UNIVERSIDADE CATÓLICA PORTUGUESA

Impact of Data Breaches on Accounting Narratives

A Study on S&P 500 MED Firms

Gonçalo Monteiro Clemente

Universidade Católica Portuguesa, Católica Porto Business School
October of 2023

UNIVERSIDADE CATÓLICA PORTUGUESA

Impact of Data Breaches on Accounting Narratives

A Study on S&P 500 MED Firms

Final project in the form of Dissertation presented to the Universidade Católica Portuguesa to obtain the degree of Master in Auditing and Taxation

by

Gonçalo Monteiro Clemente

Under the guidance of
Professor Eleonora Monaco
Professor Ricardo Ribeiro

Universidade Católica Portuguesa, Católica Porto Business School
October of 2023

Acknowledgements

Completing this master's thesis has been one of the most demanding, yet intellectually rewarding challenges of my life. It involved balancing a full-time job as a financial auditor with the difficulties of academic research. However, we often find personal growth in overcoming arduous circumstances and I could not have achieved this milestone without the crucial support from those around me.

To Professor Eleonora Monaco and Professor Ricardo Ribeiro, for sharing their expertise and guiding me through this project.

To my parents, who have instilled invaluable values in me and provided me with countless opportunities. Nothing would have been possible without their unconditional support.

To my girlfriend, who inspires me to improve every day and offers me her unconditional love.

To my lifelong friends, who have accompanied and supported me through every academic and personal phase.

To all the professors of Católica Porto Business School, who consistently go the extra mile for their students. Your efforts do not go unnoticed.

To the Privacy Rights Clearinghouse, for generously providing the database on breaches. Their generosity made this research possible.

Resumo

No contexto do aumento das preocupações com a cibersegurança, as empresas estão, cada vez mais, a priorizar a gestão de riscos e a segurança de dados. Este estudo explora a divulgação de incidentes de violação de segurança de dados como um indicador de risco, com foco no tom narrativo contabilístico dos relatórios trimestrais 10-Q e anuais 10-K das empresas que pertenceram à indústria médica do S&P 500 de 2010 a 2019. Esta investigação tem por base a literatura existente relacionada com narrativas e violação de segurança de dados, sendo complementada através da literatura sobre as características intrínsecas aos conselhos de administração, qualidade dos lucros e desempenho financeiro. Este estudo tenta preencher um vazio na literatura ao analisar como o tom das narrativas se altera após a ocorrência e divulgação de uma violação de segurança de dados. Utilizando uma abordagem maioritariamente quantitativa, este estudo realiza uma análise trimestral destes relatórios financeiros de forma a avaliar como estes anúncios afetam o tom das narrativas contabilísticas nos trimestres que precedem ao evento e no próprio trimestre do evento. Os resultados indicam um impacto visível das divulgações de fugas de informação no tom das narrativas. Este estudo contribui para a literatura existente, enfatizando o papel da análise do tom das narrativas como uma ferramenta na avaliação de riscos, tendo implicações para auditores, analistas e stakeholders de interesse.

Palavras-chave: Fugas de informação; Cibersegurança; Tom narrativo;

Número de palavras: 6683

Abstract

In light of rising cybersecurity concerns, companies are increasingly focusing on risk management and data security. This study explores the disclosure of cybersecurity incidents as a proxy for changes in financial reporting tone. Specifically, I expect a change in tone around the publication of the annual and quarterly reports of U.S. S&P 500 healthcare and medical providers industry (MED) companies during the 2010 to 2019 time period. Building upon existing literature on narrative accounting tone and data security breaches (DSBs) and further complemented by literature on board characteristics, earnings quality, and financial performance, this research aims to fill a gap by analyzing how narrative tone shifts following DSBs. Using a quantitative approach, this study conducts a quarterly analysis of the SEC's 10-Q and 10-K reports to assess how narrative tone shifts in the quarters preceding a DSB announcement and in the quarter a DSB is disclosed and announced. The findings underscore a noticeable impact of DSB disclosures on narrative tone. This study contributes to the existing literature by highlighting the importance of the analysis of narrative tone as a tool in risk evaluation and has implications for auditors, analysts and stakeholders of interest.

Keywords: Cybersecurity Incidents; Data Security Breaches; Narrative Accounting Tone;

Number of Words: 6683

Table of Contents

Index of Tables

Abbreviation List

10-K – Annual report filling required by the SEC

10-Q - Quarterly report filling required by the SEC

CEO – Chief Executive Officer

DSB(s) – Data Security Breaches

EBIT – Earnings Before Interest and Taxes

EPS – Earnings Per Share

IT – Information Technology

LIWC-22 – Linguistic Inquiry and Word Count

MD&A – Management Discussion and Analysis

MED – Healthcare and Medical Providers Industry

OLS – Ordinary Least Squares

Q – Quarter

ROA – Return on Assets

SEC - Securities and Exchange Commission

S&P 500 - Standard & Poor's 500

USA/US – United States of America

USD – United States Dollar

Introduction

There is an increasing use of digital technologies in the 21st century which has transformed various aspects of our daily lives, from the way we communicate to the way we do business. As companies are increasingly dependent on information technology, the integrity and confidentiality of data have become main concerns (Gordon et al., 2010; Gordon et al., 2008; Othman et al., 2019). Despite investments in cybersecurity measures and increasingly complex IT systems, instances of data security breaches (DSBs) remain frequent, which threatens the security of information systems (Steinbart et al., 2018).

Given the importance of these data assets, the Securities and Exchange Commission (SEC) has, thus, increased requirements for financial disclosures related to cybersecurity incidents both in 2011 (SEC 2011) and 2018 (SEC 2018), thereby expanding the scope of managerial and auditing tasks in financial reporting (Berkman et al., 2018; Sen & Borle, 2015).

Consequently, to ensure the quality of financial information, there have been recent advancements in text-mining techniques (Hossain et al., 2019). Whether through conference calls, financial reports, or press releases, firms use tone to shape narratives and influence stakeholder perceptions (Bassyouny et al., 2020). This tone, evident in financial reporting and business communication between managers and external users, reflects their choice of optimistic or pessimistic words. As a result, studies are investigating into the quality of disclosures through linguistic and textual analysis (Loughran et al., 2011; Tausczik & Pennebaker, 2010). As financial statements alone do not provide full information to stakeholders (Bassyouny et al., 2022), there is an increased interest in the

qualitative information disclosed by companies, known as narrative disclosures. These narratives convey crucial information about a company's performance and financial position. Among the different proxies, several studies investigate the optimistic or pessimistic language that managers use in their narrative reporting to convey essential information about the company.

My research proposes to answer the following question "How does the occurrence and subsequent disclosure of a data security breach influence the narrative accounting tone of S&P 500 companies in the MED industry?". The results of this study are an important resource for auditors, analysts, and other stakeholders of interest. Some companies withhold bad news, strategically choosing a more opportune moment to disclose them when it becomes inevitable (Amir et al., 2018; Kothari et al., 2009), as a data security breach is heavily associated with negative market impacts (Amir et al., 2018; Gwebu et al., 2018; Janakiraman et al., 2018; Rosati et al., 2019; Wang et al., 2013; Xu et al., 2019), negative consumer behavior (Janakiraman et al., 2018) and high internal costs (Xu et al., 2019). As a result, by providing evidence on the impact of the occurrence and disclosure of data security breaches as an indicator of changes around narrative accounting tone, the findings of this research can inform these groups on the importance of considering the analysis of tone in assessing a company's risk profile. Understanding the evolution of a company's narrative tone in its reports can provide information on potential data security breaches not disclosed. This question contributes to new knowledge to the field by analyzing the impact of data security breaches on narrative accounting tone, an area that has not been explored in the literature. Although the existing literature acknowledges various determinants of narrative tone, such as the impact of board characteristics on negative tone (Martikainen et al., 2023), the influence of earnings management and earnings quality on net tone (Abou-El-Sood & El-

Sayed, 2022), the role of CEO characteristics on positive tone (Bassyouny, 2020; Marquez-Illescas et al., 2019), and the correlation of financial performance with positive tone (Alalwani & Mousa, 2020), the specific interaction between data security breaches and narrative tone remains unexplored. I hypothesize that the occurrence and disclosure of a data security breach influences the narrative accounting tone. I expect an increase in negative tone in the quarter of the breach when compared to the preceding two quarters, as announcements of cybersecurity events are associated with negative market impacts (Acquisti et al., 2006; Amir & Levi, 2018; Cavusoglu et al., 2004; Goel & Shawky, 2009; Malhotra & Malhotra, 2011; Personen, 2009; Pirounias et al., 2014; Yayla & Hu, 2011).

I estimate an OLS equation that studies the effect of the occurrence and disclosure of a DSB on tone. Tone is measured using the concept of "net tone", calculated by subtracting negative words from positive words in reports and then dividing by the total number of positive and negative words. This approach is based on a textual analysis using the dictionary by Loughran and McDonald (2011), known for accurately capturing the sentiment of financial documents. The authors associate specific word lists, including positive, uncertainty, litigious, strong modal, and weak modal words, with market reactions, trading volume, unexpected earnings, subsequent stock return volatility, and material weaknesses in accounting controls. Tone was measured using LIWC software which is a leading software for word-use analysis (Tausczik & Pennebaker, 2010).

I also control for a multitude of financial variables. These variables include company's size (computed using the natural logarithm of quarterly assets), return on assets, loss (a binary variable taking values of 1 or 0 determined by whether the return on assets for the quarter is positive or negative); earnings per share and leverage. Additionally, I account for board background, captured by

the percentage of board members with an industry specific or strong financial background, and I include controls related to the CF disclosure guide: Topic No. 2 on Cybersecurity introduced in 2011 and updated in 2018. Finally, I also control for the natural logarithm of a firm's report word count.

My dataset comprises financial reports from S&P 500 companies within the Healthcare and Medical Providers (MED) industry. The research study period is set from 2010 to 2019, analyzing data for 144 reports belonging to breached companies and 144 reports belonging to non-breached companies.

In the two quarters leading up to the breach, the occurrence and disclosure of a DSB is not statistically significant in explaining tone. However, results show that the occurrence and disclosure of a DSB in the quarter of the breach is statistically significant and has a negative impact on narrative disclosure tone.

This thesis is structured as follows: Chapter 1 presents a literature review on data security breaches and narrative accounting tone; Chapter 2 presents the theoretical hypothesis to be tested and methodology applied; Chapter 3 describes the data, sample selection and presents the estimation results. The thesis concludes by defining the findings of this research, as well as the limitations found and suggestions for future investigation.

Chapter 1
Literature Review

1. Data Security Breaches, Narrative Tone and Disclosure Requirements

With the rise of the internet in the 21st century, the complexity of information systems has increased, making classified data more vulnerable. As such, companies are devoting considerable resources to risk management systems and information security practices (Othman et al., 2019). However, risk management is not homogeneous across companies and different management teams perceive risks differently within the business framework and less efficient approaches can lead to DSBs (Arena & Azzone, 2009). Consequently, cybersecurity has emerged as a critical risk management issue, particularly in a knowledge-based economy (Gordon et al., 2010; Gordon et al., 2008). Cyber-attacks, or the illegal access to corporate information systems, often result in incidents where data is stolen or made public by unauthorized entities (Ettredge et al., 2018; Rosati et al., 2017, 2019, 2022).

Cybersecurity threats include debit and credit card fraud, hackers, insider threats, loss of documents, stolen technological assets, human error, and unintended disclosure (Privacy Rights Clearinghouse, 2023). As companies increasingly rely on IT and IT outsourcing for data storage, the risk of data security breaches and information asymmetries escalates (Steinbart et al., 2018). This aligns with a growing trend of cybersecurity incidents that lead to punitive legal and financial consequences for the impacted companies (Eaton et al., 2019;

Rosati et al., 2019). DSB disclosures typically lead to negative market reactions, which can vary depending on the nature and severity of the breach (Gwebu et al., 2018).

Considering the significance of these data assets and as narratives complement financial reports by offering essential insights into a company's performance (Berkman et al., 2018), the Securities and Exchange Commission has enhanced its requirements for financial disclosures pertaining to cybersecurity risks (SEC 2011; SEC 2018). In 2011, aiming for an increase in transparency on significant cyber-related matters, the SEC introduced CF Disclosure Guidance: Topic No. 2 on Cybersecurity (SEC 2011). This directive underscores the responsibility of companies to disclose information concerning significant cybersecurity risks. The guideline implies that important sections in the 10-K reports, like the MD&A, business overview, legal proceedings, and Item 1A: Risk Factors, are where businesses should detail cybersecurity risks (SEC 2011). The SEC underlines the importance of avoiding generic disclosures, requiring detailed and relevant information specific to a company's situation in order to enable stakeholders to understand the risks the company faces (SEC 2011). In 2018, SEC issued a revised version of their 2011 cybersecurity guidance, aimed at supporting public firms in preparing disclosures concerning cybersecurity events and risks (SEC 2018).

In ensuring high-quality financial disclosures, it is crucial to consider both the content and its presentation, with recent advancements in technology and linguistics enhancing text-mining techniques for analysing financial information (Hossain et al., 2019). Whether through conference calls, annual reports or other press publications, firms and their top executives and managers have more flexibility to frame narratives with stakeholders often leveraging tone, either optimistic or pessimistic, to influence stakeholders' perceptions of a company's'

information (Bassyouny et al., 2020). Moreover, several studies are examining the quality of disclosure via a linguistic (Loughran et al., 2011) and textual analysis as the function and emotion of words used by individuals provide significant psychogenic signals that serve as an indication of their cognitive processes, affective states, objectives, and driving forces. A first wave of linguistic analysis is based on existing dictionaries and respective adjustments, a recent trend that examines the content of the disclosure of both annual reports and conference calls via more recent techniques (Gagnon et al., 2020). Financial statements alone do not provide a complete picture to stakeholders because they cannot portray companies' strategies and future plans (Bassyouny et al., 2022).

Current studies have examined various factors affecting narrative tone, including board characteristics' relation to negative tone (Martikainen et al., 2023), the relationship between earnings management and earnings quality on net tone (Abou-El-Sood & El-Sayed, 2022), CEO characteristics impact on positive tone (Bassyouny, 2020; Marquez-Illescas et al., 2019), and the association of financial performance with a positive tone (Alalwani & Mousa, 2020).

2. Impacts of a Data Security Breach Announcement

Several studies investigate the impact of cybersecurity incidents on a firm's market value, market activity, and market reactions (Amir et al., 2018; Gwebu et al., 2018; Janakiraman et al., 2018; Rosati, Cummins, et al., 2017; Rosati et al., 2018, 2019). Different levels of breaches have diverse impacts on market variables, and various breach dimensions affect how the market responds on the event day (Rosati, Cummins, et al., 2017). It was also found that breached firms lost, on average, 2.53% of their value during the event day as well as the following day

(Rosati, Cummins, et al., 2017). The nature of the data security breach disclosure leads to different market reactions (Wang et al., 2013). Withheld cyber-attacks lead to a decline of about 3.6% in equity values on the month they were discovered, while disclosed cyber-attacks lead to about a 0.7% decline (Amir et al., 2018). Few studies focus on the financial performance impacts, which may be due to the difficulty in quantifying the consequences of DSBs on accounting information quality (Xu et al., 2019).

As the source of the information on cyberattacks often comes from the firm itself, managers can be tempted to withhold this information, particularly for more severe attacks where the damage is still unclear (Amir et al., 2018; Kothari et al., 2009). This can lead to issues related to the valuation of the impact, as withholding information can result in large expenses like legal fees, loss of revenues, and fines, as well as loss of credibility and trust (Xu et al., 2019). Furthermore, a DSB impacts customer perception of the brand, leading to increased customer acquisition costs, a decline in customer spending, and migration to other retailers (Janakiraman et al., 2018). In light of the negative impacts a DSB can have on a firm's public image, companies need to develop strategies to counteract these effects. The literature finds that only selected strategies mitigate the negative impacts of a breach on lower-reputation firms, while these strategies are not as important for high-reputation firms (Gwebu et al., 2018). The literature also reveals that in the two years subsequent to a breach there is additional monitoring from auditors and regulators, resulting in a 55% lower chance of having financial restatements in the time period as well as reinforced controls (Rosati et al., 2018). Research indicates that announcements of cybersecurity events are associated with negative market impacts (Acquisti et al., 2006; Amir & Levi, 2018; Cavusoglu et al., 2004; Goel & Shawky, 2009;

Malhotra & Malhotra, 2011; Personen, 2009; Pirounias et al., 2014; Yayla & Hu, 2011).

Chapter 2
Hypothesis Development & Method

1. Hypothesis Development

The disclosure of a data security breach can significantly impact a company's market standing, affecting its market value, market activity, and financial performance (Amir et al., 2018; Gwebu et al., 2018; Janakiraman et al., 2018; Rosati et al., 2019; Wang et al., 2013; Xu et al., 2019). A crucial aspect of a company's value is its brand reputation and customer perception and the occurrence of DSB can negatively affect these factors, resulting in increased customer acquisition costs, decreased customer spending, and a migration of customers to competitors (Janakiraman et al., 2018). To mitigate the negative impact of a DSB, companies must develop strategic responses, which vary in effectiveness based on the firm's reputation (Gwebu et al., 2018). Quantifying the financial impact of cybersecurity incidents is challenging, as it involves accounting for significant expenses such as legal fees, fines, revenue losses, and credibility and trust damages, however companies must manage the disclosure of such incidents with their investors while simultaneously dealing with efficiency losses, missed deals and contracts, and lost growth opportunities (Xu et al., 2019). One of the most critical consequences of a DSB is the loss of customers, as they may choose to support other businesses (Janakiraman et al., 2018). As such, based on the literature on the ample negative impacts associated with a data security breach, I hypothesize a negative shift in tone in their reports.

Theoretical Hypothesis: *The occurrence and disclosure of a data security breach will lead to an increase in negative narrative accounting tone in the quarter of the breach compared to preceding quarters.*

I hypothesize that, when analyzing reports quarterly, the narrative tone of U.S. companies will exhibit a negative change surrounding the public announcement of a cybersecurity breach, compared to companies that have not suffered any breach. These changes in narrative tone may serve as indicators that disclosing a data security breach influences the tone of narrative accounting and can be considered a proxy for cybersecurity risk. This is also strongly backed by the literature that demonstrates that announcements of cybersecurity events are associated with negative market impacts (Acquisti et al., 2006; Amir & Levi, 2018; Cavusoglu et al., 2004; Goel & Shawky, 2009; Malhotra & Malhotra, 2011; Personen, 2009; Pirounias et al., 2014; Yayla & Hu, 2011).

2. Research Method

The current research seeks to determine whether the narrative accounting tone of a firm that has disclosed suffering a data security breach differs from the tone of the remaining firms that have not experienced any breach. This investigation will be conducted by analyzing the narrative accounting tone in the two quarters preceding the disclosure and the quarter of the disclosure. The focus is on a quarterly analysis of reports, as they represent the primary sample of narrative reporting that can showcase the narrative style of companies compared to other financial reporting documents such as press releases and conference calls (Bassyouny, 2020). A quarterly analysis allows for a more precise tracking of changes in a company's narrative tone over time, compared to analyzing reports

annually. This makes it possible to more accurately assess the potential risks and market perceptions associated with a cybersecurity breach.

The previously exposed hypothesis is empirically testable as it concentrates on quantifiable variables: the tone of narrative accounting (dependent variable) and the occurrence and disclosure of data security breaches (independent variable). In particular, I have studied my research question using the following multiple linear regression model:

$$TONE_{it} = \beta_0 + \beta_1 DSB_{it} + \beta_2 SIZE_{it} + \beta_3 ROA_{it} + \beta_4 LOSS_{it} + \beta_5 LEV_{it} + \beta_6 EPS_{it} + \beta_7 BACK_{it} + \beta_8 SEC11_t + \beta_9 SEC18_t + \beta_{10} WC_{it} + \varepsilon_{it},$$

where $TONE_{it}$ denotes the net tone score in the report of firm i in quarter t, DSB_{it} denotes an indicator variable that takes the value of 1 if the firm i has been breached and disclosed it in quarter t (and 0 if the firm has not experienced any breach), $SIZE_{it}$ denotes the natural logarithm of the total assets of firm i in quarter t, ROA_{it} denotes the return on assets of firm i in quarter t, $LOSS_{it}$ denotes an indicator variable that takes the value of 1 if ROA_{it} is negative (and 0 otherwise), LEV_{it} denotes the ratio of long-term debt to total assets of firm i in quarter t, EPS_{it} denotes the earnings per share of firm i in quarter t, $BACK_{it}$ denotes the percentage of board members of firm i in quarter t who have either an industry specific background or a strong financial background. $SEC11_t$ captures the introduction of CF Disclosure Guidance: Topic No. 2 on Cybersecurity. It denotes an indicator variable that takes the value of 1 if quarter t is dated on or after 2011 and 0 otherwise. $SEC18_t$ captures the update of CF Disclosure Guidance: Topic No. 2 on Cybersecurity. It denotes an indicator variable that takes the value of 1 if quarter t is dated on or after 2018 and 0

otherwise. Finally, WC_{it} denotes the natural logarithm of total number of words (word count) in report of firm i in quarter t.

I employed the ordinary least squares (OLS) estimator for my analysis as this is the approach adopted in the existing literature that studies tone (Abou-El-Sood & El-Sayed, 2022; Alalwani & Mousa, 2020; Ashraf, 2022; Bassyouny et al., 2020b; Marquez-Illescas et al., 2019; Martikainen et al., 2023).

2.1. Dependent Variable – Measuring Tone

The dependent variable under consideration in this research is tone. Specifically, the tone measured in reports of firms. The chosen method to measure tone is through the application of the concept of "net tone", which is computed by subtracting the count of negative words from the count of positive words. The calculation of the net tone score is premised on the lexical analysis of reports. The foundational tool in performing this analysis is the dictionary of positive and negative words developed by Loughran and McDonald (2011), which is recognized for its effectiveness in reflecting the sentiment of financial documents. The computation of the net tone score involves counting the frequency of positive and negative words. Each occurrence of positive and negative words is given equal weight.

Tone is used to get a sense of how positive or negative a report. Tone can range from -1.000 to 1.000. If all words are negative tone will be -1.000 and if the opposite happens, that is, all words positive tone will be 1.000. A value of 0.000 would suggest a report where positive and negative sentiments cancel each other out.

$$TONE_{it} = \frac{PW_{it} - NW_{it}}{PW_{it} + NW_{it}},$$

where PW_{it} denotes the number of positive words in the report of firm i in quarter t and NW_{it} denotes the number of negative words in the report of firm i in quarter t.

2.2. Independent Control Variables

In my regression model, attention is devoted to the inclusion of specific financial variables as control factors. These variables comprise of size, return on assets, loss, earnings per share, and leverage. The rationale behind the selection of these financial variables has been rooted, for many years, in the empirical literature, which identifies a relationship between the tone of financial disclosures and an array of corporate financial performance indicators (Clatworthy & Jones, 2003).

Regarding variable size, the natural logarithm of total assets normalizes skewed data, simplifies the scale of large numbers, enhances interpretation of relative changes, and allows more direct comparability across firms of different sizes. Controlling for size is essential in literature that studies narrative accounting tone (Abou-El-Sood & El-Sayed, 2022; Alalwani & Mousa, 2020; Ashraf, 2022; Bassyouny et al., 2020; Berkman et al., 2018; Florackis et al., 2023; Marquez-Illescas et al., 2019; Martikainen et al., 2023). Larger firms inherently vary in baseline tone due to a broader stakeholder base, higher regulatory scrutiny, and greater public attention. They also possess more resources for crisis management, which could independently influence disclosure tone. The

maturity and organizational complexity of bigger firms could also affect their baseline risk levels and thus the tone of disclosures. This is rooted in early literature finding firm size as determinants of disclosure choices (Lang & Lundhold, 1993).

Return on assets (ROA) is computed as earnings before interest and taxes scaled by the mean of lagged and current total assets.[1] Controlling for ROA is important when examining tone as presented in narrative accounting literature (Ashraf, 2022; Berkman et al., 2018; Florackis et al., 2023; Marquez-Illescas et al., 2019; Martikainen et al., 2023). ROA serves as an indicator of a firm's financial health and operational efficiency, factors that naturally influence the tone of corporate communications. ROA is associated with management and stakeholder confidence, both of which could independently affect the tone of narrative disclosures. ROA may signify management capabilities, influencing how they communicate post-breach. Controlling for ROA ensures a more direct comparison.

$$ROA_{it} = \frac{EBIT_{it}}{(TA_{it} + TA_{it-1})/2},$$

where $EBIT_{it}$ denotes earnings before interest and taxes firm i in quarter t and TA_{it} denotes the total assets for firm i in quarter t.

A negative ROA indicates financial stress, which can independently lead to a more negative tone in narrative disclosures. By controlling for loss, it is possible to isolate the specific impact of a data security breach on narrative tone, separate from financial underperformance which is known to impact tone (Schleicher &

[1] If the lagged total assets are missing for the previous quarter, the current assets as reported on December 31st of the previous year will be used.

Walker, 2010). This binary variable simplifies the model, making it easier to interpret while still capturing the essence of a firm's financial health. Factoring loss is vital for research focused on narrative accounting tone (Ashraf, 2022; Marquez-Illescas et al., 2019; Martikainen et al., 2023).

$$LOSS_{it} = \begin{cases} 1 \; if \; ROA_{it} \leq 0 \\ 0 \; if \; ROA_{it} > 0 \end{cases}.$$

High leverage often indicates greater financial risk, which can independently shift the tone of narratives (Linsley & Shrives, 2006). By controlling for this, it is possible to more precisely attribute changes in narrative tone to the data breach rather than underlying financial risk. Including leverage as a control variable is important in studies concerning the tone of accounting narratives (Abou-El-Sood & El-Sayed, 2022; Alalwani & Mousa, 2020; Ashraf, 2022; Bassyouny et al., 2020a; Berkman et al., 2018; Florackis et al., 2023; Martikainen et al., 2023).

$$LEV_{it} = \frac{LTD_{it}}{TA_{it}},$$

where LTD_{it} denotes long term debt for firm i in quarter t.

A high earnings per share (EPS) might enable a more optimistic tone, regardless of a data breach, while a low EPS could worsen the negative impact of such an event. Also, EPS is a widely recognized measure of a company's profitability which is driver for disclosure choices (Prencipe, 2004). Controlling for EPS is important in narrative accounting literature (Berkman et al., 2018; Marquez-Illescas et al., 2019). While both ROA and EPS relate to profitability, ROA is related to how efficiently a company uses its assets to generate profit, while EPS shows the profit per share available to shareholders.

$$EPS_{it} = \frac{NI_{it}}{S_{it}},$$

where NI_{it} denotes net income of firm i in quarter t and S_{it} denotes the weighted average number of outstanding shares of firm i in quarter t.

Expertise may influence the tone of its narrative disclosures. Boards with relevant experience may convey messages differently, leading to a more confident or transparent tone that could either mitigate or intensify the impact of a data breach on public disclosures. Controlling for board characteristics/background is rooted in narrative accounting literature (Alalwani & Mousa, 2020; Ashraf, 2022; Bassyouny et al., 2020; Martikainen et al., 2023). There is also relevant literature correlating board background and narrative tone. This was first introduced in early studies linking background to company decisions, including tone of disclosures (Mason & Hambrick, 1984). In fact, board members use disclosure tone factoring their financial reporting strategy (Patelli & Pedrini, 2015).

$$BACK_{it} = \frac{BMB_{it}}{TBM_{it}},$$

where BMB_{it} denotes the number of board members of firm i in quarter t with either industry or financial background and TBM_{it} denotes the total board members of firm i in quarter t.

$SEC11_{it}$ and $SEC18_{it}$ are important control variables. In 2011, SEC introduced CF Disclosure Guidance: Topic No. 2 on Cybersecurity with the aim of enhancing clarity around significant cyber-related concerns (SEC 2011). This guidance

underlines the responsibility of companies to share details about cybersecurity matters. Key sections in the 10-K/10-Q reports, like the MD&A, business overview, legal proceedings, and Item 1A: Risk Factors, are where businesses should detail cybersecurity risks (SEC 2011). The guideline suggests that companies outline the most critical elements concerning the investment risks associated with them (SEC 2011). In 2018, SEC released a revised version of their 2011 cybersecurity guidance, aimed at supporting public firms in preparing disclosures concerning cybersecurity events and risks (SEC 2018). As such, it is important to control for these variables to ensure that my model captures the effect of data breaches on narrative tone, rather than potential changes in disclosure practices driven by regulatory changes.

Word count is an important control variable as longer reports naturally have more words, and therefore, the probability of having more occurrences of both positive and negative words is higher. If not controlled for, the length of the report might tilt the tone calculation, making it seem like longer reports are inherently more positive or negative. Controlling for word count ensures that tone is accurately captured across reports of varying lengths.

Variable	Measurement
TONEit	Denotes the net tone score in the report of firm i in quarter t
DSBit	Denotes an indicator variable that takes the value of 1 if the firm i has been breached and disclosed it in quarter t, and 0 if the firm has not experienced any breach
SIZEit	Denotes the natural logarithm of the total assets of firm i in quarter t
ROAit	Denotes the return on assets of firm i in quarter t
LOSSit	Denotes an indicator variable that takes the value of 1 if ROAit is negative and 0 otherwise
LEVit	Denotes the ratio of long-term debt to total assets of firm i in quarter t
EPSit	Denotes the earnings per share of firm i in quarter t
BACKit	Denotes the percentage of board members of firm i in quarter t who have either an industry specific background or a strong financial background
SEC11t	Denotes an indicator variable that takes the value of 1 if quarter t is dated on or after 2011 and 0 otherwise
SEC18t	Denotes an indicator variable that takes the value of 1 if quarter t is dated on or after 2018 and 0 otherwise
WCit	Denotes the natural logarithm of total number of words (word count) in report of firm i in quarter t

Table 1 - Variable Definition (Source: Own Systematization)

Chapter 3
Empirical Application

1. Data and Sample Selection

I restrict my analysis to companies in the Healthcare and Medical Providers (MED) industry that were listed in the S&P 500 at any point between the years 2010 and 2019. This includes firms that may have been part of the S&P 500 during that timeframe but were subsequently removed. This targeted approach aims to ensure the validity of results within a specific industry as different industries can produce different results. It also avoids the 2008 financial crisis and 2020 COVID-19 crisis, which could impact narrative accounting tones substantially.

As a result, I constructed a database with all the companies that ever joined and left the S&500 and the respective dates. This was done with the help of Refinitiv Eikon software and resulted in 88 MED companies that were, at some point, in the S&P 500 between 2010 and 2019.

Sample Selection Criteria	Lost observations	Remaining Observations
Refinitiv Eikon - Leavers & Joiners for years 1994-2023		1226
Exclude all companies that weren't in the S&P 500 during 2010-2019	513	713
Exclude all industries except "MED"	625	88

Table 2 - S&P 500 - Leavers and Joiners (Source: Own Systematization)

I gathered information on data breach events from Privacy Rights Clearinghouse, an organization that has been monitoring public data breaches

since 2005. The Privacy Rights Clearinghouse database contains breaches that have been confirmed either by governmental bodies or credible media outlets. The database has important information such as: Company names; Date of breach; Date of disclosure; Type of breach; Short summary (Privacy Rights Clearinghouse, 2023).

Privacy Rights Clearinghouse database also contains information about organization type, which made it easy to connect the two databases.

Code	Description
BSF	Businesses (Financial Services, Banking, Insurance Services)
BSO	Businesses (Manufacturing, Technology, Communications, Other)
BSR	Businesses (Retail/Merchant including Grocery Stores, Online Retailers, Restaurants)
EDU	Educational Institutions (Schools, Colleges, Universities)
GOV	Government & Military (State & Local Governments, Federal Agencies)
MED	Healthcare and Medical Providers (Hospitals, Medical Insurance Services)
NGO	Nonprofits (Charities and Religious Organizations)
UNKN	Unknown

Table 3 - Organization Types (Source: Privacryrights.org)

Utilizing data from the Privacyrights.org (covering Data Security Breaches from 2005 to 2023) and Refinitiv Eikon (tracking S&P 500 entries and exits), I identified 48 unique breaches related to 11 S&P 500 MED companies. I began with an initial pool of 20,161 observable breaches. After eliminating breaches occurring outside the USA and other unusable data, I was left with 20,106 breaches. I then filtered out organizations not classified as "MED," followed by the exclusion of entries lacking breach or disclosure dates. Further narrowing the scope to the 2010–2019 time frame, the dataset was reduced to 4,932 breaches. Using Refinitiv Eikon database results, I then isolated breaches related to companies that were in the S&P 500 during that period, reducing the sample to 91 breaches. Finally, after removing duplicates, a limitation of the Privacy Rights

Clearinghouse database, the final data sample consisted of 48 unique breaches associated with 11 S&P 500 MED companies.

Sample Selection Criteria	Lost observations	Remaining Observations
Privacyrights.org database 2005-2023		20 161
Removed breaches outside the USA	15	20 146
Removed unusable data:	40	20 106
Removed all industries except "MED"	12 778	7 328
Removed all entries where date of breach/date of disclosure was not provided	1 868	5 460
Removed all entries on breaches that occurred outside the 2010-2019 time frame:	528	4 932
Removed all entries on breaches that were not from S&P 500 companies:	4 841	91
Removed duplicate breach entries for remaining sample:	43	48

Note: This table outlines the process used for sample selection. The final sample comprises 48 unique breaches across 11 different companies. For every individual breach, three financial reports were analyzed: one from the quarter of the breach and the two immediately preceding quarters.

Table 4 - Sample Selection Process (Source: Own Systematization)

As my research focus on determining how the occurrence and disclosure of a DSB affects the narrative accounting tone in financial reports, I identify the need for a control group who did not suffer any breaches. I utilized the Refinitiv Eikon Peer Company Ranking tool to select this control group, and the details of the selection process can be found in the accompanying Table 5.

Table 5 - Control Group Selection Process (Source: Own Systematization)

Database company (Breached)	Company Code (Breached)	Peer Company (Refinitiv Eikon) - Best match (Not breached)	Company Code (Not breached)	Refiniti Eikon Competitor Rank (Not breached)	Comments
Abbott	ABT.N	Medtronic	MDT.N	2	Rank 1 (BSX.N) was breached and included in my database
Baxter Intl	BAX.N	Stryker	SYK.N	2	Rank 1 (BSX.N) was breached and included in my database
Boston	BSX.N	Edwards Lifesciences Corp	EW.N	3	Rank 2 (ABT.N) was breached and included in my database Rank 1 (MDT.N) only has avaiable fillings starting from July 14, 2014. Breaches were before this date.
Centene	CNC.N	Elevance Health	ELV.N	3	Rank 1 (HUM.N); Rank 2 (CI.N); was breached and included in my database
Cigna Group	CI.N	Elevance Health	ELV.N	3	Rank 1 (UNH.N); Rank 2 (HUM.N); was breached and included in my database
CVS Health	CVS.N	Elevance Health	ELV.N	8	Rank 1 (CI.N); Rank 2 (UNH.N); Rank 7 (HUM.N) was breached and included in my database. Rank 3 (RAD.N) was not in S&P 500 from 2010-2019. Rank 4 (WMT.N); Rank 5 (AMZN.OQ); Rank 6 (WBA.OQ) are not from Healthcare industry.
DaVita	DVA.N	HCA Healthcare	HCA.N	2	Rank 3 (FMEG.DE) was not in S&P 500 from 2010-2019.
Humana DE	HUM.N	Elevance Health	ELV.N	1	
Laboratory Corp	LH.N	McKesson	MCK.N	4	Rank 1 (DGX.N) was breached and included in my database Rank 3 (COR.N) was not in S&P 500 from 2010-2019. Rank 2 (WBA.OQ) is not from Healthcare industry.
QuestDiagnostics	DGX.N	McKesson	MCK.N	4	Rank 1 (LH.N) was breached and included in my database Rank 2 (WBA.OQ) is not from Healthcare industry. Rank 3 (COR.N) was not in S&P 500 from 2010-2019.
UnitedHlth Grp	UNH.N	Cardinal Health	CAH.N	1	

After the control group and the treatment group are defined, I proceeded with the collection of reports: Q-10 reports or K-10 reports depending on the quarter of the breach. To enhance the rigor and conclusiveness of my research findings, I focus on examining financial reports corresponding to the quarter of the data breach, as well as the two quarters immediately preceding the breach. This approach allows for a better understanding of how narrative disclosure tone shifts before and after a breach occurs and is disclosed. I focus on gathering the following parts: Legal Proceedings (Item 1 in Q-10 reports and Item 3 in K-10 reports); Risk Factors (Item 1A in Q-10 and K-10 reports); Management's Discussion and Analysis of Financial Condition and Results of Operations (Item 2 of Part I in Q-10 reports and Item 7 in K-10 reports) as per SEC regulations (SEC 2023).

As per SEC rulings section "Legal Proceedings" outlines any significant legal matters that a firm or its subsidiaries are involved in. Specifies the court, the date initiated, the principal parties, the nature of the proceedings, and the relief sought. Companies should disclose cases that present a significant financial burden, are material to the business, or involve a governmental authority (SEC 2023). A DSB can lead to lawsuits or investigations by governmental agencies. How a firm discloses these proceedings in its financial reports can offer valuable insights on my study on how narrative disclosure tone shifts in response to such breaches.

Section "Risk Factors" outlines material risks a company faces. According to SEC, this section is expected to be organized logically, with each risk factor clearly described under relevant subheadings (SEC 2023). Companies are expected to update this section quarterly for any material changes (SEC 2023), as such, it could suffer changes as a result of a DSB which can impact tone.

Management's Discussion and Analysis (MD&A) section aims to provide material information, relevant for assessing the financial and operational results. It discusses material events and uncertainties that could have financial and operation impacts. MD&A provides retrospective and prospective analysis of material events impacting the company. It intends to present stakeholders a better view of a company's financial situation, operational results, and cash flows (SEC 2023). As a section that reflects management's views, discusses financial condition, operational results and material events affecting the company it is important to include in my analysis of narrative text. The narrative in MD&A also offers a qualitative view of the financial numbers that can be impacted by the occurrence of a DSB.

The final sample consists of 144 reports related to breached companies (treatment group) and 144 reports related to non-breached companies (control group). For each report I created a text file containing Legal Proceedings; Risk Factors and MD&A. This resulted in 288 text files.

I conduct the analysis of tone based on the dictionary of positive and negative words created by Loughran and McDonald (2011). This dictionary is well-regarded for its ability to accurately capture the sentiment expressed in financial documents. For this I used LIWC-22 software which is a leading software for word-use analysis used in over 20,000 scientific articles (LIWC 2023). I organized the data into two distinct folders: one for the control group and another for the treatment group, each containing the relevant text files. These folders were then individually imported into the LIWC-22 software, where I applied the Loughran and McDonald (2011) dictionary to calculate the percentage of positive and negative words in each report.

Subsequently after having collected the measurement of tone for the treatment group and control groups, as well as the information for the remaining independent variables of my model using Refinitiv Eikon for all 288 reports, we can observe the initial measurements in Table 6.

Variables	Mean	Median	Std.Dev.	Min	Max
TONE	-0.305	-0.247	0.213	-0.811	0.344
DSB	0.500	0.500	0.501	0.000	1.000
SIZE	24.488	24.804	0.730	21.555	26.116
ROA	0.013	0.013	0.012	-0.123	0.073
LOSS	0.028	0.000	0.165	0.000	1.000
LEVERAGE	0.208	0.191	0.110	0.081	0.965
EPS	2.143	1.760	1.358	0.100	6.050
BBACKGROUND	0.587	0.600	0.204	0.000	1.000
SEC2011	0.868	1.000	0.339	0.000	1.000
SEC2018	0.208	0.000	0.407	0.000	1.000
WC	9.363	9.343	0.594	7.854	10.970

The statistics presented are computed across 288 observations

Table 6 - Data description (Source: Own Systematization)

According to the data, the mean tone is -0.305, indicating that financial reports, on average, contain more negative words than positive words. The average firm size in the dataset corresponds to approximately 43.152 billion USD of total assets, based on the mean log value of 24.488, which is to be expected of S&P 500 companies. The mean ROA of 1.300% is positive but close to zero, suggesting that firms are, on average, slightly profitable. 2.800% of the observations refer to firms with quarterly losses. The average quarterly earnings per share (EPS) for firms in the dataset is 2.143 USD. In terms of leverage, data suggests that, on average, 20.800% of assets are financed by long-term debt. With regards to board backgrounds, 58.700% of board members, on average, have either an industry-specific or strong financial background. An analysis of the SEC11 variable reveals that 86.810% of the observations in my dataset fall on or after 2011. Similarly, variable SEC18 shows that 20.830% of the quarterly reports in my dataset are dated on or after 2018. As for the word count variable the dataset contains an

average of 11,649.28 words per report, based on the mean log value of 9.363. Lastly, the dataset is balanced in terms of companies that have and have not experienced a data security breach, as 50% of the observations refer to firms with DSBs.

2. Preliminary Analysis

Table 7 compares the mean tone between the treatment and control groups for each quarter.

Group	Quarter	Variables	Mean	Median	Std.Dev.	Min	Max	Mean % Negative Words	Mean % Positive Words
Treatment	Q - 2	TONE	-0.325	-0.316	0.242	-0.767	0.344	1.991	0.862
Treatment	Q - 1	TONE	-0.360	-0.344	0.236	-0.748	-0.026	2.105	0.898
Treatment	Q (Breach)	TONE	-0.414	-0.369	0.190	-0.742	-0.004	2.465	0.883
Control	Q - 2	TONE	-0.227	-0.235	0.184	-0.811	0.210	1.443	0.847
Control	Q - 1	TONE	-0.258	-0.219	0.133	-0.761	-0.070	1.445	0.839
Control	Q (Breach)	TONE	-0.247	-0.236	0.220	-0.729	0.221	1.428	0.804

The statistics presented are computed across 48 observations for each quarter belonging to each group (Total: 288 observations).
Q (Breach) denotes the quarter of the breach. Q-1 and Q-2 denotes the two quarters preceding the ocurrance and disclosure of the breach.

Table 7 - Preliminary Analysis - Treatment and Control Group (Source: Own Systematization)

In quarter of the breach, the mean tone for the treatment group is significantly lower than the one for the control group. The same is observable for the two preceding quarters, however, the gap decreases. There is also a noticeable a decrease in the mean tone from the preceding quarters to the quarter of the breach in the treatment group, however the same does not happen in the control group. This rationale is coherent with my hypothesis. I predicted that the occurrence and disclosure of a DSB influences the narrative accounting tone. Both the mean and median tone for the treatment group is significantly lower than the control group, peaking in the quarter of the breach. This could indicate that the occurrence and disclosure of a DSB influences narrative accounting tone. My theoretical hypothesis predicted that there would be an increase in negative tone

in the quarter of the breach when compared to preceding quarters. This preliminary analysis supports my hypothesis as mean tone for the treatment group in the quarter of the breach is significantly lower than the preceding quarters. Data also shows that the percentage of negative words increases from the preceding quarters to the quarter of the breach for the treatment group while the percentage of negative words stays relatively the same for the control group.

However, it is not possible to distinguish between the effects of DSB from other factors and firms in the two groups can be different on those observed factors. This motivates the use of a multiple linear regression approach, to account for the control variables discussed above.

3. Estimation Results

I estimated the equation outlined in Chapter 2 using the ordinary least squares estimator. Table 8 presents the estimation results.

Estiamation Results			
	OLS		
Variables	Q-2	Q-1	Q
DSB	-0.054	-0.084 *	-0.190 ***
	(0.046)	(0.042)	(0.051)
SIZE	0.009	0.004	-0.001
	(0.036)	(0.029)	(0.032)
ROA	-2.391	-2.879	-0.233
	(2.701)	(3.838)	(1.839)
LOSS	-0.309 *	-0.273 *	-0.294 *
	(0.175)	(0.140)	(0.160)
LEVERAGE	-0.471 **	-0.505 ***	-0.580 ***
	(0.195)	(0.179)	(0.203)
EPS	0.051 *	0.021	-0.004
	(0.027)	(0.027)	(0.022)
BBACKGROUND	0.048	0.198 *	0.042
	(0.121)	(0.108)	(0.117)
SEC2011	0.013	0.096	0.041
	(0.067)	(0.059)	(0.072)
SEC2018	-0.062	0.016	0.027
	(0.069)	(0.056)	(0.067)
WC	-0.077	0.041	0.013
	(0.048)	(0.040)	(0.040)
R-squared	0.243	0.256	0.26

The statistics presented are computed across 96 observations for each quarter (Total: 288 observations)
**** denote p-values <0.01, ** denote p-values <0.05, and * denote p values <0.10. Standard-errors in parenthesis.*

Table 8 - Estimation Results (Source: Own Systematization)

Results show that the control group is well-constructed. DSB is not statistically significant during the preceding quarters of the breach, however DSB is highly statistically significant during the breached quarter, suggesting that there is a considerable difference in narrative disclosure tone between firms that have experienced a data breach and those that have not, confirming that the control group (firms that did not suffer a breach) is different from the treatment group (breached firms).

For a firm that experiences a data security breach, the tone score would be expected to decrease by approximately 0.190 in the quarter of the breach, compared to a firm that did not experience a breach, holding all other variables constant. Given that the standard deviation of the tone variable (see Table 6) is of 0.213, the result is substantial. Results are also coherent with my hypothesis. I argued in my theoretical hypothesis that the occurrence and disclosure of a data security breach influence the narrative accounting tone.

Conclusion

This thesis examined the impact of the occurrence and disclosure of data breaches on the narrative accounting tone of 10-Q and 10-K reports in S&P 500 companies within MED industry. By employing a multiple linear regression approach and focusing on specific sections of those reports, such as Legal Proceedings, Risk factors and Management's Discussion and Analysis (MD&A), my research has provided valuable insights into how tone shifts in the quarter of the breach as well as the two preceding quarters.

Results demonstrate that the occurrence and disclosure of a DSB in the quarter of the breach impacts negatively narrative disclosure tone when compared to the two preceding quarters. It is also noticeable that DSB is not statistically significant in the quarters preceding the DSB. My research has important implications for auditors, analysts and interested stakeholders. It aims to inform stakeholders about the significance of narrative tone as an important tool for understanding a company's risk profile. Tracking the changes in a company's report tone can offer insights into undisclosed data security breaches.

The findings of this study are subject to limitations. Firstly, my research only focused on S&P 500 companies and the MED industry. As such, the results may not be generalizable to companies in other sectors or of different sizes. Secondly, my research is constrained to the time period between 2010 and 2019. It is possible that the impact of data breaches on narrative tone could vary in different periods. Thirdly, my research uses a quantitative approach to analyze the tone of narrative disclosures and it does not capture the context.

This research lays some basis for subsequent studies in the field. First, future research could expand the scope to include different industries and time frames. My research does not account for specific types of breaches, so future research could explore the impact of different types of data breaches, as well as, consider the scale of the breach when examining its effect on narrative tone. Second, period of analysis could also be expanded, as I only focused on the quarter of the breach and preceding quarters. As such, future research can also focus on the next two quarters. Third, future research can examine Legal Proceedings (Item 1 in 10-Q reports and Item 3 in 10-K reports); Risk Factors (Item 1A in 10-Q and 10-K reports) in isolation. These sections hold very little weight in my research as they are quite brief compared to the MD&A discussion. Additionally, there's rarely any change in risk factors and legal proceedings in a quarterly analysis, as companies usually update them only annually. Research focusing solely on the evolution of Section 1A. Risk Factors or Section 1. Legal Proceedings could yield different results, especially in an annual analysis.

References

Abou-El-Sood, H., & El-Sayed, D. (2022). Abnormal disclosure tone, earnings management and earnings quality. *Journal of Applied Accounting Research*, *23*(2), 402–433. https://doi.org/10.1108/JAAR-07-2020-0139

Acquisti, A., Friedman, A., Telang, R., Frank, S., Williams, J., & Ho, F. (2006). *IS THERE A COST TO PRIVACY BREACHES? AN EVENT STUDY 1*.

Alalwani, Z., & Mousa, G. A. (2020). Optimistic disclosure tone in corporate annual reporting and financial performance. *2020 International Conference on Decision Aid Sciences and Application, DASA 2020*, 1128–1133. https://doi.org/10.1109/DASA51403.2020.9317105

Amir, E., & Levi, S. (2018). *Do firms underreport information on cyber-attacks? Evidence from capital markets*. https://ssrn.com/abstract=3136193Electroniccopyavailableat:https://ssrn.com/abstract=3136193Electroniccopyavailableat:https://ssrn.com/abstract=3136193

Amir, E., Levi, S., & Livne, T. (2018). Do firms underreport information on cyber-attacks? Evidence from capital markets. *Review of Accounting Studies*, *23*(3), 1177–1206. https://doi.org/10.1007/s11142-018-9452-4

Arena, M., & Azzone, G. (2009). Identifying Organizational Drivers of Internal Audit Effectiveness. *International Journal of Auditing Int. J. Audit*, *13*, 43–60.

Ashraf, M. (2022). The Role of Peer Events in Corporate Governance: Evidence from Data Breaches. *Accounting Review*, *97*(1), 1–24. https://doi.org/10.2308/TAR-2019-1033

Bassyouny, H. (2020). *Narrative Disclosure Tone in the UK: Determinants and Consequences from Upper Echelons Theory*.

Bassyouny, H., Abdelfattah, T., & Tao, L. (2022). Narrative disclosure tone: A review and areas for future research. *Journal of International Accounting, Auditing and Taxation*, *49*, 100511. https://doi.org/10.1016/j.intaccaudtax.2022.100511

Berkman, H., Jona, J., Lee, G., & Soderstrom, N. (2018). Cybersecurity awareness and market valuations. *Journal of Accounting and Public Policy*, *37*(6), 508–526. https://doi.org/10.1016/j.jaccpubpol.2018.10.003

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. In *International Journal of Electronic Commerce / Fall* (Vol. 9, Issue 1).

Clatworthy, M., & Jones, M. J. (2003). Financial reporting of good news and bad news: Evidence from accounting narratives. *Accounting and Business Research*, *33*(3), 171–185. https://doi.org/10.1080/00014788.2003.9729645

Eaton, T. V., Grenier, J. H., & Layman, D. (2019). Accounting and Cybersecurity Risk Management. *Current Issues in Auditing*, *13*(2), C1–C9. https://doi.org/10.2308/ciia-52419

Ettredge, M., Guo, F., & Li, Y. (2018). Trade secrets and cyber security breaches. *Journal of Accounting and Public Policy*, *37*(6), 564–585. https://doi.org/10.1016/j.jaccpubpol.2018.10.006

Florackis, C., Louca, C., Michaely, R., & Weber, M. (2023). Cybersecurity Risk. *Review of Financial Studies*, *36*(1), 351–407. https://doi.org/10.1093/rfs/hhac024

Gagnon, J., Young, S., & Alves, P. (2020). *The Linguistic Properties of Award-winning Annual Reports The Linguistic Properties of Award-winning Annual Reports The Linguistic Properties of Award-winning Annual Reports*. https://ssrn.com/abstract=3575679Electroniccopyavailableat:https://ssrn.com/abstract=3575679

Goel, S., & Shawky, H. A. (2009). Estimating the market impact of security breach announcements on firm values. *Information and Management*, *46*(7), 404–410. https://doi.org/10.1016/j.im.2009.06.005

Gordon, B. L. A., Smith, R. H., & Loeb, M. P. (2010). M Arket V Alue of V Oluntary D Isclosures C Oncerning I Nformation S Ecurity 1. *MIS Quarterly*, *34*(3), 567–594.

Gordon, L. A., Loeb, M. P., Sohail, T., Tseng, C. Y., & Zhou, L. (2008). Cybersecurity, capital allocations and management control systems. *European Accounting Review*, *17*(2), 215–241. https://doi.org/10.1080/09638180701819972

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. https://doi.org/10.1080/07421222.2018.1451962

Janakiraman, R., Lim, J. H., & Rishika, R. (2018). The effect of a data breach announcement on customer behavior: Evidence from a multichannel retailer. *Journal of Marketing*, *82*(2), 85–105. https://doi.org/10.1509/jm.16.0124

Kothari, S. P., Shu, S., & Wysocki, P. D. (2009). Do managers withhold bad news. *Journal of Accounting Research*, *47*(1), 241–276. https://doi.org/10.1111/j.1475-679X.2008.00318.x

Lang, M., & Lundhold, R. (1993). Quality of Intellectual Capital and Human Resources Disclosure on the Firm Valuation. *Journal of Accounting Research*.

Linguistic Inquiry and Word Count (LIWC). 2023. Software for textual analysis. Available at: https://www.liwc.app/

Linsley, P. M., & Shrives, P. J. (2006). Risk reporting: A study of risk disclosures in the annual reports of UK companies. *British Accounting Review*, *38*(4), 387–404. https://doi.org/10.1016/j.bar.2006.05.002

Loughran, T., Mcdonald, B., Battalio, R., Easton, P., Fuehrmeyer, J., Gao, P., Harvey, C., Hirschey, N., Marietta-Westberg, J., & Schultz, P. (2011). When Is a Liability Not a Liability? Textual Analysis, Dictionaries, and 10-Ks. In *THE JOURNAL OF FINANCE •: Vol. LXVI* (Issue 1).

Malhotra, A., & Malhotra, C. (2011). Evaluating customer information breaches as service failures: An event study approach. *Journal of Service Research*, *14*(1), 44–59. https://doi.org/10.1177/1094670510383409

Marquez-Illescas, G., Zebedee, A. A., & Zhou, L. (2019). Hear Me Write: Does CEO Narcissism Affect Disclosure? *Journal of Business Ethics*, *159*(2), 401–417. https://doi.org/10.1007/s10551-018-3796-3

Martikainen, M., Miihkinen, A., & Watson, L. (2023). Board characteristics and negative disclosure tone. *Journal of Accounting Literature*, *45*(1), 100–129. https://doi.org/10.1108/jal-03-2022-0033

Mason, P., & Hambrick, D. (1984). Upper Echelons: The Organization as a Reflection of Its Top Managers. *Academy of Management*.

Othman, S. H., Zainal, A., Bharu, J., Bharu, J., & Bharu, J. (2019). Review of Cybersecurity Audit Management and Execution Approaches. *International Conference on Research and Innovation in Information Systems, ICRIIS*, *December-2*(IEEE Computer Society).

Patelli, L., & Pedrini, M. (2015). Is Tone at the Top Associated with Financial Reporting Aggressiveness? *Journal of Business Ethics*, *126*(1), 3–19. https://doi.org/10.1007/s10551-013-1994-6

Personen, W. (2009). *The Effect of Data Breaches on Shareholder Wealth*.

Pirounias, S., Mermigas, D., & Patsakis, C. (2014). The relation between information security events and firm market value, empirical evidence on recent disclosures: An extension of the GLZ study. *Journal of Information Security and Applications*, *19*(4–5), 257–271. https://doi.org/10.1016/j.jisa.2014.07.001

Prencipe, A. (2004). Proprietary costs and determinants of voluntary segment disclosure: evidence from Italian listed companies. *European Accounting Review*, *13*(2), 319–340. https://doi.org/10.1080/0963818042000204742

Privacy Rights Clearinghouse. 2023. Chronology of data breaches: FAQ. Available at: https://www.privacyrights.org/chronology-data-breaches-faq

Rosati, P., Gogolin, F., & Lynn, T. (2022). *Cyber-security incidents and audit quality*.

Rosati, P., Gogolin, F., Lynn, T., & School, M. (2017). *Cyber-security Incidents, External Monitoring and Probability of Restatements*. https://ssrn.com/abstract=3193880

Rosati, P., Lynn, T. G., & Gogolin, F. (2018). Cyber-Security Incidents, External Monitoring and Probability of Restatements. *SSRN Electronic Journal*, 1–33. https://doi.org/10.2139/ssrn.3193880

Schleicher, T., & Walker, M. (2010). Bias in the tone of forward-looking narratives. *Accounting and Business Research*, *40*(4), 371–390. https://doi.org/10.1080/00014788.2010.9995318

Securities and Exchange Commission (SEC). 2011. Cf disclosure guidance: Topic no. 2. Available at: https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm

Securities and Exchange Commission (SEC). 2018. Commission statement and guidance on public company cybersecurity disclosures. Available at: https://www.sec.gov/files/rules/interp/2018/33-10459.pdf

Securities and Exchange Commission (SEC). 2023. Form 10-K regulations. Available at: https://www.sec.gov/files/form10-k.pdf

Securities and Exchange Commission (SEC). 2023. Form 10-Q regulations. Available at: https://www.sec.gov/files/form10-q.pdf

Sen, R., & Borle, S. (2015). Estimating the Contextual Risk of Data Breach: An Empirical Approach. *Journal of Management Information Systems*, *32*(2), 314–341. https://doi.org/10.1080/07421222.2015.1063315

Steinbart, P. J., Raschke, R. L., Gal, G., & Dilla, W. N. (2018). The influence of a good relationship between the internal audit and information security functions on information security outcomes. *Accounting, Organizations and Society*, *71*, 15–29. https://doi.org/10.1016/j.aos.2018.04.005

Tausczik, Y. R., & Pennebaker, J. W. (2010). The psychological meaning of words: LIWC and computerized text analysis methods. In *Journal of Language and Social Psychology* (Vol. 29, Issue 1, pp. 24–54). https://doi.org/10.1177/0261927X09351676

Wang, T., Kannan, K. N., & Ulmer, J. R. (2013). The association between the disclosure and the realization of information security risk factors. *Information Systems Research*, *24*(2), 201–218. https://doi.org/10.1287/isre.1120.0437

Xu, H., Guo, S., Haislip, J. Z., & Pinsker, R. E. (2019). Earnings management in firms with data security breaches. *Journal of Information Systems*, *33*(3), 267–284. https://doi.org/10.2308/isys-52480

Yayla, A. A., & Hu, Q. (2011). The impact of information security events on the stock value of firms: The effect of contingency factors. *Journal of Information Technology*, *26*(1), 60–77. https://doi.org/10.1057/jit.2010.4