2023

Cyber Risk Exposure through Supply Chain Information Network: An Application of Social Network Analysis

Long Thai Bui

Cyber Risk Exposure through Supply Chain Information Network: An Application of Social Network Analysis

By

Long Thai (David) Bui

MASTER THESIS

Submitted to

The University of Texas at Arlington

in partial fulfillment of the requirements for the degree of

Master of Science in Information Systems

August 2023

Arlington, Texas

Thesis Committee:

Dr. Sridhar Nerur (Chair)

Dr. Nandu Nagarajan (Co-Chair)

Dr. Ram Venkataraman (Member)

Dr. Mahmut Yasar (Member)

Cyber Risk Exposure through Supply Chain Information Network: An Application of Social Network Analysis

Abstract

In this paper, I study the impact of supply chain information networks on cyber risk exposure. I document that firms that are more central in the supply chain information network have higher cyber risk exposure. The rapid advancement of information and communication technology (ICT) has led to increased interconnectedness within global supply chain networks. While this enhances efficiency and profitability, it also exposes these entities to systematic and contagious risks, as cyber criminals exploit the connectedness to infiltrate multiple firms simultaneously. High-profile cyber-attacks like NotPetya, SolarWinds, and Colonial Pipeline have devastating effects on organizations and pose threats to national security. In response to these attacks, the United States government declared vulnerabilities in the supply chain network as a national emergency in 2022, leading to efforts to reinforce cybersecurity systems. However, limited research exists on supply chain factors that determine firms' exposure to cyber-attacks and cyber risk management policies. This paper contributes to the economics of cybercrime literature by exploring the interconnections of digital infrastructure among firms in the supply chain network and demonstrating the use of network theory and empirical analysis techniques to assess firm risk profiles.

Keywords: Cyber Risk, Supply Chain, Network Analysis

Table of contents

1) Introduction 1

2) Literature Review and Hypothesis development 2

2.1. Exposure to Cyber-Attacks Through Supply Chain Network 2

2.2. Hypothesis 1: The Impact of Centrality on Supply Chain Cyber Risk Exposure 4

3) Research design 5

3.1. Proxies for cyber risk 5

3.2. Supply chain network position 6

3.3. Regression 7

3.4. Data and Sample Selection 8

4) Empirical results 8

4.1. Descriptive statistics 8

4.2. Hypothesis 1: The Impact of Centrality on Supply Chain Cyber Risk Exposure (Table 3) 8

5) Conclusion 9

References 9

Appendix A Variable Definition 12

Appendix B Tables 14

Appendix C Robustness Tests 17

Appendix D-Examples of Supply Chain Cyber Risk 19

1) Introduction

Since the early 2000s, the accelerated progress of Information and Communication Technology (ICT) has significantly augmented the electrical interconnectedness of global supply chain networks, revolutionizing the manner in which these entities exchange information. This heightened interconnectedness undoubtedly enhances the efficiency and profitability of supply chain members. However, it concurrently renders these entities interdependent and susceptible to a host of systematic and contagious risks. Particularly noteworthy are cyber criminals who adeptly exploit the interconnected supply chain information networks, employing ransomware to infiltrate multiple firms simultaneously. Illustrative instances of such cyber-attacks include NotPetya in 2017, Solar Winds in 2020, and Colonial Pipeline in 2021, each of which yielded widespread and devastating consequences for numerous organizations spanning government entities, public, and private companies within remarkably short periods[1]. Moreover, these cyber intrusions impose substantial threats on national security, encompassing critical domains such as defense, energy, and food.

In response to this series of profoundly impactful supply chain cyber-attacks, the United States government declared the vulnerabilities within the information and communication infrastructure of the national supply chain network as a matter of national emergency in 2022. This declaration galvanized efforts to reinforce cyber security systems across governmental and non-governmental entities within the United States. To this end, the Cybersecurity & Infrastructure Security Agency (CISA) established a task force dedicated to supply chain risk management in 2018 and is currently in the process of establishing a permanent supply chain office in 2023[2].

However, despite the escalating sophistication, frequency, and severity of cyber-attacks affecting multiple entities simultaneously, research on supply chain factors that determine firms' exposure to such cyber-attacks and cyber risk management policies remains relatively limited, as pointed out by Kumar and Mallipeddi in 2022. This paucity of comprehensive investigations underscores the pressing need for scholarly inquiries to address this crucial facet of supply chain resilience and security.

The majority of previous studies concerning the determinants of cyber risk have predominantly centered on the characteristics of the focal firm. Notably, certain aspects of IT governance quality have been identified as influential factors in mitigating cyber risks. For instance, research by Haislip et al. (2021) establishes that executive IT expertise is linked to a reduction in cyber risks. Similarly, Wang, Kannan, and Ulmer (2013) demonstrate the significance of cyber risk awareness in lowering the likelihood of cyber incidents. Moreover, Smith et al. (2021) find that the experience of Chief Information Officers plays a role in minimizing cyber risks for organizations. In addition to IT governance factors, the value of information possessed by companies, including trade secrets, has been implicated as a determinant of cyber risk. Ettredge, Guo, and Li (2018) establish a positive association between the value of information held by companies and the likelihood of breaches occurring. Despite the valuable insights garnered from these studies, it is important to recognize that they primarily assess firms' cyber risk by focusing solely on their internal characteristics. Consequently, these analyses do not take into consideration the potential threats emanating from economically interconnected entities, such as supply chain partners. To comprehensively

[1] https://www.whitehouse.gov/omb/briefing-room/2022/09/14/enhancing-the-security-of-the-software-supply-chain-to-deliver-a-secure-government-experience/
https://www.commerce.gov/issues/ict-supply-chain

[2] https://www.supplychaindive.com/news/supply-chain-cybersecurity-risks-what-to-know/647597/

understand and address cyber risk, future research should consider the broader network of interconnected organizations within the supply chain and their potential impact on the cyber risk landscape.

In this paper, I fill this gap by examining how supply chain information networks can impact firms' susceptibility to cyber-attacks. Specifically, I first study how a firm's centrality in the network affects its cyber risk. The potential risks stemming from supply chain cyber-attacks arise from two primary sources: deliberate strategic attacks and random attacks (Acemoglu, Malekian, and Ozdaglar, 2016). In strategic attacks, cyber criminals strategically target their initial victims to maximize the overall damage inflicted upon the supply chain network while expending minimal effort. As per network theory and relevant empirical studies (Acemoglu et al., 2012), central nodes assume a critical role in amplifying idiosyncratic shocks into more pervasive and systematic disruptions. Consequently, firms occupying central positions within the supply chain information network are more susceptible to being selected as primary targets in strategic attacks when compared to peripheral firms, all else being equal. Conversely, random attacks involve the indiscriminate targeting of initial victims, regardless of the projected extent of damages or the level of cyber security measures in place. Based on network theory (Borgatti, Everett, Johnson, and Agneessens 2022), it can be mathematically proven that the likelihood of a firm being infected by ransomware, which initially targets another firm within the same network, is positively associated with the firm's centrality. Therefore, I hypothesize and find that a firm's exposure to cyber risk is positively associated with its centrality in the supply chain information network.

Overall, my paper makes several important contributions to the literature on cyber security, a topic that has been gaining significant attention from academic researchers, practitioners, and policy makers alike in recent years. The literature has primarily focused on investigating the causes (D'Arcy, Adjerid, Angst, and Glavas, 2020; Haislip, Lim, and Pinsker, 2021) and consequences (Kamiya, Kang, Kim, Milidonis, and Stulz, 2021) of cyber-attacks on individual firms in isolation. In contrast, my paper provides a unique exploration of the digital infrastructure interconnections among firms in the supply chain network, showing how a firm's position in the information network increases its exposure to cyber risk.

Methodologically, this paper makes a valuable contribution to the growing body of literature focused on quantifying firm-level risk exposure (Florackis, Louca, Michaely, and Weber, 2023; Jamilov, Rey, and Tahoun, 2021). My study demonstrates the efficacy of combining network theory with empirical network analysis techniques as a means for researchers to comprehensively understand and evaluate firm risk profiles. Although prior work by Florackis et al. (2023) highlights the pricing of cyber risk by the capital market due to its systemic nature, this paper takes a distinct approach by investigating the contagious nature of cyber risk and elucidating its systematic aspects through the application of network analysis. By doing so, the study adds new dimensions to the understanding of cyber risk dynamics and contributes to the advancement of risk assessment methodologies.

2) Literature Review and Hypothesis development

The paper commences by elucidating the characteristics and intricacies of supply chain cyber-attacks. Subsequently, it provides a concise overview of the pertinent literature concerning network effects. Finally, the study outlines its specific hypotheses, thus setting the groundwork for the subsequent analyses.

2.1. Exposure to Cyber-Attacks Through Supply Chain Network

Supply chains have undergone significant transformation, evolving into intricate and highly interconnected networks over the past two decades, facilitated by the adoption of information and communication technology (ICT) for inter-firm coordination across diverse industries and geographical regions.

Consequently, the cyber vulnerability of a firm is no longer solely contingent on the security of its own IT system but is also intricately intertwined with the cyber resilience of its supply chain partners. The occurrence of a substantial and escalating number of cyber-attacks has been observed to propagate throughout supply chain networks, impacting numerous governmental and nongovernmental entities alike (Kumar and Mallipeddi, 2022; Crosignani, Macchiavelli, and Silva, 2023).

According to Kumar and Mallipeddi 2022, supply chain cyber-attacks manifest when a cyber-attacker initially infiltrates a firm's system and subsequently exploits the inter-firm information networks to compromise other interconnected firms.. According to the U.S. National Counterintelligence and Security Center (NCSC), supply chain attacks offer an effective means to circumvent traditional defensive measures and undermine the security of a diverse array of systems.[3],[4]. To facilitate frequent and seamless communication among supply chain partners, a system of privileged access is granted by member firms to one another, as outlined by the Cybersecurity and Infrastructure Security Agency (CISA). Privileged access denotes the level of authorization and permissions bestowed upon individuals or entities vested with higher authority or responsibility within the system. Typically, this entails granting certain users elevated privileges and permissions to access critical or sensitive information, execute administrative tasks, or effect substantial changes to the system. Consequently, privileged access presents cyber attackers with an effective avenue to circumvent conventional cyber defenses, thereby infiltrating software and delivery processes and compromising a significant number of information systems through a single attack. Firms can be exposed to supply chain cyber-attacks via either strategic attacks or random attacks (Acemoglu, Malekian, and Ozdaglar 2016). In a strategic attack, cyber intruders try to maximize expected damage to the network when determining their first target. In a random attack, targets are selected arbitrarily regardless of their security levels and expected damage to the network.

A firm might become a direct target of a strategic supply chain cyber-attack due to its possession of more information concerning access to other interconnected firms' systems, which allows intruders to maximize the extent of damage inflicted upon the network. An illustrative example is provided by Apple, which, in its 2018 10-K disclosure, acknowledges the potential for being a direct target of supply chain cyber-attacks owing to its practice of acquiring and sharing "confidential information with suppliers and other third parties," along with the intrinsic value of the confidential information it generates, owns, manages, stores, and processes (italics added). Similarly, in the Item 1A section of its 10-K filings, General Motors emphasizes the collection and storage of sensitive data, encompassing intellectual property and proprietary business information (including that of dealers and suppliers), as well as personally identifiable information of its customers, thereby underscoring its exposure to cyber risks within the supply chain context.

Conversely, a firm may be subject to indirect and random infection by supply chain ransomware. A case in point is exemplified by the Solar Winds supply chain cyber-attacks, wherein cyber intruders initially targeted Solar Winds and inserted ransomware into its software and systems. Consequently, vendors and customers of Solar Winds, including government entities and multiple S&P 500 companies, were inadvertently infected when they updated the Sunburst software package provided by Solar Winds, which contained the virus introduced by the initial attack. Another instance involves Apple, which experienced an indirect impact from a supply chain cyber-attack directed at its Taiwan supplier, Quanta, in 2021. Furthermore, in its 2016 annual report, General Motors management expressed apprehension regarding the company's susceptibility to supply chain cyber-attacks, stating, "Such parties and other third parties who

[3] https://www.dni.gov/index.php/ncsc-what-we-do/ncsc-supply-chain-threats

[4] According to the National Counterintelligence and Security Center (NCSC), hackers can compromise multiple companies in a single supply chain cyber-attack through either software-enabled attack or hardware-enabled attack.

provide us services or with whom we communicate could also be the source of a cyberattack on, or breach of, our operational systems, network, data or infrastructure."

Given the escalating severity and prevalence of supply chain cyber-attacks, it becomes imperative to grasp and quantify the extent of firm-level exposure to this burgeoning risk. As supply chain cyber risk emanates from the dynamics of supply networks, in the subsequent section, I present a theoretical framework that elucidates how a firm's network characteristics influence its susceptibility, drawing upon network theories. Subsequently, I formulate specific hypotheses, thus establishing a systematic approach to investigate and understand the relationship between firms' positions in the supply chain information network and cyber risk exposure.

2.2. Hypothesis 1: The Impact of Centrality on Supply Chain Cyber Risk Exposure

The literature exploring network effects on firm performance and strategies is extensive and continually expanding. Within business contexts, networks serve as conduits not only for the transmission of positive elements, such as valuable information (Larcker, So, and Wang, 2013; Schabus, 2022), resources (Cunat, 2007; Serpa and Krishnan, 2018), and positive corporate practices or knowledge (Serpa and Krishnan, 2018), but also for the dissemination of negative elements, including misinformation (Bushee, Kim-Gina, and Leung, 2020; Jochem and Peters, 2019), financial and non-financial risk contagion (Acemoglu, Ozdaglar, Tahbaz-Salehi, 2015; Hertzel, Li, Officer, and Rodgers, 2008; Houston, Lin, and Zhu, 2016; Morrison and White, 2013), and undesirable behaviors (Chiu, Teoh, and Tian, 2013).

The position of a node (representing either a firm or an industry) within the network is instrumental as it serves as both the receiver and sender of these elements throughout the network. Accordingly, the node's network position not only influences its own exposure to the network effect but also determines its impact on other members within the network. According to structural capital theory, as proposed by Granovetter (1973) and Burt (2004), a central position within the network grants a node (used as a theoretical general term for a firm) enhanced access to and control over information and resources. As a result, numerous empirical studies have provided evidence of the correlation between firm centrality and positive outcomes. For instance, Bellamy, Gosh, and Hora (2014) demonstrate that a firm's centrality within a supply chain network enhances its access to information from supply chain partners, consequently fostering improvements in its innovation output. Additionally, Rahaman, Rau, and Zaman (2020) find that firms occupying more central positions in the supply chain network benefit from more favorable loan terms and borrowing costs, as these positions afford greater control over inventory flow, thereby reducing operating risk. Furthermore, Larcker, So, and Wang (2013) present evidence that directors with a higher number of connections experience increased profitability and growth opportunities, attributable to the exchange of valuable information and resources facilitated through their connections. While network theory does provide support for both the advantages and disadvantages associated with being centrally positioned within a network, empirical works have relatively devoted less attention to the latter aspect. According to network theory, as articulated by Borgatti, Everett, Johnson, and Agneessens (2022), in the context of an object (such as information or a virus) traversing the network in a random walk manner, the mathematical probability of the object reaching a specific node is positively correlated with the node's degree centrality. Prior empirical research conducted by Ahern (2013), Aobdia, Caskey, and Ozel (2014), and Gao (2021) corroborates this notion by documenting that stocks of firms situated in more central industries exhibit higher systematic risk. This heightened risk exposure arises due to these firms' increased susceptibility to sectoral shocks that propagate and aggregate across industries through trade networks.

Conversely, the central node, regardless of whether it represents a firm or an industry, occupies a pivotal position that renders it more vulnerable to the influence of contagious effects, while simultaneously serving as a potential conduit for amplifying such effects within the network. Acemoglu et al. (2012) document that

central industries play a crucial role in magnifying idiosyncratic shocks into broader aggregate shocks. Notably, existing empirical studies on the contagion effects of central nodes predominantly focus on financial risks, such as stock return volatility and earnings volatility. To the best of my knowledge, this paper represents the first empirical study to explore the relationship between a firm's position within the supply chain network and its exposure to cyber risk.

Within the context of supply chain cyber-attacks, I posit that central firms exhibit a higher level of cyber risk compared to peripheral firms, both in the context of random attacks and strategic attacks. In the scenario of random attacks, the augmented number of connections possessed by central firms elevates the probability of them being infected by supply chain ransomware that initially targets their supply chain partners. In the case of strategic attacks, hackers are more inclined to target central firms, given their position within the network, as doing so maximizes the damages inflicted upon the supply chain network due to the contagion amplification characteristic associated with central firms, all else being equal. As a result, the first hypothesis is formulated as follows:

Hypothesis 1: Firms occupying more central positions within the supply chain network are linked to higher levels of cyber risk.

3) Research design

3.1. Proxies for cyber risk

In this study, I utilize two proxies to measure cyber risk exposure. The first proxy, termed the cyber risk index (CR_INDEX), is developed by Florackis, Louca, Michaely, and Weber (2023) employing the text-based similarity technique, commonly employed in the Finance and Accounting literature (Hoberg and Phillips, 2016; Hoberg and Maksimovic, 2015; Brown and Tucker, 2011). This index, previously used in their paper (Florackis et al., 2023) and by Crosignani et al. (2023), is constructed by computing the cosine similarity between a firm's disclosure of cyber risks and the disclosures of firms that have experienced cyber-attacks within the one-year period preceding the firm's current filings. The underlying rationale for this approach is grounded in two key concepts. Firstly, it acknowledges that firms which have previously encountered cyber-attacks inherently possess an elevated susceptibility to future cyber threats and, thus, convey this heightened risk through their pre-existing risk disclosures. Secondly, it recognizes that firms with comparable levels of cybersecurity risk tend to adopt similar terminologies when articulating their risk exposure and the strategies implemented to manage such exposure. By leveraging these fundamental principles, the cyber risk index provides a robust measure of a firm's cyber risk exposure within the supply chain network.

The second proxy, denoted as BREACH, operates at the firm-year level and assumes a value of one if the firm encounters a cyber-attack during the current fiscal year, and zero otherwise. Notably, the focus of my paper centers on external threats, leading to the exclusion of breach incidents caused by insiders from this particular proxy.

Additionally, an alternative indicator, CO_BREACH, is employed at the firm-year level. This variable assumes a value of one if the firm, along with at least one of its supply chain partners, experiences a cyber-attack during the same current fiscal year. Conversely, it assumes a value of zero if no such cyber-attacks occur within the fiscal year. This measure allows for an assessment of the collective cyber risk exposure within the supply chain network, capturing instances wherein multiple entities within the network are affected by cyber-attacks simultaneously.

In this study, the Florackis cyber risk index (CR_INDEX, henceforth) is employed as the primary proxy for measuring cyber risk exposure, based on the following justifications. Firstly, relying solely on reported

breaches may potentially underestimate firms' actual exposure to cyber risk. As elaborated in the preceding section, a firm's susceptibility to breaches is contingent upon two factors: its attractiveness as a target to cyber-attackers and the robustness of its security system. Conceptually, a firm's cyber risk can be depicted as a function of both its IT security strength and the inherent risk stemming from its nature of business (in this instance, its position within the supply chain information network), as presented below:

Total cyber risk of a firm = f(Inadequate focal firm IT security, inherent risks)

The utilization of the IT security strength of a firm may fluctuate from year to year, whereas its underlying business nature and consequent attractiveness to cyber-attackers tend to persist over time. For instance, the indicator of a reported breach might classify a given firm as high risk (BREACH of 1) in years with reported breaches, and as low risk (BREACH of 0) in years without reported breaches, despite the inherent cyber risk associated with its business operations (such as its position in the supply chain network, industry membership, and level of innovation) remaining stable. This potential underestimation of cyber risk exposure could be further exacerbated by certain firms' intentions to delay or underreport minor breaches before 2011 (Amir, Levi, and Livne, 2018). In contrast, the CR_INDEX offers an advantageous approach as it captures the changes in inherent risks from year to year by comparing the similarities in the operating environment and cyber risk management of a firm to those of other firms with similar cyber risk profiles that have experienced breaches. Consequently, a firm with a high inherent cyber risk can still receive a higher cyber risk index even in the absence of experiencing a cyber breach in a specific year. This index accounts for the dynamic nature of inherent risks over time. Moreover, Florackis, Louca, Michaely, and Weber (2023) have demonstrated that the CR_INDEX is robust in addressing potential issues related to risk underestimation, and their index effectively reflects the appropriate pricing of cyber risk exposure by the capital market.

The use of the breach indicator as a proxy for cyber risk exposure poses two potential issues. Firstly, this variable's distribution is highly unbalanced, with over 95 percent of firm-year observations without reported breaches and less than 5 percent with reported breaches. This severe imbalance may limit the effectiveness of the breach indicator in capturing the full range of cyber risk exposure. Secondly, the breach indicator lacks sufficient variation in measuring cyber risk exposure, which further hampers its ability to address the issue of limited sensitivity.

Conversely, the Florackis cyber risk index offers a continuous variable that spans from 0 to 1, providing a broader spectrum of variation to overcome the limitations posed by the breach indicator. As a result, following the approach of Crosignani, Macchiavelli, and Silva (2023), I adopt the Florackis cyber risk index as the primary proxy for measuring cyber risk exposure, enabling a more comprehensive assessment of cyber risk variation. However, for robustness, I also employ the breach dummy as an additional measure in a separate analysis.

3.2. Supply chain network position

Within the supply chain network, firms engage in communication through information and communication technology (ICT). Firms positioned at more central nodes within this network face a higher likelihood of encountering breaches, stemming from two primary scenarios. Firstly, as direct targets, these firms act as gateways to numerous other firms' information systems, making them susceptible to cyber-attacks. Secondly, they are also vulnerable as indirect targets, being affected by supply chain ransomware initially aimed at their supply chain partners.

To assess a firm's exposure to cyberattack contagions within the supply chain network, I begin by creating a network of firms (referred to as nodes) using data on their supply chain relationships sourced from Compustat Segment. Given that the contagion effect of a virus can travel in either direction, from supplier

to customer or vice versa, I construct undirected networks to account for bidirectional transmission possibilities.

Accordingly, I establish proxies to assess a firm's centrality within the annual supply chain information network through four distinct measures. Firstly, degree centrality quantifies the number of direct connections a node (firm) possesses within the network. Nodes with higher degrees are deemed more central due to their numerous immediate connections, which in turn increase their exposure to the risk of cyberattacks, given their contagious nature. Secondly, closeness centrality gauges how efficiently a node (firm) can access other nodes (firms) within the network. It calculates the average shortest path length between a node and all other nodes, and nodes with higher closeness centrality are considered more central due to their ability to rapidly reach or be reached by other nodes. Thirdly, betweenness centrality assesses the extent to which a node lies on the shortest paths between other nodes in the network. Nodes with higher betweenness centrality act as pivotal bridges, controlling the flow of information, materials, or, in this context, cyber risks through the network. Lastly, eigenvector centrality evaluates a node's influence based on the centrality of its neighboring nodes. A node is regarded as more central if it is connected to other highly connected nodes within the network. To construct an overall centrality measure, I perform principal factor analysis (PCA), following the prior literature on network effects (Schabus, 2022; Larcker et al., 2013; Omer et al., 2020; Borgatti et al., 2022). This factor analysis synthesizes the four centralities (degree, closeness, betweenness, and eigenvector) into a single factor termed "CENTRALITY," serving as a overall proxy for evaluating a firm's exposure to cyber risk arising from the supply chain information network. CENTRALITY is derived from the factor with the highest eigenvalue obtained from the factor analysis.

3.3. Regression

3.3.1. Hypothesis 1 Testing- The Impact of Centrality on Supply Chain Cyber Risk Exposure

To examine the association between a firm's centrality and its cyber risk exposure, I conduct regression analyses using the proxies for cyber risk (CR_INDEX, BREACH, or CO_BREACH) as the dependent variables, and the firm's centrality measures as the independent variables. The regression model can be expressed as follows:

$$Cyber\ Risk_{i,t} = \beta_0 + \beta_1\ CENTRALITY_{i,t} + \beta'\ Controls_{i,t} + year\text{-}industry\ fixed\ effects\ [Eq.\ 1]$$

For the primary analysis, I employ the cyber risk index (CR_INDEX) developed by Florackis, Louca, Michaely, and Weber in 2023 as a continuous proxy for cyber risk exposure. This allows for a comprehensive evaluation of the relationship between a firm's centrality and its cyber risk exposure.

For robustness checks, I utilize the firm-year reported breach indicator (BREACH) as an alternative measure. This binary indicator takes a value of 1 if a firm reports at least one cyber-attack in a fiscal year, and 0 otherwise. It enables a supplementary examination of the relationship between a firm's centrality and its cyber risk exposure. To analyze the main results with CR_INDEX as the dependent variable, I employ Ordinary Least Squares (OLS) regression. On the other hand, for the dependent variables BREACH and CO_BREACH, I use logistic regression, given their binary nature, to assess their relationship with firm centrality.

In the regression analysis, I include a set of firm-level variables that have been previously documented to be associated with cyber risks. These variables include the natural logarithm of total assets (firm size), the natural logarithm of the number of years since the firm's initial public offering (firm age), return on total assets (profitability), the Intensity of Research and Development (R&D expense scaled by sales), Tobin Q (a measure of market value relative to replacement cost), and Tangible Assets scaled by total assets (proportion of tangible assets within the firm). To account for potential time and industry-specific effects, I

incorporate year and industry fixed effects in the regression models. Moreover, to address issues related to heteroskedasticity and potential serial correlation, I cluster the robust standard errors by firm.

A positive coefficient of CENTRALITY would indicate that as a firm's centrality in the supply chain network increases, its cyber risk exposure also increases. This positive relationship would support the notion that more central firms are more susceptible to cyber-attacks due to their interconnectedness and pivotal role within the network.

3.4. Data and Sample Selection

I collect data on cyber risk exposure from three sources. Firstly, I obtain the firm-year level cyber risk index generously shared by Florackis and his co-authors. The data covers the period from 2007 to 2018. Following Florackis et al.'s method, I extend the data to include information up to 2020. Secondly, I retrieve actual cyber-attack incidents from Audit Analytics and Privacy Rights Clearinghouse (PRC).

Next, I utilize Compustat Segment to construct the supply chain network and calculate firms' centrality measures actively. Additionally, I retrieve financial and accounting data actively from Compustat and CRSP, along with information on internal controls from Audit Analytics, and executive background and board characteristics from Boardex. The study sample period actively ranges from 2007 to 2020.

Table 1 presents the specific information regarding the sample selection process. Initially, the sample comprises 133,867 firm-year observations from Compustat Annual. Subsequently, 103,740 observations are excluded from the analysis as they are not covered by Compustat Segment, which is essential for constructing the supply chain network. Additionally, 5,436 observations with missing main financial variables are removed. After applying these selection criteria, the final sample consists of 25,061 firm-year observations.

Insert Table 1 here

4) Empirical results

4.1. Descriptive statistics

Table 2 presents the summary statistics for the main sample. Regarding cyber risk exposure, the sample mean for CR_INDEX is 0.157. The means for BREACH and CO_BREACH are 0.013 and 0.002, respectively, indicating that approximately 1.3% and 0.2% of firm-year observations have reported cyber-attacks. Furthermore, the means of CENTRALITY and DEG_CENT are 0.057 and 0.054, respectively, which aligns with previous findings from Gao (2021).

Insert Table 2 here

4.2. Hypothesis 1: The Impact of Centrality on Supply Chain Cyber Risk Exposure (Table 3)

Table 3A presents the univariate comparison of cyber risk exposure between firms classified as having high centrality (i.e., centrality values above the median) and firms categorized as having low centrality. The results indicate that firms with high centrality exhibit significantly higher levels of cyber risk exposure across all measures, namely CR_INDEX, BREACH, and CO_BREACH. Additionally, from an economic perspective, the cyber risk exposure of firms with high centrality is nearly twice as high as that of firms with low centrality.

Table 3B presents the results for Hypothesis 1, which investigates the association between centrality and cyber risk exposure. Consistent with the prediction for H1, the coefficients of CENTRALITY and DEG_CENT are significantly positive, indicating that firms with higher centrality in the supply chain information network are associated with higher cyber risk index (CR_INDEX). In economic terms, a one

standard deviation increase in CENTRALITY is linked to an increase in CR_INDEX of 0.186, which is equivalent to 1.2 (0.8) times the mean (standard deviation) of CR_INDEX. Similarly, when DEG_CENT increases by one standard deviation, CR_INDEX increases by 0.270, corresponding to 1.17 (1.21) times the mean (standard deviation) of CR_INDEX.

Insert Table 3 here

In Appendix C, I present additional analyses to demonstrate the robustness of the results for Hypothesis 1. Specifically, I examine cyber risk exposure using alternative measures: (a) the indicator of whether a firm reports at least one cyber breach (BREACH) in Table 3R1, and (b) the indicator of whether a firm reports at least one co-breach (CO_BREACH) at the firm-year level in Table 3R2. The findings consistently show that firms with higher centrality are more likely to experience breaches and co-breaches with their supply chain partners compared to firms with lower centrality. However, it is important to interpret these results cautiously, considering the limitations and nuances discussed in section 3.1.

Table 3R3 in Appendix C presents the results at the firm-level. The dependent variable, BREACH_FIRM, represents a count variable, indicating the total number of breaches experienced by each firm during the study period. All independent variables are averaged over time for each firm. To account for the count nature of the dependent variable, I employ Poisson regression for this analysis. The findings reveal that firms with higher centrality experience cyber-attacks at a higher frequency, indicating a positive association between centrality and the occurrence of cyber breaches.

5) Conclusion

This paper investigates the impact of a firm's position in the supply chain information network on its cyber risk exposure and cyber risk management strategies. I document firms occupying more central positions in the supply chain information network exhibit higher levels of cyber risk exposure. My paper adds to the existing body of literature on the economics of cybercrime by investigating the interplay of digital infrastructure among firms within the supply chain network. Additionally, it showcases the application of network theory and empirical analysis techniques to evaluate firm risk profiles, providing valuable insights.

References

Acemoglu, D., Malekian, A., & Ozdaglar, A. (2016). Network security and contagion. *Journal of Economic Theory*, *166*, 536-585.

Acemoglu, D., Ozdaglar, A., & Tahbaz-Salehi, A. (2015). Systemic risk and stability in financial networks. *American Economic Review*, *105*(2), 564-608.

Aobdia, D., Caskey, J., & Ozel, N. B. (2014). Inter-industry network structure and the cross-predictability

of earnings and stock returns. *Review of Accounting Studies*, *19*, 1191-1224.
Ashraf, M. (2022). The role of peer events in corporate governance: Evidence from data breaches. *The Accounting Review*, *97*(2), 1-24.
Ashraf, M., & Sunder, J. (2023). Can shareholders benefit from consumer protection disclosure mandates? Evidence from data breach disclosure laws. *The Accounting Review*, 1-32.
Bana, S., Brynjolfsson, E., Jin, W., Steffen, S., & Wang, X. (2021). Cybersecurity hiring in response to data breaches. *Available at SSRN*.
Banker, R. D., & Feng, C. (2019). The impact of information security breach incidents on CIO turnover. *Journal of Information Systems*, *33*(3), 309-329.
Bauer, A. M., Henderson, D., & Lynch, D. P. (2018). Supplier internal control quality and the duration of customer-supplier relationships. *The Accounting Review*, *93*(3), 59-82.
Brown, S. V., Tian, X., & Wu Tucker, J. (2018). The spillover effect of SEC comment letters on qualitative corporate disclosure: Evidence from the risk factor disclosure. *Contemporary Accounting Research*, *35*(2), 622-656.
Brown, S. V., & Tucker, J. W. (2011). Large-sample evidence on firms' year-over-year MD&A modifications. *Journal of Accounting Research*, *49*(2), 309-346.
Bushee, B. J., Kim-Gina, J., & Leung, E. (2020). Public and private information channels along supply chains: Evidence from contractual private forecasts. *Available at SSRN 3736405*.
Chen, C., Kim, J. B., Wei, M., & Zhang, H. (2019). Linguistic information quality in customers' forward-looking disclosures and suppliers' investment decisions. *Contemporary Accounting Research*, *36*(3), 1751-1783.
Chen, G., Judd, J. S., & Pandit, S. (2021). Firm unionization and disruptions in customer relationships. *Contemporary Accounting Research*, *38*(4), 2951-2981.
Cheng, Q., Goh, B. W., & Kim, J. B. (2018). Internal control and operational efficiency. *Contemporary accounting research*, *35*(2), 1102-1139.
Chiu, P.-C., Jiu, L., & Yu, P.-H. (2022). How do suppliers benefit from customers' voluntary disclosure? the effect of customers' earnings guidance on upstream firms' investment efficiency. *Journal of Accounting and Public Policy*, *41*(1), 106880.
Chiu, T. T., Kim, J. B., & Wang, Z. (2019). Customers' risk factor disclosures and suppliers' investment efficiency. *Contemporary Accounting Research*, *36*(2), 773-804.
Crosignani, M., Macchiavelli, M., & Silva, A. F. (2023). Pirates without borders: The propagation of cyberattacks through firms' supply chains. *Journal of Financial Economics*, *147*(2), 432-448.
Cunat, V. (2007). Trade credit: suppliers as debt collectors and insurance providers. *The Review of Financial Studies*, *20*(2), 491-527.
Dai, L., Landsman, W. R., & Peng, Z. R. (2023). Private Debt Issuance and Risk Factor Disclosure. *Available at SSRN 4049334*.
Ettredge, M., Guo, F., & Li, Y. (2018). Trade secrets and cyber security breaches. *Journal of Accounting and Public Policy*, *37*(6), 564-585.
Feng, M., Li, C., McVay, S. E., & Skaife, H. (2015). Does ineffective internal control over financial reporting affect a firm's operations? Evidence from firms' inventory management. *The Accounting Review*, *90*(2), 529-557.
Florackis, C., Louca, C., Michaely, R., & Weber, M. (2023). Cybersecurity risk. *The Review of Financial Studies*, *36*(1), 351-407.
Gao, J. (2021). Managing liquidity in production networks: The role of central firms. *Review of Finance*, *25*(3), 819-861.
Garg, P. (2020). Cybersecurity breaches and cash holdings: Spillover effect. *Financial Management*, *49*(2), 503-519.
Ghadge, A., Weiß, M., Caldwell, N. D., & Wilding, R. (2020). Managing cyber risk in supply chains: A review and research agenda. *Supply Chain Management: An International Journal*, *25*(2), 223-240.
Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Zhou, L. (2015). The impact of information sharing on

cybersecurity underinvestment: A real options perspective. *Journal of Accounting and Public Policy*, *34*(5), 509-519.
Granovetter, M. S. (1973). The strength of weak ties. *American journal of sociology*, *78*(6), 1360-1380.
Haislip, J., Lim, J.-H., & Pinsker, R. (2021). The impact of executives' IT expertise on reported data security breaches. *Information Systems Research*, *32*(2), 318-334.
He, C., HuangFu, J., Kohlbeck, M. J., & Wang, L. (2020). The Impact of Customer's Reported Cybersecurity Breaches on Key Supplier's Relationship-Specific Investments and Relationship Duration. *Available at SSRN 3544245*.
Hertzel, M. G., Li, Z., Officer, M. S., & Rodgers, K. J. (2008). Inter-firm linkages and the wealth effects of financial distress along the supply chain. *Journal of Financial Economics*, *87*(2), 374-387.
Hoberg, G., & Maksimovic, V. (2015). Redefining financial constraints: A text-based analysis. *The Review of Financial Studies*, *28*(5), 1312-1352.
Hoberg, G., & Phillips, G. (2016). Text-based network industries and endogenous product differentiation. *Journal of Political Economy*, *124*(5), 1423-1465.
Houston, J. F., Lin, C., & Zhu, Z. (2016). The financial implications of supply chain changes. *Management Science*, *62*(9), 2520-2542.
Huang, A. H., Shen, J., & Zang, A. Y. (2021). The unintended benefit of the risk factor mandate of 2005. *Review of Accounting Studies*, 1-37.
Jamilov, R., Rey, H., & Tahoun, A. (2021). *The anatomy of cyber risk*.
Jochem, T., & Peters, F. S. (2019). Bias propagation in economically linked firms. *Available at SSRN 2698365*.
Kamiya, S., Kang, J.-K., Kim, J., Milidonis, A., & Stulz, R. M. (2021). Risk management, firm reputation, and the impact of successful cyberattacks on target firms. *Journal of Financial Economics*, *139*(3), 719-749.
Kim, Y., Choi, T. Y., Yan, T., & Dooley, K. (2011). Structural investigation of supply networks: A social network analysis approach. *Journal of operations management*, *29*(3), 194-211.
Klein, A., Manini, R., & Shi, Y. (2022). Across the Pond: How US Firms' Boards of Directors Adapted to the Passage of the General Data Protection Regulation. *Contemporary Accounting Research*, *39*(1), 199-233.
Kulchania, M., & Thomas, S. (2017). Cash reserves as a hedge against supply-chain risk. *Journal of Financial and Quantitative Analysis*, *52*(5), 1951-1988.
Kumar, S., & Mallipeddi, R. R. (2022). Impact of cybersecurity on operations and supply chain management: Emerging trends and future research directions. *Production and Operations Management*, *31*(12), 4488-4500.
Larcker, D. F., So, E. C., & Wang, C. C. Y. (2013). Boardroom centrality and firm performance. *Journal of Accounting and Economics*, *55*(2-3), 225-250.
Morrison, A. D., & White, L. (2013). Reputational contagion and optimal regulatory forbearance. *Journal of Financial Economics*, *110*(3), 642-658.
Radhakrishnan, S., Wang, Z., & Zhang, Y. (2014). Customers' capital market information quality and suppliers' performance. *Production and Operations Management*, *23*(10), 1690-1705.
Rahaman, M. M., Rau, P. R., & Al Zaman, A. (2020). The effect of supply chain power on bank financing. *Journal of Banking & Finance*, *114*, 105801.
Raman, K., & Shahrur, H. (2008). Relationship-specific investments and earnings management: Evidence on corporate suppliers and customers. *The Accounting Review*, *83*(4), 1041-1081.
Ronald, B. (2004). Structural holes and good ideas. *American journal of sociology*, *110*(2), 349-399.
Schabus, M. (2022). Do director networks help managers forecast better? *The Accounting Review*, *97*(2), 397-426.
Serpa, J. C., & Krishnan, H. (2018). The impact of supply chains on firm-level productivity. *Management Science*, *64*(2), 511-532.
Smith, T., Tadesse, A. F., & Vincent, N. E. (2021). The impact of CIO characteristics on data breaches. *International Journal of Accounting Information Systems*, *43*, 100532.

Tanriverdi, H., Roumani, Y., & Nwankpa, J. (2019). Structural Complexity and Data Breach Risk.
Wang, T., Kannan, K. N., & Ulmer, J. R. (2013). The association between the disclosure and the realization of information security risk factors. *Information systems research*, *24*(2), 201-218.

Appendix A Variable Definition

Variable	Definition
Panel A Dependent variables	
CR_INDEX	Cyber risk index developed by Florackis, Louca, Michaely, and Weber 2023

BREACH	A firm-fyear level indicator, which takes value of one if the firm experiences a cyber attack in the current fiscal year, zero otherwise.
CO_BREACH	A firm-fyear level indicator, which takes value of one if the firm and at least one of its supply chain partners experiences a cyber attack in the same current fiscal year, zero otherwise.
BREACH_FIRM	A firm level variable, which captures the total number of breaches that a firm experiences during the study period.
REL_STOP	A firm-fyear level binary indicator set to 1 if the customer-supplier relationship is terminated in the subsequent fiscal year (t+1), and 0 otherwise.
SCCRD	A firm-fyear level indicator, which takes value of one if the firm includes a discussion of supply chain cyber risk in its 10-K.
CASH	Cash and equivalent securities scaled by Total Assets
ICW_INVT	A firm-fyear level indicator, which takes value of one if the firm has internal controls weakness related to inventory.
ICW_IT	A firm-fyear level indicator, which takes value of one if the firm has internal controls weakness related to Information technology.
Panel B Main indepdent variables	
DEG_CENT	A firm's degree centraility in supply chain network. The higher value of this measure indicates more direct connections (supply chain partners) the firm has.
DEG_CENT_HIGH	An indicator which takes value of 1 if DEG_CENT is greater than median value of DEG_CENT of all observations in each fiscal year
CENTRALITY	a proxy for exposure to cyber risk arising from supply chain information network, which is the factor with the highest eigenvalue from the principal factor analysis based on four different measures of centrality ((degree, closeness, betweenness, and eigenvector)
CENTRALITY_HIGH	An indicator which takes value of 1 if DEG_CENT is greater than median value of CENTRALITY of all observations in each fiscal year
IT_GOV	A firm-fyear level indicator, which takes value of one for firm-years with at least one IT expert on the management team or on the board and with no IT controls weaknesses or deficiencies, and 0 otherwise
IT_GOV_SCP	IT_GOV_SCP is a firm-fyear level variable. It is constructed based the average IT_GOV values of all supply chain partners of the focal firm. IT_GOV_SCP takes value of 1 when the average IT_GOV of all the supply chain partners is higher than annual average median and 0 otherwise.
Panel C Controls variables	

ICW_others	A firm-fyear level indicator, which takes value of one if the firm has internal controls weakness in areas other than Inventory and Information technology.
FIRM_SIZE	Natural log of total asset
FIRM_AGE	Natural log of firm age
Q	Tobin-Q, total assets [at] – common/ordinary equity [ceq] + market value of equity [prcc_f x csho] to total assets [at]
ROA	Earnings before extraordinary items scaled by lagged total assets
RD_EXP	R&D expense scaled by sales. Missing values are replaced with industry average.
TANGIBLE	PP&E (ppent) scaled by total assets (at)
LEV	financial leverage is equal to ratio of total debt to total assets
BOARDSIZE	Number of board members (Source: Boardex)
BOARD_INDP	Percentage of outside directors on the board (Source: Boardex)

Appendix B Tables

Table 1 **Sample selection**	
	Firm-years
COMPUSTAT Sample (2007-2020)	133,867

Removes observations that are not covered by Compustat Segment	(103,370)
Removes observations with missing key financial data	(5,714)
Final sample (firm-year observations)	24,783

Table 2 Descriptive Statistics

VARIABLES	(1) N	(2) Mean	(3) STD	(4) p1	(5) Median	(6) p99
Panel A Cyber risk exposure						
CR_INDEX	24783	0.157	0.223	0.000	0.000	1.000
BREACH	24783	0.013	0.113	0.000	0.000	1.000
CO_BREACH	24783	0.002	0.042	0.000	0.000	0.000
Panel B Centrality measure						
CENTRALITY	24783	0.057	0.049	0.000	0.054	0.201
CENTRALITY_HIGH	24783	0.431	0.495	0.000	0.000	1.000
DEG_CENT	24783	0.054	0.038	0.000	0.062	0.157
DEG_CENT_HIGH	24783	0.389	0.488	0.000	0.000	1.000
Panel C Other firm characteristics						
ICW_INVT	21261	0.033	0.113	0.000	0.000	1.000
ICW_IT	22332	0.043	0.149	0.000	0.000	1.000
IT_GOV	21145	0.052	0.076	0.000	0.000	1.000
IT_GOV_SCP	21462	0.293	0.490	0.000	0.000	1.000
ROA	24783	0.053	0.240	-0.851	0.098	0.346
Q	24783	1.929	1.327	0.670	1.490	7.563
BOARDSIZE	20675	8.668	2.292	4.000	8.000	14.000
BOARD_INDP	20611	0.772	0.133	0.333	0.800	0.923
FIRM_SIZE	24783	7.258	2.221	2.457	7.321	11.888
FIRM_AGE	24783	3.952	0.088	3.807	3.951	4.094
RD_EXP	24783	0.110	0.241	0.000	0.002	1.000
TANGIBLE	24783	0.246	0.247	0.000	0.149	0.884

Table 3A Cyber risk by Centrality

Variable	Mean by CENTRALITY_HIGH	Difference

	0(LOW)	1(HIGH)	HIGH-LOW	p value
CR_INDEX	0.107	0.196	0.089***	0.000
BREACH	0.740%	1.833%	1.093%***	0.000
CO_BREACH	0.073%	0.259%	.186%***	0.001

t-statistics in parentheses

*** p<0.01, ** p<0.05, * p<0.1

Table 3B The Effect of Centrality on Cyber Risk measured by CR_INDEX(H1)

	(1)	(2)	(3)	(4)
VARIABLES	CR_INDEX	CR_INDEX	CR_INDEX	CR_INDEX
CENTRALITY	4.312***	3.796***		
	(6.250)	(4.992)		
DEG_CENT			5.566***	5.501***
			(5.921)	(5.566)
FIRM_SIZE		0.010***		0.010***
		(16.547)		(16.696)
FIRM_AGE		0.173***		0.172***
		(7.800)		(7.777)
Q		0.007***		0.007***
		(7.156)		(7.200)
ROA		0.005		0.004
		(0.783)		(0.760)
RD_EXP		-0.008		-0.008
		(-1.071)		(-1.107)
TANGIBLE		-0.083***		-0.083***
		(-10.978)		(-11.088)
Constant	0.151	-0.797	0.148	0.794
	(0.805)	(-0.886)	(0.703)	(0.861)
Observations	24783	24783	24783	24783
Industry FE	NO	YES	NO	YES
Year FE	NO	YES	NO	YES
Type	OLS	OLS	OLS	OLS
Adj. R-squared	0.012	0.405	0.013	0.405

This table provides the results of OLS regression of centrality on cybersecurity risk measured by CR_INDEX, a cyber risk index developed by Florackis et al 2023. All variables are defined in Appendix A. Standard errors are clustered at the firm level.

Appendix C Robustness Tests

Table 3R1-Association between firm's centrality and likelihood of breach [H1]

VARIABLES	(1) BREACH	(2) BREACH	(3) BREACH	(4) BREACH
CENTRALITY	29.647***	24.047**		
	(4.898)	(2.396)		
DEG_CENT			28.841***	25.065***
			(4.051)	(3.136)
FIRM_SIZE		0.567***		0.558***
		(13.743)		(13.817)
FIRM_AGE		12.678***		12.794***
		(3.580)		(3.609)
Q		0.093*		0.091*
		(1.841)		(1.797)
ROA		0.168		0.175
		(0.218)		(0.227)
RD_EXP		0.680		0.642
		(0.970)		(0.916)
TANGIBLE		-1.429***		-1.509***
		(-3.160)		(-3.296)
Constant	-4.449***	-57.983***	-4.463***	-58.347***
	(-75.383)	(-4.007)	(-75.213)	(-4.028)
Observations	24,783	24,783	24,783	24,783
Industry FE	NO	YES	NO	YES
Year FE	NO	YES	NO	YES
Type	LOGIT	LOGIT	LOGIT	LOGIT
Pseudo R-squared	0.017	0.248	0.016	0.249

z-statistics in parentheses

*** p<0.01, ** p<0.05, * p<0.1

This table provides the results of Logistic regression of centrality on cybersecurity risk, measured by BREACH, a firm-fyear level indicator, which takes value of one if the firm experiences a cyber-attack in the current fiscal year zero otherwise. All variables are defined in Appendix A. Standard errors are clustered at the firm level.

Table 3R2-Association between firm's centrality and likelihood of co-breach [H1]

VARIABLES	(1) CO_BREACH	(2) CO_BREACH	(3) CO_BREACH	(4) CO_BREACH
CENTRALITY	23.138***	26.931***		
	(6.298)	(3.205)		
DEG_CENT			27.684***	29.105***
			(7.158)	(2.972)
FIRM_SIZE		0.257**		0.265**
		(2.392)		(2.495)
FIRM_AGE		-41.934		-42.459
		(-1.382)		(-1.399)
Q		0.069		0.065
		(0.565)		(0.527)
ROA		-0.856		-0.845
		(-0.738)		(-0.720)
RD_EXP		-0.794		-0.874
		(-0.367)		(-0.410)
TANGIBLE		-0.659		-0.887
		(-0.506)		(-0.660)
Constant	-6.520***	165.583	-6.538***	167.682
	(-37.271)	(1.337)	(-37.524)	(1.354)
Observations	24,783	24,783	24,783	24,783
Industry FE	NO	YES	NO	YES
Year FE	NO	YES	NO	YES
Type	LOGIT	LOGIT	LOGIT	LOGIT
Pseudo R-squared	0.0330	0.180	0.0399	0.180

z-statistics in parentheses

*** p<0.01, ** p<0.05, * p<0.1

This table provides the results of Logistic regression of centrality on cybersecurity risk measured by CO_BREACH, a firm-fyear level indicator which takes value of one if the firm and at least one of its supply chain partners experiences a cyber-attack in the same current fiscal year, zero otherwise. All variables are defined in Appendix A. Standard errors are clustered at the firm level.

Table 3R3 The Effect of Centrality on Cyber risk at Firm-level

VARIABLES	(1) BREACH_FIRM	(2) BREACH_FIRM
CENTRALITY_FIRM	16.269***	
	(3.863)	
DEG_CENT_FIRM		18.357***
		(4.146)
FIRM_SIZE_FIRM	0.657***	0.659***
	(21.419)	(21.667)
FIRM_AGE_FIRM	4.924***	4.919***
	(6.334)	(6.334)
Q_FIRM	0.284***	0.284***
	(7.422)	(7.405)
ROA_FIRM	2.043***	2.077***
	(3.480)	(3.530)
RD_EXP_FIRM	0.177	0.216
	(0.409)	(0.500)
Constant	-28.063***	-28.061***
	(-8.999)	(-9.005)
Observations	4,356	4,356
Industry FE	YES	YES
Type	Poisson	Poisson

z-statistics in parentheses

*** p<0.01, ** p<0.05, * p<0.1

This table provides the results of Poisson regression of BREACH_FIRM, a firm level variable which captures the total number of breaches that a firm experiences during the study period, on centrality. All variables are aggregated at firm-level.

Appendix D-Examples of Supply Chain Cyber Risk

1. Cyber risk disclosure examples

Example 1.1: Target's Item 1A 10-K 2020

"If our efforts to provide information security, cybersecurity, and data privacy are unsuccessful or if we are unable to meet increasingly demanding regulatory requirements, we may face additional costly government enforcement actions and private litigation, and our reputation and results of operations could suffer.

We regularly receive and store information about our guests, team members, ***vendors, and other third parties***. We have programs in place to detect, contain, and respond to data security incidents. However, because the techniques used to obtain unauthorized access, disable or degrade service, or sabotage systems

change frequently and may be difficult to detect for long periods of time, we may be unable to anticipate these techniques or implement adequate preventive measures. In addition, hardware, software, or applications we develop or procure from third parties may contain defects in design or manufacture or other problems that could unexpectedly compromise information security, cybersecurity, and data privacy. ***Unauthorized parties may also attempt to gain access to our systems or facilities, or those of third parties with whom we do business***, through fraud, trickery, or other forms of deceiving our team members, ***contractors, and vendors***."

Example 1.2: General Motor Item 1A 10-K 2021

"Security breaches and other disruptions to information technology systems and networked products, including ***connected vehicles***, owned or maintained by us, GM Financial, or ***third-parties, such as vendors or suppliers***, could interfere with our operations and could compromise the confidentiality of private customer data or our proprietary information. We rely upon information technology systems and manufacture networked and connected products, some of which are managed by third parties, to process, transmit and store electronic information and to manage or support a variety of our business processes, activities and products. Additionally, we and GM Financial collect and store sensitive data, including intellectual property and proprietary business information (including that of our dealers and suppliers), as well as personally identifiable information of our ***customers and employees***, in data centers and on ***information technology*** networks (including networks that may be controlled or maintained by third parties). The secure operation of these systems and products, and the processing and maintenance of the information processed by these systems and products, is critical to our business operations and strategy. Further, customers using our systems rely on the security of our infrastructure, including hardware and other elements provided by third parties, to ensure the reliability of our products and the protection of their data. We also face the risk of operational disruption, failure, termination or capacity constraints of any of the third parties that facilitate our business activities, including vendors, service providers, suppliers, customers, counterparties, exchanges, clearing agents, clearinghouses or other financial intermediaries. ***Such parties and other third parties*** who provide us services or with whom we communicate could also be the source of a ***cyberattack on, or breach of***, our operational systems, network, data or infrastructure."

Example 1.3: Solar Winds 10-K 2020

"Cyberattacks, including the Cyber Incident, and other security incidents have resulted, and in the future may result, in compromises or breaches of our and our customers' systems, the insertion of malicious code, malware, ransomware or other vulnerabilities into our systems and products and in ***our customers'*** systems, the ***exploitation of vulnerabilities in our and our customers' environments***, theft or misappropriation of our and our customers' proprietary and confidential information, interference with our and our customers' operations, expose us to legal and other liabilities, result in higher customer, employee and partner attrition, negatively impact our sales, renewals and upgrade and expose us to reputational harm and other serious negative consequences, any or all of which could materially harm our business.

…

Moreover, the number and scale of cyberattacks have continued to increase and the methods and techniques used by threat actors, including ***sophisticated "supply-chain" attacks*** such as the Cyber Incident, continue to evolve at a rapid pace. As a result, we may be unable to identify current attacks, anticipate future attacks or implement adequate security measures. We may also experience security breaches that may remain undetected for an extended period and, therefore, have a greater impact on our systems, our products, the proprietary data contained therein, our customers and ultimately, our business. In addition, our ability to defend against and mitigate cyberattacks depends in part on prioritization decisions that we and third parties

upon whom we rely make to address vulnerabilities and security defects. While we endeavor to address all identified vulnerabilities in our products, we must make determinations as to how we prioritize developing and deploying the respective fixes, and we may be unable to do so prior to an attack. Likewise, even once a vulnerability has been addressed, for certain of our products, the fix will only be effective once a customer has updated the impacted product with the latest release, and customers that do not install and run the latest supported versions of our products may remain vulnerable to attack.

"

2. Examples of Supply Chain Cyber Attack

Example 2.1: SolarWinds 2020

Source: Sean Lyngaas, CNN 2023, *SolarWinds chief vows to fight any legal action from US regulators over alleged Russian hack*. https://www.cnn.com/2023/06/23/tech/solarwinds-chief-sec-wells-notice/index.html

"The US Securities and Exchange Commission has informed current and former SolarWinds executives that it intends to recommend "civil enforcement action" alleging the company broke federal securities laws in its public statements and ***"internal controls"*** related to the hack, SolarWinds said in a filing with regulators on Friday.

For several months in 2020, hackers ***used software made by SolarWinds*** and other technology firms ***to burrow into US government agencies*** and corporate victims in an apparent spying campaign."

Example 2.2: TSMC 2023

Source: Sean Lyngaas, CNN 2023, *TSMC confirms supplier data breach following ransom demand by Russian-speaking cybercriminal group*. https://www.cnn.com/2023/06/30/tech/tsmc-supplier-ransomware/index.html

"Taiwanese semiconductor giant TSMC, a key supplier of Apple, confirmed Friday that one of its ***hardware suppliers*** was hacked and had data stolen from it, but said the incident had no impact on business operations.

"After the incident, TSMC ***immediately terminated its data exchange*** with this concerned supplier in accordance with the Company's security protocols and standard operating procedures," TSMC said in a statement to CNN."