Association for Information Systems
AIS Electronic Library (AISeL)

WISP 2022 Proceedings

Pre-ICIS Workshop on Information Security and Privacy (SIGSEC)

Winter 12-11-2022

The value relevance of an official press release of a security breach and complementarities between the content elements of the release

Nirup M. Menon
George Mason University, nmenon@gmu.edu

Brian Ngac
George Mason University

Fatou Diouf
George Mason University

Follow this and additional works at: https://aisel.aisnet.org/wisp2022

Recommended Citation

Menon, Nirup M.; Ngac, Brian; and Diouf, Fatou, "The value relevance of an official press release of a security breach and complementarities between the content elements of the release" (2022). *WISP 2022 Proceedings*. 9.
https://aisel.aisnet.org/wisp2022/9

This material is brought to you by the Pre-ICIS Workshop on Information Security and Privacy (SIGSEC) at AIS Electronic Library (AISeL). It has been accepted for inclusion in WISP 2022 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.

The Value Relevance of an Official Press Release of a Security Breach and Complementarities between the Content Elements of the Release

Nirup M Menon[1]
George Mason University,
Fairfax, VA, USA

Brian Ngac
George Mason University,
Fairfax, VA, USA

Fatou Diouf
George Mason University,
Fairfax, VA, USA

ABSTRACT

The importance of signaling to inform the public of a security incident occurrence at a firm through an official press release is discussed. The majority of prior research has discussed the impact of public knowledge of a security incident occurrence on the share prices of a firm. This study analyzes two competing models of the relationship between a firm's reputation and the firm doing a press release, and the subsequent impact on the market valuation of the firm. Content of the press release that is specific to information security, overt CEO involvement and transparency in data affected, serves as an additional signal for the market. A switching regression model of 169 security incidents (with and without an official press release) versus a Heckman Sample Selection model of 111 security incidents (with an official press release) of publicly traded firms between 2014 and 2021 upholds the logic of the signaling characteristic of the decision to do an official press release with respect to the reputation of the firm. The roles of overt CEO involvement and transparency in data affected under this framework is statistically significant.

Keywords: Information security, data breach, reputation, cumulative abnormal returns, CEO role

[1] Corresponding author. nmenon@gmu.edu

INTRODUCTION

After an information security incident becomes public knowledge, the breached firm experiences significant costs related to information systems and security retooling, investigation, and recovery (Andriole 2022). There is evidence that the financial market will account for the intangible and tangible costs after the breach, including revenue losses, and as a result, reduces its valuation of the firm (Cavasoglu et al. 2004). Some firms choose to disclose breach incidents that they suffer via official press releases, whereas other firms choose to let the disclosure of their breach to the public occur by the mass media who were likely informed by law enforcement agencies (Cheng and Walton 2019, Kim and Lee 2021).

When a breached firm chooses an official press release to disclose the breach, they are signaling the financial market, which the market observes and incorporates into the valuation of the firm on the day of the incident. The theory from finance, strategy, and information systems posits that because of the information asymmetry between investors in a firm and the firm, investors look for signals about a firm's current and potential actions to decide whether to invest in it (e.g., Zhang and Wiersema 2009, Cavasoglu et al. 2004). Further, by using official press releases, the firms are able to choose the message about the security incident, so as to prevent a significant decrease in its market valuation (Knight and Nurse 2020). Firms, for example, announce the remedies being undertaken, and may add an apology, an excuse, a correction action, and other content to the press release. This heterogeneity in press releases would result in the heterogeneity in the amount by which the stock price of a firm decreases after a breach becomes public knowledge.

Recent research has looked into value relevance, i.e., impact on current market valuation or stock price, of the content of the press releases made about a breach and the role of prior

reputation of the breached firm. For example, a low reputation firm, when reputation is measured by the appearance or not of a firm on the Most Admired Companies list, would not experience as much decrease in its market valuation when committing to stakeholder value in a press release as it would when apologizing in it (Gwebu et al. 2018). Unlike the elements of a low reputation company's press release, none of the elements of a high reputation company's press release affects its market valuation (Gwebu et al. 2018).

In contrast to Gwebu et al. (2018)'s findings about the elements of an information security press release, in the general context of organizational crisis, a firm's prior reputation does not affect its valuation, and apologizing in the press release for a preventable crisis can alleviate the negative effect of the crisis on the its valuation (Racine et al. 2020). The reputation of a firm is not static and will change by a signal received by observers about the firm. For example, the occurrence of a breach can affect reputation, as can whether or not a firm issued an official press release about a breach incident. The choice to issue or not issue an official press release can signal the financial market to update its priors about the reputation of the firm. It then follows that doing a press release can be value relevant via the reputation mechanism for the financial market.

While this study follows prior work on the contents of the security breach press release and uses Situational Crisis Communication Theory (SCCT) framework from the crisis management literature (Coombs 2007, Ma and Zhan 2016) just as those studies did, the study also deviates from those studies by incorporating the role of CEO and the transparency of data disclosure from the general information systems literature in the analysis of the phenomenon. There have been accounts of CEOs being fired from their positions following an information security incident (Lending et al. 2018). Indeed, research finds that top management support

which includes the CEO promotes the success of information systems and information security projects (Jarvenpaa and Ives 1991, Kwon et al. 2013). With overt CEO involvement, the press release receives legitimacy and the value relevance of the remaining elements improves. Thus, overt CEO involvement, hereafter *OCI* in this paper, supplements a missing element in the SCCT framework.

Security breaches involve data, and the public, law enforcement, and policy makers are concerned about the loss of individuals' data. Thus, the press release about the breach must describe the data affected so that it is clear how the remedies address the safety and privacy of customer data. The transparency about the data affected, hereafter *TADA*, is an element of a crisis that is specific to information security, and is missing from the SCCT framework in the context of security breaches.

The specific research questions are: 1) does prior reputation and the change in reputation play a role in how an official press release about a security breach affects the market valuation (i.e., stock prices) of the breached firm? 2) Does *OCI* play a role in how the contents of the official press release, conceptualized using the SCCT framework, affect the stock prices of the breached firm? 3) Does *TADA* play a role in how the contents of the official press release, conceptualized using the SCCT framework, affect the stock prices of the breached firm?

HYPOTHESES

Our first hypothesis is on the value relevance of an official press release by the affected firm. In our sample, approximately double the number of firms chose this way to let the public learn about the occurrence of the breach incident than the number of firms that chose not to make such a press release. Two explanations are possible. On the one hand, firms that chose to make the press release wanted to signal to the market that they are being transparent and quick to act,

so that the signal instigates the market to update its estimate of the reputation of these firms. The change in reputation in turn mitigates the fall in stock price that is likely to occur as a result of the security incident. On the other hand, firms that did not chose to make such a press release already had a high reputation and did not think that the security incident would affect its stock price. These explanations point to the possibility that the press release is either a consequence of the prior reputation of the firm, and that its elements do not directly affect the stock price which is primarily affected by the security incident, or a driver of a change in reputation which in turn drives the impacts of the elements of the press release on the stock price (Figure 1). The formal hypothesis statement for the alternate is:

H1: The impact on stock price will be through a change in reputation driven by prior reputation and the press release.

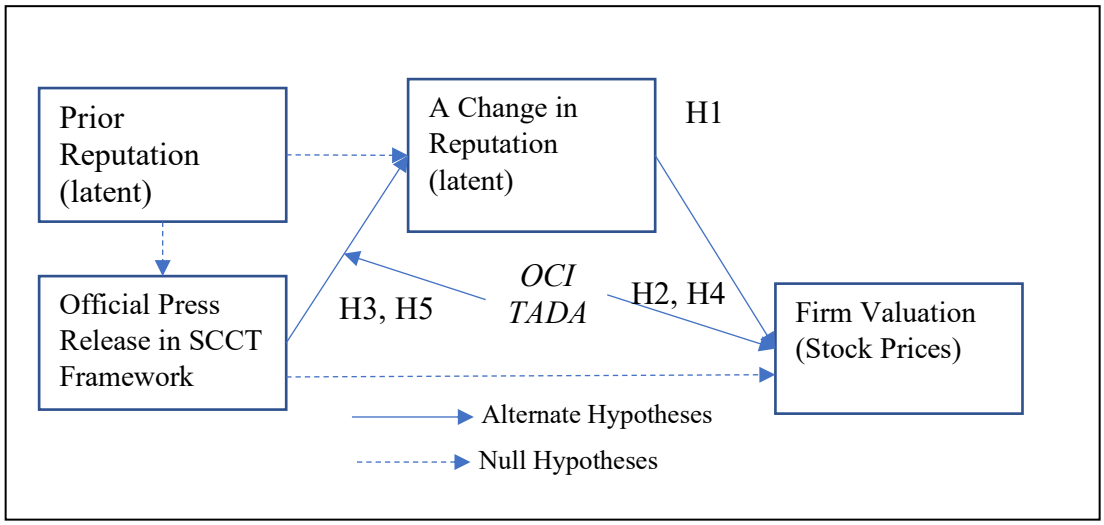

Figure 1. Two Paths for Press Release & Reputation

Overt CEO Involvement (*OCI*)

Executive or top management support is a critical success factor in all information technology projects (Jarvenpaa and Ives 1991). Top management support particularly the CEO is also critical for information security project success because top management can influence the

organizational culture through their policies and allocation of resources, which in turn leads to better information security compliance by employees (Puhakainen and Siponen 2010, Hu et al. 2012). Top management support through programs such as security education, training, and awareness can lead to employees' understanding of the need to protect organizational assets (Posey et al. 2016). A consequence of the important role that top management plays in information security is that, though information security performance is the responsibility of the technical staff in the company, a failure in information security reflects not only on the technical employees, but also on the CEO of the company.

The question then arises is whether the CEO should front the communication when a breach occurs so as to continue to show support for information security. Communication experts believe that a well-briefed CEO may be capable of effectively delivering the message, whereas others argue that the CEO should not front communications for small breaches lest the breach is misconstrued as a large data breach (Knight and Nurse 2020). From the perspective of signaling, costly signals are more credible to receivers (Connelly et al. 2011). CEOs are typically an expensive resource. Similarly, authoritative senders such as CEOs make the signal more credible. One answer to why the CEO must front the official press release is to control the impact on the valuation of the firm. Thus, the hypothesis to be tested is the direct effect of CEO on the financial metric as follows:

H2: Overt CEO Involvement (OCI) is positively correlated with market value of the firm.

On the one hand, the voice of the CEO in the press release has a complementary effect on the rest of the press release. The support of the information security function by the CEO lends legitimacy to the apology and remedial measures presented in the release (Beelitz and Merkel-

Davis 2012). The signal to the market is that there will be resources behind the initiatives laid out in the communication. On the other hand, it is possible that the CEO and the company is not completely aware of the level of damage and remedies needed, and the market may not completely trust the communication because it has no other information to go on. In such a case, one would expect that CEO will not complement the other elements of the communication. To present a testable hypothesis, the latter is assumed to the null hypothesis and the former rationale holds for the alternate hypothesis which is:

H3: Overt CEO Involvement (OCI) and other elements of the communication complement each other in affecting the market value of the firm.

Transparency About Data Affected (*TADA*)

Data is an information security-specific aspect of the press release that is not subsumed in the typology of communication. A central reason for negative reactions from the public and policy makers to an information security incident is the potential theft of individuals' data. In addition to the effect on customers due to the loss of their privacy and their fear of a potential financial fraud that the data loss invites, there is also a fear that the company may have lost data and information that provide competitive advantage. The audience for the public message in the aftermath of a security incident are all stakeholders, so that the message must attempt to describe the data affected for the sake of the public and upholders of law. Such a description provides confidence that the firm knows the amount of data stolen. If no mention of data is made, the opposite may be inferred by the public that the firm does not know the amount of data stolen. Therefore, the hypothesis is:

H4: Transparency about Data Affected (TADA) is positively correlated with market value of the firm.

According to the SCCT, the reason why message types affect market value is that an effective press release represents the firm as responsible, well-prepared, and transparent. When data description is included in the message, the effectiveness mechanism is enhanced, so that the direct impact of the press release on market valuation is given a push in the positive direction. Therefore, transparency about data affected has a complementing effect and the testable hypothesis is:

H5: TADA and other elements of the communication complement each other in affecting the market value of the firm.

DATA COLLECTION AND CONSTRUCTION

The breach data for publicly-traded companies were collected from Identity Force[2] which has a year-by-year list of breaches and contains consistent overview data of each security breach including company, data of breach, and for most – a link to an authoritative source on the breach. The data on the site were collected from public sources and includes links to news articles about each breach. Public notifications of a breach such as a press release, notification of security incident letter to affected customers, notification letter to the state attorney general, or filing to the Securities and Exchange Commission were coded by undergraduate research assistants along the SCCT framework, *OCI*, and *TADA* variables. Details of the data collection and coding are available in Menon et al. (2023).

The data coded from the press releases were subjected to a polychoric correlation analysis for binary data (Rigdon et al. 1991). This analysis revealed severe multicollinearity between the variables: Apology, Ingratiation, Justification, Excuse, Correction Commitment, Stakeholder Commitment, Value Commitment.[3] Three rotated factors emerged with eigenvalues

[2] https://www.identityforce.com/blog/2021-data-breaches accessed last on 10/1/2022.
[3] None of the announcements contained a denial, so Denial was dropped from further consideration.

greater than one: 1) Excuse, Justification, and Value Commitment, 2) Apology and Correction Commitment, 3) Ingratiation and Stakeholder Commitment. The factors were respectively named $ExcuseJustifyValue$, $ApologyCorrect$, and $IngratiationStakeholder$. Another set of highly correlated variables was Technical Security Enhancements, Customer Action Recommendations Present, Consumer Protection Efforts Available, Customer Questions Center Available, Company to Reach out to Affected Customers, Company Notified Authorities, Company Reaction to Mitigate Current Breach, Security Controls in Place, News Article has Quote from Company Rep. Three rotated factors emerged with eigenvalues greater than one: one factor (named *RemedialAction2*) consisted mainly of Security Controls in Place, another factor (named *RemedialAction3*) consisted mainly of News Article has Quote from Company Rep, while the third factor (named *RemedialAction1*) consisted of highest loadings on the remaining variables. The factor scores of the three factors were used in the analysis going forward.

Financial Data

The 169 data breach events that were identified were attributed to 79 unique public companies due to some firms were breached multiple times during the investigated period. The financial data such as share prices for the corresponding ticker identifiers were collected from The Center for Research in Security Prices (CRSP)[4] data and Compustat data. Only publicly traded companies with sufficient number of data points (records available for at least 240 days prior to the company's breach incident) were included in the dataset. The final list of 169 firms from 2014 to 2021 is shown in Table A4 in the appendix. Three financial variables from Compustat included in our analysis to control for some firm characteristics as seen in prior research (Racine et al. 2018) are the $Firm\_Size$, $Leverage$, $Market\_to\_Book$.

[4] Like Compustat, CRSP data on stock prices is used as the authoritative source by researchers.

DATA ANALYSIS

An event study methodology is used after marking the security breach of a company as the event in its timeline of changes in stock prices. It is customary in event studies to use the cumulative abnormal return (CAR) computed from the stock prices over a period of time to include the event rather than the stock prices themselves to test for the reaction of the price to the event. CAR parcels out the expected returns from the firm's stock prices so that firm- and industry-specific confounds do not affect the shock to the stock price because of an isolated event. For each firm *i*, the CAR over an event window from the day of the press release (*t*=0) to the day after the release (*t*=1) is calculated as a sum of the stock's abnormal returns as follows (Binder 1998):

$$CAR_i(0,1) = \sum_{t=0}^{1} AR_{it}. \quad (1)$$

The abnormal return of firm *i* at time *t* is calculated using the Capital Asset Pricing Model (Rosati et al. 2017):

$$AR_{it} = R_{it} - E(R_{it}) \quad (2)$$

where R_{it} is the firm's actual return at time *t*. $E(R_{it})$, the expected return of firm *i* at time *t*, is calculated as follows:

$$E(R_{it}) = \alpha_i + \beta_i R_{mt} \quad (3)$$

where, R_{mt}, the total market return, represents the value-weighted index without dividends (cite). α_i and β_i are, respectively, the intercept and the slope of the market model which are calculated by regressing daily firm returns on daily market returns over 160 days, starting at *t*=190 days before the event and ending at *t*=30 days before the event. Cutting off the market returns regression period 30 days prior to the beginning of the event period ensures that the firm's returns are not impacted by information about the breach event prior to the firm's official press release.

$E(R_{it})$ are predicted values of the dependent variable, i.e., the firm's expected stock prices, after the regression model is run. These values are substituted back into equation (2), and computed AR_{it} are plugged into equation (1) to obtain the CAR values.

A Switching Regression Model

Consider the basic model for a breached firm that does not announce the breach and the associated remedies formally. This basic model for $CAR_i^N(0,1)$ for the firm in the absence of a press release is a function of its financial descriptors such as $Firm\_Size_i$, $Leverage_i$, and $Market\_to\_Book_i$:

$$CAR_i^N(0,1) = \alpha_0 + \alpha_1 Firm\_Size_i + \alpha_2 Leverage_i + \alpha_3 Market\_to\_Book_i + \varepsilon_{1i} \quad (4)$$

The error term ε_{1i} is distributed normally with a mean zero and standard deviation of σ_1 which must be estimated from the data. The model for $CAR_i^Y(0,1)$ with press release characteristics as explanatory variables is given by:

$$\begin{aligned} CAR_i^Y(0,1) = {} & \beta_0 + \beta_1 OCI_i + \beta_2 TADA_i + \beta_3 ExcuseJustifyValue_i + \beta_4 ApologyCorrect_i \\ & + \beta_5 IngratiationStakeholder_i + \beta_6 RemedialAction1_i \\ & + \beta_7 RemedialAction2_i + \beta_8 RemedialAction3_i \\ & + \beta_9 OCI_i \times ExcuseJustifyValue_i + \beta_{10} OCI_i \times ApologyCorrect_i \\ & + \beta_{11} OCI_i \times IngratiationStakeholder_i + \beta_{12} OCI_i \times RemedialAction1_i \\ & + \beta_{13} OCI_i \times RemedialAction2_i + \beta_{14} OCI_i \times RemedialAction3_i \\ & + \beta_{15} TADA_i \times ExcuseJustifyValue_i + \beta_{16} TADA_i \times ApologyCorrect_i \\ & + \beta_{17} TADA_i \times IngratiationStakeholder_i + \beta_{18} TADA_i \times RemedialAction \\ & + \beta_{19} TADA_i \times RemedialAction2_i + \beta_{20} TADA_i \times RemedialAction3_i \\ & + \beta_{21} Firm\_Size_i + \beta_{22} Leverage_i + \beta_{23} Market\_to\_Book_i + \varepsilon_{2i} \end{aligned} \quad (5)$$

The error term ε_{2i} is distributed normally with a mean zero and standard deviation of σ_2, also to be estimated from data. Suppose the z-score of the change in reputation rep of a firm follows a normal distribution with a mean zero and a standard deviation of one. We do not observe the change in reputation or the resulting reputation prior to its effect on the stock price. But we can model the probability of the press release for a breached firm in terms of its newly updated reputation as:

$$p[REP] = [p|rep \leq REP]. \quad (6)$$

Because we know which firms did a press release, we use this information to model REP by placing $Announce$ as one of the explanatory variables of the new realization of this variable. In addition, we use explanatory variables that can proxy the prior reputation of the firm. The first proxy is whether the firm appears in the Most Admired Company List ($Admired$). The second proxy for the prior reputation of the firm is whether the firm is listed on the New York Stock Exchange ($NYSE$). In the form of an equation, the latent variable REP is:

$$REP = p_1 Announce + p_2 Admired + p_3 NYSE. \quad (7)$$

The model for observed $CAR_i(0,1)$ is an expected value of the two CARs in equations 4 and 5 as follows:

$$CAR_i(0,1) = p[REP]CAR_i^Y(0,1) + \{1 - p[REP]\}CAR_i^N(0,1) + \omega\,. \quad (8)$$

ω in equation 8 is the error term that is normally distributed with a mean zero and standard deviation of one. The information contained in the above models is used to generate the logarithm of a joint likelihood function for the three error terms $(\omega, \sigma_1, \sigma_2)$ for estimation as following:

$$Log(L) = \frac{1}{2}\left\{log(2\pi) + log(\sigma_1^2[p^2] + \sigma_2^2[1-p]^2) + \frac{W^T W}{1/(\sigma_1^2[p^2] + \sigma_2^2[1-p]^2)}\right\}. \quad (9)$$

$W^T W$ is the cross-product of matrices of the error terms of equation 8. The set of equations 4, 5, 7, 8, and 9 are jointly estimated by maximizing the log likelihood function with respect to all the unknown parameters and fitting the data. The estimation process uses Marquardt algorithm for convergence.

RESULTS AND CONCLUSIONS

The model fit statistics for the switching regression were compared with linear regression and found to be better, hence supporting hypothesis H1. H2 is not supported as the coefficient of *OCI* is not statistically significant at $p<0.05$ in Table 1. H3 is also not supported because none of the coefficients of interaction terms with OCI is negative and statistically significant at a *p*-value of 0.05. H4 is supported because the coefficient of $TADA$ is significant at 0.05 *p*-value. H5 is partially supported because the coefficient of $TADA \times IngratiationStakeholder$ and $TADA \times RemedialAction1$ are both positive and statistically significant; the former at *p*-value of 0.001 and the latter at *p*-value of 0.05.

Table 2. Results of the Switching Regression

Variable (Parameter Estimated)	Est.	Err.	
Intercept (β_0)	-0.015	0.005	
OCI (β_1)	-0.034	0.019	
$TADA$ (β_2)	0.016	0.008	*
$ExcuseJustifyValue$ (β_3)	-0.009	0.005	
$ApologyCorrect$ (β_4)	0.021	0.007	**
$IngratiationStakeholder$ (β_5)	-0.030	0.004	***
$RemedialAction1$ (β_6)	-0.012	0.004	*
$RemedialAction2$ (β_7)	-0.006	0.004	
$RemedialAction3$ (β_8)	-0.007	0.005	
$OCI \times ExcuseJustifyValue$ (β_9)	-0.011	0.004	*
$OCI \times ApologyCorrect$ (β_{10})	0.003	0.003	
$OCI \times IngratiationStakeholder$ (β_{11})	-0.002	0.002	
$OCI \times RemedialAction1$ (β_{12})	0.002	0.006	
$OCI \times RemedialAction2$ (β_{13})	0.0007	0.003	
$OCI \times RemedialAction3$ (β_{14})	-0.0006	0.002	
$TADA \times ExcuseJustifyValue$ (β_{15})	0.002	0.004	
$TADA \times ApologyCorrect$ (β_{16})	-0.015	0.005	**
$TADA \times IngratiationStakeholder$ (β_{17})	0.032	0.004	***
$TADA \times RemedialAction1$ (β_{18})	0.006	0.002	*
$TADA \times RemedialAction2$ (β_{19})	0.004	0.004	
$TADA \times RemedialAction3$ (β_{20})	0.005	0.005	
$Firm\_Size$ (β_{21})	-0.001	0.003	
$Leverage$ (β_{22})	-0.007	0.01	
$Market\_to\_Book$ (β_{23})	0.003	0.005	

More details of the results are in Menon et al. 2023.

$* p < 0.05$; $** p < 0.01$; $*** p < 0.001$

Reputational loss is indicated as a consequence of public knowledge of a security incident (Campbell et al. 2003). However, our study finds that there is a heterogeneity in the level of reputational loss across firms. Our results show that the level of the reputational loss may depend on how the public is made aware of the security incident. Further, not all firms make an official press release even if it serves as a reputation-signaling mechanism. Firms that do not do a press release are typically firms with good prior reputation. The results also show that not all firms suffer a similar drop in market valuation. This heterogeneity is explained both by the reputation-building mechanism of making an official press release and by the elements of the press release.

Two pathways involving reputation and the choice to make an official press release were modeled. The pathway in which a firm's press release serves as a signal for the financial market to update its belief about the reputation of the firm is superior to the pathway in which the press release is not a signal for reputation. In the latter pathway, a firm's prior reputation drives the release of the press release. The findings here explain the phenomenon of stock market reaction to information security incidents. Most of the prior work focused only on the value relevance of the public knowledge of such an incident, without modeling the sample biasedness because the public is made aware of the incidents either by the firm itself or by the news media. The logic here surfaces this difference, and dives deeper into the value relevance of two elements of the content of the press release.

ACKNOWLEDGEMENTS

The authors are grateful to their undergraduate research assistants, Mark Cayanan, Vy Nguyen, Julien Ward, and Divya Arvapalli, for their help with the data collection and data coding.

REFERENCES

Andriole, S. (2022). Are we spending too much on cybersecurity when costs, reputation risks & fines are so small? July 26, 2022. https://www.forbes.com/sites/steveandriole/2022/07/26/are-we-spending-too-much-on-cybersecurity-when-costs-reputation-risks--fines-are-so-small/?sh=7e00c70a4763. Accessed August 23, 2022.

Beelitz, A., & Merkl-Davies, D. M. (2012). Using discourse to restore organisational legitimacy:'CEO-speak'after an incident in a German nuclear power plant. *Journal of Business Ethics*, *108*(1), 101-120.

Binder, J. (1998). The event study methodology since 1969. *Review of Quantitative Finance and Accounting*, *11*(2), 111-137.

Campbell, K., Gordon, L. A., Loeb, M. P., & Zhou, L. (2003). The economic cost of publicly announced information security breaches: empirical evidence from the stock market. *Journal of Computer Security*, *11*(3), 431-448.

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers. *International Journal of Electronic Commerce*, *9*(1), 70-104.

Connelly, B. L., Certo, S. T., Ireland, R. D., & Reutzel, C. R. (2011). Signaling theory: A review and assessment. *Journal of Management*, *37*(1), 39-67.

Gwebu, K. L., Wang, J., & Wang, L. (2018). The role of corporate reputation and crisis response strategies in data breach management. *Journal of Management Information Systems*, *35*(2), 683-714.

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing employee compliance with information security policies: The critical role of top management and organizational culture. *Decision Sciences*, *43*(4), 615-660.

Jarvenpaa, S. L., & Ives, B. (1991). Executive involvement and participation in the management of information technology. *MIS Quarterly*, 205-227.

Kwon, J., Ulmer, J. R., & Wang, T. (2013). The association between top management involvement and compensation and information security breaches. *Journal of Information Systems*, *27*(1), 219-236.

Lending, C., Minnick, K., & Schorno, P. J. (2018). Corporate governance, social responsibility, and data breaches. *Financial Review*, 53(2), 413-455.

Menon, N.M., B. Ngac, F. Diouf. On reputational mechanism, CEO participation, and data description in official press releases following security incidents, and market reactions, GMU WP, 2023.

Rigdon, E. E., & Ferguson Jr, C. E. (1991). The performance of the polychoric correlation coefficient and selected fitting functions in confirmatory factor analysis with ordinal /data. *Journal of marketing research*, *28*(4), 491-497.