IF YOU CANNOT MEASURE IT, YOU CANNOT MANAGE IT: THREE ESSAYS ON CYBERSECURITY RISK ASSESSMENT

By ARION CHEONG

A dissertation submitted to the
Graduate School-Newark
Rutgers, The State University of New Jersey
In partial fulfillment of requirements
for the degree of
Doctor of Philosophy
Graduate Program in Management
Written under the direction of
Dr. Miklos A. Vasarhelyi and Dr. Won Gyun No
and approved by

____________________________________

____________________________________

____________________________________

____________________________________

Newark, New Jersey

May 2021
ABSTRACT OF THE DISSERTATION

If you cannot measure it, you cannot manage it: Three essays on cybersecurity risk assessment

By Arion Cheong

Dissertation Director(s):

Dr. Miklos A. Vasarhelyi and Dr. Won Gyun No

Cybersecurity has received enormous attention in recent years. The volume of cyberattacks is dramatically increasing, in line with the explosive growth in the number of cybersecurity breaches. A computerized business environment makes the organization exposed to a greater cybersecurity vulnerability. Top managements are deeply concerned about the potential for cybersecurity threats that hinder the growth of their firms (Symantec, 2016). While cybersecurity risk measures have been developed, many of them are based on attributes that reflect technical aspects (e.g., IT infrastructure) and managerial considerations (e.g., cybersecurity policies). The complex nature of cybersecurity, however, renders it difficult to assess a firm's cybersecurity risks. In light of this challenge, I will introduce three different empirical methodologies in my dissertation to assess cybersecurity-related events using a data analytic approach. The first chapter proposes a methodology to measure the firm-specific information in cybersecurity risk disclosure. The second chapter assesses the insider threat after the massive layoff during the COVID-19 period by utilizing a unique dark web dataset. Finally, the last chapter introduces a new methodology to measure latency inequality in order execution for stock exchanges.
ACKNOWLEDGMENTS

I express my deepest appreciation to my advisors, Dr. Miklos A. Vasarhelyi and Dr. Won Gyun No. Your guidance taught me how to become a researcher, and from your valuable mentoring and sincere encouragement, I was able to complete this dissertation as well as my doctoral studies. Also, I am very grateful to my committee members, Dr. Alexander Kogan and Dr. Soohyun Cho, for their continuous support and guidance. Your caring feedbacks and academic spirit had let me complete my doctoral studies successfully. I would also like to appreciate Dr. Dan Palmon for your whole-hearted support and insightful comments that made me motivated and focused on research. And, I hope to express my gratitude to Dr. Michael Alles, who has always provided me constructive feedbacks and suggestions during my research and doctoral studies. I would also like to show my great respect to my mentors, Dr. Lawrence A. Gordon and Dr. J. Efrim Boritz, who have been great supporters of my academic journey. Also, I hope to mention Dr. Tawei Wang for his continuous guidance. At last, I am so thankful to my family and Emma for their continuous faith and love from the bottom of my heart.
# TABLE OF CONTENTS

ABSTRACT OF THE DISSERTATION .................................................................................. ii

ACKNOWLEDGMENTS .................................................................................................. iii

TABLE OF CONTENTS ................................................................................................. iv

LIST OF TABLES ........................................................................................................... viii

LIST OF FIGURES ........................................................................................................ ix

CHAPTER 1: INTRODUCTION ...................................................................................... 1

CHAPTER 2: BACKGROUND ......................................................................................... 5

  Traditional Approach to Measure in Cybersecurity Risk ........................................... 5

  Measuring the Firm-specific Information in Cybersecurity Risk Disclosure ............... 6

  Measuring the Insider Threat ..................................................................................... 7

  Measuring the Fair-trading Opportunities in the Stock Exchange ............................. 8

CHAPTER 3: AN APPLICATION OF TEXTUAL ANALYSIS TO QUANTIFY FIRM-
  SPECIFIC INFORMATION IN CYBERSECURITY RISK DISCLOSURES .................. 10

  Introduction ................................................................................................................ 10

  The Quality of Cybersecurity Risk Disclosure ......................................................... 14

    The Significance of Cybersecurity Risks ................................................................. 14

    The Need for Quantifying Cybersecurity Risk ......................................................... 14

    Earlier Studies on Disclosure Quality Using Textual Analysis .............................. 15

  Cybersecurity Risk Disclosure Score ......................................................................... 17

    Data Collection ....................................................................................................... 18
Weighted Cybersecurity Risk Topic Modeling (WCRTM) – Quantifying the Context of the Cybersecurity Risk Disclosure.................................- 19 -

Textual Imagification (TI) – Dealing with the Multicollinearity among Cybersecurity Risk Topics..........................................................- 21 -

Cybersecurity Risk Disclosure Score (CRDS) – Measuring the Aggregated Level of Cybersecurity Risk Disclosure.............................................- 23 -

Dynamic Peer Group Identification (DPGI) – Identifying Industry Peer Firms..............- 23 -

Industry-adjusted Cybersecurity Risk Disclosure Score (Industry-adjusted CRDS).......- 26 -

Results..........................................................................................................................- 27 -

Risk Topics and Multicollinearity..............................................................................- 27 -

Industry-adjusted Cybersecurity Risk Disclosure Score.............................................- 29 -

Industrial Aspects of Cybersecurity Risk..............................................................- 31 -

Breached Firm and Non-Breach Firm.................................................................- 33 -

WCRTM and DPGI Comparison Based on Human-Judgement..............................- 34 -

The Market Reaction to Firm-specific Cybersecurity Risk .......................................- 35 -

Conclusion, Limitations, and Future Research..........................................................- 38 -

CHAPTER 4: MEASURING THE INSIDER THREAT AFTER MASSIVE LAYOFF USING DARK WEB MARKET DATA..........................................................- 41 -

Introduction.............................................................................................................- 41 -

Literature Review.....................................................................................................- 48 -

Reciprocal loyalty .....................................................................................................- 48 -

Employee-driven cybersecurity threats......................................................................- 50 -
Hypotheses..................................................................................................................................................- 52 -

Data Sources, Variable Measurement Methods, and Descriptive Statistics ..................- 56 -

Data Sources and Sample Construction .......................................................................................- 57 -

Insider Information Leakage Measurement and Sample Characteristics ......................- 61 -

Data Analysis and Results .............................................................................................................- 63 -

Layoff and Insider Threat .............................................................................................................- 63 -

Insider Threat and Employee Loyalty ..........................................................................................- 67 -

Managerial Implication of the Results .......................................................................................- 69 -

Conclusions .......................................................................................................................................- 71 -

CHAPTER 5: A FRAMEWORK TO MEASURE LATENCY INEQUALITY FOR FAIR-
TRADING IN THE STOCK EXCHANGE .........................................................................................- 72 -

Introduction ......................................................................................................................................- 72 -

The Arms Race of Low Latency ....................................................................................................- 74 -

Real-time Latency Information .......................................................................................................- 76 -

Gini-based Latency Inequality Index (GiniLI) .............................................................................- 76 -

Stage 1: Measuring the Latency Inequality ..................................................................................- 77 -

Stage 2: Anomaly Detection in Latency Inequality ....................................................................- 78 -

Stage 3: Identifying the Cause of GiniLI Anomaly .....................................................................- 79 -

Results and Performance ...............................................................................................................- 81 -

GiniLI Statistics and Predictability ...............................................................................................- 81 -

Deterrence Effect of GiniLI on Latency .......................................................................................- 85 -
Conclusion .......................................................................................................................... - 88 -

CONCLUSION ................................................................................................................... - 90 -

BIBLIOGRAPHY ................................................................................................................ - 92 -

APPENDICES ..................................................................................................................... - 104 -

Appendix A: Detail of the CRDS Measurement Process ......................................................... - 104 -
  A.1. Simplified Flowchart ................................................................................................ - 104 -
  A.2. Detailed Flowchart ................................................................................................... - 105 -

Appendix B: A Platform of CRDS for U.S. Public Firms ..................................................... - 106 -

Appendix C .......................................................................................................................... - 107 -
  C.1. Business Description (Item 1) Extraction ................................................................ - 107 -
  C.2. Risk Factors (Item 1A) Extraction ............................................................................. - 107 -

Appendix D .......................................................................................................................... - 108 -
  D.1. Risk Topic Classification ........................................................................................ - 108 -
  D.2. Saturation Process .................................................................................................... - 109 -
  D.3. Distributed Firm Vector Representation .................................................................... - 109 -

Appendix E: Alternative Approach to Identify Dark Web Post ............................................. - 111 -
LIST OF TABLES

Table 1. Sample Selection..................................................................................................................- 19 -
Table 2. Glossary of Terms..................................................................................................................- 21 -
Table 3. Risk Topic Images and Keywords ......................................................................................- 29 -
Table 4. Industry-adjusted CRDS Descriptive Statistics .................................................................- 30 -
Table 5. Facebook Industry-adjusted CRDSs by Year and DPGI Keywords .................................- 33 -
Table 6. OLS Regression Results ....................................................................................................- 37 -
Table 7. Sample selection ..................................................................................................................- 60 -
Table 8. Descriptive Statistics for Insider Information Leakage ..................................................- 62 -
Table 9. Insider Information Leakage after Layoff ........................................................................- 63 -
Table 10. The Effect of Layoff on Insider Information Leakage .....................................................- 66 -
Table 11. The Effect of Employee Loyalty on Insider Information Leakage ..................................- 68 -
Table 12. GiniLI Statistics ...............................................................................................................- 82 -
Table 13. Augmented Dickey-Fuller Test .........................................................................................- 82 -
Table 14. Latency and Cancellation Rate .........................................................................................- 84 -
LIST OF FIGURES

Figure 1. Summary of the CRDS Measurement Process .................................................. - 18 -
Figure 2. Example of Distributed Vector Representations .............................................. - 25 -
Figure 3. Pair-wise Pearson Correlation between Topic-Word Embedding Vectors ........... - 28 -
Figure 4. Analysis of Industry-adjusted CRDS by Year.................................................. - 31 -
Figure 5. Scatterplot of firm-year observations (Industry-adjusted CRDS) ..................... - 34 -
Figure 6. Unemployment and insider threat-related news ............................................. - 52 -
Figure 7. The fraud triangle (Cressey 1953) ................................................................. - 53 -
Figure 8. Sample selection process .............................................................................. - 57 -
Figure 9. Illustration of Time Windows for Key Variable Construction ......................... - 61 -
Figure 10. Layoff and Insider Information Leakage ....................................................... - 67 -
Figure 11. Employee Loyalty and Insider Information Leakage (Layoff Firms) ............. - 69 -
Figure 12. Inspection Window Determination .............................................................. - 79 -
Figure 13. Overview of GiniLI Process ......................................................................... - 81 -
Figure 14. Rolling Mean and Standard Deviation of GiniLI .......................................... - 83 -
Figure 15. GiniLI and Latency ...................................................................................... - 86 -
Figure 16. The Cost of Latency ..................................................................................... - 88 -
CHAPTER 1: INTRODUCTION

In 2013, FBI director James B. Comey testified before the U.S. Senate Committee on Homeland Security and Governmental Affairs that the “resources devoted to cyber-based threats will equal or even eclipse the resources devoted to non-cyber based terrorist threats” (FBI, 2013). Admittedly, we live in an era where nation-states, hacktivist entities, sophisticated hackers, and even insiders are prompting to steal sensitive information across firms, vendors, clients, and even mass individuals. Cybersecurity has received enormous attention in recent years, and cybersecurity breaches have become a material threat to the firm. Yet, most of the predeveloped cybersecurity risk assessment only reflects the technical aspects (e.g., IT infrastructure, system failures). Especially, the complex nature of cybersecurity renders it difficult to assess a firm's cybersecurity risks. In accordance, most of the standards and certifications in cybersecurity, such as the International Standard Organization (ISO), promote the use of an ordinal scoring method that highly depends on professional judgment.

Considering the lack of preciseness of such rough ordinal measures, experts have been concerned about the consequence of the management's business decisions relying on such rough measures. An excerpt from the bestseller “How can we measure anything in cybersecurity risk” by Hubbard and Seiersen (2016) addresses that, “There is no evidence that the types of scoring and risk matrix methods widely used in cybersecurity improve judgment. On the contrary, there is evidence these methods add noise and error to the judgment process. One researcher—Tony Cox—goes as far as to say they can be “worse than random.”
What if we could measure the cybersecurity risk quantitatively? Since the risk management builds upon the risk assessment, the continuous measurement of cybersecurity risk can improve the business judgment to specify the likelihood and impact of an adverse cybersecurity incident (Cherdantseva et al., 2016). Most importantly, proper risk measurement could reduce the uncertainty in cybersecurity, of which Hubbard and Seiersen (2016) point out as follows: “Yet resources are limited. Therefore, the cybersecurity professional must effectively determine a kind of “return on risk mitigation.” Whether or not such a return is explicitly calculated, we must evaluate whether a given defense strategy is a better use of resources than another. In short, we have to measure and monetize risk and risk reduction.”

Despite the benefits of measuring the risk of cybersecurity, the dynamicity and multidimensionality of the attack surface make it hard to assess and measure the risk quantitatively. In light of this challenge, I introduce three studies that propose an empirical approach to evaluating cybersecurity-related events by utilizing advanced data analytic methods. Compared to the literature that mostly uses financial attributes to gauge the firm's cybersecurity risk, I utilize non-financial information from exogenous sources such as the dark web to better measure a firm’s cybersecurity. Further, in my dissertation, I detail how to obtain and analyze such unstructured data.

The first chapter proposes a methodology to assess the quality of the firm’s cybersecurity risk disclosure. This research is motivated by a large number of cyberattacks or data breaches and the related needs of market participants such as investors, regulators, and other stakeholders for better cybersecurity breach notification. This study suggests a comprehensive measurement mechanism for quantifying the degree of firm-specific
cybersecurity risk specified in the cybersecurity risk disclosure provided by the management. Prominent text analytic technique (LDA2vec) and an advanced machine learning technique (Autoencoder) are used to capture the firm-specific information. In specific, I introduce the application of textual analytical methods that can consider both the disclosures' context (i.e., the data that information providers discuss therein) and intensity (i.e., degree of details) of discussion while weighing the high correlation of the context (i.e., risk factors). Moreover, since a firm's textual disclosure includes firm-specific contents and the contents shared with peer firms, a new approach is introduced to separate those two different content types from the disclosure.

The second chapter examines the impact of layoffs on an insider threat in IT firms, specifically whether lay offing IT roles can lead to insider information leakage in the dark web market. I investigate how employee loyalty associates with insider threats once massive layoffs are announced. Notably, the study utilizes a unique dataset collected from the dark web market, where illegally obtained information and insider information are traded. Moreover, employee loyalty is measured from the crowd-contributed online platform in which employees provide reviews of their firm. The results indicate that an insider threat originates from a massive layoff and that the degree of an insider threat depends on the level of employee loyalty. I observe higher dark web market exposure after a massive layoff after three weeks from the layoff announcement date. Overall, this study alerts the regulators and managers about the prevalence of insider threats during the pandemic period.

Finally, the last chapter introduces a new methodology to measure the latency inequality in the stock exchange. This research is motivated by the rapid stock market
downturn, known as the "flash crash" in 2016, that recorded the second-largest point swing in the U.S. stock market (Lewis, 2014). Despite the high-frequency trading (HFT) industry protestations, the regulators are suspecting high-frequency algorithms as the principal cause of the flash crash. Such traders are suspected of utilizing algorithmic trading, quoting an unusual amount of stock orders within a short period, and immediately canceling the order, to manipulate the market. This study measures the inequality in quote latency that can serve as a means to provide a fair-trading opportunity to the market participants. In specific, I suggest a measure, the Gini-based Latency Inequality Index (GiniLI), which is inspired by the Gini coefficient that measures the statistical dispersion of income distribution. The proposed model centered on the GiniLI dynamically determines abnormal transactions based on forecasting analysis and identifies the factors that cause the inequality (e.g., system attributes, brokerage services). GiniLI can further serve as a benchmark of latency inequality to alert the regulators for suspicious machine-driven market manipulative activities.

My dissertation offers three main contributions to the literature and practice. First, the measurement mechanism can enable the stakeholders and the practitioners to make a better-informed managerial decision using public disclosures. Second, the regulators and auditors can develop similar cybersecurity risk measures following the analytical approaches introduced in this research to evaluate cybersecurity risk. Finally, the results provide the strength of the data that are mostly publicly available and serve as evidence that cybersecurity events can be measured quantitatively.
CHAPTER 2: BACKGROUND

Traditional Approach to Measure in Cybersecurity Risk

Major organizations in cybersecurity claim various types of cybersecurity scoring systems and risk metrics. For example, the National Institute of Standards and Technology (NIST) provides a vulnerability metric known as the Common Vulnerability Scoring System (CVSS). Also, the International Standards Organization (ISO) and the Open Web Application Security Project (OWASP) promotes their self-developed cybersecurity scoring system. In particular, scale-based measures are widely used to rate the impact and the likelihood of an adverse cybersecurity incident. Based on the practitioner’s professional judgment, the impact and likelihood are rated between a certain range of scales and plotted on a cybersecurity risk matrix or a risk map.

While the measures are endorsed by credible organizations, the measurement is based on rough estimates such as an ordinal score represented as low, medium, or high. Despite the expert’s concerns on the preciseness of such rough measures (Hubbard and Seiersen, 2016), OWASP asserts that “It is not necessary to be over-precise in this estimate. Generally, identifying whether the likelihood is low, medium, or high is sufficient.” While most security vendors and standard bodies promote the usage of the risk matrix, the literature in cybersecurity risk assessment has consistently asserted the possibility of replacing the scale-based measure with quantitative metrics (Agrafiotis et al., 2016; Rathod and Hämäläinen, 2017). Notably, Hubbard and Seiersen (2016) address that the traditional cybersecurity measures can be improved by utilizing “a variety of existing and newly emerging sources” and “can be measured and tracked to make continuous improvements.”
Measuring the Firm-specific Information in Cybersecurity Risk Disclosure

As cybersecurity-related issues have emerged as a critical risk to the firm, the importance of cybersecurity risk disclosure and incident reporting has been demanded by stakeholders and investors (Srinivas et al., 2019). The regulators have also responded to the market demand for informative cybersecurity risk disclosure by laws and regulations (Bensoussan et al., 2020; Tang and Whinston, 2020; Wang et al., 2020; Yang et al., 2020). Notably, the U.S. Security Exchange Commission (SEC) has issued interpretive guidance on cybersecurity risk disclosures (SEC, 2011; SEC, 2018). Furthermore, the Association of International Certified Professional Accountants (AICPA) announced a cybersecurity risk management reporting framework for organizations that engage in System and Organization Controls (SOC) for cybersecurity examination.\(^1\)

In general, prior studies in cybersecurity risk disclosure have focused on the determinants and the impact of informative cybersecurity risk disclosure (Walton et al., 2020). Studies that investigated the determinants have mostly focused on the regulators’ influence. Gordon et al. (2006) empirically identified that the Sarbanes-Oxley Act (SOX) of 2002 had increased the amount of information conveyed on the information security risk disclosure. Further, Brown et al. (2018) found that firms include more cybersecurity-related information on their subsequent disclosures when their industrial peer group receives an SEC comment letter. Studies on the impact of informative cybersecurity risk disclosure have identified that the market positively reacts when the firm provides more informative cybersecurity risk disclosure (Berkman et al., 2018; Gordon et al., 2010).

Even while firms are required to provide an informative cybersecurity risk

---

\(^1\) More information about SOC for Cybersecurity is accessible at AICPA (https://tinyurl.com/saz47pkw).
disclosure (SEC, 2018), there are no explicit guidelines or requirements on “what should be disclosed” and “how much informative it should be” (Meiers, 2006). Further, the SEC (2018) emphasizes that firms should disclose firm-specific cybersecurity risk rather than industry-general cybersecurity risk: “Companies should avoid generic cybersecurity-related disclosure and provide specific information that is useful to investors.” The first chapter of the dissertation will suggest a measurement mechanism to examine the amount of firm-specific cybersecurity risk disclosure.

**Measuring the Insider Threat**

Cybersecurity has been viewed as a technical issue, where most practitioners focused on the internal system and control to assess the cybersecurity risk. In contrast, recent surveys on cybersecurity breaches found that most of the incidents are related to insiders. Based on the report from Securonix (2020), 80% of employees leave the organization with data, also known as the flight-risk, and these individuals with the flight-risk cause roughly 60% of insider threats. In fact, such insider threat is infeasible to be prevented or even detected, even by implementing the most advanced security measures (Wall, 2013; Young et al., 2014; Homoliak et al., 2019).

In spite of the challenges, most of the audit protocols for IT assurance specific to insider threats are focused on examining the effectiveness of information security.² For instance, ISO 17799 provides a list of controls (ISO, 2000), which are mostly preventive measures (e.g., personnel screening and confidentiality agreement), under the category of “Personnel Security” to protect the organizations from insider threats. Zeadally et al. (2012) describe that “Unfortunately, given the complexity of the problem and the human

---

² For more details about the evaluation process, refer to SEI (https://tinyurl.com/52j787k8).
factors involved, many solutions which have been proposed face strict constraints and limitations when it comes to the working environment. As a result, many past insider threat solutions have in practice failed in their implementations.”

Recently, insider threats have enormously risen due to the increased use of the dark web by malicious insiders. Insider forums, such as “Kickass” or “Insider Trading”, have become the Amazon for malicious actors who are seeking insider information, which is also referred to as the “Insider Threat-as-a-service.” WulKan et al. (2016) describes in their recent report that: “The dark web has created a market for employees to easily monetize insider access. Currently, the dark web serves as a vehicle insider use to “cash-out” on their services through insider trading and payment for stolen credit cards.” The rise of the insider information marketplace provides the means to measure the insider threat by inspecting the information that is “actually leaked and traded” rather than “what can potentially be leaked or traded.” In the second chapter of the dissertation, I conduct an empirical analysis on the incremental insider threat imposed by the recent massive layoff caused by COVID-19.

*Measuring the Fair-trading Opportunities in the Stock Exchange*

Jeffrey Craig Sprecher, the chairman of the New York Stock Exchange, stated at the Futures Industry Association (FIA) futures industry conference in Boca Raton that “the markets had undergone an arms race for speed.” SEC (2014) notes that “estimates of HFT typically exceeded 50% of total volume in U.S.-listed equities … HFT is a dominant component of the current market structure and likely to affect nearly all aspects of its performance.”

In the era of an arms race for speed, the fair-trading opportunities highly depend on the order execution latency. Compared to the broker-dealers' processing delay, which is
strictly regulated and monitored by the regulators, the latency caused by the internal system in the stock exchange is less discussed. Furthermore, trading firms are spending millions of dollars each year to place their trading computers in the same location where the exchange servers reside, which practice is known as collocation (Rogow, 2012). Despite the high cost of owning a space in the data center, collocation allows firms to reduce the latency caused by the network (GBFR, 2013).

Consequently, in the third chapter, I propose a framework for the stock exchange to monitor and control latency inequality caused by the processing delay. Notably, the framework is centered on the newly suggested measure, the Gini-based Latency Inequality Index, that can serve as a standardized benchmark to determine the fair-trading opportunity within the electronic exchange platform within the stock exchange.
CHAPTER 3: AN APPLICATION OF TEXTUAL ANALYSIS TO QUANTIFY FIRM-SPECIFIC INFORMATION IN CYBERSECURITY RISK DISCLOSURES

Introduction

IT innovation has developed in tandem with increased cyberattacks and data breaches (Ji et al., 2016; Pala and Zhuang, 2019). Various global firms, including Equifax, Target, Sony, and Yahoo, have suffered cybersecurity incidents (Armerding, 2018) that have exacted a severe toll on their business. A recent report from Audit Analytics (2020) addresses that incident reporting and cybersecurity risk disclosure affects stock market values and leads to enforcement penalties. Due to the significant cost associated with the negative disclosure, management has strong incentives to disclose general risks (e.g., boilerplate) and withhold information on firm-specific cybersecurity risks, which risks are uncertain to outsiders (Zhu et al., 2015; Amir et al., 2018; Sen et al., 2020). A firm’s cybersecurity risk disclosure is voluntary and often available in the form of a text document. Since cybersecurity risk has a significant adverse effect on a firm’s performance, the stakeholders need to assess the risk kept increasing (August et al., 2019; Zhang et al., 2020). However, assessing such risk is not a simple task, considering the lack of a quantitative method measuring a firm’s cybersecurity risk using its cybersecurity risk disclosure.

This study proposes a new approach to measure cybersecurity risk that a firm discloses and presents a new quantitative measure of firm-specific cybersecurity risk disclosed by the firm. Specifically, I measure the amount of cybersecurity risk disclosed by a firm and disentangle its unique cybersecurity risk (i.e., firm-specific cybersecurity
risk) from the shared risk by its industry peer firms (i.e., industry-level cybersecurity risk).

Many stakeholders, such as investors, researchers, and regulators, will find this method useful for assessing firms’ cybersecurity risks using publicly available disclosures. For instance, the measure responds to the U.S. Securities and Exchange Commission (SEC) guidance on cybersecurity risk disclosure in 2011 (SEC, 2011) that requires firms to disclose more on industry-level than firm-specific cybersecurity risk. In particular, industry-level risk disclosure increases year to year while firm-specific risk disclosure remains the same even after 2011. Further, by replicating Gordon et al. (2010)’s study about the market reaction to cybersecurity risk disclosure, the result suggests that the market reacts to firm-specific information (i.e., firm-specific cybersecurity risk) rather than industry-level information (i.e., industry-level cybersecurity risk).

When measuring cybersecurity risk disclosed by a firm, it is necessary to consider the intrinsic properties of cybersecurity. Cybersecurity vulnerabilities provided by the National Institute of Standards and Technology (NIST)’s National Vulnerability Database show that many cybersecurity risks are interlinked in both internal and external to the firm’s security activities. According to Hubbard and Seiersen (2016), the factors related to cybersecurity vulnerabilities, consequences, and threats feature a high level of correlation that can hinder the development of a mechanism to measure cybersecurity risks. In order to quantify the amount of information conveyed in the firm’s cybersecurity risk disclosure while considering the interconnectedness between the risks, I transform the cybersecurity risk disclosure into an image. Such image is designed 1) to identify specific cybersecurity risks, referred to as risk topics, depicted in the cybersecurity risk disclosure and 2) to capture the degree of the information regarding risk topics. In other words, the image
represents the interconnectedness between risk topics by capturing the mutual (semantic) relationship between the risk topics in a given cybersecurity risk disclosures.

To this end, I first identify the types of cybersecurity risk (i.e., risk topics) and the degree of risk topics depicted in each firm’s cybersecurity risk disclosure (i.e., Item 1A portions addressing cybersecurity risks) by applying text analytics. Next, a neural network, Autoencoder, is applied to generate a measure by considering high correlations between risk topics taken from textual analysis. Autoencoder is used to handle these highly interlinked risk topics since machine learning (or neural network) methods overcomes multicollinearity issues compared to traditional regression methods (Clarke et al., 2009; Garg and Tai, 2013). The measure is referred to as the Cybersecurity Risk Disclosure Score (CRDS).

Next, I disentangle the cybersecurity risks disclosed by the firm into two components: industry-level CRDS (i.e., disclosed risks that a firm shares with its industry peer firms) and firm-specific CRDS (i.e., disclosed risks that belong to a specific firm). According to the SEC (2016), firms’ risk factor disclosures (i.e., Item 1A of 10-K) are often generic, rather firm-specific, and mirror those of their industry peers. If firm-specific risks can be distinguished from other commonly shared risks, stakeholders and policymakers (e.g., SEC) can make better-informed investment and regulation decisions by considering a firm’s unique cybersecurity risks. To measure firm-specific CRDS, industry peer groups (similar to industry sectors) are considered and then evaluated whether a given firm possesses higher cybersecurity risks relative to other firms in its peer group. Instead of adapting existing industry classification schemes (e.g., Fama-French Industry Classification), this study suggests an alternative method to identify a firm’s industry peer
group, which updates annually based on its business activities to timely capture the business environment that the firm faces. Specifically, each firm’s business description is extracted from Item 1 of 10-K and analyzed by applying a textual classification technique. Since Item 1 presents each firm’s business, including products and services, markets, and operating activities, the proposed method classifies firms based on the description of their business activities. The classified peer groups enable to generate CRDS per industry peer group (industry-level CRDS) and CRDS that captures the discrete deviations from its peer group (firm-specific CRDS).

This work offers three main contributions to the literature and practice: 1) the measurement mechanism (i.e., CRDS of individual firms) can enable stakeholders to make better-informed decisions by assisting them in assessing cybersecurity risks using publicly available firms’ disclosures; 2) the mechanism also helps policymakers seeking to develop enhanced cybersecurity-related guidelines by providing a means of evaluating the quality and degree of firms’ cybersecurity risk disclosures; and 3) the suggested procedures and techniques offer a new approach by addressing the problems of existing methodologies (e.g., correlations among various factors, known as multicollinearity in a statistical term).

The remainder of this paper proceeds as follows. The next section further explains the need to quantify cybersecurity risks and provides an overview of the relevant literature. The following section provides details on a methodology for quantifying cybersecurity risks. Next, the results are presented and an application of my cybersecurity risk measure. Finally, I conclude by summarizing the study and discussing the limitations of the study and trajectories for future research.
The Quality of Cybersecurity Risk Disclosure

In this section, the timeliness of this study is discussed, along with potential policymaking and research areas to which the study might contribute. A subsequent amount of existing literature was reviewed that helped to motivate this research and enabled the development of the study.

The Significance of Cybersecurity Risks

This research is motivated by the prevalence of cyberattacks or data breaches and the related needs of market participants, such as investors, regulators, and other stakeholders of firms. Among the significant challenges that firms faced in recent years, cybersecurity-related issues have emerged as a critical risk factor to be considered by stakeholders and investors (Srinivas et al., 2019). Reflecting on the growing seriousness of cyberattacks and threats, regulators also have revealed their concerns and responded to this increasingly pressing issue through laws and regulations (Bensoussan et al., 2020; Tang and Whinston, 2020; Wang et al., 2020; Yang et al., 2020). The SEC has issued interpretative guidance on cybersecurity risk disclosures (SEC, 2011; 2018). The Federal Communications Commission (FCC) has also introduced strict disclosure requirements for firms that fall under their jurisdiction (FCC, 2016). Furthermore, with the cost of cybercrime projected to hit $6 trillion per year on average through 2021 (Eubanks, 2017), state and local governments have bolstered efforts to detect cyberattacks and data breaches. For example, since 2017, the New York Department of Financial Services (NYDFS) has required firms to report data breaches within 72 hours of their discovery (NYDFS, 2017).

The Need for Quantifying Cybersecurity Risk

Timely and relevant cybersecurity risk disclosure is critical for market participants
because such risks exert material adverse effects on firms’ business operations, financial
In an effort to prompt market participants to identify and access firms’ risks, the SEC
mandated public firms to disclose significant risks, including cybersecurity risks, in Item
1A of their annual reports (10-Ks) and quarterly reports (10-Qs) in 2005 (SEC, 2005).
Additionally, the SEC issued guidance on cybersecurity risk disclosures in 2011 and
announced additional specific guidelines related to cybersecurity risk disclosures in 2018,
including the reporting of firm protocols related to cybersecurity incidents and the types of
cybersecurity incidents a firm experienced in a given year (SEC, 2011; 2018).

Market participants appear eager to have a measurement mechanism that can assess
the quality of cybersecurity risk disclosure using various resources. According to previous
studies, a comparable and accessible measuring mechanism of firms’ cybersecurity risk
disclosures could contribute to improving social welfare (Kunreuther and Heal, 2003; Gal-
Or and Ghose, 2005; Moore and Clayton, 2011). Moreover, by utilizing a cybersecurity
risk disclosure measure, firms can compare the level of their cybersecurity risks with those
of their peer groups, potentially motivating them to reduce their security vulnerabilities to
improve their performances and attract investors (Tang et al., 2013). In response to this
growing need, this study proposes a measurement mechanism to identify and ultimately
measure each firm’s cybersecurity risk addressed in its cybersecurity risk disclosure.

Earlier Studies on Disclosure Quality Using Textual Analysis

Previous studies identified a broad range of firm risks from voluntary risk
disclosures and their quality using textual analytic techniques. Huang and Li (2008) first
proposed a supervised learning model to categorize risk topics in risk factor disclosures
(i.e., Item 1A of 10-K). Echoing this approach, more recent studies have analyzed the tone, sentiment, and readability of disclosures related to risk topics to examine the disclosure quality using the bag-of-words model (Tetlock et al., 2008; Feldman et al., 2010, Loughran and McDonald, 2011). Other approaches to analyze firm risks using textual analytics are introduced by Bao and Datta (2014) and Wang et al. (2013). Their studies examine the content of risk topics by applying an unsupervised learning model to the results derived from the bag-of-words or LDA models.3

Further, an increasing number of studies have focused their investigative scope on cybersecurity risks in line with the growing awareness of the inherent dangers of cyberattacks and data breaches and with the expanded availability of cybersecurity-related resources (i.e., mandated reporting of cyberattacks). Notably, Li et al. (2018) addressed their frustration on measuring the firm-specific information contained in the cybersecurity risk disclosure due to the challenges associated with the bag-of-words approach. In specific, a predefined dictionary has shown limitations on capturing the evolving nature of cybersecurity environments (e.g., not capturing newly introduced malware or security terms).

This study is the first to develop a quantitative measuring mechanism of firm-specific cybersecurity risk by applying textual analytics to the qualitative disclosures of all public firms (i.e., generating scores based on the textual analysis of firms’ disclosures). With this mechanism, market participants can assess a firm’s cybersecurity risk at a glance and compare severity levels among a cross-section of firms promptly. In addition,

3 Refer to Blei et al. (2003) for more details about Latent Dirichlet Allocation (LDA) model.
policymakers could potentially use the mechanism to craft regulatory guidelines for disclosures on cybersecurity risks since firms often fail to unveil their cybersecurity content adequately or disclose cybersecurity risks in a timely manner (Moore and Clayton, 2011).

**Cybersecurity Risk Disclosure Score**

To generate the Cybersecurity Risk Disclosure Score (CRDS), I quantify the cybersecurity risks disclosed by all public firms (hereafter disclosed cybersecurity risks) by first applying text analytics to the firms’ qualitative disclosures. Then a machine learning technique is used to analyze the risks. In this section, the data source and a series of applications (e.g., text analytics and machine learning techniques) are discussed for quantifying cybersecurity risk. The applications are structured based on the design science approach, a methodology used to develop and evaluate novel and innovative artifacts (Simon, 1996; Hevner et al., 2004; Hevner and Chatterjee, 2010; Adomavicius et al., 2013). Figure 1 summarizes the approach to generating CRDS. The CRDS measurement process consists of three main components: conducting textual analysis on Item 1A (Weighted Cybersecurity Risk Topic Modeling), quantifying cybersecurity risks (Textual Imagification), and identifying industry peer groups (Dynamic Peer Group Identification). The generated CRDSs are presented through the platform, as shown in Appendix A.

---

4 See Appendix A for more detailed measurement process.
Data Collection

A Form 10-K is a detailed annual report that all public firms are required to file with the SEC. It provides an appropriate data source for measuring a firm’s disclosed cybersecurity risk because of two main reasons. First, the SEC mandates that each firm provides adequate cybersecurity-related disclosures in its 10-K (e.g., the impact of cybersecurity incidents, responses to such incidents, and protocols to address potential incidents). Second, there are no other publicly available sources reporting the cybersecurity risks of all public firms in the U.S.

This study compiles the 10-Ks of all public firms for the period between 2006 and 2019 from the SEC’s Electronic Data Gathering, Analysis, and Retrieval (EDGAR) system. The data consist of 119,344 10-Ks from 22,761 firms. Next, each Item 1 (business description) and Item 1A (risk factors) from each 10-K are parsed out, resulting in the final sample of 75,441 10-Ks from 9,654 firms that contain both Item 1 and Item 1A. The final sample of Item 1 is different from that of Item 1A because smaller reporting companies are not required to provide risk factor disclosure (Item 1A).
provides a summary of the sample selection procedures. I then eliminate observations that have missing values on any of the variables of interest in Compustat and CRSP. These procedures result in a subsample consisting of 19,061 disclosures from 3,732 firms for examining the market reaction to firm-specific cybersecurity risk in the following section.

Table 1. Sample Selection

<table>
<thead>
<tr>
<th>No. of Disclosures</th>
<th>No. of Firms</th>
</tr>
</thead>
<tbody>
<tr>
<td>10-K filings for FYR 2006-2019</td>
<td>119,344</td>
</tr>
<tr>
<td>Less: No Item 1</td>
<td>(19,608)</td>
</tr>
<tr>
<td>Less: No Item 1A</td>
<td>(24,295)</td>
</tr>
<tr>
<td>Total Sample Used in Industry-adjusted CRDS Measurement</td>
<td>75,441</td>
</tr>
<tr>
<td>Less: No Financial Information provided by Compustat</td>
<td>(10,570)</td>
</tr>
<tr>
<td>Less: No Stock Information provided by CRSP</td>
<td>(27,665)</td>
</tr>
<tr>
<td>Less: Fiscal Years before the SEC guidance in 2011</td>
<td>(18,145)</td>
</tr>
<tr>
<td>Total Sample Used in An Application of CRDS</td>
<td>19,061</td>
</tr>
</tbody>
</table>

Weighted Cybersecurity Risk Topic Modeling (WCRTM) – Quantifying the Context of the Cybersecurity Risk Disclosure

Cybersecurity is broad and constantly changing, so does cybersecurity risk. Within the general blanket of cybersecurity risk are various types of risk, and each firm may have different types of cybersecurity risk (e.g., insider threats and access controls). Given the vast volume of text data (i.e., cybersecurity risk disclosures), and due to the infeasibility of manually analyzing the disclosures to understand and gain meaningful insights, I leverage topic modeling, a powerful textual analytic technique to organize, understand, and summarize large collections of textual information. Specifically, the types (i.e., topics) of disclosed cybersecurity risk are identified by applying an advanced textual analytic
technique (LDA2vec) to cybersecurity risk disclosures in 10-Ks (see Appendix A – WCRTM). The reason for applying this technique is twofold. We need to consider risk topics addressed in a firm’s cybersecurity disclosure (Item 1A of 10-K). At the same time, we need to determine the number of times each risk topic is mentioned in the disclosure to assess each firm’s cybersecurity risk level. The process is referred to as the Weighted Cybersecurity Risk Topic Modeling (WCRTM) in this study.

To measure the disclosed cybersecurity risks by applying LDA2vec to the disclosures, I first extract Item 1A from each 10-K and then obtain the text that addresses cybersecurity risks from each Item 1A (see Step 1 in Appendix A). After preprocessing the extracted text (henceforth preprocessed risk disclosure), LDA2vec is applied to the preprocessed risk disclosures (see Step 2 in Appendix A). Applying LDA2vec provides two components that are essential to quantifying cybersecurity risks (considering that the portion is a mixture expressed as \( \bar{d}_j = p_{j0} \cdot \bar{t}_0 + p_{j1} \cdot \bar{t}_1 + \ldots + p_{jn} \cdot \bar{t}_n \) in the disclosure): 1) \( \bar{t}_k \) (risk topic word embedding vector), which consists of a risk topic \( k \) and a vector representation showing the semantic spatial relationship of the risk topic; and 2) \( p_{jk} \) (risk topic weight), which represents the percentage breakdown (i.e., how often each risk topic is mentioned in each document \( \bar{d}_j \)) of the different risk topics. Table 2 summarizes the terms discussed in this paper.

---

6 The specified text of each Item 1A consists of the paragraphs that include keywords related to cybersecurity risks. A detailed description of the procedures can be found in Appendix C.2.

7 According to Moody (2016), LDA2vec enables not only to obtain powerful representations in Word2vec but also to construct human-interpretable representations through LDA.

8 Detailed mathematical representation of LDA2vec can be found in Appendix D.1.
### Table 2. Glossary of Terms

<table>
<thead>
<tr>
<th>Term</th>
<th>Symbol</th>
<th>Composition</th>
<th>Format</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Topic Word Embedding Vector</td>
<td>$\vec{t}_k$</td>
<td>Word embedding for risk topic $k$</td>
<td>Vector</td>
</tr>
<tr>
<td>Risk Topic Weight</td>
<td>$p_{jk}$</td>
<td>Cybersecurity risk disclosure $j$’s membership likelihood for risk topic $k$</td>
<td>Scalar</td>
</tr>
<tr>
<td>Weighted Risk Topic Vector</td>
<td>$\vec{p}_j$</td>
<td>Vector representation of $p_{jk}$ for cybersecurity risk disclosure $j$’s risk topic $k$</td>
<td>Vector</td>
</tr>
<tr>
<td>Risk Topic Image</td>
<td>$I(\vec{u}_k)$</td>
<td>$i$-dimensional vector (\vec{u}_k) mapped to RGB color space</td>
<td>Vector</td>
</tr>
<tr>
<td>Weighted Risk Topic Image</td>
<td>$I(p_{jk}\vec{u}_k)$</td>
<td>$I(\vec{u}<em>k)$ adjusted by $p</em>{jk}$</td>
<td>Vector</td>
</tr>
</tbody>
</table>

Twenty risk topics risk topics are extracted from the disclosures between the fiscal year 2006 and 2019, based on the optimal number of topics determined by the Within Cluster Sum of Squares (WCSS). As a subsequent step, a machine learning technique is applied to the textual analysis results (aforementioned two components from LDA2vec) in order to quantify cybersecurity risk (i.e., compute CRDS).

**Textual Imagification (TI) – Dealing with the Multicollinearity among Cybersecurity Risk Topics**

As discussed, high correlations among the risk topics deter an accurate and comprehensive measurement of cybersecurity risk. To address this correlation issue when computing CRDS, this paper proposes Textual Imagification (TI) (see Appendix A – TI). The process involves converting the results of textual analysis (LDA2vec) into weighted risk topic images, becoming the input for a machine learning technique (Autoencoder). A specific color is assigned to each risk topic vector and symbolizes the context of the vectors (i.e., the semantic association of the risk topics). More specifically, similar colors with varying intensity levels are assigned to similar topic vectors, and contrasting colors are assigned to dissimilar topic vectors. Hence, the topic images capture the similarity (i.e.,
color) among topics and the significance (i.e., intensity) of each topic.

For a specific color to be assigned to a risk topic vector, $i$-features in the vector need to be encapsulated within three features because the RGB color model represents a color by combining three features (red, green, and blue). By applying principal component analysis (Pearson 1901), I produce a 3-dimensional vector that represents the embedding of a topic word in an $i$-dimensional vector ($\vec{u}_k$). The 3-dimensional vector is then mapped into the RGB color model to generate a risk topic image, $I(\vec{u}_k)$. The weight of each risk topic, $p_{jk}$, is represented by the intensity of the color (i.e., if a risk topic is represented as blue by the RGB model, a weighted risk topic can be represented with a deeper blue or a lighter blue, depending on the weight). Appendix D.2 contains a detailed mathematical representation of the saturation process. The final output of the process is a weighted risk topic image for each risk topic, $I(p_{jk}, \vec{u}_k)$.

To sum up, a series of analytic processes produces the weighted risk topic image as an input to Autoencoder. In specific, the processes map a risk topic word embedding vector into an RGB color while representing the weight of the risk topic using the intensity of the color (see Step 3 in Appendix A). These processes ultimately allow capturing the textual analysis results from cybersecurity risk disclosures (i.e., Item 1A portions addressing cybersecurity risks) in a “snapshot” representing each weighted risk topic as an image. These images can be useful as visual results of cybersecurity risk disclosures (i.e., the results of LDA2vec applications) since visualization may allow to garner considerable amounts of information at a single glance (Anscombe, 1973; Tufte, 1983; Bera et al., 2019), and the visual results can be easily interpreted and verified by a human.
Cybersecurity Risk Disclosure Score (CRDS) – Measuring the Aggregated Level of Cybersecurity Risk Disclosure

As the next step, I compute CRDS by applying a neural network, Autoencoder, to the weighted risk topic images (see Step 4 in Appendix A). Autoencoder is a useful technique for processing risk topics (resulted from LDA2vec) that are highly correlated to each other. An average pattern of weighted risk topic images is generated by applying Autoencoder. Based on Dua and Du (2011)’ workflow process, I then obtain each firm’s CRDS by measuring the deviation of its weighted risk topic image from the aforementioned average pattern.

Specifically, an average pattern is generated using the weighted risk topic images of all firms from the 2006 to 2017 period (66,409 observations); this pattern generation is a training step in machine learning. The model developed in the training step is then applied to the test step with the weighted risk topic images of firms in 2018 and 2019 (9,032 observations). After comparing the weighted risk topic image of a given firm against the average pattern (i.e., the reconstructing error in the Autoencoder application), the deviation between the two images is computed as the firm’s CRDS (see Step 5 in Appendix A).

Dynamic Peer Group Identification (DPGI) – Identifying Industry Peer Firms

Industry-specific governance and corporate structures can cause firms in the same industry group to tend to share similar cybersecurity risks as opposed to the risks faced by firms from different industries. Therefore, the cybersecurity risks and security environment confronting a firm are highly likely to be affected by the industry to which the firm belongs. For instance, the assessed cybersecurity risk level of firms in the energy/utilities sector is likely to be higher than that of firms in the agriculture and construction sectors (Redteam,
Accordingly, when assessing the cybersecurity risks of a firm, it is necessary to consider the risks shared among its peer firms as well as the unique risks facing the firm itself.

In order to measure industry-level CRDS, it is essential to determine peer groups. There are various existing industry classification schemes, including the Standard Industrial Classification (SIC), the North American Industrial Classification System (NAICS), and the Fama-French Industry Classification. However, considering the dynamic nature of firms’ businesses in recent years, this study suggests a new industry classification that more reasonably reflects firms’ business areas and activities rather than adopting the aforementioned existing classification schemes. Accordingly, this study uses the business description of each firm (i.e., Item 1 of 10-K), which encompasses the focus areas and current business activities of the firm as well as considerations that exert a significant influence over the decisions of its stakeholders. Based on the textual analysis results of Item 1, each firm is classified into an industry peer group (see Appendix A – DPGI).

The Dynamic Peer Group Identification (DPGI) process represents a series of analytical procedures. First, after downloading all available 10-Ks between 2006 and 2019 from the SEC’s EDGAR system, I extract Item 1 from each 10-K and preprocess them (see Step 6 in Appendix A and Appendix C.1). Next, each preprocessed Item 1 is transformed into a paragraph vector (Le and Mikolov 2014), more popularly known as Doc2vec, to represent all words in a distributed vector form (see Appendix D.3 for a detailed

---

9 For example, in recent years, Amazon has changed its business focus from e-commerce to cloud services. Since the existing classification schemes are 20th century constructs, they are less likely to accurately reflect Amazon’s changes in its business activities.
mathematical representation of the model). In addition to word embedding (i.e., the co-occurrence of words in a given text), Doc2vec also considers document-unique textual features by adding a paragraph vector to the multidimensional distributed vector representation. The results of the distributed vector identify the words that describe each firm’s business in Item 1 as well as the semantic relationships between the words themselves (see Step 7 in Appendix A). Figure 2 shows an example of my distributed vector representation. For the sake of brevity and illustrative purposes, the example displays only representative words.

![Figure 2. Example of Distributed Vector Representations](image)

The figure illustrates the Doc2vec results of Amazon and Facebook. The $\vec{d}_1$ and $\vec{d}_2$ indicate the paragraph vectors of Facebook and Amazon, respectively. The paragraph vectors are mapped based on the relevance between the words (i.e., word embedding) describing the firms’ businesses in Item 1. Facebook’s Item 1 ($\vec{d}_1$) describes the firm’s business using the following four representative words (i.e., words closer to $\vec{d}_1$): Advertiser
Similarly, Amazon’s Item 1 ($d_2$) describes its business with the following four words: Subscriber ($\bar{w}_2$), platform ($\bar{w}_3$), Commerce ($\bar{w}_5$), and Service ($\bar{w}_6$). A linkage between the words and the length of the linkage between two words represent the semantic relationships determined by the similarity of the words’ context (i.e., the co-occurrence of words).

Based on the Doc2vec results, I identify peer firms and then cluster peer firms into industry peer groups by applying the K-means algorithm to the paragraph vectors (see Step 8 in Appendix A). After determining the industry peer groups, each cluster is labeled by LDA topic modeling and their representative words.

**Industry-adjusted Cybersecurity Risk Disclosure Score (Industry-adjusted CRDS)**

Finally, to facilitate comparisons within an industry group and between industry groups, I generate an Industry-adjusted Cybersecurity Risk Disclosure Score (Industry-adjusted CRDS) of each firm (see Step 8 in Appendix A.2). The Industry-adjusted CRDS of a specific firm $i$ belonging to a given industry $v$ is represented as follows:

$$Industry\text{-}adjusted \ CRDS_i = \frac{CRDS_i}{\sigma_{CRDS_v}} = \frac{\mu_{CRDS_v}}{\sigma_{CRDS_v}} + \frac{CRDS_i - \mu_{CRDS_v}}{\sigma_{CRDS_v}}$$

where $\sigma_{CRDS_v}$ and $\mu_{CRDS_v}$ are the standard deviation and mean of CRDS in industry $v$, respectively.

Industry-adjusted CRDS, which is computed by dividing a firm’s CRDS by the

---

10 The number of clusters is adjusted based on the elbow method by considering the distance between clusters and the distance between firms within each cluster. Depending on the number of firms in each cluster, a cluster may consist of several sub-clusters.
standard deviation of the CRDSs of a specific industry, can be segmented into two components: Industry-level CRDS \( \left( \frac{\mu_{\text{CRDS}}}{\sigma_{\text{CRDS}}} \right) \) and Firm-specific CRDS \( \left( \frac{\text{CRDS}_i - \mu_{\text{CRDS}}}{\sigma_{\text{CRDS}}} \right) \). With these two components, we can compare the disclosed cybersecurity risks of firms that belong to different industry groups. More specifically, the Industry-level CRDS allows to capture the amount of disclosed cybersecurity risks common to a specific industry group (i.e., homogeneously shared within the industry), which is described as the industry effect (Mauri and Michaels 1998). On the other hand, the Firm-specific CRDS, which represents the deviation from the average of the industry group, enables us to compare the relative risk levels of firms from different industries. In other words, the Firm-specific CRDS presents a given firm’s unique cybersecurity risk, which is affected by the heterogeneous characteristics of its peer firms. Therefore, Industry-adjusted CRDS can help stockholders and researchers identify the disclosed cybersecurity risks of specific industry sectors and/or compare specific firms from different industry sectors.

Results

Risk Topics and Multicollinearity

We observe high correlations among the risk topics, which hinder an accurate and comprehensive measurement of cybersecurity risk. The risk topics captured from WCRTM show the partial or full dependency (or homogeneity) that cannot be mutually exclusive (or heterogeneous). Figure 3 shows a Pearson correlation heat map, which represents the correlations between topic-word embeddings. The results suggest that the risk topics are indeed correlated.
Traditional topic model analysis (i.e., regression analysis) cannot handle correlated topics since it requires variables to be mutually exclusive. As an alternative approach, this study introduces TI, which enables to recognize correlated risk topics as homogeneous inputs and identify representative topics. More specifically, as seen in the examples in Table 3, risk topics 9, 16, and 17 include similar keywords and contexts, and similar colors are thus assigned to the topics (i.e., most of the topics describing data vulnerable to potential cybersecurity threat). On the other hand, risk topics 2, 3, 6, 13, 14, 18 comprise different keywords and contexts, and thus dissimilar colors are assigned (i.e., violation of security objectives – confidentiality, integrity, and availability). Other topics assigned blue colors are related to the business risk imposed by cybersecurity threats and vulnerabilities. The colors, which reflect the semantic information in the risk topics as well as the relationships among the topics, can help to derive more appropriate representative risk topics as opposed to merely deriving them according to their weight in a given document (e.g., counting specific words in a given document), without considering the relations among the topics.
Table 3. Risk Topic Images and Keywords

<table>
<thead>
<tr>
<th>Color Class</th>
<th>Risk Topic</th>
<th>Label</th>
<th>Representative Keywords</th>
<th>Risk Topic Image</th>
</tr>
</thead>
<tbody>
<tr>
<td>Red Max (R,G,B) = R</td>
<td>Topic 9</td>
<td>Customer Data</td>
<td>Customer, Confidential, Data</td>
<td>Red</td>
</tr>
<tr>
<td>Topic 16</td>
<td>Third-party Data</td>
<td>Third, Party, Data</td>
<td>Orange</td>
<td></td>
</tr>
<tr>
<td>Topic 17</td>
<td>Business Data</td>
<td>Operation, Product, Data</td>
<td>Orange</td>
<td></td>
</tr>
<tr>
<td>Green Max (R,G,B) = G</td>
<td>Topic 2</td>
<td>Integrity</td>
<td>Misstated, Unscrupulous, Overlap</td>
<td>Green</td>
</tr>
<tr>
<td>Topic 3</td>
<td>Information Leakage</td>
<td>Leakage, Mismanage, Damage</td>
<td>Green</td>
<td></td>
</tr>
<tr>
<td>Topic 6</td>
<td>Availability</td>
<td>Information, Inaccessible, DDoS</td>
<td>Green</td>
<td></td>
</tr>
<tr>
<td>Topic 13</td>
<td>Confidentiality</td>
<td>Confidential, Personal, Data</td>
<td>Green</td>
<td></td>
</tr>
<tr>
<td>Topic 14</td>
<td>Infrastructure Failure</td>
<td>Infrastructure, System, Computer</td>
<td>Green</td>
<td></td>
</tr>
<tr>
<td>Blue Max (R,G,B) = B</td>
<td>Topic 1</td>
<td>Reputational Loss</td>
<td>Reputational, Loss, Customer</td>
<td>Blue</td>
</tr>
<tr>
<td>Topic 4</td>
<td>Copyright Infringement</td>
<td>Copyright, Prohibition, Holder</td>
<td>Blue</td>
<td></td>
</tr>
<tr>
<td>Topic 5</td>
<td>System Maintenance Cost</td>
<td>Billed, Proposal, Rising</td>
<td>Blue</td>
<td></td>
</tr>
<tr>
<td>Topic 7</td>
<td>Political Advocacy</td>
<td>Congress, Advocacy, Violence</td>
<td>Blue</td>
<td></td>
</tr>
<tr>
<td>Topic 8</td>
<td>Financial Damage</td>
<td>Financial, Damage, Risk</td>
<td>Blue</td>
<td></td>
</tr>
<tr>
<td>Topic 10</td>
<td>Insider Threat</td>
<td>Employee, Engineer, Policy</td>
<td>Blue</td>
<td></td>
</tr>
<tr>
<td>Topic 11</td>
<td>Security Regulation</td>
<td>Regulation, Law, Impose</td>
<td>Blue</td>
<td></td>
</tr>
<tr>
<td>Topic 12</td>
<td>Third-Party Risk</td>
<td>Third, Party, Loss</td>
<td>Blue</td>
<td></td>
</tr>
<tr>
<td>Topic 15</td>
<td>System Interruption</td>
<td>Service, System, Interruption</td>
<td>Blue</td>
<td></td>
</tr>
<tr>
<td>Topic 19</td>
<td>Breach Event</td>
<td>Breach, Event, Business</td>
<td>Blue</td>
<td></td>
</tr>
<tr>
<td>Topic 20</td>
<td>Cyber Liability</td>
<td>Harm, Claim, Customer</td>
<td>Blue</td>
<td></td>
</tr>
</tbody>
</table>

Industry-adjusted Cybersecurity Risk Disclosure Score

Table 4 provides the descriptive statistics of the Industry-adjusted CRDS results. Specifically, the Firm-specific CRDS and Industry-level CRDS are scaled between 0 to 1 (Score 0 – the least disclosing firm and Score 1 – the most disclosing firm). To better understand the results, the results are visualized in Figure 4. Each line in Figure 4.A represents the distribution of firms’ Industry-adjusted CRDSs from 2006 to 2019. The red dashed lines show the average of firms’ Industry-adjusted CRDSs for years before the SEC guidance, introduced in 2011 (i.e., fiscal years until 2011). The solid blue line represents
the average Industry-adjusted CRDSs for fiscal years between 2012 to 2017 after the SEC issued guidance on cybersecurity risk disclosure in 2011. At last, the green dashed line shows the average of Industry-adjusted CRDSs for the fiscal years between 2018 and 2019. Figure 4.A reveals that the shape of the Industry-adjusted CRDS distribution for fiscal years before the SEC guidance is significantly more right-skewed (i.e., higher mean) than other years. Figure 4.B provides the segmentation of Industry-adjusted CRDS between Industry-level and Firm-specific CRDS. there is significant increase in the disclosure of overall cybersecurity risk in 2011, which corresponds with the introduction of the SEC guidance. In specific, the graph shows a significant increase in industry-level cybersecurity risk disclosure in 2011, while the amount of firm-specific cybersecurity risk disclosure remains the same toward the entire observation period. This indicates that the SEC guidance increased the industry-level cybersecurity risk disclosure but not the firm-specific risk information.

**Table 4. Industry-adjusted CRDS Descriptive Statistics**

<table>
<thead>
<tr>
<th></th>
<th>Count</th>
<th>Mean</th>
<th>Std</th>
<th>Min</th>
<th>25%</th>
<th>50%</th>
<th>75%</th>
<th>Max</th>
</tr>
</thead>
<tbody>
<tr>
<td>CRDS</td>
<td>75,441</td>
<td>256.12</td>
<td>461.59</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>321.28</td>
<td>2519.75</td>
</tr>
<tr>
<td>Industry-level CRDS</td>
<td>75,441</td>
<td>0.41</td>
<td>0.19</td>
<td>0</td>
<td>0.24</td>
<td>0.42</td>
<td>0.56</td>
<td>1.00</td>
</tr>
<tr>
<td>Firm-specific CRDS</td>
<td>75,441</td>
<td>0.09</td>
<td>0.06</td>
<td>0</td>
<td>0.05</td>
<td>0.07</td>
<td>0.10</td>
<td>1.00</td>
</tr>
<tr>
<td><strong>PRC-3M</strong></td>
<td>19,061</td>
<td>31.04</td>
<td>100.09</td>
<td>0</td>
<td>2.30</td>
<td>12.13</td>
<td>36.98</td>
<td>4,284.70</td>
</tr>
<tr>
<td><strong>BVPS</strong></td>
<td>19,061</td>
<td>10.34</td>
<td>53.29</td>
<td>-173.06</td>
<td>0.39</td>
<td>4.44</td>
<td>13.18</td>
<td>2,900.93</td>
</tr>
<tr>
<td><strong>EPS</strong></td>
<td>19,061</td>
<td>0.58</td>
<td>9.27</td>
<td>-798.17</td>
<td>-0.43</td>
<td>0.04</td>
<td>1.52</td>
<td>309.96</td>
</tr>
<tr>
<td><strong>Assets</strong></td>
<td>19,061</td>
<td>4,983.64</td>
<td>23,580.49</td>
<td>0.00</td>
<td>43.81</td>
<td>380.90</td>
<td>2,209.20</td>
<td>717,242.00</td>
</tr>
</tbody>
</table>

Notes:
CRDS Industry-adjusted Cybersecurity Risk Disclosure Score
IL_CRDS Industry-level CRDS
FS_CRDS Firms-specific CRDS
PRC-3M Stock price of firm i for year t, 90 days after fiscal year close
BVPS Book value of equity divided by the number of shares outstanding for firm i for year t, year-end
EPS Earnings per share (basic excluding extraordinary items) for firm i for year t, year-end
Assets Assets for firm i for year t
Figure 4. Analysis of Industry-adjusted CRDS by Year

A. Distribution of Industry-adjusted CRDS

Note: The density plot is smoothed by Kernel Density Estimation (i.e., a continuous version of a histogram).

B. Industry-level Industry-adjusted CRDS and Firm-specific Industry-adjusted CRDS

Industrial Aspects of Cybersecurity Risk

Firms in the same industry are often exposed to similar types of cybersecurity risk, while those in different industries have dissimilar types of risk. More specifically, if a firm belongs to a specific industry for several years and is subsequently classified into a new
industry due to changes in its business activities, this change in industry designation is likely to influence my Industry-adjusted CRDS measure. For instance, Facebook’s Industry-adjusted CRDSs have consistently increased since 2013, ostensibly due to significant changes in its business activities. Since 2014, according to Item 1 of its 10-K and news reports, Facebook has defined itself as an advertisement and e-commerce provider rather than a platform provider, which had been its main business area in previous years. Table 5 shows the changes in Facebook’s business areas. Consider the Facebook-Cambridge Analytica scandal. Cambridge Analytica, a data analytics firm, used Facebook users’ data for political campaigning. Given that Facebook users’ data was initially collected for targeting customers with digital ads and later accessed by Cambridge Analytica, Facebook’s privacy problem is relevant to the change in its designated business activities in 2014 (Cadwalladr and Graham-Harrison, 2018).

In 2018, Facebook was classified as a financial institution, mainly due to their new business introduction to cryptocurrency and blockchain, which industry has shown the highest industry-level CRDS in 2019 (i.e., industry that is disclosing the most amount of information about their cybersecurity risk). In accordance, Facebook’s Industry-adjusted CRDS increased significantly in 2018. Indeed, the designation change in main business areas is not a one-time event for many IT firms. These types of businesses, which include Facebook, are continually changing their business focus and, as a result, are likely to be exposed to different types and levels of cybersecurity risks. In sum, the analysis indicates that it is essential to consider the dynamic aspects of a firm’s business that change over time when measuring its cybersecurity risk. This measure captures these dynamic aspects of a firm’s business.
Table 5. Facebook Industry-adjusted CRDSs by Year and DPGI Keywords

<table>
<thead>
<tr>
<th>Fiscal Year</th>
<th>Industry</th>
<th>Industry-adjusted CRDS</th>
<th>Industry-level CRDS</th>
<th>Firm-specific CRDS</th>
</tr>
</thead>
<tbody>
<tr>
<td>2013</td>
<td>Video, Voice, Search</td>
<td>198.15</td>
<td>0.613</td>
<td>0.052</td>
</tr>
<tr>
<td>2014</td>
<td>Advertiser, Ad, Campaign</td>
<td>466.25</td>
<td>0.599</td>
<td>0.076</td>
</tr>
<tr>
<td>2015</td>
<td>Advertiser, Virtual, Subscription</td>
<td>797.80</td>
<td>0.675</td>
<td>0.093</td>
</tr>
<tr>
<td>2016</td>
<td>Advertiser, Ad, Commerce</td>
<td>914.48</td>
<td>0.659</td>
<td>0.103</td>
</tr>
<tr>
<td>2017</td>
<td>Advertiser, Subscription, Server</td>
<td>937.64</td>
<td>0.762</td>
<td>0.091</td>
</tr>
<tr>
<td>2018</td>
<td>Bank, Merchant, Institution</td>
<td>1362.74</td>
<td>0.880</td>
<td>0.107</td>
</tr>
<tr>
<td>2019</td>
<td>Bank, Money, Merchant</td>
<td>1010.99</td>
<td>1.000</td>
<td>0.069</td>
</tr>
</tbody>
</table>

Breached Firm and Non-Breach Firm

I evaluate the performance of the Autoencoder scoring mode based on well-known evaluation metrics. Furthermore, the model is examined to differentiate non-breached firms from breached firms by exploring the distribution of Industry-adjusted CRDS. The result shows a significant distributional difference (untabulated results) between non-breached and breached firms. As shown in Figure 5, non-breached firms mostly have reconstruction errors lower than 500. In contrast, most of the breached firms are located above 500 in the scatterplot, which indicates a higher level of firm-specific cybersecurity risk disclosure. The result aligns with the literature, where the amount of cybersecurity risk disclosure can be a predictive indicator of future breaches (Wang et al., 2013).

---

11 I have identified 244 incidents between year 2006 to 2019 from the State of California Department of Justice (https://oag.ca.gov), Privacy Right Clearing House (https://privacyrights.org), and Audit Analytics https://www.auditanalytics.com). For the sake of readability, 59 incidents are depicted in Figure 5.
As an additional evaluation for WCRTM and DPGI, a web-based survey of 33 undergraduate students was performed to evaluate whether the risk topics identified by the LDA2vec reasonably represent cybersecurity risks that appear in firms’ disclosures. First, each participant received the cybersecurity risk disclosures (i.e., Item 1A portions addressing cybersecurity risks) of four randomly selected firms from my sample. To screen out participants paying little or no attention, I provided them risk topics from the LDA2vec analysis for three disclosures, while the risk topics for one disclosure were deliberately wrong. Each participant was then asked to read each disclosure and answer “Yes” if the provided risk topics represented risks that appeared in the disclosure and “No” otherwise.

Of the 33 participants, two did not complete the survey, and nine did not correctly answer the screening question (i.e., identify the disclosure with the wrong risk topics). Hence, responses from 22 participants are used in this analysis. On average, 83.3% of the 22 participants reported that the risk topics from the LDA2vec analysis correctly represent risks that appear in the disclosures: 90.9%, 77.2%, and 81.8% for each disclosure,
respectively. Similarly, the participants were provided with the business descriptions (i.e., Item 1) of four firms randomly selected from the sample. Each participant read each firm’s business description and chose the most closely aligned industry with its business activities from a randomly selected list of 10 industries. On average, 84.8% of the 22 participants selected the industry identified by the DPGI: 95.4%, 86.3%, and 72.7% for each firm, respectively.

The Market Reaction to Firm-specific Cybersecurity Risk

This section presents an application of Industry-adjusted CRDS by examining the market reaction to firm-specific cybersecurity risk ($FS_{CRDS}$) and industry-level cybersecurity risk ($IL_{CRDS}$). According to Gordon et al. (2010), the market positively reacts to firms that voluntarily disclose items concerning information security. The finding suggests that firms’ stock price increases when the firms provide value-relevance information (i.e., useful information for decision making) to the stakeholders. Compared to the proposed measure in this paper, which measures the amount of information as a continuous variable for each firm-specific cybersecurity risk and industry-level cybersecurity risk, Gordon et al. (2010)’s measure is a dummy indicator: Disclosure = 1 if the firm has any security-related disclosure, 0 otherwise.

I replicate the analysis to compare the market reaction to the level of firm-specific CRDS and industry-level CRDS by performing an ordinary least squares (OLS) regression on the stock price of a firm ($PRC - 3M_{it}$), 90 days after fiscal year close. The value-relevance methodology that focuses on the “incremental association over a long-time window” is suitable to be examined by the suggested measure (CRDS) since cybersecurity risk disclosure is a part of a bundle of other disclosures that deal with different types of
information (Gordon et al. 2010). A modified version of the original model is examined based on a model suggested by Ohlson (1995).

\[ \text{PRC-3M}_{it} = \beta_0 + \beta_1 \text{FS}_{CRDS} + \beta_2 \text{IL}_{CRDS} + \beta_3 \text{BVP}_{S,t} + \beta_4 \text{EPS}_{it} + \beta_5 \text{LnAst}_{it} + \beta_6 \text{Neg}_{it} + \Sigma \beta_k \text{Year}_{it} + \Sigma \beta_j \text{Industry}_{it} + \varepsilon_{it} \]

In specific, three models are examined, the original Gordon et al. (2010)’s model, a model with the total \textit{Industry-adjusted CRDS} (\textit{FS}_{CRDS}+\textit{IL}_{CRDS}), and a model for each \textit{FS}_{CRDS} and \textit{IL}_{CRDS}. The sample includes the firm disclosures after the SEC guidance publicized in 2011 and before the updated guidance in 2018 (i.e., fiscal years from 2011 to 2018) and consists of 19,061 disclosures from 3,732 firms (see Table 1).

The results given in Table 6 show that \textit{Industry-adjusted CRDS} measure (see Table 6 - Model 3) is consistent with Gordon et al.’s (2010) measure (see Table 6 - Model 2), where the market positively reacts to cybersecurity risk disclosure (i.e., value relevant). Interestingly, the results of Model 4 show that the market positively reacts to firm-specific cybersecurity risk rather than industry-level cybersecurity risk. The coefficient on the \textit{FS}_{CRDS} has a magnitude of 23.274, which is positive and statistically significant at \( p < 0.001 \). On the other hand, \textit{IL}_{CRDS} is not statistically significant while showing a negative coefficient with a magnitude of -0.456. This supports the argument that the firm-specific cybersecurity risk is value-relevant, while the market devalues the industry-level cybersecurity risk.
### Table 6. OLS Regression Results

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>(-6.729***)</td>
<td>(-6.328***</td>
<td>(-5.886***</td>
<td>(-7.165***</td>
</tr>
<tr>
<td>Disclosure</td>
<td>3.066</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>(3.283***</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Industry-adjusted CRDS</td>
<td></td>
<td>0.0054</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>(6.085***</td>
<td></td>
<td></td>
</tr>
<tr>
<td>FS_CRDS</td>
<td></td>
<td></td>
<td></td>
<td>23.274</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>(3.719***</td>
</tr>
<tr>
<td>IL_CRDS</td>
<td></td>
<td></td>
<td></td>
<td>-0.456</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>(-0.134</td>
</tr>
<tr>
<td>BVPS</td>
<td>1.372</td>
<td>1.373</td>
<td>1.373</td>
<td>1.373</td>
</tr>
<tr>
<td></td>
<td>(160.461***</td>
<td>(160.510***</td>
<td>(160.705***</td>
<td>(160.554***</td>
</tr>
<tr>
<td>EPS</td>
<td>1.672</td>
<td>1.671</td>
<td>1.671</td>
<td>1.672</td>
</tr>
<tr>
<td></td>
<td>(33.364***</td>
<td>(33.348***</td>
<td>(33.376***</td>
<td>(33.366***</td>
</tr>
<tr>
<td>LnAst</td>
<td>3.346</td>
<td>3.160</td>
<td>3.113</td>
<td>3.234</td>
</tr>
<tr>
<td></td>
<td>(21.703***</td>
<td>(19.243***</td>
<td>(19.617***</td>
<td>(19.553***</td>
</tr>
<tr>
<td>Neg</td>
<td>-6.042</td>
<td>-6.067</td>
<td>-6.160</td>
<td>-6.174</td>
</tr>
<tr>
<td></td>
<td>(-6.393***</td>
<td>(-6.422***</td>
<td>(-6.523***</td>
<td>(-6.515***</td>
</tr>
<tr>
<td>Year</td>
<td>Included</td>
<td>Included</td>
<td>Included</td>
<td>Included</td>
</tr>
<tr>
<td>Industry</td>
<td>Included</td>
<td>Included</td>
<td>Included</td>
<td>Included</td>
</tr>
<tr>
<td>Adjusted $R^2$</td>
<td>0.715</td>
<td>0.716</td>
<td>0.716</td>
<td>0.716</td>
</tr>
<tr>
<td>No. of Observations</td>
<td>19,061</td>
<td>19,061</td>
<td>19,061</td>
<td>19,061</td>
</tr>
</tbody>
</table>

Notes:

- **PRC-3M**: Stock price of firm $i$ for year $t$, 90 days after fiscal year close
- **Disclosure**: Generic security disclosure, where Disclosure = 1 if the firm has any security-related disclosure, 0 otherwise – Adopted from Gordon et al. (2010)
- **Industry-adjusted CRDS**: Industry-adjusted Cybersecurity Risk Disclosure Score
- **FS_CRDS**: Firms-specific Industry-adjusted CRDS
- **IL_CRDS**: Industry-level Industry-adjusted CRDS
- **BVPS**: Book value of equity divided by the number of shares outstanding for firm $i$ for year $t$, year-end
- **EPS**: Earnings per share (basic excluding extraordinary items) for firm $i$ for year $t$, year-end
- **LnAst**: Log of Assets for firm $i$ for year $t$
- **Neg**: 1 if EPS is negative for firm $i$ for year $t$, 0 otherwise
- **Year**: 1 if current year, 0 otherwise
- **Industry**: 1 if in industry, 0 otherwise

*, **, *** represent significance at the 0.10, 0.05, and 0.01 levels, respectively
Conclusion, Limitations, and Future Research

Cybersecurity has received enormous attention in recent years, and the volume of cyberattacks is increasing dramatically. Cybersecurity threats can pose a dire and existential risk to all firms, regardless of their sizes, reputation, or pedigree. Top management teams are deeply concerned about the potential for cybersecurity threats to hinder their firms’ growth (Symantec 2016). While countable cybersecurity risk measures have been developed, many of them are based on attributes that reflect technical aspects (e.g., IT infrastructure) and managerial considerations (e.g., cybersecurity policies). No study has yet attempted to measure the firm-specific cybersecurity risk using firms’ public disclosures (i.e., 10-Ks).

However, the complex nature of cybersecurity renders measuring a firm’s cybersecurity risk difficult, even though recently developed methodologies in text analytics allow for analyzing unstructured textual information. In light of this challenge, the series of suggested tailored procedures and techniques (i.e., the CRDS measurement process) provide a meaningful and useful quantitative measure for gauging firms’ cybersecurity risks, leading to the hope that the measure may eventually be deployed in various ways to enhance the cybersecurity environment of firms. The CRDS measurement process proposes a dynamic way to identify risk topics and classify industries, thereby providing a more accurate assessment of firm-specific cybersecurity risks that can potentially be applied to a wide range of domains. Specifically, I introduce a new approach, Weighted Cybersecurity Risk Topic Modeling (WCRTM), to identify various cybersecurity risk topics and topic weights. Furthermore, this study leverages Textual Imagification (TI) to classify risk topics while minimizing the effect of multicollinearity. Finally, a new
approach is proposed, Dynamic Peer Group Identification (DPGI), to classify industries more dynamically to capture a firm’s business activities in a timely and relevant manner. The application of DPGI enables to reflect the industrial effect of cybersecurity risk in the CRDS (i.e., Industry-adjusted CRDS). I then entangle a firm’s unique cybersecurity risk (i.e., firm-specific CRDS) from the shared risk by its industry peer firms (i.e., industry-level CRDS).

This approach has several limitations that can be further discussed in future studies. First, the DPGI focuses solely on firms’ business activities. Other factors can be incorporated into the DPGI. For example, considering firms’ financial characteristics can introduce the interaction effect between a financial performance indicator (e.g., gross profit margin, return on investment, and debt-to-equity ratio) and a firm’s business focus. Future studies may benefit by including additional relevant factors into the DPGI to provide a better industry classification. Second, the CRDS (also the Industry-adjusted CRDS) is based on the assumption that firms have a comprehensive range of views toward their cybersecurity risks and adequately disclose their risks in a timely and relevant manner. This assumption may not necessarily hold. If firms are not aware of cybersecurity risks or consider significant risks to be immaterial, they are likely to provide less informative disclosures. Future research can use other sources (e.g., commercial websites, news articles, and social networking site postings) to produce the CRDS and verify the cybersecurity risks specified in firms’ risk disclosures. At last, this study focuses on cybersecurity risks. However, the CRDS measurement process (i.e., WCRTM, TI, and DPGI) can be used to measure other risks, such as financial, operational, litigation, and internal controls risks. The process is designed to identify and quantify an abnormality on
various textual data and generic enough to be applied to other subjects of interest. For instance, the creativeness of patents can be measured using my approach to the textual description of the patent data. Another avenue for future research is to see whether the WCRTM, TI, and the DPGI are applicable in other fields.

The CRDS measurement process using firm disclosures makes several contributions to the literature. In particular, TI allows the semantic analysis results to be contained in a compact array while minimizing the loss of informative semantic features. Therefore, it allows measuring characteristics extracted from any textual data and analyze them. In addition, various users, including researchers, auditors, regulators, and other stakeholders, can benefit from the proposed methodology, which provides a quantitative method for gauging cybersecurity risks using publicly available firm disclosures.
CHAPTER 4: MEASURING THE INSIDER THREAT AFTER MASSIVE LAYOFF USING DARK WEB MARKET DATA

Introduction

In the words of Kelly (2018, emphasis in original),

“There was a time around World War II that the traditional idea of company loyalty was born: you got hired by a company and they would keep you employed (given good behavior) for your career, and in return for 40 years of service you’d receive a nice gold watch and a pension. Those days don’t exist anymore. Only a fraction of employment opportunities offer pensions, and most of those are government-related… This is absolutely their right to do so, especially when times get tough. But here is the rub: when a company’s first reaction to a bad quarterly earnings announcement is to cut the workforce by 5-10%, how can you ever expect an employee to be loyal? If you look at your employees like commodities, then you cannot be surprised when they look at your company the same way.”

A Google search of “corporate loyalty is dead” results in 329,000 results. Similarly, searching for “employee loyalty is dead” yields 374,000 entries. The post-World War II era of lifetime employment, strong unions, defined benefit pensions, and dedicated employees laboring for paternalistic employers ended decades ago. In an age of globalization, hyper-competition, and hedge fund-driven stakeholder capitalism, mass layoffs are routine, and employees—especially those in Generation Y and Z—expect to have not just multiple jobs but also multiple careers in their lifetimes (Friedman, 2017). To put it another way, the implicit contract of reciprocal loyalty between employee and employer is now null and void, having fallen even in its last holdouts: partnerships in the big-4 accounting firms and leading law firms.12

12 The following link provides ongoing coverage of job and pay cuts in accounting firms: https://tinyurl.com/advtv8p8. Also, the same for law firms: https://tinyurl.com/pvteruvz.
In an ideal world (or, rather, in an idealized vision of white, heterosexual, and male workplaces of the 1950s), employees would remain loyal even to companies that laid them off because they understood that management took that decision only after they had exhausted all other options to retain them and remain a viable business. In turn, employers would commit to rehiring employees as soon as possible, seeing them as valuable assets to be protected. Employees today seem unlikely to believe the former, and companies are less likely to do the latter.

A discussion in Knowledge Wharton (2012, emphasis in original) summarizes the decline in reciprocal loyalty that has given rise to the purely transactional workplaces of today: “Wharton management professor Adam Cobb sees another reason for what is clearly an evolving relationship. “When you are talking about loyalty in the workplace, you have to think about it as a reciprocal exchange,” says Cobb. “My loyalty to the firm is contingent on my firm’s loyalty to me. But there is one party in that exchange which has tremendously more power, and that is the firm.” Employee behavior, Cobb says, has been influenced by the dramatic organizational restructuring that began 30 years ago. “Firms have always laid off workers, but in the 1980s, you started to see healthy firms laying off workers, mainly for shareholder value.”

In their announcements of pending staff cutbacks, “firms would say, ‘We are doing this in the long-term interest of our shareholders,’” Cobb notes. “You would also see cuts in employee benefits — 401(k)s instead of defined benefit pensions, and health care costs being pushed on to employees. The trend was toward having the risks be borne by workers instead of firms. If I’m an employee, that’s a signal to me that I’m not going to let firms control my career… People have always wanted to be more in control of their lives.”
What’s different now, he notes, is how firms treat employees. “It seems strange to me to be loyal to a firm that I know has no loyalty to me.”

What are the implications of this decline in reciprocal loyalty in the workplace? Millions of words have been written on this topic, ranging from the rise of the gig economy, the outsourcing of work overseas in the “flat economy,” deaths of despair, the increase in political polarization, and so forth. Academic research examines the issue from the perspective of strategy, economics, psychology, organizational behavior, political science, sociology, and anthropology.

This paper takes advantage of a unique dataset to measure the reciprocal relationship between corporate disloyalty and employee disloyalty quantitatively. Specifically, I treat the unexpected economic shutdown brought about by the COVID-19 pandemic as a natural experiment: it resulted in a sudden reverse of a booming economy and millions of jobs being lost through no fault on the part of the employees. Moreover, those jobs were lost rapidly and with little planning, with employees thrust unexpectedly into a crisis economy with unknown prospects of finding a new position.13

This event creates a setting to examine how affected employees respond to being laid off: in particular, how they monetize the knowledge that they possess from their previous employment. The concept of monetizing employment might seem an odd one, but that is exactly what we all do when we list our employment history on a resume. Experience and private knowledge about the workings of the business are both assets that laid-off

---

13 15.9 million jobs were lost in the US in April 2020, the first month after the COVID-19 shutdown, the fastest increase in unemployment numbers ever recorded. See the announcement made by the U.S. Bureau of Labor Statistics: https://tinyurl.com/w5bzhts.
employees walk out of the door with, and the question is how restrained those employees feel about exploiting one and not the other when they no longer feel any sense of loyalty to an employer that they feel clearly showed them none.

Precisely because private information about the business is of value, employers threaten both current and leaving employees with civil and even criminal penalties if they disclose what they know. Rationally employers should, in particular, take proactive steps to minimize their vulnerability to laid-off employees over whom they have the least control. Popular media often depicts the brutal process where even long-standing employees are given a cardboard box and supervised by security personnel as they clear out their offices of personal items, thus ensuring that they do not also remove corporate assets. Businesses can also adopt risk mitigation strategies such as sidelining those employees targeted to be let go weeks or months in advance to limit their access to cutting-edge corporate information. This strategy requires time to work and cannot be implemented when there are unexpected mass layoffs. This is another reason to use the COVID-19 round of layoffs beginning March 2020 as a natural experiment. Not only did that see an extraordinarily large number of workers lose their jobs in a very short period, but it is improbable that employers followed best risk mitigation practices when carrying out those sudden layoffs.

Moreover, contrary to economic theory, not all employers follow a rational procedure for undertaking layoffs in the first place. As Joyce (2020, emphasis in original) writes, “Preparing for a Layoff in 2020—Things to Do at Work: According to the experts, many of us will be laid off more than once. Don’t expect a layoff to be rational—who

---

14 Refer to an image used to illustrate this news article on COVID-19-related layoffs in Canada: https://tinyurl.com/fyeeknwd.
stays and who is shown the door is not necessarily logical. Even if you are one of the “stars” in your workplace, you are not immune. Stars get laid off, too. So, be prepared, especially if news about your employer and/or the economy is bad. Have that lifeboat ready before the ship (your employer) sinks.”

An excerpt from the recent bestseller “Billion Dollar Loser” by Wiedeman (2020) about the co-working company WeWork—the co-working industry itself arising due to the need for office space by workers unable to get traditional full-time work from corporations—illustrates that companies follow fads and trends rather than some equilibrium theory when it comes to dealing with their employees: “In addition to her role as WeWork’s top lawyer, [Jen] Berrent had taken on the job of running human resources, which many early start-ups leave to their attorneys. She often echoed a goal Adam had set out for the company of laying off 20 percent of WeWork’s staff every year—a blitzscaled version of [former GE CEO] Jack Welch’s belief that the bottom 10 percent of a company’s workers should be regularly culled. “We met those expectations, and I’m not proud of that,” one member of WeWork’s HR team said. He started referring to the quiet, rolling rounds of layoffs that regularly took place at WeWork as Jenocides.” (Wiedeman, 2020)

Wiedeman (2020) also provides details about how WeWork not only did not offer reciprocal loyalty to their employees but took advantage of that which their employees possessed: “Employees began to recognize a WeWork life cycle. New hires would arrive buoyed with excitement for six months—maybe nine. A slow decline would begin until they hit the eighteen-month mark, by which time they would be exhausted and disillusioned and something like the company’s meat ban would push them over the edge. Those employees would leave and be replaced—rinse and repeat.”
In short, even in normal circumstances, layoffs are a standard operating procedure in corporations, and when economic prospects darken, there is no hesitation in reducing headcount quickly. This has two consequences whose interaction is examined in this paper. First, in a crisis, the business has not laid the groundwork to minimize the information about-to-be terminated employees. And second, that employees feel fewer ethical compunctions about taking advantage of any private information that they might possess when laid off than they would have in another age with stronger bonds of reciprocal loyalty between employer and employee. Employees also know that their private information is a perishable commodity that must be used or lost. Hence, if employees choose to monetize it, they will do so sooner rather than later.

That leaves the question that of how an ex-employee might go about selling their private information. Doing so openly obviously places them in legal jeopardy. As Joyce (2020) warns laid-off employees: “your employer probably “owns” what you have created at work… Use your own judgment and ethics, but be very careful. If something is marked “company confidential,” leave it alone. Former employees can be, and are, sued for violating confidentiality agreements. They can even be accused of theft.”

In the last decade, however, technology has become available, making it much safer for individuals to undertake transactions of sensitive goods, be it child pornography, illegal drugs, hacking codes, or insider information. That is the so-called “dark web,” reached through communication platforms that incorporate built-in end-to-end cryptography effectively so that it challenges the capabilities of even advanced law enforcement and intelligence agencies. This is the marketplace of choice for any individual with a bare
minimum of technological capability. Such level of technological literacy can be obtained with a bit of effort through innumerable guides online, including on YouTube.\footnote{For example, see courses on the Dark Web Academy: https://tinyurl.com/jtd2ctts.}

The use of dark web market is facilitated by the fact that unlike in the industrial past where critical information was physical, such as blueprints, a prototype, or a sample of a material, today’s critical corporate information is much more likely to be in portable digital form. That is also why the increasing incidence of hacking, such as that conducted at the end of 2020 of major corporate and US government databases, allegedly by Russia (Perlroth, 2021). Digital material is ideal for selling on various marketplaces on the dark web, especially with bitcoin enabling confidential payment. Hence, the dark web markets will provide the best indication today of how disloyal employees feel about the layoffs many businesses undertook when the COVID-19 lockdown unexpectedly took place.

This paper utilizes a unique database collected from the postings in dark web market where people offer their proprietary information about specific businesses: what is referred to as insider information leakage. The sellers of this information are not necessarily laid-off employees of those companies: they could also be current employees or third-party hackers. If we look at the volume of data being offered for sale immediately following COVID-19 related layoffs in those companies, the increase in insider information leakage, if any, is highly likely to stem from those layoffs. The new market-entrants are either ex-employees wishing to monetize the information they possessed when they were laid off or surviving employees whose loyalty to their employer has been undermined by the experience of witnessing a psychologically brutal round of mass layoffs.
By exploring whether a surge of dark web market transactions took place after the COVID-19 related layoffs, we can measure the joint effect of declining reciprocal loyalty and the lack of risk mitigation by firms that reacted in panic to the virus. The unique database gives a metric of the consequences of the decline in reciprocal disloyalty that is unique in the literature.

In the next section of the paper, I provide an overview of the literature on corporate and employee loyalty. The following section provides a summary of the literature on hacking and other digital crimes against corporations. In the following section, I discuss my data and research methodology. Next, I provide the empirical analysis and finally discuss with concluding comments.

**Literature Review**

**Reciprocal loyalty**

Hart and Thompson (2007) define loyalty as the “psychological state that (1) characterizes the employee’s relationship with the organization and (2) has implications for the decision to continue or discontinue membership in the organization.” Compared to commitment, which is a one-way construct (i.e., the duty imposed on the employee), loyalty requires mutuality, where it relies on the normative relationship between the employee and employer (Meyer and Allen, 1997; Hart and Thompson, 2007). Specifically, the commitment literature focuses on employees’ emotional response to their job (Landsberger, 1958’ Locke, 1976), while the literature on loyalty addresses the two-way relationship of mutual enrichment between employee and employer (Larmer, 1992; Probst and Lawler, 2006; Pierce et al., 2008).
Employee loyalty related to downsizing has been widely examined in the literature on organizational behavior and labor economics (Nathan, 1995; Stroh and Reilly, 1997; Clancy, 1998; Orlando, 1999; Niehoff et al., 2001; Hart and Thompson, 2007). Organizational scholars recognize that employee loyalty relies on the set of expectations developed by the employee about their relationship with the employer (e.g., management, corporate culture). Such expectations or obligations are perceived by the employee even though they are often unwritten in the formal contract with the employer. Instead, they are termed as psychological contracts (Rousseau and Parks, 1993; Parks and Schmedemann, 1994; Robinson et al., 1994; Robinson, 1996; Morrison and Robinson, 1997; Turnley and Feldman, 1999). Unlike the explicit agreement between the employee and employer, a psychological contract depends on the individual’s perception about how they view the organizational activity (Rousseau, 1990; Parks and Schmedemann, 1994; Morrison and Robinson, 1997; Hart and Thompson, 2007). Hence, the employee’s reactions to the organizational decisions can be influenced by their perceived expectation and obligation to the organization (Rousseau and Tijoriwala, 1998; Butler et al., 2020).

An unexpected layoff that results in an employee losing their job despite being loyal to the business will be perceived as unfair (Skarlicki et al., 2008). From the employer’s perspective, the layoff decision is based on the imperatives of profit maximization with little consideration of loyalty issues in either direction (Duska, 1985; De Meuse et al., 1994; Shannon et al., 2001). Laid-off employees can perceive the employer’s actions as a violation of the psychological contract between them (Turnley and Feldman, 2000). The layoff can reduce the performance, loyalty, and job satisfaction of even the employees that remain through what is termed the survivor syndrome (Rousseau, 1995; Robinson, 1996).
The survivors also perceive the layoff as unfair organizational activity toward their colleagues and a violation of the psychological contract (Morrison & Robinson, 1997; Wiesner et al., 1999; Farrell and Mavondo, 2004; Draper, 2015; Hulume, 2020). Such unfairness can reduce the surviving employees’ loyalty who fear being inevitably included in future layoffs (Sverke et al., 2002). Moreover, during the pandemic, the layoff announcement can be perceived as a decision against civic virtue, which in turn leads to a decrease in employee loyalty (Robinson and Morrison, 1995).

Employee-driven cybersecurity threats

Much media attention is paid to cybersecurity risks arising from parties external to a business, such as hacking by national actors. Cybersecurity experts, though, are also focused on the implications of coronavirus-related layoffs (Security Boulevard, 2019; Deloitte, 2020; EY, 2020; KPMG, 2020; Verizon, 2020).

On March 29, 2020, a Wall Street Journal article noted that “the COVID-19 pandemic is forcing the fastest reallocation of labor since World War II.” Surveys show that both laid-off employees and survivors react with negative emotions against their employers rather than seeing the job cuts as primarily the consequence of the epidemic (Forbes Human Resources Council, 2020). While downsizing is a common activity in organizational life (Gilson et al., 2004), an unexpected economic downturn (e.g., the subprime crisis, oil shock, and COVID-19 pandemic) allows no sufficient time to consider multiple operational factors when determining the right size for downsizing, nor providing sufficient time to the laid offs to prepare for the career transition (Cornfield, 1983; Downs, 1986).

16 Full article can be accessible at WSJ (https://tinyurl.com/3x5tu64u).
The confluence of mass layoffs that are insufficiently prepared gives rise to a potential for employees—both current and former—to seek to monetize their private information. This is one instance of what I call the “insider threat,” as opposed to the external threat of hackers.

The cost of insider threat has skyrocketed during the recent two years, approximates to $11.45 million (Ponemon, 2020), which is more than doubled the cost from external threat (e.g., malware attack, Denial-of-service attack). Insider threats occur once human-vulnerable factors (e.g., disgruntled behavior, security policy violation) cause information leakage, either intentionally or unintentionally (Gelles, 2020). An unprecedented number of security incidents related to information leakage on exfiltrated data have been reported during the COVID-19 pandemic (Hulume, 2020; ISC2, 2020). Figure 6 shows the trend of news reports related to insider threat (dark grey line) and telecommunication (light grey line) obtained from Google Trends. It shows a clear spike concerning insider threat-related news reports after the COVID-19 related layoffs, which is measured by the Insured Unemployment Rate (IURNSA).  

---

17 U.S. Employment and Training Administration, Insured Unemployment Rate (IURNSA), retrieved from the Federal Reserve Bank of St. Louis (https://tinyurl.com/y659nkj4).
**Figure 6. Unemployment and insider threat-related news**

*Hypotheses*

The widely used “fraud triangle” is a conceptual model of the circumstances under which an individual will commit fraud. Its reasoning applies to any kind of illegal activity, including selling private information. The fraud triangle assumes that people undertake a crime only when it is rational to do so. Hence, they must have both a pressing need for the proceeds of that crime, and they must assess that the probability of being caught is low enough that the expected costs will not exceed those benefits. This cost and benefit analysis of the tangible outcomes of the crime is only a necessary, not sufficient, condition for the criminal act to be proceeded with. Otherwise, far more people will ignore red lights on empty intersections or cheat on online exams. To take that final fateful step into illegality also requires the ability to justify to oneself the necessity of overcoming the inherent psychological barriers that most people have towards breaking the standards of conventional behavior in a society. That is why the most crucial driver of criminal behavior
for people who are not career criminals is rationalization: to give their own conscience an excuse for why what they are about to do is not as bad as it appears. Something along the lines of “I had no choice but to do it” or “it was owed to me.”

Figure 7. The fraud triangle (Cressey 1953)

The decline of loyalty by businesses today to their employees—as best exemplified by the constant threat and reality of layoffs—results in a reciprocal lack of loyalty by employees towards their employer. That context provides the basis for rationalizing monetizing any assets the employee obtains from the workplace. Although by no means, all workers currently employed by a business have less motivation and more to lose from taking that risk, those constraints are removed once the business itself has dispensed with them. In those circumstances, both current and especially recently laid-off employees have fewer reasons to remain loyal to the business, with the selling of proprietary information in their possession perceived as differing only in degree from such minor indiscretions as helping themselves from the supply cupboard. Adam Cobb’s (Knowledge Wharton, 2012) argument that “It seems strange to me to be loyal to a firm that I know has no loyalty to me” provides a sufficient rationalization for affected workers to put their own interests first.

Whether an employee will behave disloyally towards their employer relies not only on their justification (i.e., their rationalizations for that act) but also on their fear of being
found out and paying the penalty. A panicked mass layoff without proper planning and control procedures put in place proactively provides the opportunity, as does the existence today of a market in which dubious transactions can be undertaken with less risk of detection.

An employee’s motivation to sell his or her private information ranges from pure revenge to a need for money. The latter, by itself, does not translate into a pressing need if the laid-off employee is confident of obtaining a replacement job in a short period. To those who have this optimistic mindset, the downside risk of being caught and the psychological costs of committing a crime, though slight, are not worth bearing. Even if their beliefs of finding a new job subsequently prove to be unfounded, by the time the laid-off employee comes to that realization, the market value of their private information may well have diminished.

That is why it is expected to see a much more pronounced effect of employee monetization of their information with the COVID-19 layoffs of March 2020 when mass layoffs took place and workers faced a period of unemployment of unknown duration. Looking back now with COVID-19 vaccinations in full swing, it is hard to overstate the sense of panic and uncertainty that prevailed at the beginning of the shutdown when there was no idea about what the extent or duration of the crisis would be.

From this underlying story, this study derives testable hypotheses. While there is always the sale of private information about a specific business by both active and former employees, such activity is likely to rise after a mass layoff from that business. Furthermore, when layoffs are widespread across all businesses in the economy to the extent that the
aggregate employment market significantly deteriorates, the incidence of insider threats will be the highest of all. This gives the following central hypothesis:

**Hypothesis 1:** *Insider information leakage increase after mass rapid layoffs.*

The COVID-19 layoffs from mid-March to mid-April 2020 are an ideal natural experiment to test this hypothesis. The COVID-19 pandemic resulted in an entirely unexpected economy-wide shock to employment. Hence, businesses could not plan to mitigate the risk of information leakage, and laid-off employees faced enormous uncertainty about when they could expect to get new jobs. It was a perfect storm for the fraud triangle to operate and lead even previously loyal employees to consider what they could do with the private information that they possessed while it still had a market value.

While hypothesis 1 applies to all businesses, the relative effect will be particularly pronounced if the comparison between businesses that fired and those that hired during the COVID-19 crisis period. Even to new employees, getting a job during a nationwide downturn is a golden goose that they are unlikely to jeopardize through leaking inside information. Focusing on the difference between layoff firms and hiring firms magnifies the loyalty issues that are being examined in this study.

Thus, we can elaborate on this hypothesis in further detail. The greater the disrepute in which its employees hold their employer, the more likely ongoing insider information leakage. Further, the magnitude of those transactions is likely to rise even further if the business undertakes layoffs. What about businesses that are relatively more highly regarded beforehand? If they undertake layoffs, will the shock to employees be greater given that they expected more from their employer? Or does the general cynicism towards
the declining loyalty of businesses mean that employees are not surprised even though the businesses that are highly regarded places to work in good times promptly let people go when bad times occur? Only empirical analysis can answer this question. Accordingly, I examine the following hypothesis.

**Hypothesis 2:** Businesses that are less regarded by their employees will see more insider information leakage during the COVID-19 shock than those with higher employee loyalty.

**Data Sources, Variable Measurement Methods, and Descriptive Statistics**

The data used in this study come from three unique data sources. First, the list of layoffs and hiring firms are collected from *Layoffs.fyi*, which was opened during the COVID-19 pandemic to support the tech workers to find a new job after being laid off. *Layoffs.fyi* provides a list of job announcements on IT employees for both layoff and hiring. Our analysis focuses on IT employees since employees with greater technical knowledge have privileged access to information assets and may find it easier to turn to dark web market to sell proprietary information. The second dataset is the dark web market posts collected by *DarkOwl*, one of the major dark web monitoring firms.\(^\text{18}\) The dark web market posts are utilized to measure the insider information leakage of each firm. Finally, I hand collected the average annual ratings of employee reviews from an online job platform, *Indeed*, where employees share their reviews about their employers.\(^\text{19}\) Figure 8 provides

\(^{18}\) *DarkOwl* is a leading security service and threat intelligence provider that owns the most advanced proprietary tools to analyze the dark web. Especially, I utilize *DARKINT™* data and *Hackisness™* score to identify dark web posts that includes hacking information. The data I have utilized in this paper is sponsored by *DarkOwl* strictly limited to academic research purposes. For more details, refer to *Darkowl*’s website ([https://www.darkowl.com/](https://www.darkowl.com/)).

\(^{19}\) *Indeed* is an online job platform for listings including the job boards, employee review, and company information. I have hand collected the average annual ratings of the firms’ employee reviews without usage
the list of data sources utilized in the study and the sample construction process explained in the next section.

**Figure 8. Sample selection process**

*Data Sources and Sample Construction*

The dark web market posts are collected from the *DarkOwl* database that is crawled from various dark web forums, including dark web blogs, membership-based forums (including insider forums), and pastes – a forum where hackers share hacked information. Among the dark web posts, I identify posts that contain insider information of a specific firm, often referred to as material non-public information (MNPI), in which information should normally be kept confidential. Accordingly, our initial sample is the posts that contain contents relate to criminal activities and not searchable on the surface web (e.g.,

of automated system by following *Indeed’s* Terms and Services and Publisher’s Obligations ([https://www.indeed.com/legal](https://www.indeed.com/legal)). For more details, refer to *Indeed’s* website ([https://www.indeed.com](https://www.indeed.com)).
Google, Bing). In specific, a supervised machine learning algorithm is utilized for identification that is trained with over 100 independent decision variables by DarkOwl. The algorithm is trained by features including malicious domain addresses, patterns of personally identifiable information, and keywords related to criminal activities. The initial sample includes 297,935 dark web posts from 714 dark web websites posted between February 1 to July 31, 2020.

In general, insider information is exclusively traded among the participants in certain forums, which is known as the insider trading forum (ITF). To search insider trading forum, I further identify forums with posts that mostly deals about business-related information (e.g., business documents, operational agreement). The identification process follows the approach suggested by Fu et al. (2010) to crawl topical information (i.e., a set of information about a specific topic) from the dark web forum. In specific, I group the posts based on the root URL (i.e., domain URL of each website) by following a breadth-first search (BFS) method (Menczer et al., 2004). Next, for each root URL, I rank the title keywords based on their frequency. Similar to previous literature, I examined whether the keywords among 714 dark web websites relate to terms about sales or exchange of business information (Aggarwal et al., 2001; Pant et al., 2002). As shown in Table 7, six websites are identified as insider trading forum.

In addition, the posts with no narrative discussions are excluded from the sample, such as a post that provides only combinations of usernames and passwords or a pile of social security numbers. Non-English posts are further excluded since this study focuses on the insider information provided from employees mainly residing in the United States. Based on our analysis, non-English posts contain small amount of business-related
information about the firms included in our dataset. Further, I exclude non-English posts due to limited capability to accurately translate the information conveyed in the post.20 Finally, I obtain 45,941 dark web posts from six websites that show business-related keywords. Panel A in Table 7 provides a summary of dark web posts, and Panel B describes the representative keywords of dark web posts in each website. Further, Appendix E details an alternative way to identify the dark web posts with LDA topic modeling. Notably, the analysis results are consistent with the alternatively identified sample.

Layoff and hiring announcements during the COVID-19 pandemic are collected from an IT job tracking blog, Layoffs.fyi, which provides IT job announcements among 25 industries compiled from public reports. From Layoffs.fyi, 1,692 job announcements between March 11 to July 31, 2020, are retrieved for 635 layoff firms and 1,057 hiring firms.21 Firms with no available financial information and foreign firms (227 layoff firms and 595 hiring firms) are excluded. Further, to properly identify the dark web market posts that are related to each firm, I check whether the firm or product name is a dictionary word that is commonly used and exclude those firms from my sample.

Next, employees’ reviews are collected from an online platform, Indeed, a crowd-contributed platform where present and former employees share their workplace experience. Each employee can post only one review per year, and each review is examined manually by Indeed. This limits any manipulative activity. In specific, I obtain the annual average of individual ordinal ratings (scaled between 1 to 5) in 2020. Compared to the

---

20 Recent research in cross-lingual text retrieval states that the accuracy of language translation varies between 65.5% to 83.7% (Google AI Blog, 2020)
21 I compare the firms with layoff announcements to firms with hiring announcements during the analysis. Hiring firms are chosen as a comparison group since it is not feasible to identify firms that neither layoff nor layoff. Firms that lay off or hire employees may not publicly disclose such information.
traditional survey, a crowd-contributed platform enables to collect a larger sample of reviews on employee’s experience (Huang et al. 2015). The final sample consists of 129 layoff firms and 132 hiring firms for the analysis. Panel C in Table 7 summarizes the sample selection process on layoff and hiring firms.

**Table 7. Sample selection**

Panel A. Dark Web Post Selection

<table>
<thead>
<tr>
<th>Dark Web Posts Related to Criminal Activities</th>
<th>Posts</th>
<th>Domains</th>
</tr>
</thead>
<tbody>
<tr>
<td>Less: Dark Web Websites not defined as ITF</td>
<td>297,935</td>
<td>1,037</td>
</tr>
<tr>
<td>Less: Posts with no contents (narrative discussion)</td>
<td>(48,719)</td>
<td>(534)</td>
</tr>
<tr>
<td>Less: Posts without non-English contents</td>
<td>(19,554)</td>
<td>(352)</td>
</tr>
<tr>
<td>Total Sample</td>
<td>45,941</td>
<td>6</td>
</tr>
</tbody>
</table>

Panel B. Selected Domain and Keywords

<table>
<thead>
<tr>
<th>Root URL</th>
<th># of Posts</th>
<th>Post Title Keywords</th>
</tr>
</thead>
<tbody>
<tr>
<td>4gj66***.onion</td>
<td>16,514</td>
<td>Corporation, Forum, Hacker, Thread, Verified</td>
</tr>
<tr>
<td>3bbad***.onion</td>
<td>11,343</td>
<td>Corruption, Document, Enterprise, Exclusive, Guide</td>
</tr>
<tr>
<td>3bbaa***.onion</td>
<td>10,795</td>
<td>Document, Exchange, Exclusive, Invite, Subscriber</td>
</tr>
<tr>
<td>i2pse***.onion</td>
<td>6,929</td>
<td>Invite, Department, Employment, Private, Verified</td>
</tr>
<tr>
<td>w2pv7***.onion</td>
<td>184</td>
<td>Agreement, Contract, Petition, Regulation, Review</td>
</tr>
<tr>
<td>brckkp***.onion</td>
<td>176</td>
<td>Agreement, Contract, Decision, Petition, Resolution</td>
</tr>
<tr>
<td>Total Sample</td>
<td>45,941</td>
<td></td>
</tr>
</tbody>
</table>

Note: From the most frequent keywords, keywords irrelevant to business activities and common for every forum are excluded (e.g., Porno, Drug, Sex Trafficking)

Panel C. Firm Selection on Layoff and Hiring Firms

<table>
<thead>
<tr>
<th>Layoff / Hiring Announcement</th>
<th>Layoff</th>
<th>Hiring</th>
</tr>
</thead>
<tbody>
<tr>
<td>Layoff / Hiring Announcement</td>
<td>635</td>
<td>1,057</td>
</tr>
<tr>
<td>Less: Firms with no available financial information and foreign firms</td>
<td>(227)</td>
<td>(595)</td>
</tr>
<tr>
<td>Less: Firms with commonly used name (Dictionary Word)</td>
<td>(38)</td>
<td>(27)</td>
</tr>
</tbody>
</table>
Less: Firms with commonly used name (Product) (17) (13)
Less: Firms with no employee review (198) (284)
Less: Firms not fulfilling 5-week window (26) (6)

| Total Sample | 129 | 132 |

Note: Example of commonly used name (Product) - eBay, Etsy, Facebook, GoPro, Juul, Lyft, Nvidia, PayPal, Uber

Insider Information Leakage Measurement and Sample Characteristics

Insider information leakage is the number of posts containing the firm name within the 5-week window before and after the layoff or hiring job announcement. Based on the survey conducted by Ekran System, which states that 87% of insider threats are detected within one month\(^\text{22}\), the insider information leakage is compared between previous and after the job announcement until 5 weeks. In specific, this study compares the number of posts containing insider information for each firm within the time window defined between one week to five weeks. Figure 9 illustrates the time windows used to construct insider information leakage.

![Figure 9. Illustration of Time Windows for Key Variable Construction](https://tinyurl.com/9t7eneva)

Panel A in Table 8 provides the descriptive statistics of Insider Information

\(^{22}\) The full survey is accessible at Ekran System: https://tinyurl.com/9t7eneva.
Leakage before the layoff or hiring job announcement, whereas Panel B provides the post-announcement statistics. We observe a low level of insider information leakage for both layoff and hiring firms during the entire period. Among 261 firms, 29 firms had experienced insider information leakage while the other 232 firms had shown no evidence of insider information leakage. Further, the employee loyalty (hereafter Loyalty) is measured based on the average employee review on the current year. As shown in Figure 9, the average employee review corresponds to the period where the job announcements were made. The individual review of employees varies between one to five. As shown in Panel C in Table 8, there is no significant difference in Loyalty between layoff and hiring firms.

<table>
<thead>
<tr>
<th>Panel Window</th>
<th>Layoff Firms</th>
<th>Hiring Firms</th>
</tr>
</thead>
<tbody>
<tr>
<td>(-7, 0)</td>
<td>129</td>
<td>0.12</td>
</tr>
<tr>
<td>(-14, 0)</td>
<td>129</td>
<td>0.32</td>
</tr>
<tr>
<td>(-21, 0)</td>
<td>129</td>
<td>0.43</td>
</tr>
<tr>
<td>(-28, 0)</td>
<td>129</td>
<td>0.56</td>
</tr>
<tr>
<td>(-35, 0)</td>
<td>129</td>
<td>0.70</td>
</tr>
<tr>
<td>(0, +7)</td>
<td>129</td>
<td>0.17</td>
</tr>
<tr>
<td>(0, +14)</td>
<td>129</td>
<td>0.31</td>
</tr>
<tr>
<td>(0, +21)</td>
<td>129</td>
<td>0.53</td>
</tr>
<tr>
<td>(0, +28)</td>
<td>129</td>
<td>0.96</td>
</tr>
<tr>
<td>(0, +35)</td>
<td>129</td>
<td>1.49</td>
</tr>
<tr>
<td>Loyalty</td>
<td>129</td>
<td>3.46</td>
</tr>
<tr>
<td>Revenue</td>
<td>129</td>
<td>11.98</td>
</tr>
<tr>
<td>Employee</td>
<td>129</td>
<td>3.55</td>
</tr>
<tr>
<td>Age</td>
<td>129</td>
<td>10.39</td>
</tr>
</tbody>
</table>
Notes:
- Window (-, -) The count of insider information leakage within the window of each firm
- Loyalty The average annual rating of employee reviews in the current year of each firm
- Employee The logarithmic value of the number of employees
- Age Firm age of each firm

Data Analysis and Results

The empirical analysis is divided into two parts. I first examine the effect of layoff on insider information leakage and further compare the effect of employee loyalty between layoff and hiring firms. The following subsections explain the empirical settings of hypotheses discussed in the previous section, along with the results.

Layoff and Insider Threat

As an initial analysis, t-test is performed to examine the mean difference of insider information leakage between the ex-ante and ex-post periods of the job announcement. The analysis is centered on the job announcement dates: the layoff firm’s layoff announcement date and the hiring firm’s hiring announcement date. Table 9 shows that the mean difference of insider information leakage between before and after the layoff announcement is positive and significant after three weeks (3-week window: $t$-statistic = 1.73; 4-week window: $t$-statistic=2.11; 5-week window: $t$-statistic = 1.66). The positive and significant $t$-statistic shows that layoff firms suffer higher insider information leakage after the layoff announcement. On the other hand, hiring firms shows lower insider information leakage after 3 weeks (3-week window: $t$-statistic = -1.64; 4-week window: $t$-statistic = -1.80).

<table>
<thead>
<tr>
<th>Coefficients</th>
<th>(1)</th>
<th>(2)</th>
<th>(3)</th>
<th>(4)</th>
<th>(5)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(-7, +7)</td>
<td>(-14, +14)</td>
<td>(-21, +21)</td>
<td>(-28, +28)</td>
<td>(-35, +35)</td>
<td></td>
</tr>
</tbody>
</table>
The analysis on the mean difference between ex-post and ex-ante job announcement shows a significant increase in insider information leakage on layoff firms while hiring firms to show a significant decrease after three weeks. However, the result shows that the impact of layoff (or hiring) announcement is not immediately affecting the insider information leakage. Such a simple before-and-after comparison would not rule out the temporal factors (e.g., increasing or decreasing insider information leakage trends during the COVID-19). To rule out the temporal factors, I perform a difference-in-difference analysis to further examine the treatment effect of layoff on insider information leakage. In specific, to examine the association between layoff and insider threat with multiple treatment periods, I adopt the staggered difference-in-differences model (Stevenson and Wolfers, 2006; Angrist and Pischke, 2008; Pierce et al., 2015). The staggered difference-in-differences model allows to compare the amount of insider information revealed in the dark web market after the Layoff (i.e., treatment effect) when the layoff period varies among firms. The following empirical specification is used to test for the impact of layoff on insider information leakage:

\[
\text{Insider Information Leakage}_{i,t} = \alpha_i + \gamma_i \text{Layoff}_i + \lambda_i \text{Week}_t + \delta_i D_t + \beta_i \Sigma \text{Controls}_{i,t} + \epsilon_{i,t}
\]

where \( D_t = \text{Layoff}_i \times \text{Post}_t \)
The *Insider Information Leakage*$_{it}$ is the number of posts that contains insider information for firm $i$ in week $t$. *Week*$_t$ is the week dummy with a continuous-time trend between three weeks prior to the layoff or hiring and three weeks posterior to the layoff or hiring. *D*$_t$ is a dummy variable which equals one for layoff firms in the post-layoff period (*Post*$_t$ = 1) and zero otherwise. Most importantly, a positive coefficient on $\delta$, the difference-in-difference estimator, will support my hypothesis that the layoff firms experience higher leakage of insider information than hiring firms.

I control the variables related to the information security effectiveness of internal control and internal control compliance. Prior literature mainly considered the firm’s size, primarily based on their economic value (e.g., revenues, total assets), as a proxy for the internal control effectiveness (DeFond and Jiambalvo, 1991). Accordingly, the firm’s size is controlled by *Revenue*. Among the variables introduced in the internal control literature (Ashbaugh-Skaife et al., 2007; Doyle et al., 2007), I selectively control firm age (*Age*) and an IPO status (*Public*) since “smaller and younger firms are less likely to invest in sophisticated information systems,” as stated by Feng et al. (2015). In addition, security experts highlight the employee’s negligence as a leading cause of cybersecurity incidents. Not complying with the recommended best practices and controls eventually hamper the internal control effectiveness (McCann, 2018; Reinicke, 2018). McCann (2018) further states, “*negligent employees remain the number-one cause of data breaches at small businesses,*” especially firms with fewer than 500 employees. To address the human aspect, I control the number of employees (*Employees*). Panel D in Table 8 also shows the list of descriptive statistics of the control variables introduced in my model.
Table 10 presents the regression result of a baseline model with no controls in Column 1 and a model with controls in Column 2. The results show that the coefficient of \( \text{Layoff} \) and \( \text{Week} \) are both negligible, while the coefficient of \( \text{Layoff} \times \text{Post} \) is positive and significant. These findings suggest that layoff firms, which had no difference in insider information leakage than hiring firms before the layoff, experience a significant increase in insider information leakage after a massive layoff.

**Table 10. The Effect of Layoff on Insider Information Leakage**

<table>
<thead>
<tr>
<th>Coefficients</th>
<th>(1) Base (No Controls)</th>
<th>(2) With Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>Constant</td>
<td>1.161 (3.424*** )</td>
<td>1.375 (1.648*)</td>
</tr>
<tr>
<td>Layoff</td>
<td>-1.033 (-1.617)</td>
<td>-1.023 (-1.604)</td>
</tr>
<tr>
<td>Week</td>
<td>-0.024 (-1.310)</td>
<td>-0.027 (-1.500)</td>
</tr>
<tr>
<td>( \text{Layoff} \times \text{Post} )</td>
<td>0.123 (1.911*)</td>
<td>0.127 (1.968**)</td>
</tr>
<tr>
<td>Revenue</td>
<td>-</td>
<td>-0.000 (-0.109)</td>
</tr>
<tr>
<td>Employee</td>
<td>-</td>
<td>-0.003 (-0.225)</td>
</tr>
<tr>
<td>Public</td>
<td>-</td>
<td>0.173 (0.230)</td>
</tr>
<tr>
<td>Industry</td>
<td>Included</td>
<td>Included</td>
</tr>
<tr>
<td># of OBS</td>
<td>2,610</td>
<td>2,610</td>
</tr>
<tr>
<td>Adj. ( R^2 )</td>
<td>0.311</td>
<td>0.312</td>
</tr>
</tbody>
</table>

Figure 10 presents the trend of average counts of insider information leakage for each layoff and hiring firm. A parallel trend is observed before the treatment (i.e., layoff or hiring announcement) between layoff firms (solid black line) and hiring firms (dashed grey line) until three weeks after the job announcement. However, layoff firms show a
significant increase in insider information leakage after three weeks, while hiring firms show a decrease in insider information leakage. Thus, Hypothesis 1 holds with an increase in insider information leakage immediately after the layoff announcement shown in Table 10 and Figure 10, where the insider information leakage shows the largest increase three weeks after the layoff announcement.

![Figure 10. Layoff and Insider Information Leakage](image)

**Insider Threat and Employee Loyalty**

This section examines the effect of employee loyalty on insider information leakage and compares how it differs between layoff and hiring firms. The measure of employee loyalty, $Loyalty_{i,t}$ is the average review score of firm $i$ in period $t$. The specified model examines how employee loyalty affects insider information leakage when the firm layoffs their employees:

$$
\Delta Insider\ Information\ Leakage_{i,t} = \beta_0 + \beta_1 Layoff_{i} + \beta_2 Loyalty_{i,t} + \beta_3 Layoff_{i} \times Loyalty_{i,t} + \beta_k \sum Controls_{i,t} + \epsilon_{i,t}
$$
The analysis focuses on the coefficient of the interaction between $Loyalty_{it}$ and $Layoff_{i}$. The results of these estimations are presented in Table 11. The coefficient of $Layoff \times Loyalty$ is significant and negative for both the baseline model (untabulated) and model with control variables, while the coefficient of $Layoff$ shows significant and positive. As expected, insider information leakage after massive layoff can be prevented when the firm has higher employee loyalty. The result also suggests that firms with lower employee loyalty experience higher insider information leakage after a layoff.

**Table 11. The Effect of Employee Loyalty on Insider Information Leakage**

<table>
<thead>
<tr>
<th></th>
<th>(1)</th>
<th>(2)</th>
<th>(3)</th>
<th>(4)</th>
<th>(5)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Coefficients</strong></td>
<td>(-7, +7)</td>
<td>(-14, +14)</td>
<td>(-21, +21)</td>
<td>(-28, +28)</td>
<td>(-35, +35)</td>
</tr>
<tr>
<td>$Constant$</td>
<td>-0.263</td>
<td>-7.500</td>
<td>-6.804</td>
<td>-6.603</td>
<td>-7.949</td>
</tr>
<tr>
<td></td>
<td>(-0.603)</td>
<td>(-2.732***)</td>
<td>(-2.166**)</td>
<td>(-1.441)</td>
<td>(-0.991)</td>
</tr>
<tr>
<td>$Layoff$</td>
<td>0.194</td>
<td>0.581</td>
<td>1.209</td>
<td>1.794</td>
<td>2.913</td>
</tr>
<tr>
<td></td>
<td>(2.210*)</td>
<td>(1.215)</td>
<td>(2.209**)</td>
<td>(2.247**)</td>
<td>(2.085**)</td>
</tr>
<tr>
<td>$Loyalty$</td>
<td>0.068</td>
<td>0.185</td>
<td>1.095</td>
<td>1.377</td>
<td>1.782</td>
</tr>
<tr>
<td></td>
<td>(0.420)</td>
<td>(0.407)</td>
<td>(2.097**)</td>
<td>(1.808*)</td>
<td>(1.337)</td>
</tr>
<tr>
<td>$Layoff \times Loyalty$</td>
<td>-0.249</td>
<td>-0.723</td>
<td>-1.518</td>
<td>-1.811</td>
<td>-2.739</td>
</tr>
<tr>
<td></td>
<td>(-2.102**)</td>
<td>(-1.123)</td>
<td>(-2.062**)</td>
<td>(-1.686*)</td>
<td>(-1.457)</td>
</tr>
<tr>
<td>$Revenue$</td>
<td>0.008</td>
<td>0.029</td>
<td>0.027</td>
<td>0.021</td>
<td>0.040</td>
</tr>
<tr>
<td></td>
<td>(2.093**)</td>
<td>(1.404)</td>
<td>(1.143)</td>
<td>(0.603)</td>
<td>(0.656)</td>
</tr>
<tr>
<td>$Employee$</td>
<td>-0.002</td>
<td>-0.010</td>
<td>0.032</td>
<td>0.094</td>
<td>0.208</td>
</tr>
<tr>
<td></td>
<td>(-0.203)</td>
<td>(-0.180)</td>
<td>(0.624)</td>
<td>(0.974)</td>
<td>(1.232)</td>
</tr>
<tr>
<td>$Public$</td>
<td>-0.005</td>
<td>0.235</td>
<td>-0.877</td>
<td>1.154</td>
<td>1.522</td>
</tr>
<tr>
<td></td>
<td>(-0.109)</td>
<td>(0.092)</td>
<td>(-0.301)</td>
<td>(-0.272)</td>
<td>(-0.205)</td>
</tr>
<tr>
<td>$Age$</td>
<td>-0.004</td>
<td>-0.011</td>
<td>-0.005</td>
<td>-0.037</td>
<td>-0.039</td>
</tr>
<tr>
<td></td>
<td>(-2.216**)</td>
<td>(-1.103)</td>
<td>(-0.486)</td>
<td>(-2.126)</td>
<td>(-1.285)</td>
</tr>
<tr>
<td>$Industry$</td>
<td>Included</td>
<td>Included</td>
<td>Included</td>
<td>Included</td>
<td>Included</td>
</tr>
<tr>
<td><strong># of Obs</strong></td>
<td>261</td>
<td>261</td>
<td>261</td>
<td>261</td>
<td>261</td>
</tr>
<tr>
<td><strong>Adj. $R^2$</strong></td>
<td>0.228</td>
<td>0.079</td>
<td>0.030</td>
<td>0.000</td>
<td>0.000</td>
</tr>
</tbody>
</table>

Figure 11 depicts how employee loyalty affects insider information leakage within
layoff firms. As shown in the grey dashed line, layoff firms with low employee loyalty show no significant changes in the average count of insider information leakage after the layoff announcement. However, layoff firms with lower employee loyalty draw in the solid black line, show a significant increase in insider information leakage, especially after three weeks. A potential explanation of the lower impact on firms’ insider threat with higher employee loyalty is that employees, both present and former, perceive the layoff as unavoidable to the firm and thus do not recognize the layoff as a “violation of psychological contract” between the employee and employer. Besides, we can consider reciprocal loyalty as a measure that mitigates the risk of insider threat. Thus, we show that Hypothesis 2 holds based on the result given in Table 11 and Figure 11, and the results are consistent with Table 10 and Figure 10, where a substantial increase in insider information leakage is observed three weeks after the layoff announcement.

Figure 11. Employee Loyalty and Insider Information Leakage (Layoff Firms)

Managerial Implication of the Results

The result can be summarized into two folds. First, a significant increase in insider information exchanged in the dark web market is observed three weeks after the layoff announcement. Second, based on the premise that layoff firms have higher insider
information leakage after the massive layoff, firms with lower employee loyalty experience higher information leakage than firms with higher employee loyalty.

Most employees do not have the intent to harm their firm even after being laid off. However, some of the employees seek monetary compensation to break loyalty with their firm. A recent survey conducted by Deep Source (2019) reveals that the price of employees would accept to sell information is far less than expected. The survey finds that 45% of 1,500 UK office workers will share the firm’s information with a third party for £1,000. In fact, 8.5% of the workers answered that they had sold the information to a third party. Unfortunately, such existential threat is mostly overlooked by the management when dealing with a massive layoff. The results suggest that the insider information leakage is observed within a short period after the layoff (i.e., three weeks) in the dark web market, where the actual breach (i.e., the action taken by the malicious insider) might occur much before then it. Before conducting the layoff, firms should ensure that they have a comprehensive view of who has privileged access and IT knowledge to harvest sensitive data. Further, firms should take preventive and restrictive measures to limit the data access to each employee that can minimize the potential data loss after the layoff.

Most importantly, the results provide implications of the human side of insider threat reduction. We observe that employee loyalty is the key driver to mitigate insider threats after a massive layoff. Even employee loyalty is a rare commodity in a modern workplace environment; firms should understand the value of employee loyalty and consistently engage in increasing employee loyalty. In specific, such layoff can be perceived as a breach of psychological bond between the employee and employer (i.e., reciprocal loyalty), the employer should be transparent and engage in credible explanations
before the layoff. During the layoff, firms should provide proper economic compensation and thorough support to reduce the chance of employees selling sensitive information to third parties for a few hundred dollars that can potentially devastate the firm’s reputation.

**Conclusions**

This paper discusses the impact of massive layoffs on an insider threat for IT firms, where the employees have easier access to information assets. The result shows that an insider threat increases after a massive layoff announcement, and it depends on employee loyalty prior to the layoff. This study’s findings provide an insight into the impact of layoffs on an insider threat that can alert regulators, management, and stakeholders with two major policy implications. First, the IT firm should have a definitive security policy for employment termination that can mitigate the risk of insider threat. The firm should recognize the importance of a cybersecurity program and have dedicated personnel that can focus on such insider attacks. Second, IT firms should carefully monitor the dark web market. My analysis reveals that sensitive information, including employee credentials and PII, are publicly traded in the dark web market. To prevent subsequent cybersecurity incidents, the firm should identify the firm-related information in the dark web market and take proactive actions to mitigate the associated risk.

As with any study, several limitations must be considered when interpreting the findings of this study. One obvious drawback is the small sample. Furthermore, the sample limits to IT employees while examined for only the early pandemic period, as well as inheriting the limitation of data obtained from the dark web where it is not feasible to collect the entire dark web market posts. In future studies, I hope to examine the long-term effect of the layoff on insider threats.
“The markets had undergone an arms race for speed.” Jeffrey Craig Sprecher (Chairman, NYSE)

“It was like a broken slot machine in the casino that pays off every time. It would keep paying off until someone said something about it; but no one who played the slot machine had any interest in pointing out that it was broken.” Lewis (2014, emphasis in original).

Introduction

On May 6, 2010, the U.S. stock market had lost approximately 1,000 points, which rebounded in 20 minutes. The rapid stock market downturn is known as the "flash crash" that recorded the second-largest point swing in the U.S. stock market (Lewis, 2014). Quote stuffing is a market manipulative activity where malicious high-frequency traders send an unusual amount of quotes within a short period, resulting in higher order execution latency for other broker-dealers. Such market manipulative activities against the stock market are widespread. Egginton et al. (2016) find that more than 74% of listed securities experienced at least one episode of quote stuffing that severely decreased the liquidity. One early survey in latency estimates that a one-millisecond advantage can worth $100 million to major financial brokerage firms.23

A common misconception in stock investment is that the acceptance and completion of buy or sell order will be instantaneous in an electronic stock market. In general, order execution takes two stages where; first, the order directs to the broker-dealers, who decide the market that the order will be executed, and next, sent out to the

---

23 Full survey is accessible at Information Week (https://tinyurl.com/7cetf4p8).
stock exchange where orders can be delayed both intentionally and unintentionally. Currently, the U.S. Securities and Exchange Commission (SEC) is strictly requiring the broker-dealers to provide a competitive speed of order execution “to assure that the investors receive the best possible prices for the orders.” On the other hand, in May 2017, the SEC initially approved the New York Stock Exchange American (NYSE American)’s proposal to implement a delay mechanism to impose a 350-microsecond delay upon order entry.²⁴ The proposal purposed to prevent high-frequency traders from taking advantage of predatory techniques on trading for small-cap firms. Two years later, the NYSE removed the speed bump since it led to worse market conditions, such as lower average daily trading volume and higher spread.²⁵

In light of this previous trial and challenges to manage latency, this study proposes a new measure, the Gini-based Latency Inequality Index (GiniLI). GiniLI is a latency inequality measure inspired by the Gini coefficient that calculates the statistical dispersion. Compared to the 350-microsecond delay mechanism implemented by the NYSE, which is an across-the-board rise in latency to prevent market manipulative activities, GiniLI is a continuous measure utilized by the stock exchange to monitor and identify any anomaly in the processing delay in order execution. Notably, GiniLI can be an exemplary measure that complies to the European Union’s Market Abuse Regulation (EU 38 MAR), which emphasizes the need of measure for market manipulation: “Regulation should provide measures regarding market manipulation that are capable of being adapted to new forms.

²⁴ The timetable of implementation of 350-microsecond delay is accessible at SPG Global (https://tinyurl.com/498a88zk).
²⁵ NYSE announcement to remove the 350-microsecond delay is accessible at NYSE (https://tinyurl.com/33dawu87).
of trading or new strategies that may be abusive.”

The proposed model in this study, which is centered on the usage of GiniLI, dynamically determines abnormal transactions based on forecasting analysis on GiniLI and identifies the factors that cause the inequality (e.g., system attributes, brokerage services). In sum, GiniLI can serve as a benchmark of latency inequality that can alert the practitioners for potential issues that can be detrimental to the fair-trading environment.

I further evaluate the performance of the suggested measure by examining the predictability of GiniLI on future order latency (i.e., how well does GiniLI predict future latency?) and the deterrence effect of GiniLI on latency (i.e., how the latency is effectively managed when the stock exchange maintains a certain level of GiniLI while the number of transaction increases). Based on the result, I observe that GiniLI improves the latency predictability and enhances the order execution capability for fair trading among broker-dealers.

The Arms Race of Low Latency

HFT serves as an intermediate between the liquidity demander and the supplier that facilitates faster liquidation (Cartea and Penalva, 2012). However, HFT is known to worsen the market quality (Tong 2014, Korajczyk and Murphy, 2019). Such machine-driven market manipulative activity is associated with asymmetric information and toxic flow that eventually leads to an arbitrage (Hoffmann, 2014; Biais et al., 2015; Foucault et al., 2017).

---

26 Full regulation is accessible at EUROPA (https://tinyurl.com/yu994jp8).
First to market is a critical strategy in HFT, where the trading profit varies by the speed of execution. The order execution latency depends on both external latency and internal latency, where external latency is the speed of network transmission between the broker-dealers and the stock exchange, while internal latency is the processing delay generated by the stock exchange. Precisely, the internal latency is the time difference between the recipient of the quote by the stock exchange and the execution completion of the quote (order book listing). Prior literature in high-frequency trading suggests that the latency primarily derives from the delay in the internal process (i.e., processing delay) rather than the external factors (i.e., bandwidth delay) (Brown, 2020). Hence, latency is considered as an additional transaction cost to the market. Accordingly, the Financial Industry Regulatory Authority (FINRA 2020) 3110 Supervision rule requires the security business and investment banks to adopt a supervisory control system.

Recent research in HFT argues about the effectiveness of the cancellation ratio as a proxy for market manipulative activity that harms the fair-trading opportunity toward the market participants. Early studies suggest that the cancellation ratio increase could capture quote stuffing, where massive inbounding quotes get immediately canceled (Arnuk and Saluzzi, 2008; Yang et al., 2012). However, Seddon (2017) addresses that such order cancellation is a regular price-seeking activity. The market participants are looking for a better price, leading to better market liquidity and fair price setting (Cartea and Penalva, 2012). In specific, Hagströmer and Nordén (2013) see an insignificant difference in the high cancellation ratio between the HFTs and non-HFTs. Eggington et al. (2016)’s further addressed that quote stuffing increases both the number of the new order and cancellation
order. Hence, the degree of an increase in either placing a new order or canceling an order does not solely depict the existence of market manipulative activity.

**Real-time Latency Information**

In this study, I validate my measure on real-time latency information provided by the Brazilian Stock Exchange (B3). B3 recorded approximately 16.8 million average daily trading volume in 2020, which is the third-largest amount in global and the second-largest market in the Americas after the U.S. A sample result collected from five gateways of the daily trading volume is provided for demonstration purposes. For each quote, I obtain the information about the requested equity to be traded, type of the message (e.g., new order request, order cancellation request, order replacement request), brokerage service, server information processing the transaction, and the latency for each transaction that is measured in nanoseconds (i.e., $10^{-9}$ seconds). In specific, the server information includes the gateways that are the entry point of each quote received by the B3. Once the gateway receives the broker-dealer’s quotes, a designated session is initiated that connects to the processor that executes the quote, which is dedicated to each equity.

**Gini-based Latency Inequality Index (GiniLI)**

The proposed measurement process for GiniLI is mainly composed of three stages. The first stage is the calculation of GiniLI where the application of Gini coefficient to latency inequality measurement is introduced. In Stage 2, I structure a forecasting model to detect an abnormal trend in GiniLI. Finally, Stage 3 introduces a mechanism to identify the significant factors that cause latency inequality by using a machine learning algorithm.
Stage 1: Measuring the Latency Inequality

To develop a measure of latency inequality among the quotes, I adopted the Gini coefficient, which measures the inequality within the distribution. Initially, the Gini coefficient was developed by Corrado Gini (1912), an Italian statistician. The statistical measure has often been used to scale income inequality, known as the Gini Index. Wang et al. (2017) suggested that the Gini coefficient is a superior metric to standard deviation to measure the market uncertainty. Shakeel and Srivastava (2020) utilized the Gini coefficient to measure the trading volume inequality between small and large firms.

$GiniLI$ is calculated based on the percentile distribution of latency. The latency is the time duration of a transaction that takes within the B3’s electronic exchange platform. The latency is measured in nanoseconds, which is the time period between the recipient of the quote from the broker-dealers to B3 and the execution completion by B3. In theory, the time duration should be identical among the quotes that are processed through the same gateway. However, the market condition or even market manipulative activities can potentially impose an overload on the internal system that increases latency inequality, leading to substantial market uncertainty.

$GiniLI$ is calculated for every predefined time window. For example, if the time window is for $k$ seconds, $GiniLI$ is calculated based on the entire latency measures for each quote ($Latency_i$) between time $t$ to $t + k$ in a specific gateway (gateway $g$). Notably, I calculate the Gini coefficient without using the Lorenz curve since my dataset follows the discrete distribution. The formula of the $GiniLI$ is composed as follows:

$$GiniLI_{t,k,g} = \frac{1}{n} \left( n + 1 - \frac{2 \sum_{i=1}^{n} (n + 1 - i)Latency_{i,t,k,g}}{\sum_{i=1}^{n} Latency_{i,t,k,g}} \right)$$
where Latency\_i is indexed in a non-decreasing order \((\text{Latency}_{i,t,k,g} \leq \text{Latency}_{i+1,t,k,g})\).

**Stage 2: Anomaly Detection in Latency Inequality**

Based on the GiniLI calculated for each time window, I perform a time series forecasting to detect anomalies in the trend of GiniLI. Time series forecasting enables the identification of abnormal GiniLI that does not follow the historical movement of GiniLI. The typical forecasting algorithms are the Moving Average (MA) method and exponential smoothing method for both smoothing and forecasting. Furthermore, Seasonal Autoregressive Integrated Moving Average (SARIMA), Long Short-term Memory (LSTM), and Holt-Winters’ seasonal method are used to decompose time series data with seasonality. In particular, a MA method is utilized to forecast future GiniLI since the stock trade depends on the market expectation and is affected by an extremely short historical time interval. Furthermore, the MA method well suits our purpose to smooth the calculated GiniLI to assure a stationary trend.\(^{27}\) MA utilizes the historical movement of GiniLI to identify the acceptable boundary of future GiniLI. The acceptable boundary, both upper and lower bound, is defined by the prediction interval calculated by the historical GiniLI.

\[
\hat{G}iniLI_t \pm t_{crit} \times \sqrt{MSE}
\]

where \(t_{crit}\) is the predetermined critical \(t\)-value, and \(MSE\) is the mean squared error.

When the actual GiniLI exceeds the prediction interval (i.e., lower or higher than the acceptable boundary), I calculate the sign of the second-order derivatives of the nearby GiniLI at time \(T_0\) to determine the inspection window. The inspection window is a time interval

\(^{27}\) Costa and Vasconcelos (2003) had shown the nonstationary trend in the Brazilian stock market.
interval that is considered where a potential attack is executed. In particular, based on
the sign of the second-order derivatives, I identify the shape of the GiniLI trend (see Figure
12). If there is a change of the form of the trend nearby $T_0$ (i.e., concave up to concave
down or concave down to concave up), a boundary (before and after the $T_0$) is set to
determine the inspection window. The inspection window is between the nearest Point of
Inflections (POI), and the time period after the nearest POI from $T_0$ is the monitoring
window to identify a potential anomaly in latency. The time period after the first POI is the
monitoring window, which will be further described in Stage 3.

![Figure 12. Inspection Window Determination](image)

**Figure 12. Inspection Window Determination**

**Stage 3: Identifying the Cause of GiniLI Anomaly**

The forecasting model in Stage 2 detects the anomaly in GiniLI trend. In Stage 3, I
identify the attributes that are the significant determinants of the anomaly. Since my target
variable (i.e., dependent variable) is $GiniLI$ that is a continuous variable, the regression tree,
which is also known as the continuous variable decision tree, is used to identify the
significant attributes that determine the $GiniLI$ value. The regression tree splits the quotes
made within the inspection window with the categorical attributes (e.g., quote type, server, brokerage service) that features each quote. The machine learning algorithm repeats the procedure until the quotes in each leaf node share identical classes.\(^{28}\)

Starting from the tree root, quotes are split based on the features that maximize the information gain, which is named Latency Inequality Impact Score (\(LIIS\)). The \(LIIS\) measures how well each attribute determines the target variable (i.e., \(GiniLI\)). The \(LIIS\) is formalized as follows:

\[
LIIS(Q_{\text{parent}}) = I(Q_{\text{parent}}) - \frac{N_{\text{left}}}{N_{\text{parent}}} I(Q_{\text{left}}) - \frac{N_{\text{right}}}{N_{\text{parent}}} I(Q_{\text{right}})
\]

where \(I\) is the entropy measure, \(Q\) is the quote, and \(N\) is the number of quotes that belongs to the node.

Notably, \(I\) is the impurity measure, such as entropy measure and Gini index\(^{29}\). I utilize the entropy measure even it requires higher computation than the Gini index since it provides stationary effect by its logarithmic function. The entropy impurity measure is defined as follows:

\[
Entroy(q) = -\sum_v p(q = v) \log_2 p(q = v)
\]

where \(p(q = v)\) is the probability that the GiniLI associates to a specific class \(v\) for each attribute.

By calculating \(LIIS\) for each attribute, the model identifies significant determinants of the GiniLI anomaly. For example, assuming that an anomaly is identified by my

\(^{28}\) The depth of the tree is limited with a technique known as pruning to avoid a deep tree problem (i.e., overfitting).

\(^{29}\) Gini index as an impurity measure is different to the Gini coefficient used in calculating GiniLI.
forecasting algorithm, as discussed in Stage 2, the algorithm shortly determines the inspection window and measures the \( LIIS \) to identify the attributes that caused the anomaly. Simultaneously, during the predetermined monitoring window period, the system monitors quotes to find one that relates to the flagged attributes' characteristics. For example, I identify quotes that share the common characteristic, such as a broker-dealer identifier and massive cancellation quotes to offset the original quote. In sum, Figure 13 summarizes the process of \textit{GiniLI} measurement and monitoring process.

![Figure 13. Overview of GiniLI Process](image)

\textit{Results and Performance}

\textit{GiniLI Statistics and Predictability}

Table 12 provides the daily descriptive statistics of \textit{GiniLI} by each session. GiniLI is calculated for every second and using every quote executed in a certain time period. The result shows that \textit{GiniLI} mostly nears zero, which implies low inequality. Technically, each gateway can handle a certain number of quotes until it reaches its threshold. When the number of quotes exceeds the threshold, the gateway slows down and simultaneously increases the latency inequality.
Table 12. GiniLI Statistics

<table>
<thead>
<tr>
<th>Date</th>
<th>Count</th>
<th>Mean</th>
<th>Std</th>
<th>Min</th>
<th>25%</th>
<th>50%</th>
<th>75%</th>
<th>Max</th>
</tr>
</thead>
<tbody>
<tr>
<td>Day 1</td>
<td>32,400</td>
<td>.0238</td>
<td>.0622</td>
<td>.0000</td>
<td>.0000</td>
<td>.0000</td>
<td>.0298</td>
<td>.4477</td>
</tr>
<tr>
<td>Day 2</td>
<td>32,400</td>
<td>.0264</td>
<td>.0584</td>
<td>.0000</td>
<td>.0000</td>
<td>.0000</td>
<td>.0271</td>
<td>.4569</td>
</tr>
<tr>
<td>Day 3</td>
<td>32,400</td>
<td>.0325</td>
<td>.0651</td>
<td>.0000</td>
<td>.0000</td>
<td>.0000</td>
<td>.0377</td>
<td>.4571</td>
</tr>
<tr>
<td>Day 4</td>
<td>32,400</td>
<td>.0514</td>
<td>.0731</td>
<td>.0000</td>
<td>.0000</td>
<td>.0278</td>
<td>.0766</td>
<td>.4553</td>
</tr>
<tr>
<td>Day 5</td>
<td>32,400</td>
<td>.0495</td>
<td>.0716</td>
<td>.0000</td>
<td>.0000</td>
<td>.0239</td>
<td>.0735</td>
<td>.4541</td>
</tr>
</tbody>
</table>

I perform an Augmented Dickey-Fuller (ADF) to examine the stationarity of GiniLI that can influence the performance of the forecasting algorithm (refer to Stage 2). Based on the result given in Table 13, GiniLI does not show significant stationary until smoothing the trend by taking the rolling mean for 180 seconds. To further inspect other non-stationarity features in the GiniLI trend, I visualize the trend of GiniLI with a rolling mean for 180 seconds. A gradual increase in GiniLI is observed during the market opening and closure in Panel A in Figure 14. However, the rolling standard deviation shown in Panel B in Figure 14 shows no evidence of significant stationarity, which is supported by the ADF test result.

Table 13. Augmented Dikey-Fuller Test

<table>
<thead>
<tr>
<th>GiniLI</th>
<th>Day 1</th>
<th>Day 2</th>
<th>Day 3</th>
<th>Day 4</th>
<th>Day 5</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Rolling Mean (60)</strong></td>
<td>-10.574***</td>
<td>-10.683***</td>
<td>-10.635***</td>
<td>-6.512***</td>
<td>-6.607***</td>
</tr>
<tr>
<td><strong>Rolling Mean (180)</strong></td>
<td>-5.466***</td>
<td>-5.716***</td>
<td>-5.292***</td>
<td>-3.124**</td>
<td>-3.047**</td>
</tr>
</tbody>
</table>
Figure 14. Rolling Mean and Standard Deviation of GiniLI

a. Rolling Mean

![Rolling Mean graph]

b. Rolling Standard Deviation

![Rolling Standard Deviation graph]

I further examine the predictability of $GiniLI$ by using a time series regression model. The prediction model relies on the premise that if $GiniLI$ can effectively capture anomaly in latency, it should be capable of predicting an increase in latency that leads to higher market uncertainty. In particular, the regression model is specified to find the
association between the $t+1$ period latency (i.e., one second ahead) and the current period cancellation rate by $t$ period anomalies. The regression model is specified as follows:

$$Latency_{t+1} = Cancellation\ Rate_t + Anomalies_t + Cancellation\ Rate_t \times Anomalies_t + Day_t + Hour_t$$

In Model 1 of Table 14, the $t+1$ period latency (including new order and cancellation order) significantly increases when an anomaly occurs at period $t$. On the other side, in general, the $t+1$ period latency significantly increases when the cancellation rate at period $t$ decreases (i.e., new order exceeds cancellation order). Notably, a lower cancellation rate and anomaly detected at period $t$ led to higher $t+1$ period latency. In fact, the interaction with anomaly increases the magnitude of the cancellation rate coefficients, which exacerbates higher latency. In Model 2 and 3 of Table 14, I conduct a regression analysis on average latency among new orders and cancellation orders to test for robustness. The results in Model 2 and 3 show a consistent result with Model 3.

### Table 14. Latency and Cancellation Rate

<table>
<thead>
<tr>
<th>Dependent Variables</th>
<th>(1) Latency_Total_{t+1}</th>
<th>(2) Latency_New_{t+1}</th>
<th>(3) Latency_Cancel_{t+1}</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Coefficients</td>
<td>$t$-statistics</td>
<td>Coefficients</td>
</tr>
<tr>
<td>Intercept</td>
<td>14.065***</td>
<td>1476.75 (0.000)</td>
<td>13.980***</td>
</tr>
<tr>
<td>Cancellation_Rate{t}</td>
<td>-0.007***</td>
<td>-5.93 (0.000)</td>
<td>-0.002***</td>
</tr>
<tr>
<td>Anomalies{t}</td>
<td>0.916***</td>
<td>104.90 (0.000)</td>
<td>0.355***</td>
</tr>
<tr>
<td>Cancellation_Rate *</td>
<td>-0.015***</td>
<td>-7.70 (0.000)</td>
<td>-0.008***</td>
</tr>
<tr>
<td>Anomalies</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Adjusted $R$-squared</td>
<td>0.148</td>
<td>0.068</td>
<td>0.147</td>
</tr>
<tr>
<td># of Observations</td>
<td>72,362</td>
<td>72,362</td>
<td>72,362</td>
</tr>
</tbody>
</table>
Deterrence Effect of GiniLI on Latency

In order to demonstrate the deterrence effect of GiniLI on latency, a Monte Carlo experiment is performed with synthetic data. The purpose of the simulation is to measure the effect of GiniLI on latency when the number of transactions increases. In specific, a set of data are generated that follow a certain degree of GiniLI by changing the expected rate of occurrences ($\lambda$) in a Poisson distribution. Notably, I use Poisson distribution to approximate the actual latency distribution observed from the B3 dataset. Poisson distribution is often used to represent the signal latency generated by system, network, and even in neurons (Pike, 1973; Linderman and Adams, 2014; Sun and Ansari, 2017). The model is constructed based on two components that are 1) the Poisson distribution that represents a latency of transactions controlled by a certain degree of GiniLI and 2) exogenous market effect that is assumed to be a random walk following previous literature.

In specific, four different Poisson Distributions are generated, $P(\lambda, k)$, where $\lambda$ is the expected rate of occurrences of transactions within a specific time span, and $k$ is the number of actual transactions entering the system. Higher $\lambda$ represents lower GiniLI threshold implemented by the stock exchange (more strict control), and lower $\lambda$ represents higher GiniLI (less strict control). I define the relative latency as an inverse function of the probability of occurrence of transactions within a specific period ($\frac{1}{P(\lambda, k)}$). Further, the market effect is considered since it can potentially impact the occurrence of transactions. In the model, the market effect is assumed to follow a random walk. Accordingly, the model incorporates the market effect as a random variable that follows a normal distribution.
The simulation result shown in Figure 15 indicates that lower $GiniLI$ (e.g., less strict threshold) results in a significant increase in latency compared to higher $GiniLI$. In general, higher $GiniLI$ (e.g., Model 1 and Model 2) leads to an increase in latency with a relatively smaller number of transactions within a specific time span, where lower $GiniLI$ (e.g., Model 3 and Model 4) shows a significantly lower range of latency. The simulation result suggests that the latency can be managed by $GiniLI$ even incorporating the random effect introduced by the market.

<table>
<thead>
<tr>
<th>Model 1: $\lambda = 1, GiniLI = 0.511$</th>
<th>Model 2: $\lambda = 2, GiniLI = 0.388$</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Model 1]</td>
<td>![Model 2]</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Model 3: $\lambda = 4, GiniLI = 0.276$</th>
<th>Model 4: $\lambda = 10, GiniLI = 0.178$</th>
</tr>
</thead>
<tbody>
<tr>
<td>![Model 3]</td>
<td>![Model 4]</td>
</tr>
</tbody>
</table>

*Figure 15. Gini LI and Latency*
Next, I estimate the cost of latency by following Moallemi and Sağlam (2013)’s analytical representation of latency cost. The representation of latency cost is obtained from an explicit closed-form solution in a low latency regime. Given a latency of $\Delta t$, price volatility of $\sigma$, and a bid-offer spread of $\delta$, the latency cost is defined as:

$$\frac{\sigma \sqrt{\Delta t}}{\delta} \sqrt{\log \frac{\delta^2}{2\pi \sigma^2 \Delta t}} \quad \text{as} \quad \Delta t \to 0$$

The model is based on the assumption that the price volatility and bid-offer spread are consistent among the transactions within the specific time span. This is possible since in the real implementation of $GiniLI$, the time span is limited under one minute. Hence, the form of latency cost can be simplified as $\sqrt{\Delta t \log \frac{1}{\Delta t}}$. Similar to the previous Monte Carlo experiment, I simulate the latency cost for Model 1 to 4. The result in Figure 16 shows the latency cost for each model, where each curve from the top represents the latency cost of Model 1, Model 2, Model 3, and Model 4, respectively. It shows that approximately 0.1 index points drop in $GiniLI$ results in 10% drop in latency cost for each broker-dealer in the market.
Figure 16. The Cost of Latency

Conclusion

Low latency and fair trading opportunities are crucial to the market to prevent substantial market instability. The objective of the effort to measure latency inequality is to develop a quantitative mechanism to identify processing delay of order execution in advance and to take timely meditative countermeasures. As more market participants utilize machine-driven trading mechanisms, the suggested latency control mechanism will support the stock exchanges to provide a fair trading opportunity to the market participants. The structure of the suggested model enables not only to identify and predict potential processing delay but also to deter latency that can improve the market stability. The suggested inequality measure can be further utilized to identify market manipulative activities in the future. The approach will be implemented by the Brazilian Stock Exchange and be evaluated with population transaction information. Hence, our approach and efforts
to counter latency inequality will enhance the fair-trading opportunity for the market participants and will ultimately lead to better market transparency.
CONCLUSION

In 2016, Michael Vatis, the founding director of the FBI’s National Infrastructure Protection Center had stated that: “In the very near future, cybersecurity exercises are going to be absolutely expected of all companies by regulators.” Today, firms possess and process a substantial amount of valuable assets in a digital form that is vulnerable to cybersecurity threats. As anticipated by Mr. Vatis, a number of regulators and standard setters are requiring firms to perform rigorous risk assessments toward their cybersecurity infrastructure and informational assets. However, risk assessment challenges derive from a lack of knowledge and experience in risk measurement. Compared to the technological aspects of cybersecurity, we do not understand how other external factors, such as human and managerial aspects, can affect a firm’s cybersecurity risk.

In my dissertation, I introduce three examples of cybersecurity risk measurement by adopting a data analytic approach. For each chapter, I provide an illustrative guideline on collecting information related to cybersecurity risk and analyzing it to derive a credible quantitative measure. I understand the subject of matters discussed in the dissertation is relatively narrowed, which is a small portion of the cybersecurity risk we are confronting. However, taking the first step leads to the budding of an opportunity to be able to develop a comprehensive cybersecurity measure. Yet, we have limited knowledge and data to measure matters in cybersecurity. However, the small steps made by researchers could lead to a level where we can analyze cybersecurity risk as like financial ratio analysis.

30 The statement is accessible at https://tinyurl.com/dmzc6v9f.
Further, I hope more researchers and practitioners in cybersecurity assurance can utilize unstructured information. Notably, the usage of unstructured information can extend my discussion on topics that were traditionally treated as unobservable. For example, if the practitioners know how to analyze textual data, they can obtain an evidence of an insider threat by analyzing the posts in the insider forum. Future researchers may utilize the methodologies introduces in the dissertation and apply them to other topics where measurements are needed.
BIBLIOGRAPHY


Cressey, D. R. (1953). Other people’s money; a study of the social psychology of embezzlement.


Forbes Human Resources Council. (2020). With a second wave of layoffs looming,


APPENDICES

Appendix A: Detail of the CRDS Measurement Process

A.1. Simplified Flowchart
A.2. Detailed Flowchart
Appendix B: A Platform of CRDS for U.S. Public Firms

Note: A platform can be found at https://tinyurl.com/tpo78mr.
Appendix C

C.1. Business Description (Item 1) Extraction

To obtain a business description for each firm, I first download all 10-K filings (including Form 10-KT) for 13 years (between 2006 and 2019) from the SEC’s Electronic Data Gathering, Analysis, and Retrieval (EDGAR) system. I then preprocess each filing to retrieve HyperText Markup Language (HTML) tags and remove characters (Unicode Normalization) that are unrelated to my analysis (e.g., symbols). To exclude the “Table of Contents,” I remove the portion by identifying the tags indicating the table. Next, based on the tags which indicate the beginning of Item 1 (e.g., “Item 1,” “Item 1.,” and ‘Item 1:”) and Item 1A (e.g., “Item 1A,” “Item 1A.,” and “Item 1A:”), the contents are parsed out between those two tags. Firms that are not required to disclose Item 1A (smaller reporting firm) are treated as exceptions, and the contents are parsed out from Item 1 through Item 1B or Item 2.

C.2. Risk Factors (Item 1A) Extraction

Several Item 1As include graphs. I retrieve only the textual contents from the 10-K filings and filter out non-alphanumerical characters. Similar to Item 1 Extraction, Item 1A is parsed out using HTML tags indicating the beginning and end of Item 1A (e.g., “Item 1A,” “Item 1A.,” and “Item 1A:”). Smaller reporting firms that are not required to disclose risk factors are excluded from my analysis.

---

31 For more details, see https://unicode.org/faq/normalization.html.
32 For more details, see https://www.sec.gov/smallbusiness/goingpublic/SRC.
Appendix D

D.1. Risk Topic Classification

My objective is to produce an optimal $\vec{d}_j$ that represents each cybersecurity risk disclosure as a function of the topic word embedding vector ($\vec{t}_k$) and risk topic weights ($p_{jk}$).

$$
\vec{d}_j = p_{j0} \vec{t}_0 + p_{j1} \vec{t}_1 + \ldots + p_{jk} \vec{t}_k + p_{j20} \vec{t}_{20}
$$

where $0 \leq p_{jk} \leq 1$.

The training process for the model consists of minimizing the total loss $L$:

$$
L = L^d + \sum_{mn} L_{mn}^{\text{neg}}
$$

where $m, n$ represents the position of each word $w_{mn}$ in a given sentence.

In general, to obtain a proper topic word embedding vector ($\vec{t}_k$) and risk topic weight ($p_{jk}$), I train the model to minimize Dirichlet-likelihood loss ($L^d$) over each cybersecurity risk disclosure and Skip-Gram negative sampling loss ($L_{mn}^{\text{neg}}$) for each word. Following Kingma and Ba (2014), $L^d$ is calculated by Adam optimizer as follows:

$$
L^d = \lambda \sum_{jk}(\alpha - 1) \log p_{jk}.
$$

The second term, $\sum_{mn} L_{mn}^{\text{neg}}$, is minimized when each word embedding can be properly segregated from other word embeddings. Note that, according to Mikolov et al. (2013), each word is represented by the nearby words in a sentence (i.e., word embedding).

---

33 This section is adopted from Moody (2016).
34 I assume 20 existing topics to align with our analysis. The number of topics is determined by the Within Cluster Sum of Squares (WCSS) measurement methodology.
**D.2. Saturation Process**

The saturation process utilizes a Hue, Saturation, and Value (HSV) model in which I convert the RGB image into an HSV color space, where the conversion of the RGB color space to HSV color space is mathematically defined by Loesdau et al. (2014) as follows:

\[
R, G, B \in [0, 1] \text{ where } \text{Max} = \text{argmax}(R, G, B), \text{Min} = \text{argmin}(R, G, B)
\]

\[
H: \begin{cases} 
0, & \text{if } R = G = B \\
60^\circ \left(0 + \frac{G - B}{\text{Max} - \text{Min}}\right), & \text{if Max} = R \\
60^\circ \left(2 + \frac{B - R}{\text{Max} - \text{Min}}\right), & \text{if Max} = G \\
60^\circ \left(4 + \frac{R - G}{\text{Max} - \text{Min}}\right), & \text{if Max} = B
\end{cases}
\]

\[
S: \begin{cases} 
0, & \text{if } R = G = B \\
\frac{\text{Max} - \text{Min}}{\text{Max}}, & \text{else}
\end{cases}
\]

\[
V: = \text{Max}
\]

Following the rules of conversion, I determine a new RGB color space \((R', G', B')\) that satisfies all systematic equations for conversion with a predefined \(f_{jk}\). Without loss of generality, I can compute the RGB color space for each firm.

**D.3. Distributed Firm Vector Representation**

The first step to generate an embedded map of firms is to train Item 1 to learn the distributed vector representation of words. Every word that I tokenized during data preparation is mapped to a single word vector \(\vec{W}\). Item 1 provides the sequence of training words \(w_1, w_2, w_3, \ldots, w_T\). In addition, each firm’s Item 1 is labeled as a paragraph vector.

---

\[^{35}\text{This section refers to Le and Mikolov’s (2014) approach to distributed vector representation of words and documents.}\]
\( \vec{D} \) as \( d_1, d_2, d_3, \ldots, d_Q \), where \( Q \) is the total number of firms. After the given sequence of the word vector \( \vec{W} \), I add paragraph vector \( \vec{D} \) as a memory to recall the missing token, \( \vec{W} \), a mechanism is known as the distributed memory model of paragraph vectors (PV-DM).

I solve the average log probability maximization problem given by Le and Mikolov (2014) as follows:

\[
\frac{1}{T} \sum_{t=k}^{T-k} \log p(w_t | w_{t-k}, \ldots, w_{t+k})
\]

It is preferable to use the predictor function \( p \) as a hierarchical Softmax (Morin and Bengio 2005; Mikolov et al. 2013), which allows to determine the predictor function \( p \):

\[
p(w_t | w_{t-k}, \ldots, w_{t+k}) = \frac{e^{y_{w_t}}}{\sum_i e^{y_i}}
\]

As follows, I derive \( y \), which is a function of \( h \), from the concatenation or average of word vectors extracted from \( \vec{W} \):

\[
y = b + U(h(w_{t-k}, \ldots, w_{t+k}; \vec{W}))
\]

Next, I map paragraph vector \((\vec{D})\)—which uniquely represents Item 1 of each firm—on top of the word vector \( \vec{W} \) based on the PV-DM. Finally, I introduce the “inference stage” to tune the parameters by using an unseen paragraph vector \( \vec{D} \), which is an additional new Item 1.
Appendix E: Alternative Approach to Identify Dark Web Post

As an alternative approach for identifying the dark web posts containing insider information, each dark web market post can be clustered by comparing the contents. In specific, a Doc2Vec model is constructed with Noun words within each post by following Mikolov et al. (2013). Accordingly, the dark web posts are clustered into 13 different categories, as provided in Figure E1. The representative keywords of each category are extracted with Latent Dirichlet Allocation (LDA) Topic Modeling.

![Figure E1. Categories of dark web market posts](image)

Next, for each post included in “Topic 6 – Business Information,” I count the dark web post containing the firm’s name. To prevent counting the republished posts multiple times, the contents for each post are compared and the later posts are excluded that are republished. Table E1 provides the topics discussed in the final sample of insider information posts.
Table E1. Categories of Insider Information Posts

<table>
<thead>
<tr>
<th>Topic</th>
<th>Representative Keywords</th>
<th>Number of Posts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Employee Account</td>
<td>Account, Admit, Human, Number, People</td>
<td>8,961</td>
</tr>
<tr>
<td>Executive Information</td>
<td>Board, Contact, Number, Social, Security</td>
<td>22,659</td>
</tr>
<tr>
<td>Vendor Information</td>
<td>Certificate, Company, File, License, Vendor</td>
<td>16,473</td>
</tr>
<tr>
<td>System Access</td>
<td>Password, Software, Status, System, Username</td>
<td>12,570</td>
</tr>
<tr>
<td>Proprietary Information</td>
<td>Cellular, Conference, Data, Scientist, Work</td>
<td>7,672</td>
</tr>
<tr>
<td>Information Sharing</td>
<td>Contribution, Information, Note, People, Worth</td>
<td>6,076</td>
</tr>
<tr>
<td>Arbitrage Information</td>
<td>Business, Company, Leaked, Seller, Silence</td>
<td>16,372</td>
</tr>
</tbody>
</table>

Table E2 shows a consistent result of Hypothesis 1. We also observe more robust result compared to the previous result provided in Table 4. However, the result driven by ITF identification is presented as a main result since it is more feasible to verify the result.

Table E2. Effect of Layoff on Insider Information Leakage

<table>
<thead>
<tr>
<th>Coefficients</th>
<th>(1)</th>
<th>(2)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Base (No Controls)</td>
<td>With Controls</td>
</tr>
<tr>
<td>Constant</td>
<td>0.796 (1.792*)</td>
<td>1.626 (5.499****)</td>
</tr>
<tr>
<td>Layoff</td>
<td>-0.854 (-2.856***)</td>
<td>-1.280 (0.036**)</td>
</tr>
<tr>
<td>Week</td>
<td>-0.134 (-2.581***)</td>
<td>-0.1340 (-2.581**)</td>
</tr>
<tr>
<td>Layoff × Post</td>
<td>0.405 (2.619***</td>
<td>0.405 (2.619***</td>
</tr>
<tr>
<td>Revenue</td>
<td>-</td>
<td>-0.014 (0.715)</td>
</tr>
<tr>
<td>Employee</td>
<td>-</td>
<td>0.142 (0.245)</td>
</tr>
<tr>
<td>Public</td>
<td>-</td>
<td>-0.649 (-2.343***)</td>
</tr>
<tr>
<td>Industry</td>
<td>-</td>
<td>Included</td>
</tr>
<tr>
<td>( \text{# of OBS} )</td>
<td>1,758</td>
<td>1,758</td>
</tr>
<tr>
<td>-----------------</td>
<td>-------</td>
<td>-------</td>
</tr>
<tr>
<td>( \text{Adj.} R^2 )</td>
<td>0.456</td>
<td>0.456</td>
</tr>
</tbody>
</table>