [\[CrossRef\]](#)
- Cutler, David M., James M. Poterba, and Lawrence H. Summers. 1989. What moves stock prices? *J. Portf. Manag.* 15: 4–12. [\[CrossRef\]](#)
- de la Garza Montemayor, Daniel J., and Xunaxhi M. Pineda Rasgado. 2023. Relationship between the Use of Social Networks and Mistrust of Mass Media among Mexican Youth: A Mixed-Methods and NLP Study. *Social Sciences* 12: 179. [\[CrossRef\]](#)
- Dias Canedo, Edna, Ana P. Morais do Vale, Rafael L. Patrão, Leomar Camargo de Souza, Rogério Machado Gravina, Vinicius Eloy dos Reis, Fábio Lúcio Lopes Mendonça, and Rafael T. de Sousa Jr. 2020. Information and Communication Technology (ICT) Governance Processes: A Case Study. *Information* 11: 462. [\[CrossRef\]](#)
- Dyck, Alexander, Natalya Volchkova, and Luigi Zingales. 2008. The corporate governance role of the media: Evidence from Russia. *The Journal of Finance* 63: 1093–135. [\[CrossRef\]](#)
- Fama, Eugene F., Lawrence Fisher, Michael C. Jensen, and Richard Roll. 1969. The adjustment of stock prices to new information. *International Economic Review* 10: 1–21. [\[CrossRef\]](#)
- Fang, Lily, and Joel Peress. 2009. Media coverage and the cross-section of stock returns. *The Journal of Finance* 64: 2023–52. [\[CrossRef\]](#)
- Grigaliūnas, Šarūnas, Rasa Brūzgienė, and Algimantas Venčkauskas. 2023. The Method for Identifying the Scope of Cyberattack Stages in Relation to Their Impact on Cyber-Sustainability Control over a System. *Electronics* 12: 591. [\[CrossRef\]](#)
- Holdford, David. 2008. Content analysis methods for conducting research in social and administrative pharmacy. *Research in Social and Administrative Pharmacy* 4: 173–81. [\[CrossRef\]](#) [\[PubMed\]](#)
- Hovav, Anat, and John D'Arcy. 2003. The impact of denial-of-service attack announcements on the market value of firms. *Risk Management and Insurance Review* 6: 97–121. [\[CrossRef\]](#)
- Hovav, Anat, and John D'Arcy. 2005. Capital market reaction to defective IT products: The case of computer viruses. *Computers & Security* 24: 409–24.
- Hung, Chia-Ching. 2019. Analysis of Information Security News Content and Abnormal Returns of Enterprises. *Big Data and Cognitive Computing* 3: 24. [\[CrossRef\]](#)
- Joe, Jennifer R., Henock Louis, and Dahlia Robinson. 2009. Managers' and investors' responses to media exposure of board ineffectiveness. *Journal of Financial and Quantitative Analysis* 44: 579–605. [\[CrossRef\]](#)

- Jouini, Mouna, Latifa B. Rabai, and Anis B. Aissa. 2014. Classification of security threats in information systems. *Procedia Computer Science* 32: 489–96. [\[CrossRef\]](#)
- Kankanhalli, Atreyi, Hock-Hai Teo, Bernard C. Y. Tan, and Kwok-Kee Wei. 2003. An integrative study of information systems security effectiveness. *International Journal of Information Management* 23: 139–54. [\[CrossRef\]](#)
- Kannan, Karthik, Jackie Rees, and Sanjay Sridhar. 2007. Market reactions to information security breach announcements: An empirical analysis. *International Journal of Electronic Commerce* 12: 69–91. [\[CrossRef\]](#)
- Karaman Aksentijević, Nada, Zoran Ježić, and Petra A. Zaninović. 2021. The Effects of Information and Communication Technology (ICT) Use on Human Development—A Macroeconomic Approach. *Economies* 9: 128. [\[CrossRef\]](#)
- Kassarjian, Harold H. 1977. Content analysis in consumer research. *Journal of Consumer Research* 4: 8–18. [\[CrossRef\]](#)
- Kim, Jawon, Jaesoo Kim, and Hangbae Chang. 2020. Research on Behavior-Based Data Leakage Incidents for the Sustainable Growth of an Organization. *Sustainability* 12: 6217. [\[CrossRef\]](#)
- Kitsios, Fotis, Elpiniki Chatzidimitriou, and Maria Kamariotou. 2022. Developing a Risk Analysis Strategy Framework for Impact Assessment in Information Security Management Systems: A Case Study in IT Consulting Industry. *Sustainability* 14: 1269. [\[CrossRef\]](#)
- Kolbe, Richard H., and Melissa S. Burnett. 1991. Content-analysis research: An examination of applications with directives for improving research reliability and objectivity. *Journal of Consumer Research* 18: 243–50. [\[CrossRef\]](#)
- Konchitchki, Yaniv, and Daniel E. O’Leary. 2011. Event study methodologies in information systems research. *International Journal of Accounting Information Systems* 12: 99–115. [\[CrossRef\]](#)
- Kondracki, Nancy L., Nancy S. Wellman, and Daniel R. Amundson. 2002. Content analysis: Review of methods and their applications in nutrition education. *Journal of Nutrition Education and Behavior* 34: 224–30. [\[CrossRef\]](#)
- Lacy, Stephen, Brendan R. Watson, Daniel Riffe, and Jennette Lovejoy. 2015. Issues and Best Practices in Content Analysis. *Journalism & Mass Communication Quarterly* 92: 791–811.
- Laskin, Alexander V., and Natalya Mikhailovna Nesova. 2022. The Language of Optimism in Corporate Sustainability Reports: A Computerized Content Analysis. *Business and Professional Communication Quarterly* 85: 80–98. [\[CrossRef\]](#)
- Loch, Karen D., Houston H. Carr, and Merrill E. Warkentin. 1992. Threats to information systems: Today’s reality, yesterday’s understanding. *Mis Quarterly*, 173–86. [\[CrossRef\]](#)
- Luyckx, Dorien, and Steve Paulussen. 2022. In Service of News Subscribers: Exploring Belgian Journalists’ Perceptions of Stakeholder Relations in the Digital News Ecosystem. *Journalism and Media* 3: 81–98. [\[CrossRef\]](#)
- MacKinlay, A. Craig. 1997. Event studies in economics and finance. *Journal of Economic Literature* 35: 13–39.
- Maqsood, Haider, Muazzam Maqsood, Sadaf Yasmin, Irfan Mehmood, Jihoon Moon, and Seungmin Rho. 2022. Analyzing the Stock Exchange Markets of EU Nations: A Case Study of Brexit Social Media Sentiment. *Systems* 10: 24. [\[CrossRef\]](#)
- Masip-Bruin, Xavi, Eva Marín-Tordera, José Ruiz, Admela Jukan, Panagiotis Trakadas, Ales Cernivec, Antonio Lioy, Diego López, Henrique Santos, Antonis Gonos, and et al. 2021. Cybersecurity in ICT Supply Chains: Key Challenges and a Relevant Architecture. *Sensors* 21: 6057. [\[CrossRef\]](#)
- Merton, Robert C. 1987. A simple model of capital market equilibrium with incomplete information. *The Journal of Finance* 42: 483–510. [\[CrossRef\]](#)
- Moreno, Julio, Manuel A. Serrano, Eduardo B. Fernandez, and Eduardo Fernández-Medina. 2020. Improving Incident Response in Big Data Ecosystems by Using Blockchain Technologies. *Applied Sciences* 10: 724. [\[CrossRef\]](#)
- Pabian, Arnold, and Barbara Pabian. 2023. Role of Social Media in Managing Knowledge of the Young Generation in the Sustainability Area. *Sustainability* 15: 6008. [\[CrossRef\]](#)
- Pandey, Dharen K., and Vineeta Kumari. 2021. Event study on the reaction of the developed and emerging stock markets to the 2019-nCoV outbreak. *International Review of Economics & Finance* 71: 467–83.
- Perera, Srinath, Xiaohua Jin, Alana Maurushat, and De- Graft J. Opoku. 2022. Factors Affecting Reputational Damage to Organisations Due to Cyberattacks. *Informatics* 9: 28. [\[CrossRef\]](#)
- Sadiq, Olusegun, Dieu Hack-Polay, Ted Fuller, and Mahfuzur Rahman. 2022. Barriers to the Effective Integration of Developed ICT for SMEs in Rural NIGERIA. *Businesses* 2: 501–26. [\[CrossRef\]](#)
- Škrinjarić, Tihana. 2019. Stock Market Reactions to Brexit: Case of Selected CEE and SEE Stock Markets. *International Journal of Financial Studies* 7: 7.
- Tetlock, Paul C. 2007. Giving content to investor sentiment: The role of media in the stock market. *The Journal of Finance* 62: 1139–68. [\[CrossRef\]](#)
- Tetlock, Paul C., Maytal Saar-Tsechansky, and Sofus Macskassy. 2008. More than words: Quantifying language to measure firms’ fundamentals. *The Journal of Finance* 63: 1437–67. [\[CrossRef\]](#)
- Wang, Tawei, Jackie R. Ulmer, and Karthik Kannan. 2013. The textual contents of media reports of information security breaches and profitable short-term investment opportunities. *Journal of Organizational Computing and Electronic Commerce* 23: 200–23. [\[CrossRef\]](#)

Zhou, Ligang. 2015. A comparison of dynamic hazard models and static models for predicting the special treatment of stocks in China with comprehensive variables. *Journal of the Operational Research Society* 66: 1077–90. [[CrossRef](#)]

Zhou, Ligang, Dong Lu, and Hamido Fujita. 2015. The performance of corporate financial distress prediction models with features selection guided by domain knowledge and data mining approaches. *Knowledge-Based Systems* 85: 52–61. [[CrossRef](#)]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.