Profiting from Rival Firms' Cyberattacks: Evidence from Informed Trading by Insiders with Social Ties

Jun-Koo Kang, Jungmin Kim, and Fangbo Si*

January 2023

Abstract

We examine a new, attenuated type of informed trading in which insiders exploit private information transmitted via their ties to rival firms' insiders. We find that insiders earn abnormal profits by trading their firms' stocks before the disclosure of rival firms' cyberattacks, particularly when their firms and rivals are exposed to higher cyber risk. Social networks formed through nonworkplace and nonboard ties are the main sources of trading profits. The litigation risk of rivals and the information asymmetry of rivals and peer firms increase peer insiders' trading profitability, whereas the SEC's 2011 disclosure requirements on cybersecurity risk reduce profitability.

Keywords: Insider trading, Peer firm, Cyberattack, Cyber risk, Social network, Nonworkplace tie, Nonboard tie, Private information

JEL Classification: G14, G18, G32, G38

* Kang is from the Nanyang Business School, Nanyang Technological University, Singapore (Email: jkkang@ntu.edu.sg); Kim is from the School of Accounting and Finance, The Hong Kong Polytechnic University, Hong Kong (Email: jungmin.kim@polyu.edu.hk); and Si is from School of Management, Jinan University, China (Email: sifangbo@jnu.edu.cn). We are grateful for the helpful comments from Chao Jiang, Chang-Mo Kang, Jiang Luo, Hong Ru, Bo Sang, and Yen Hee Tong. We thank seminar participants at the Hong Kong Polytechnic University, Iowa State University, Jinan University, Korea University, Michigan State University, Nanyang Technological University, and University of California at Riverside, and participants at the 2022 Asia Finance Association Annual Conference, 2022 China International Conference in Finance, 2022 FMA Annual Meeting, 2022 Annual Conference on Asia-Pacific Financial Markets, and 2002 SFS Cavalcade Asia-Pacific for their useful comments. All errors are ours.

I. Introduction

Attenuated types of informed trading by insiders who are largely exempt from market discipline and regulatory scrutiny have recently drawn increasing attention from academics, regulators, and industry experts. For example, a recent Securities and Exchange Commission (SEC) legal dispute involving Matthew Panuwat illustrates the regulator's move toward increased scrutiny for an unconventional type of insider trading activity that has not yet been subject to regulatory enforcement and sanction. According to the SEC, the former employee of Medivation Inc., the oncology-focused biopharmaceutical firm, allegedly profited from trading shares of the other biopharmaceutical firm, not from trading shares of Medivation, based on his private information about Medivation as a merger target.[1]

In this paper, we examine how insiders obtain private information about other firms' bad news and exploit this private information in their trading, another new type of unconventional insider trading. Specifically, we investigate whether directors or senior executives of industry peer firms (hereafter, *peer insiders*) obtain nondisclosed cyberattack news from the attacked firm's directors or senior executives (hereafter, *target insiders*) and earn abnormal profits by trading their own firms' shares.[2] As an illustration, consider the case of Target Corp., a Minneapolis-based retailer, which announced a massive cyberattack on December 13, 2013. Our analysis examines, for example, whether insiders of Walmart Store Inc., one of Target Corp.'s industry peer firms, earn abnormal profits by trading Walmart's shares prior to the public disclosure of Target Corp.'s cyberattack news.

We focus on cyberattacks as the setting for our study because outside investors tend to have limited information about the loss distribution of cyber risk due to its exogenous,

[1] For a detailed description on the legal dispute, see https://www.whitecase.com/publications/alert/sec-extends-misappropriation-theory-insider-trading-beyond-targets-acquisitions.

[2] Following the prior literature on social networks (e.g., Fracassi and Tate, 2012; Cao et al., 2015), we consider board members and senior executives whose titles include CEO, CFO, CIO, COO, president, executive vice president, senior vice president, managing director, and treasurer to be target and peer insiders because they tend to have privileged access to firm-specific private information.

unpredictable, and emerging nature (Kamiya et al., 2021). Moreover, Kamiya et al. (2021) show that target firms face weaker public and private enforcement sanctions than misconducting firms and bankrupt firms. Due to these characteristics of cyberattacks and the lack of legal enforcement, target insiders are incentivized to exploit such information for various purposes, such as sharing the information with connected peer insiders.[3] While firms often restrict insider trading by imposing strict blackout periods for regularly scheduled corporate events (e.g., quarterly earnings announcements) (Bettis, Coles, and Lemmon, 2000) and ad-hoc blackout periods for other irregular and pending/planned events that contain material nonpublic information (e.g., mergers and acquisitions (M&As), major personnel changes, new product launches (Guay, Kim, and Tsui, 2022),[4] it is difficult to enforce similar firm-level insider trading policies to cyberattacks due to their unpredictable and emerging nature.

Moreover, in addition to negative information about target firms' exposure to cyber risk, cyberattacks convey information about industry-wide cyber risk in general (Kamiya et al., 2021). This contagious effect of cyberattacks on industry peers suggests that peer insiders engage in trading by considering both target firms' cyberattack information and information about their own firms' exposure to cyber risk.

Cyberattacks are also different from other adverse corporate events in terms of information disclosure. For example, unlike other corporate events (e.g., earnings restatements and bankruptcies), which often reveal warning signals and red flags to outside investors, auditors, and enforcement bodies (e.g., the SEC and Department of Justice) long before the events take

[3] Target insiders who are less subject to legal risk and stakeholder scrutiny might directly engage in sales of their firms' shares ahead of the release of the news. We provide evidence on this issue in Section VI.D. However, other target insiders who face high legal risk and stakeholder scrutiny could take advantage of private information by trading shares of their firms' industry competitors or providing such information to connected parties via social networks. A lack of data on target insiders' transactions of shares belonging to their firms' industry peers prevents us from investigating target insiders' ability to profit from such trading.

[4] Ahern (2017) reports that M&As and earnings announcements account for 78% of 465 corporate events that are identified as illegal insider trading by the SEC and Department of Justice (DOJ) during his sample period 1996-2013.

place,[5] the disclosure of cyberattack information depends largely on the discretion of the target firm's managers, limiting outside investors' ability to gain access to such information.[6] This high information asymmetry between insiders and outside investors increases the value of private information specific to the target firm and thus incentivizes target insiders to exploit such information for various purposes, such as sharing the information with connected peer insiders. This information sharing allows peer insiders to engage in informed trading using private information pertaining to the rival firm's cyberattack.

Among various types of social networks that help facilitate information transfer between connected parties, we focus on two types of social networks: a social network in which personal ties are more likely to develop and a social network that is less subject to regulatory oversight and market scrutiny. Prior studies on social networks indicate that personal ties formed through nonworkplace activities (e.g., common educational background and membership in the same non-business organizations) promote more trust and sympathy among connected parties (e.g., Domhoff, 2009), whereas professional connections that arise from common employment tend to be transactional and competitive in nature (e.g., Ingram and Zou, 2008). These studies suggest that nonworkplace connections are more likely to help develop mutual trust between target and peer insiders, better facilitating information transmission between them. The potential benefits of selective information sharing between insiders connected through nonworkplace ties include enrichment of trust and friendship among insiders and improvement of loyalty to each other over a long period of time (e.g., Cao et al, 2015). Supporting this view, Cohen, Frazzini, and Malloy (2008, 2010) show that shared education networks significantly

[5] Seyhun and Bradley (1997) find that insiders of firms filing bankruptcy petitions begin to engage in sales of their firms' shares five years before the filing of Chapter 11 proceedings, suggesting that market participants can learn about firms' financial health from long-standing, pre-filing insider trading.

[6] Although the State Security Breach Notification Laws mandate that firms disclose breaches resulting in the loss of personal information in a timely manner, breached firms have large discretion in disclosing the details of events. For example, Amir, Levi, and Livne (2018) find that firms underreport cyberattacks, especially when the potential damage caused by the incidents is greater.

improve portfolio managers' investment performance and analysts' performance. Thus, peer insiders' trading profitability should be higher when social ties are formed via nonworkplace ties than when they are formed through workplace ties.[7]

Social connections are also more likely to facilitate information transfer between target and peer insiders if target insiders face weak regulatory scrutiny and stakeholder monitoring. For example, target insiders who are board members of their firms tend to be closely scrutinized by regulators and markets and face higher litigation and enforcement risk because of the requirements of fulfilling their statutory and fiduciary duties. Thus, these target insiders should have a weaker incentive to leak information about their firms' cyberattacks to outsiders than target insiders who are not board members, suggesting that peer insiders' trading profitability is higher when they are connected to nonboard executives of the target firm (hereafter, nonboard ties) than when they are connected to directors of the target firm (hereafter, board ties).

We test the predictions outlined above using insider transactions that occur in industry competitors of firms experiencing cyberattacks reported in the Privacy Rights Clearinghouse and Audit Analytics over the period 2005–2017. We first examine whether peer insiders earn abnormal profits by trading their own firms' shares prior to the target firm's cyberattack disclosure date. We find that peer insiders who trade shares of their firms prior to the target firm's cyberattack disclosure date earn significantly higher market-adjusted abnormal buy-and-hold returns of 4.5% over 180 calendar days. In untabulated tests, we find that the results are robust to using an intercept from Carhart's (1997) four-factor model estimated over the 180 calendar days after the transaction date as an alternative measure of trading profitability.[8] Thus,

[7]

[8] In comparison, Cao et al. (2015) report an average buy-and-hold abnormal return of -0.7% for their sample of sales transactions made by independent directors. Dai et al. (2016) report an average buy-and-hold abnormal return of -0.6% for their sample of sales transactions made by insiders of firms listed on the New York Stock Exchange (NYSE), American Stock Exchange (AMEX), or Nasdaq from 1998 to 2011.

peer insiders exploit their information advantage over other market participants before the market learns about target firms' bad news, and they earn abnormal profits that are economically large and significant. Peer insiders' ability to earn abnormal profits is evident for both sales and purchase transactions, which account for 94.8% and 5.2% of the total number of transactions, respectively.

To further examine whether peer insiders' trading profits indeed come from private information pertaining to rivals' cyberattacks, we assess whether these profits are associated with the exposure of target and peer firms to cyber risk. Kamiya et al. (2021) show that cyberattacks reveal information about industry-wide cyber risk in general, thereby negatively affecting individual peer firms' market values; however, some peer firms are less hurt by such incidents, and they can even benefit from them. These findings suggest that peer insiders' trading profits should be significantly related to the extent to which target and peer firms are exposed to cyber risk. Consistent with our expectation, we find that peer insiders' trading profitability in the pre-disclosure period, particularly that from purchase transactions, is positively associated with the severity of the incident, measured by the target firms' lower abnormal returns around the cyberattack announcement date. Using peer firms' lower abnormal returns around the rival firm's cyberattack announcement date as their exposure to cyber risk, we further find that peer insiders avoid larger potential losses by engaging in sales transactions in the pre-disclosure period when their firms' exposure to cyber risk is greater, while they earn higher profits from their purchase transactions when their firms' exposure is lower. These results are in line with those of Kamiya et al. (2021), who show that the valuation effect of a cyberattack on industry peers varies with their exposure to cyber risk. Thus, peer insiders engage in different trading strategies depending on their assessment of the firm's exposure to cyber risk and its ability to remediate such risk: peer insiders engage in sales transactions when

their firms' exposure to cyber risk is higher to avoid potential losses, while they engage in purchase transactions to earn abnormal profits when such exposure is lower.

We next examine the channel through which peer insiders obtain target firms' private cyberattack information and exploit such information in their trading by focusing on shared networks between target and peer insiders. We find some weak evidence that peer insiders' trading profits are higher when they are socially connected to target insiders. However, when we divide social ties according to the strength of personal ties between peer and target insiders and target insiders' board membership status, we find that peer insiders' trading profitability is evident only for transactions in which peer insiders are connected to target insiders through nonworkplace or nonboard ties, not for transactions in which peer insiders are connected to target insiders through workplace or board ties.

To better understand the circumstances under which peer insiders earn higher trading profits, we examine cross-sectional heterogeneity in the results across target firms with different litigation risk and information asymmetry. We focus on target firms' litigation risk because high litigation risk discourages insiders from leaking their firms' private information to outsiders. We also focus on target firms' information asymmetry because a poor information environment makes it difficult for outsiders, including peer firms' non-insider shareholders, to access cyberattack information, which increases the value of target-specific private information for trading. We find that the impact of nonworkplace and nonboard ties on peer insiders' trading profits is greater when target firms have lower litigation risk (i.e., when there are no common institutional blockholders that hold equity in both the target and peer firms,[9] when firms operate

[9] Prior studies show that common institutional blockholders perform an active monitoring role and increase litigation risk spillover among their portfolio firms (Kang, Luo, and Na, 2018; He, Huang, and Zhao, 2019; Donelson, Flam, and Yust, 2021). A target insider's leakage of cyberattack information to a peer insider can place common institutional blockholders that hold equity in the peer firm at a significant information disadvantage when they trade shares, increasing potential litigation risk of the target insider. Thus, the presence of common institutional blockholders would discourage target insiders from leaking their firm-specific private information to peer insiders.

in low litigation industries (Rogers and Stocken, 2005), and when firms are located in areas with lower liberal court scores on the federal judge ideology (Huang, Hui, and Li, 2019)). We also find that this impact is more evident among target firms with higher information asymmetry (i.e., younger firms, firms with higher absolute discretionary accruals, and firms with positive research and development (R&D) expenses).

As further tests, we examine whether the ability and incentives of peer insiders with nonworkplace ties and those with nonboard ties are affected by their own firms' information environments. Since peer firms' high information asymmetry increases the value of nonpublic cyberattack information that their insiders have over other market participants (Aboody and Lev, 2000; Huddart and Ke, 2007), we expect these peer insiders to enjoy higher trading profits when their firms have poor information environments. Consistent with this view, our results are more pronounced when peer firms are younger and when they have higher absolute discretionary accruals.

We conduct several additional tests. First, we exploit the SEC's issuance of guidance on October 13, 2011, regarding firms' disclosure obligations relating to cybersecurity risk and incidents to examine how such regulatory oversight affects informed trading by connected peer insiders. With increasing regulatory scrutiny and disclosure requirements for firms' cybersecurity risk, we expect target insiders' incentives to selectively disclose news about their firms' cyberattacks and peer insiders' ability to exploit private information to be attenuated in the post-SEC guidance period. Consistent with this expectation, we find that peer insiders' trading profits prior to the disclosure of cyberattacks are significantly lower in the post-SEC guidance period than in the pre-SEC guidance period. This result is evident only for transactions by peer insiders with nonworkplace ties or nonboard ties. However, peer insiders with nonboard ties continue to earn abnormal profits during the post-SEC guidance period. Thus, the regulatory oversight for a firm's timely disclosure of its cyberattack information

appears to be effective in limiting information sharing among connected parties, although it cannot completely eliminate it.

Second, we examine whether the volume of peer insiders' sales transactions increases before target firms' public disclosure of their cyberattacks. We find that connected peer insiders sell a large number (amount) of shares ahead of the disclosure of the news, reflecting their general perception that rival firms' cyberattacks are bad news for their firms.

Third, we examine whether peer insiders' abnormal trading profits are due to their ability to better assess and process publicly available industry-level information about cybersecurity risk rather than due to their target firm-specific private information. We use the number of cyberattacks in an industry prior to the focal incident as the measure of the availability of industry-level public information about cybersecurity risk because the frequent occurrence of cyberattacks in the industry increases such information available to peer insiders. We find that the number of cyberattacks in an industry is insignificantly related to peer insiders' trading profits, indicating that common industry knowledge is unlikely to be an important source of peer insiders' profitability.

Fourth, we classify peer insiders into routine and opportunistic traders based on their history of trades (Cohen, Malloy, and Pomorski, 2012) and find that our main results are mainly driven by opportunistic traders.

Finally, we examine the trading profitability of target firms' insiders conditional on firms' litigation risk. We find that target insiders earn higher abnormal returns by trading their firms' shares in the pre-disclosure period than in the post-disclosure period only when their firms do not face higher litigation risk.

Our study contributes to the literature in several important ways. First, we add to the literature on insider trading and informed trading. For example, Ahern (2017) shows that corporate insiders share their firms' private information with their family, friends, and other

individuals and that these individuals earn abnormal profits from trading. Similarly, Mehta, Reeb, and Zhao (2021) find that insiders facilitate informed trading by sophisticated investors in economically-linked firms, such as business partners and competitors, in an attempt to circumvent insider trading restrictions. Our study differs from these studies in that we focus on a new, attenuated type of insider trading in which peer insiders exploit industry rival-specific private information in trading their own firms' shares. Our study is also distinct from other recent studies that examine how insiders exploit their superior ability to process industry-level public information in trades of their firms' shares (Alldredge and Cicero, 2015) and industry rivals' shares (Ben-David, Birru, and Rossi 2019; Deuskar, Khatri, and Sunder, 2021). We examine how a target firm's non-public bad news (i.e., cyberattacks) reaches its industry peers and show that target insiders' selective information disclosure leads to peer insiders' abnormal trading profits.

Second, we contribute to the literature on social networks by showing that specific types of social connections are particularly important information transmission channels that improve trading performance (e.g., Cohen, Frazzini, and Malloy, 2008; Cao et al., 2015). For example, Cohen, Frazzini, and Malloy (2008) show that connections between mutual fund managers and corporate board members via shared education networks help improve fund managers' performance in connected firms.[10] By focusing on the information transmission role of social networks within a firm, Cao et al. (2015) also show that socially connected independent directors outperform unconnected independent directors in sales transactions. We extend this literature by documenting that investors with access to other firms' nonpublic information via more personal-based networks (i.e., nonworkplace ties) and networks that are

[10] Berkman, Koch, and Westerholm (2020) show that directors outperform when they purchase stocks of the firms in board interlock networks, suggesting that board interlock allows interlocking directors to obtain firm-specific private information. We cannot perform the analysis about the effect of board interlock on peer insiders' trading profitability because the proportion of transactions made by interlocking directors (i.e., peer insiders serving on the target firm's board) is very low. The low proportion is likely because the Clayton Act of 1914 bans directors to serve on the boards of competing firms, including those operating in the same industry (Dooley, 1969).

less subject to regulatory scrutiny and attention (i.e., nonboard ties) earn abnormal profits by trading their firms' shares.

Third, our study adds to the literature on the economy-wide effects of cybersecurity risk, one of the most important emerging operational risks. Unlike Kamiya et al. (2021) who find the ex-post disclosure effects of cyberattacks on industry rivals, we examine how insiders selectively share information about their firms' cyberattacks with connected parties in other firms before the disclosure of cyberattacks and show that these connected parties make abnormal trading profits. Thus, our study provides new evidence for the negative externalities of cyber risk.

The remainder of this paper is organized as follows: Section II describes the sample and defines the key variables. Section III presents the results on peer insiders' trading profitability. Sections IV and V show the results for the role of social networks as an information transmission channel of informed trading and those on the cross-sectional heterogeneity in peer insiders' trading profits, respectively. Section VI presents the results from additional tests, including the analyses of whether the SEC's 2011 guidance on the disclosure of cybersecurity risk affects peer insiders' trading profitability and the analyses of target insiders' trading profitability. Finally, Section VII concludes the paper.

II. Data and Variable Definitions

A. Sample

We obtain data on cyberattacks (i.e., external attacks that breach firms' defenses by hacking or malware-electronic entry) by combining incidents reported in the Privacy Rights Clearinghouse (PRC) database with those reported in the Audit Analytics database over the

period from 2005 to 2017.[11] Our initial sample consists of 589 unique cyberattacks. For each incident, we obtain information on target firm identifiers (e.g., company name, company Central Index Key (CIK) number), the date when the incident was disclosed to the public (i.e., disclosure date), and other incident-related information from the PRC and Audit Analytics databases. We require target firms to be listed on the NYSE, AMEX, or Nasdaq; to have financial and stock return data available in Compustat and the Center for Research in Securities Prices (CRSP), respectively; and to be traded as common shares (CRSP share code = 10 or 11). We exclude firms in the financial industries (Standard Industrial Classification (SIC) codes 6000–6999) and utility industries (SIC codes 4900–4999). These procedures yield a sample of 372 cyberattacks for 228 unique target firms.

For each cyberattack incident, we identify the target firm's peers, defined as industry competitors that have the same four-digit SIC code as the target firm. For multiple cyberattacks that occur in the industry in a given fiscal year, we keep the earliest incident in that year. We further exclude cyberattacks that occur within 180 days after the preceding incidents in the same industry to avoid overlapping effects. We require peer firms not to experience cyberattacks in a given year and to have at least one insider transaction during the pre- or post-disclosure period. We define the pre-disclosure period as the period from 90 calendar days to one calendar day before the cyberattack disclosure date and the post-disclosure period as the period from one calendar day to 90 calendar days after the cyberattack disclosure date.[12] Using

[11] In our sample, we do not include data breaches caused by insiders' mishandling of sensitive information or by theft of laptops and physical devices because they are likely to be caused by target firms' weak internal control system and governance; thus, they are less likely than cyberattacks to be exogenous. In untabulated tests, we examine the cumulative abnormal return (CAR) for target firms around the cyberattack announcement date to investigate the potential information leakage before the public disclosure of the cyberattack incident. We find that the mean CAR from five (ten) days before the announcement date to one day before the announcement date is insignificantly different from zero, suggesting no information leakage prior to the cyberattack announcement date.

[12] We do not use the period between the cyberattack disclosure date and the discovery date (i.e., the date in which cyberattack is discovered for the first time) to define the pre-disclosure period in the analysis because the information about discovery dates is not available for most of incidents (72.2% of the sample of 266 cyberattacks). Even for incidents in which the discovery date is available, the identity of the person who first discovers the incident and the exact date of the actual discovery are seldom available. For incidents with discovery dates available, the mean (median) date from the discovery to the disclosure of the incident is 40.78 (20) days. In

alternative pre- and post-disclosure periods, such as 120 and 150 calendar days, does not change our results.

We obtain insider trading information from Thomson Reuters Insider Filing Data, which covers all trade information on insider activity as reported on SEC forms 3, 4, 5, and 144. We focus on valid open market purchase and sales transactions of common shares made by officers and directors[13] and delete the transactions by beneficial owners, who are typically institutions, from the analysis. Following prior literature, we also exclude transactions in which shares traded exceed trading volume on the trading day and purge all transactions whose prices fall outside the daily trading range reported on CRSP. We also require transactions to be of more than 100 shares and to have trading prices of more than $2 to analyze economically meaningful transactions. Our final sample consists of 44,639 and 48,960 insider transactions occurring in 3,021 peer firm-year observations for 266 unique cyberattack events during the pre- and post-disclosure periods, respectively.

Table 1 presents the distribution of cyberattacks by year and industry. We observe that the number of cyberattacks significantly increases over our sample period. Cyberattacks are the most frequent in service industries (33.08%), followed by wholesale trade and retail trade industries (24.81%), manufacturing industries (24.81%), and transport and communications industries (14.66%). These results are in line with those of prior studies showing that firms are more likely to become targets of cyberattacks when they rely more on customers' personal information in doing business (Kamiya et al., 2021).

untabulated tests, we construct an indicator for whether the disclosure of a target firm's cyberattack is made at least one day after the discovery date and include it in the regressions together with its interaction with *Pre-disclosure period*. We find that the coefficient on the interaction term is positive and significant, suggesting that peer insiders' trading profits are particularly evident among incidents in which the public disclosure of cyberattack news is being withheld for some reasons. However, the interpretation of the results should be made with caution given small sample size and imited information about withholding.

[13] A valid transaction is the one without a cleanse code of "A" or "S" in the IDF.

B. Summary statistics and variable definitions

Panel A of Table 2 presents summary statistics for target firms and their peer firms that have never been targets of cyberattacks. We winsorize all continuous variables at the 1% and 99% levels. Target firms are larger, are more profitable (i.e., have a lower frequency of income loss), and are less volatile. They also have a lower frequency of reporting positive R&D expenses, larger analyst followings, and lower institutional block ownership.

Panel B of Table 2 compares the transaction characteristics of peer insiders between the pre- and post-disclosure periods. We find that peer insiders' trade size measured by *Daily trade size* and *Recent trade size* is larger during the pre-disclosure period than during the post-disclosure period. We measure *Daily trade size* as the ratio of the absolute value of the net number of shares purchased by all peer insiders on the transaction date to the peer firm's total number of shares outstanding and *Recent trade size* as the ratio of the sum of absolute values of the daily net numbers of shares purchased by all peer insiders during the ten days prior to the transaction date to the peer firm's number of total shares outstanding.

We also find that *All-tie transactions* (i.e., transactions made by a peer insider who is socially connected to a target insider) account for about 14.3% of all pre-disclosure transactions made by peer insiders, whereas the corresponding number during the post-disclosure period is significantly lower, at 10.5%. We further classify each *All-tie transaction* according to whether the focal social connection fosters more trust and friendship (i.e., *Nonworkplace-tie transaction* and *Workplace-tie transaction*) and according to whether the target insiders currently serve as board members of their firms (i.e., *Nonboard-tie transaction* and *Board-tie transaction*). Specifically, *Nonworkplace-tie transaction* is a transaction made by a peer insider connected to target insiders exclusively through nonworkplace ties, such as a common educational background or membership in the same non-business organization; *Workplace-tie transaction* is a transaction made by a peer insider connected to at least one target insider through

workplace ties (i.e., current or prior common employment); *Nonboard-tie transaction* is a transaction made by a peer insider who is socially connected only to nonboard executives of the target firm; and *Board-tie transaction* is a transaction made by a peer insider who is socially connected to at least one director of the target firm. A peer insider can be connected to target insiders via nonworkplace ties (nonboard ties) and workplace ties (board ties) simultaneously. Since our study focuses on social ties that are more informal by nature (i.e., nonworkplace ties) and those less subject to market scrutiny (i.e., nonboard ties), which tend to better facilitate information transmission between connected parties, we include only ties in which peer insiders are connected to target insiders exclusively through common educational background and membership in the same non-business organizations when we define nonworkplace ties and only ties in which peer insiders are connected exclusively to nonboard members of the target firms when we define nonboard ties. We find that *Nonworkplace-tie transaction* (*Workplace-tie transaction*) and *Nonboard-tie transaction* (*Board-tie transaction*) account for about 7.9% (6.5%) and 4.5% (9.8%) of all pre-disclosure transactions made by peer insiders, respectively, whereas the corresponding numbers during the post-disclosure period are significantly lower, at 5.8% (4.7%) and 3.1% (7.3%). Thus, transactions made by socially connected peer insiders are significantly higher in the pre-disclosure period than in the post-disclosure period, regardless of the type of social connection.

In untabualted tests, we examine the distribution of our sample of peer insiders according to their type of social connection with target insiders and find that about 11% of peer insiders are socially connected to target insiders.

III. Peer Insiders' Trading Profitability

A. Measure of trading profitability

Following prior literature, we define the profitability of insider trading as the unrealized capital gains made by purchasing and the losses avoided by selling company stocks. Specifically, we compute insider trading profitability using two abnormal profit measures (e.g., Ravina and Sapienza, 2010; Jagolinzer et al., 2011). First, we use the market-adjusted abnormal buy-and-hold return over the 180 calendar days after the insider trading date (*BHAR180*), where we use the CRSP value-weighted index as a proxy for the market portfolio.[14] Second, we use the average daily abnormal return estimated with Carhart's (1997) four-factor model over the 180 calendar days after the insider trading date (*ALPHA180*). For sales transactions, *BHAR180* and *ALPHA180* are multiplied by −1. Since our results using *BHAR180* and *ALPHA180* are qualitatively similar, for the sake of brevity, we report only the results using *BHAR180*.

B. Transaction-level analysis of peer insiders' trading profitability and cyber risk

Panel A of Table 3 presents univariate results for peer insiders' trading profitability during the pre- and post-disclosure periods using transaction-level data. The mean (median) *BHAR180* for the pooled sample of sales and purchase transactions during the pre-disclosure period is 2.0% (3.3%), whereas the corresponding mean (median) *BHAR180* during the post-disclosure period is -3.4% (-1.0%), both of which are significant at the 1% level. The difference in these returns between the pre- and post-disclosure periods is significant at the 1% level.

Panel B of Table 3 presents the results from ordinary least squares (OLS) regressions in which the dependent variable is *BHAR180*. Our key independent variable of interest is *Pre-disclosure period*, which takes the value of one for transactions made during the period from

[14] In untabulated tests, we use the industry-adjusted abnormal buy-and-hold return over the 180 calendar days after the insider trading date as a measure of peer insiders' trading profits and repeat the analyses in Tables 3-9. Our inference does not change although some of the results become weaker. In addition, we exclude three days, ten days and 20 days around the cyberattack disclosure date when computing *BHAR180* and find that our results are qualitatively similar.

90 calendar days to one calendar day before the target firm's cyberattack disclosure date, and zero for transactions made during the period from one calendar day to 90 calendar days after the disclosure date.[15] We control for various firm-specific characteristics that affect insider trading profitability, such as firm size (Seyhun, 1986; Lakonishok and Lee, 2001), past performance (book-to-market ratio, past six-month stock returns, net income loss), stock return volatility (Rozeff and Zaman, 1998; Piotroski and Roulstone, 2005), information asymmetry (analyst coverage, R&D expenses) (Aboody and Lev, 2000; Frankel and Li, 2004), and institutional block ownership, to mitigate the concerns that a firm's performance, risk, information environment, and governance affect trading profitability. Following Brochet (2010) and Dai et al. (2016), we also control for several trade-specific characteristics, including *Daily trade size* and *Recent trade size*, in the regressions. In addition, since prior studies suggest that insiders opportunistically trade stocks in advance of the revelations of corporate events, we include indicators for transactions made prior to major corporate events that are likely to have significant effects on stock prices, such as dividend declarations, earnings announcements, merger and acquisition (M&A) announcements, and 10K/10Q filings (John and Lang, 1991; Ke, Huddart, and Petroni, 2003; Huddart and Ke, 2007).[16] All regressions include year fixed effects. In column (1), we additionally control for industry (four-digit SIC code) fixed effects, and in column (2), we replace industry fixed effects with firm fixed effects to control for time-invariant firm characteristics that affect peer insiders' trading incentives and

[15] To address the potential concern that firm characteristics, target insiders' incentives, and peer insiders' trading behaviors may change in the post-disclosure period, we use two (three) years before the pre-disclosure period as an alternative benchmark period and find that our results remain the same. One important drawback of using these alternative benchmark periods is that the composition of target and peer insiders may significantly change during these long periods of time. Given that the actual date in which cyberattacks occur is unavailable in many cases, it is highly feasible that some cyberattacks occur during these benchmark periods. If target insiders already started to share nonpublic cyberattack information with peer insiders during these periods, then peer insiders should also make abnormal profits in the periods, which leads to potential measurement biases in our analysis.

[16] Peer insiders' abnormal returns could be associated with their personal attributes, such as expertise in information technology, finance, and law, job titles, committee membership status on the board, age, tenure, the number of outside directorships. Including these peer insiders' personal attributes as additional controls in the regressions does not affect our results.

trading performance. In column (3), we replace year fixed effects in column (2) with industry-by-year fixed effects to further control for unobserved heterogeneity across industries over time. Controlling for industry-by-year fixed effects also allows us to partially address potential concerns that peer insiders earn trading profits using industry-specific public information (e.g., Ben-David, Birru, and Rossi, 2019) rather than their private information on rival firms' cyberattacks. In untabulated tests, we also control for firm-by-year fixed effects in the regressions and find that our results remain qualitatively similar. We report robust standard errors clustered at the peer firm and event levels. All peer firm characteristics are measured as of the fiscal year immediately before the trading date, and all trade characteristics are measured as of the trading date.

We find that the coefficient on *Pre-disclosure period* is positive and significant in all three regressions. The coefficient estimates of 0.031 to 0.045 indicate that peer insiders who trade shares in the pre-disclosure period earn market-adjusted returns from their purchase and sales transactions that are 3.1 to 4.5 percentage points higher than those of peer insiders who trade shares in the post-disclosure period.

A priori, it is unclear whether peer insiders' trading profits are driven by their sales or purchase transactions. If peer insiders perceive that the adverse information about a target firm's cyberattack is idiosyncratic to the target firm, their firms should benefit from the attack as a result of an increase in firm competitiveness in the product market. In this case, peer insiders are expected to earn abnormal profits by engaging in purchase transactions. In contrast, if peer insiders believe that the information about a cyberattack is related to more general industry-wide cyber risk and that their firms are highly exposed to such risk due to poor risk management, we expect peer insiders to engage in sales transactions to avoid potential losses. In Panel C of Table 3, we reestimate the regressions in Panel B separately for the subsamples of sales and purchase transactions; consistent with the arguments above, we find that peer

insiders make higher abnormal returns in the pre-disclosure period from both their sales and purchase transactions. Although sales transactions account for more than 95% of the total transactions in both pre- and post-disclosure periods, as shown in Section VI.B, connected peer insiders sell a larger number (amount) of shares in the pre-disclosure period than in the post-disclosure period. Thus, a large number of peer insiders perceive private information about industry competitors' cyberattacks as bad news for their own firms. Nevertheless, some peer insiders who believe that their firms stand to benefit from these incidents earn profits by engaging in purchase transactions.

To further assess whether a rival firm's undisclosed information on a cyberattack is indeed the source of trading profits, we examine whether peer insiders' trading profitability is related to the extent to which target firms and peer firms are exposed to cyber risk. When cyberattacks are more severe and impose a larger shareholder wealth loss on target firms, peer insiders' sales and purchases are likely to be more informative because their private information about cyberattacks has greater value. To test this prediction, we measure cyberattack severity using *Target firm's low CAR (-1, 1)*, which takes the value of one if the target firm's cumulative abnormal return (CAR) from one day before the cyberattack announcement date to one day after the cyberattack announcement date is below the sample median, and zero otherwise.[17] Daily abnormal returns are estimated using the market model with 220 trading days of return data ending 61 days before the cyberattack disclosure date, where the CRSP value-weighted return is used as a proxy for the market return. The results including this indicator and its interaction with *Pre-disclosure period* in the regressions are presented in Panel A of Table 4. We find that the coefficient on the interaction term is positive and significant in columns (1)–(3), in which we use the pooled sample of sales and purchase transactions in the regressions.

[17] The sample median *Target firm's CAR (-1, 1)* is -0.2%. Using an indicator for whether a target firm's CAR (-1, 1) is negative as a measure of the severity of a target firm's cyberattack does not change the results.

In columns (4) and (5), we reestimate the regression in column (3) using the subsamples of sales and purchase transactions, respectively. We find that the coefficient on the interaction term is positive and significant in purchase transactions and positive and marginally insignificant in sales transactions. Given that nonpublic information about cyberattacks is more material when cyberattacks are more severe, the leakage of such information is likely to significantly increase litigation and enforcement risk for target insiders. This increase in risk should disincentivize target insiders to share cyberattack information with peer insiders, making sales transactions less informative than purchase transactions. In untabulated tests, we also reestimate the regressions in columns (1) and (2) using the subsamples of sales and purchase transactions, respectively, and find that the coefficients on the interaction term are positive and significant in all regressions except the one in which we use a subsample of purchase transactions and include firm and year fixed effects.

Overall, these findings suggest that peer insiders' profitability comes mainly from the target firm's material cyberattack information that has yet to be made public.

Peer insiders' trading profitability is also likely to be related to their own firms' exposure to cyber risk if their trading is based on cyberattack-specific information. To avoid potential losses, informed peer insiders should have greater financial incentives to sell their firms' shares prior to the public disclosure of cyberattack news if they perceive that cyberattacks have negative spillover effects on industry competitors with higher exposure to cyber risk. In contrast, if peer firms are hurt less by the incidents or even take advantage of the rival's bad news to increase their competitive position in the market, peer insiders should engage in purchase transactions to exploit such information. To measure peer firms' exposure to cyber risk, we use the variable *Peer firm's low CAR (-1, 1)*, which takes the value of one if a peer firm's CAR from one day before to one day after the target firm's cyberattack announcement is below the sample median peer CAR (-1, 1), and zero otherwise. Kamiya et al. (2021) show

that the announcements of successful cyberattacks adversely affect peer firms' market values and argue that this adverse valuation effect reflects peer firms' exposure to industry-wide cyber risk and the costs of cyberattacks in general. Therefore, peer insiders are more likely to engage in sales (purchase) transactions prior to the release of negative cyberattack news on the target firms if their firms' exposure to cyber risk is higher (lower).

The results using *Peer firm's low CAR (-1, 1)* as a measure of peer firms' exposure to cyber risk are reported in Panel B of Table 4. We find that the coefficients on the interaction term between *Peer firm's low CAR (-1, 1)* and *Pre-disclosure period* are all positive and significant in columns (2) and (3), in which we use the pooled sample of sales and purchase transactions, respectively.[18] When we divide the pooled sample into the subgroups of sales (column (4)) and purchases (column (5)), the coefficient on the interaction term is positive and significant in the former subgroup, whereas the corresponding coefficient is negative and significant in the latter subgroup.

In sum, these findings suggest that peer insiders' abnormal trading profits are higher when their rivals suffer more from cyberattacks. They also earn abnormal profits when their own firms' exposure to cyber risk is higher (lower) by engaging in sales (purchase) transactions.

C. Portfolio-level analyses of peer insiders' trading profitability

To examine whether our results using transaction-level data in Panels A and B of Table 3 are robust to the use of portfolio-level data, we repeat the analyses in these panels with portfolio-level data. Specifically, for each cyberattack event, we construct an equally weighted portfolio of all transactions made by peer insiders in the pre- (post-) disclosure period. Since

[18] The sample median *Peer firm's CAR (-1, 1)* is 0.1%. Using an indicator for whether a peer firm's CAR (-1, 1) is negative as an alternative measure of its cyber risk exposure yields similar results.

each event includes both purchase and sales transactions, we focus only on the pooled-sample analysis.

Panel A of Table 5 presents the univariate results. Consistent with the results using transaction-level data, we find that peer insiders' portfolio abnormal returns measured by *BHAR180* in the pre-disclosure period are positive and significant at the 1% level. In contrast, the corresponding returns in the post-disclosure period are negative and insignificant. The difference in portfolio returns between the two subperiods is significant at the 5% level.

Panel B of Table 5 presents the OLS regressions in which the dependent variable is *Portfolio BHAR180*. Since we use a relatively small sample of portfolios of all transactions made by peer insiders in the analysis, the regressions include only industry (two-digit SIC code) and year fixed effects in addition to target firm characteristics. We report robust standard errors clustered at the event level. In column (1), we include only *Pre-disclosure period* and industry and year fixed effects; in column (2), we include target firm characteristics as additional controls. We find that the coefficient on *Pre-disclosure period* is positive and significant at the 5% level in both columns, suggesting that peer insiders earn significantly higher market-adjusted abnormal returns from their pre-disclosure transactions than from their post-disclosure transactions.

IV. Channel of Peer Insiders' Trading Profitability: Social Networks

In this section, we examine social ties between target and peer insiders as a potential channel through which peer insiders obtain information on target firms' cyberattacks and use this information to earn abnormal profits from their transactions. Prior studies on social networks suggest that connections formed through more personal relationships can better facilitate information transfer between connected parties (Ingram and Zou, 2008; Domhoff, 2009; Cohen, Frazzini, and Malloy, 2008, 2010). In addition, information transmission

between connected parties is more likely to occur when the information provider faces lower litigation and reputation risks. Thus, we expect peer insiders' trading to be more profitable when they are connected to target insiders through non-professional activities (i.e., nonworkplace ties) and when they are connected to senior executives in the target firm who do not hold board membership (i.e., nonboard ties).

Panel A of Table 6 presents the results of OLS regressions in which we use all types of connections between target and peer insiders as a measure of peer insiders' social ties to target insiders. We find that the coefficient on the interaction term between *All-tie transaction*, which takes the value of one for transactions made by a peer insider who is socially connected to target insiders, and zero otherwise, and *Pre-disclosure period* is positive in all regressions but significant only in column (2), in which we control for firm and year fixed effects.

We then decompose *All-tie transaction* into *Nonworkplace-tie transaction* and *Workplace-tie transaction* according to whether peer insiders' transactions are based on social connections that are more likely to promote trust and friendship between target and peer insiders, and we include their interactions with *Pre-disclosure period* in the regressions. The results are reported in Panel B of Table 6. We find that the coefficients on the interaction terms involving *Nonworkplace-tie transaction* are positive and significant in all regressions. However, none of the coefficients on the interaction terms involving *Workplace-tie transaction* are significant. The difference in coefficient estimates between the two interaction terms is significant in two of three columns. Our results suggest that personal connections better facilitate the transmission of nonpublic cyberattack news between connected parties beyond the target firm.

Next, we decompose *All-tie transaction* into *Nonboard-tie transaction* and *Board-tie transaction* according to whether peer insiders are connected to target insiders who currently serve as board members of the target firms and include their interactions with *Pre-disclosure period* in the regressions. The results are presented in Panel C of Table 6. We find that the

coefficients on the interaction term involving *Nonboard-tie transaction* are positive and significant at least at the 5% level or better in all regressions, whereas those on the interaction term involving *Board-tie transaction* are negative and insignificant. The differences in coefficient estimates between the two interaction terms are all statistically significant at the 1% level. Thus, a connected peer insider's abnormal trading profit is concentrated in transactions in which target insiders do not have board membership in their firms and are thus less likely to face regulatory scrutiny and attention. In untabulated tests, we control for *Nonboard-tie* and *Board-tie transaction* (*Nonworkplace-tie* and *Workplace-tie transaction*) as additional control variables in the regressions of Panel B (Panel C) of Table 6 and find that our results are almost the same.

V. Cross-sectional Heterogeneity in Peer Insiders' Trading Profitability

In this section, we examine cross-sectional heterogeneity in peer insiders' trading profitability across target firms and peer firms with different characteristics. We first focus on the litigation risk and information asymmetry of a target firm because these characteristics are likely to significantly influence target insiders' incentives to leak bad news to their connected parties before the public disclosure of the incident. We then focus on a peer firm's information asymmetry, which can significantly affect peer insiders' ability to exploit their information advantage over other investors, particularly when they are connected to target insiders through nonworkplace or nonboard ties.[19]

[19] We do not investigate the effects of peer firms' litigation risk on their insiders' trading profitability because of legal ambiguity of peer insider's transactions examined in our study: our private discussion via email with several legal experts indicate that the legal interpretation of the cases requires specific conditions and circumstances, such as the details of the firm-level insider trading policy and the details of the information transfer process. For example, Jesse Fried, Professor of Law at Harvard Law School points out that "…depending on the information involved, there might be a dispute over whether the information is non-public and/or legally material. If it is not both, there is no violation of Rule 10b-5. Because each side (trader, government) faces a risk of loss at trial, there is typically a settlement to avoid (a) the cost of trial and (b) the risk of loss. Generally, 99% (or more) of cases settle. This is true for all kinds of cases, not just 10b-5 cases." Stephen Diamond, Professor of Law at Santa Clara University also indicates that peer insiders could be liable for their trading if they obtain rival firms' cyberattack information because of their current employment Peer insiders would also face tippee liability if they are directly

A. Target firms' litigation risk and information environment

As the first measure of the target firm's legal risk, we use an indicator for the presence of common institutional blockholders who hold large equity ownership in both the target and peer firms.[20] If target insiders leak cyberattack information to peer insiders, it places common institutional blockholders holding ownership in peer firms at a significant information disadvantage in protecting their equity position. To avoid potential losses arising from such information disadvantages, common institutional blockholders are likely to have strong incentives to closely monitor target insiders (Kang, Luo, and Na, 2018; He, Huang, and Zhao, 2019; Donelson, Flam and Yust, 2021). Thus, the presence of common institutional blockholders increases the litigation risk of target insiders who selectively disclose information about incidents to connected parties in peer firms. Following prior studies, we also include two additional variables as measures of a target firm's legal risk: an indicator for whether the target firm operates in one of the high-litigation industries of the biotechnology (SIC codes 2833-2836), computer hardware (SIC codes 3600-3674), retail (SIC codes 5200-5961), and computer (SIC code 7379) industries (Rogers and Stocken, 2005) and an indicator for whether the target firm's ex ante litigation risk measured by federal judge ideology (*Liberal court score*) is above the sample median.[21] We then divide the sample into two subgroups according to each of these

tipped off by target insiders: these peer insiders would breach their fiduciary obligations to their firms and thus can be guilty of misappropriating their firms' assets. ." We thank Professors Fried and Diamond for sharing their thoughts and opinions on the issue. Nevertheless, we examine whether peer insiders' trading profitability is affected by their firms' litigation risk measured by variables used below and find that it is lower when their firms face higher litigation risk. Thus, it appears that peer insiders care about legal risk even when they use other firms' nonpublic information in their trading.

[20] Consistent with the findings of prior studies that institutional cross-ownership is increasingly common among U.S. public firms (Kang, Luo, and Na, 2018; He, Huang, and Zhao, 2019), we find that about 36.4% of the 3,107 target firms and their peer firms in our sample are held by common institutional blockholders, measured as of the beginning of the pre-disclosure period.

[21] The liberal court score is computed by estimating the probability that the three-judge panel on the circuit court of the jurisdiction of the firm's headquarters has at least two Democratic appointees (Huang, Hui, and Li, 2019). A higher score means greater litigation risk. The sample size is decreased when we use the liberal court score as a measure of litigation risk since headquarters information is missing for some firms. We thank Allen Huang for sharing the data on the liberal court score with us.

litigation risk measures and reestimate the regressions in columns (2) and (3) of Panels B and C of Table 6 separately for the subgroups. For the sake of brevity, we report only the results estimated with the regression specification that controls for firm and year (industry-by-year) fixed effects. Controlling for industry and year fixed effects does not change the results.

The key independent variables are the interactions of *Pre-disclosure period* with *Nonworkplace-tie transaction* and *Workplace-tie transaction* (*Nonboard-tie transaction* and *Board-tie transaction*). In columns (1)-(4) of Table 7, we find that the impacts of nonworkplace ties on peer insiders' profitability are positive and significant among a subgroup of peer insiders whose firms do not have common institutional blockholders, whereas they are negative among subgroups of peer insiders whose firms have common institutional blockholders. The differences in coefficients on the interaction terms involving *Nonworkplace-tie transaction* between the two subgroups are significant at the 5% level. We find no discernable patterns on the impacts of workplace ties on peer insiders' profitability. We also find that the impacts of nonboard ties on peer insiders' profitability are more evident in the absence of common institutional blockholders, whereas the impacts of board ties on peer insiders' profitability are not affected by the presence of these blockholders. In columns (5)-(8), we split the sample using a target firm's industry as a measure of its litigation risk. We find that the coefficients on both the interaction term involving *Nonworkplace-tie transaction* and the interaction term involving *Nonboard-tie transaction* are positive and significant for a subgroup of peer insiders who have social ties with insiders in target firms operating in low-litigation-risk industries. In contrast, the coefficients on these interaction terms are negative and insignificant for a subgroup of peer insiders who have social ties with insiders in target firms operating in high-litigation-risk industries. The differences in coefficients on the interaction terms involving *Nonworkplace-tie transaction* (*Nonboard-tie transaction*) between the high- and low-litigation-risk groups are significant in all regressions. In columns (9)-(12), we use the target

firm's liberal court score as the measure of its litigation risk. We find similar results as those in columns (5)-(8), although the difference in the effects of nonworkplace ties on peer insiders' profitability between the subsamples of firms with low and high litigation risk is not significant. Overall, the findings suggest that the target firm's high litigation risk limits the profitability of transactions made by peer insiders connected through non-professional (nonboard) ties.

A target firm's information asymmetry can also influence its insiders' incentives and abilities to leak firm-specific private information about a cyberattack to peer insiders, affecting peer insiders' trading profitability. A poor information environment in the target firm would make it easier for target insiders to leak information about their firms' cyberattack to connected parties in other firms. Moreover, high information asymmetry makes it more costly for outsiders, including investors who own peer firms' shares, to gain access to cyberattack information, increasing the value of private information that target insiders share with peer insiders. To measure the level of target firms' information asymmetry, we use their firm age, absolute discretionary accruals estimated using a modified Jones model (Dechow, Sloan, and Sweeney, 1995), and positive R&D (indicator) (e.g., Aboody and Lev, 2000; Gu and Li, 2007; Bhattacharya et al., 2012). We then divide the sample into two subgroups according to whether the target firm's age is below the sample median age, whether its absolute discretionary accruals are above the sample median accrual, and whether its R&D expenditure is positive, and we reestimate the regressions in Table 7 separately for each subgroup.

The results are presented in Table 8. Consistent with our predictions, we find that the effects of nonworkplace and nonboard ties on peer insiders' trading profitability are more pronounced when target firms are more informationally opaque (i.e., younger firms, firms with higher absolute discretionary accruals, and firms with positive R&D). Thus, a poor information environment in the target firm makes target insiders' private information more valuable and allows peer insiders to exploit such information.

B. Peer firms' information environment

A peer firm's poor information environment can affect its insiders' abilities and incentives to exploit their private information and engage in opportunistic trading. As shown in Section III.B, peer insiders need to assess their own firm's cyber risk exposure and ability to manage this risk to capitalize on their private information on the rival firms' cyberattacks. Thus, greater information asymmetry in peer firms increases their insiders' information advantage obtained from target insiders over other market participants, providing peer insiders with better opportunities to exploit this advantage. Supporting this argument, studies show that insiders earn higher trading profits when their firms are informationally opaque than when their firms are informationally transparent (e.g., Aboody and Lev, 2000; Huddart and Ke, 2007; Rogers, 2008). To examine how peer firms' information environment affects their insiders' trading profitability and whether this trading profitability varies with the type of social connection, we use the same approach and information asymmetry variables as those used for target firms. The results are reported in Table 9. We find that our prior results for the effects of nonworkplace and nonboard ties on peer insiders' trading profitability are concentrated in the subsamples of younger firms and firms that have higher absolute discretionary accruals. Thus, peer firms' high information asymmetry increases the value of nonpublic cyberattack information held by their insiders connected to target insiders, and it provides peer insiders with more opportunities to exploit such information.[22] However, we do not find any consistent results when we use *Positive R&D (indicator)* as a measure of peer firms' information asymmetry.

[22] Prior studies show that a firm's good internal governance restrains its insiders from exploiting their information advantage in trading shares and thus affects their trading performance (e.g., Ravina and Sapienza, 2010; Dai et al., 2016). Given that good governance makes firms more transparent and provides managers with strong incentives to undertake risk-mitigating actions that help reduce firms' exposure to cyber risk, good governance limits peer insiders' ability to exploit their information advantage. To examine this issue, in untabulated tests, we construct *Poor governance (indicator)* that takes the value of one if the peer firm's institutional block ownership is below the sample median institutional block ownership, if its proportion of outside directors on the board is below the sample median proportion, or if it is a firm with CEO–chair duality, and zero otherwise. We then estimate regressions in which our key independent variable is the interaction term between *Pre-disclosure period* and *Poor governance*

VI. Additional Tests

A. SEC's guidance on the disclosure of cybersecurity risk in 2011

Regulatory disclosure requirements on cybersecurity risk management can deter the transfer of information about cybersecurity incidents to peer insiders and thus reduce their ability to exploit such information. To examine this issue, we focus on the SEC's issuance of guidance in 2011 regarding registrants' disclosure obligations relating to cybersecurity risks and incidents.[23]

The results are reported in Table 10. In Panel A, the key independent variables are *Pre-disclosure period* and its interaction with *Post-SEC guidance*, which takes the value of one for transactions made on October 13, 2011 (the SEC's issuance date of the guidance on disclosure obligations relating to cybersecurity risks and incidents) and onward, and zero otherwise. We find that the coefficient on *Pre-disclosure period* is positive and significant and the coefficient on its interaction with *Post-SEC guidance* is negative and significant in both regressions. These results suggest that although peer insiders earn higher abnormal trading profits prior to the cyberattack disclosure date, these profits are significantly reduced in the post-SEC guidance period.

(indicator). We find that the interaction terms between *Pre-disclosure period* and each indicator for poorer governance are positively and significantly related to peer insiders' abnormal returns. Thus, peer firms' governance affects their insiders' ability to earn abnormal profits from trading based on their private information about other firms' cyberattacks.

[23] The SEC's 2011 issuance of cybersecurity disclosure guidance is the U.S. financial regulatory body's first attempt to influence its registrants to make timely disclosures about the information about their cybersecurity risk. According to the Willis Fortune 1000 Cyber Disclosure Report in August 2013, the SEC's 2011 guidance is in the form of advice rather than statutory regulation. Nevertheless, it has influenced listed firms to undertake necessary actions for the disclosure of cyberattacks because the SEC's Division of Corporation Finance selectively reviews company securities filings to ensure the compliance of the filings with relevant disclosure and accounting requirements. In the review process, the division's staff issues comments to the company, such as requesting the revision of its financial statements, amendment of its disclosures, additional information, and other disclosures in future filings (https://www.sec.gov/divisions/corpfin/cfabout.shtml).This 2011 guidance is followed by the SEC's issuance of cybersecurity interpretive guidance in February 2018, including details on the prohibitions of insider trading in connection with information about cybersecurity risks and incidents. In March 2022, the SEC proposes amendments to the rules on firms' cybersecurity practices and incident reporting (https://www.sec.gov/files/33-11038-fact-sheet.pdf). We do not examine the effects of the SEC's subsequent guidance since the issuance does not fall into our sample period.

In Panel B, we divide the sample into the pre- and post-SEC guidance periods to examine whether the effects of nonworkplace and nonboard ties on peer insiders' trading profitability weaken in the post-SEC guidance regime. We find that the coefficient on the interaction term between *Pre-disclosure period* and *Nonworkplace-tie transaction* is positive and significant in the pre-SEC guidance period (columns (1) and (3)), while it is insignificant in the post-SEC guidance period (columns (2) and (4)). The difference in the coefficients between the two subperiods is significant. In contrast, none of the coefficients on the interaction term between *Pre-disclosure period* and *Workplace-tie transaction* is significant. Thus, the effects of the SEC's issuance of guidance in 2011 on the disclosure of cybersecurity risk are mainly concentrated in transactions based on nonworkplace ties that are more likely to stimulate trust and friendship between the target and peer insiders. When we replace *Nonworkplace-tie transaction* and *Workplace-tie transaction* with *Nonboard-tie transaction* and *Board-tie transaction*, respectively, we find similar results although peer insiders make abnormal returns from their nonboard-tie transactions during the pre-disclosure period in both the pre- and post-SEC guidance regimes. However, the magnitude of the coefficient on the interaction term between *Pre-disclosure period* and *Nonworkplace-tie transaction* is significantly greater in the pre-SEC guidance regime than in the post-SEC guidance regime.

Overall, regulatory oversight in cyber risk disclosure requirements appears to reduce target insiders' incentives to share their firms' cyberattack information with others and thus limits peer insiders' abilities to access the information, although it does not completely eliminate such incentives and abilities.

B. Peer insiders' trade volume

Thus far, our analysis has focused on peer insiders' trading profitability and shows that they earn abnormal trading profits from both sales and purchase transactions. If peer insiders

view their rival firms' cyberattacks as bad news for their firms, we expect the volume of peer insiders' sales transactions to increase before the public disclosure of cyberattack news. To examine this issue, we aggregate each peer insider's transaction volume in the pre- and post-disclosure periods, respectively, and compare the changes in the aggregate volume between the two periods. When peer insiders do not make any transactions in a pre- or post-disclosure period, we set their trading volume in such a period to zero.

The results are reported in Table 11. In Panel A, we use the number of shares sold by peer insiders scaled by the number of shares outstanding as the dependent variable. Column (1) uses the full sample of peer insiders, and column (2) uses the subsample of peer insiders who are socially connected to target insiders, *all-tie peer insiders*. While we find little evidence that peer insiders' sales transactions are different between the pre- and post-disclosure periods, all-tie peer insiders engage in significantly more sales transactions in the pre-disclosure period than in the post-disclosure period. In columns (3) and (4) (columns (5) and (6)), we divide all-tie peer insiders into two subgroups according to whether they have nonworkplace ties (nonboard ties) with target insiders. We find that the coefficient on *Pre-disclosure period* is positive and significant at the 5% level only for the subsamples of nonworkplace-tie and nonboard-tie peer insiders. However, the differences in coefficients on *Pre-disclosure period* between the two subgroups are insignificant. In Panel B, we repeat our analyses in Panel A using the dollar value of shares sold by peer insiders scaled by market capitalization as the dependent variable and find that the results do not change.

Overall, the results suggest that connected peer insiders sell a large number (amount) of shares ahead of the public disclosure of target firms' cyberattacks, indicating that they generally view rival firms' cyberattacks as events that adversely affect their firms.

C. Common industry knowledge as an alternative source of peer insiders' information

Prior studies show that insiders take advantage of their industry familiarity or better ability to process industry-specific public information when trading shares of their own firms or other industry peers (e.g., Alldredge and Cicero, 2015; Ben-David, Birru, and Rossi, 2019). For example, Ben-David, Birru, and Rossi (2019) find that insiders trade shares of their firms' industry peers more frequently than shares of firms in other industries and earn abnormal returns from both purchases and sales transactions. However, they find no evidence that insiders' trading profitability is related to the use of private information. These findings suggest that our results for connected peer insiders' high trading profitability are driven by their superior ability to process publicly available information about industry-wide cyber risk, not necessarily by their private information obtained from target insiders. To examine this issue, we count the number of cyberattacks that occur in each industry prior to the focal incident and construct an indicator that takes the value of one if the number of cyberattacks that occur in an industry is above the sample median, and zero otherwise (*Higher incidence of cyberattacks*).[24] We then reestimate the regressions in Panel A of Table 4 after replacing *Target firm's low CAR (-1, +1)* with *Higher incidence of cyberattacks*. The frequent occurrence of cyberattacks in an industry should increase the availability of industry-specific public information, allowing peer insiders to better understand the exposure of their firms' industries to cyber risk. If peer insiders exclusively rely on industry-specific public information for their trading, we expect their trading profits to be concentrated among industries experiencing a higher incidence of cyberattacks. Thus, the coefficient on the interaction term between *Pre-disclosure period* and *Higher incidence of cyberattacks* is predicted to be positive and significant. In untabulated tests, we find that the coefficient on the interaction term is negative and significant (insignificant) in column (1) (columns (2) and (3)). In columns (4) and (5), we use the subsamples of sales and purchase transactions, respectively, and find that the coefficient on the

[24] The mean (median) number of incidents is 2.35 (2) in our sample industries.

interaction term is insignificant in both regressions.[25] Thus, it is unlikely that the primary source of peer insiders' trading profitability is common industry knowledge rather than target firm-specific private information obtained through social connections.

D. Target firms' insider trading profitability

Thus far, we have shown that peer insiders earn abnormal trading profits by exploiting private information on their rival firms' cyberattacks obtained from connected target insiders. Although target insiders in general face high litigation and enforcement risks when they use their firms' nonpublic material information in trading, some target insiders of firms with low litigation risk might still exploit their information advantage by engaging in trading of their firms' shares. We use a difference-in-differences approach to examine this issue. For each target firm, using a propensity score matching approach, we identify a control firm that does not experience a cyberattack. The propensity score is calculated using the logit regression of *Cyberattack*, an indicator that takes the value one if a firm experiences a cyberattack in a given year, and zero otherwise, on firm size, stock performance, stock return volatility, positive R&D (indicator), missing R&D (indicator), analyst coverage, loss (indicator), and institutional block ownership. Since prior studies show that cyberattacks tend to be clustered in certain industries (e.g., Kamiya et al., 2021), we require both treatment and control firms to be in the same (two-digit SIC code) industry. We also require treatment and control firms to be in the same fiscal year.

[25] Our finding that peer insiders' abnormal trading profits are not significantly related to *High incidence of cyberattacks* could be explained by an alternative argument that information conveyed by news of subsequent cyberattacks is less informative in industries in which the occurrence of cyberattacks is more frequent. However, given that cyber risk is evolving over time and emerging in nature (Kamiya et al., 2021), it is unlikely that subsequent cyberattacks in a certain industry in a given year do not contain new information. Consistent with this view, we find that the mean CAR (-1, 1) for subsequent cyberattacks that occurring in an industry in a given year is -0.6%, which is significant at the 10% level, suggesting that the subsequent events contain incremental information to investors.

Panel A of Appendix B presents descriptive statistics for the sample of 232 propensity-score-matched firms (116 treatment and 116 control firms). We find no significant difference in firm characteristics between target firms and their matched firms, suggesting that our matching approach identifies matched firms that are very close to target firms. Panel B presents the results of transaction-level OLS regressions in which the dependent variable is *BHAR180*. The key independent variable of interest is the interaction term between *Cyberattack* and *Pre-disclosure period*. We control for all variables used in the regressions of Panel B of Table 3. In columns (1)-(3), we find that the coefficients on the interaction term are positive and significant in all three regressions. The coefficient estimates suggest that the transactions made by insiders of target firms in the pre-disclosure period have 13 percentage points higher market-adjusted abnormal buy-and-hold returns than other transactions.[26] Thus, as is the case for other negative corporate events (e.g., filings of bankruptcy petitions (Gosnell, Keown, and Pinkerton, 1992; Seyhun and Breadley, 1997) and financial restatements (Summers and Sweeney, 1998; Thevenot, 2012)), target insiders exploit their private information about cyberattacks in their trading.

In columns (4)-(6), we include *Low liberal court score (indicator)* and its interactions with *Cyberattack* and *Pre-disclosure period* to examine whether higher litigation risk prevents target insiders from using their privileged information about target firms' cyberattacks to earn abnormal profits. We find that the coefficient on the triple interaction term is positive and significant at the 5% level in all three regressions, suggesting that the results in columns (1)-(3) are mainly driven by target insiders who are less exposed to litigation risk. Target insiders

[26] Our findings complement those of recent studies showing that target insiders exploit the private information about their firms' cyberattacks (Amir, Levi, and Livne, 2019; Lin et al., 2020). For example, Amir, Levi, and Livne (2019) find that insiders of firms that withhold information on cyberattacks engage in sales transaction, and Lin et al. (2020) report that target insiders save an average of $35,009 by selling their firms' shares in the three months before the announcement of a data breach. In a related paper, Chen, Hilary, and Tian (2021) focus on the impact of mandatory state-level data breach disclosure regulations on selling activity and show that the passage of such laws prompts insiders to sell their shares to limit future losses.

who face higher litigation risk do not make any higher profits in the pre-disclosure period as shown by insignificant coefficients on the interaction term between *Cyberattack* and *Pre-disclosure period*. Using an indicator for high litigation industries as an alternative measure of litigation risk yields similar results.

E. Opportunistic versus routine trading

Cohen, Malloy, and Pomorski (2012) find that opportunistic traders are more likely than routine traders to trade in advance of firm-level information events. To examine whether peer insiders who engage in opportunistic trading make higher trading profits than those who engage in routine trading, we classify peer insiders according to their past history of trades into two groups: routine peer insiders who traded their firms' shares in the same month for at least three consecutive years before the cyber disclosure date and opportunistic peer traders who do not show such trading behavior. We then reestimate the regressions in Panel B of Table 3. In untabulated tests, we find that the coefficient on *Pre-disclosure period* is positive and significant (0.035 to 0.057) only in a subsample of transactions made by opportunistic peer traders, while none of the corresponding coefficients are significant in a subsample of transactions made by routine peer insiders. The results suggest that our findings are largely driven by a group of opportunistic traders who have privileged access to private information about their rival firms' cyberattacks.

VII. Summary and Conclusion

Informed trading beyond the boundaries of conventional insider trading regulations has attracted growing attention from researchers, media, and regulators. In this paper, we examine a new, attenuated type of informed trading by insiders who obtain private information about

cyberattacks that occurred in their firms' industry rivals via their social connections with rival firm insiders.

We find that peer insiders earn economically large and significant abnormal returns by trading shares of their own firms prior to the target firm's public disclosure of its cyberattack. We further find that peer insiders' trading profits are higher when target firms experience more severe cyberattacks and that peer insiders' profitability in sales (purchases) transactions is evident only among peer firms that have higher (lower) exposure to cyber risk. We also find that peer insiders earn abnormal trading profits only when they are connected to target insiders through nonworkplace and nonboard ties. Thus, shared networks that are more informal and those that are less subject to regulatory scrutiny and stakeholder monitoring are important channels through which insiders with access to other firms' private negative information enjoy an information advantage over other market participants.

Our tests of cross-sectional heterogeneity in peer insiders' trading profitability show that their trading profitability is higher when they are connected through nonworkplace or nonboard ties to insiders of target firms with lower litigation risk and insiders of target firms with higher information asymmetry. The trading profitability of such connected peer insiders is also higher when their own firms have higher information asymmetry.

We further examine how the introduction of disclosure requirements for a firm's reports of its cybersecurity risk affects informed trading by connected peer insiders. We find that the SEC's 2011 disclosure requirements on cybersecurity risk and incidents limit peer insiders' ability to access private information about their rival firms' cyberattacks, although it does not entirely eliminate it. We also examine the difference in the volume of peer insiders' sales transactions between the pre- and post-disclosure periods and find that connected peer insiders sell a larger number (amount) of shares in the pre-disclosure period than in the post-disclosure period. In addition, we examine whether connected peer insiders earn high trading profits

because of their superior ability to process public information, such as common industry knowledge, and find that common industry knowledge is unlikely to be a primary source of peer insiders' trading profitability. We further examine whether target insiders can also make abnormal profits by exploiting their firms' nonpublic cyberattack information in trading their firms' shares. We find that target insiders earn abnormal trading returns only when their firms are less exposed to litigation risk. Finally, we examine whether the strategic use of peer insiders' information advantage in target firms' cyberattacks affects their trading profitability and find that their opportunistic transactions are associated with higher trading profits than their routine transactions.

Overall, our study provides new evidence for an attenuated type of informed trading by peer insiders who obtain private information about their firms' industry rivals from the connected insiders in rivals. We show that shared networks formed through friendships and those that are less subject to regulatory oversight and market scrutiny enable peer insiders to engage in opportunistic trading by exploiting privileged information about rival firms' cyberattacks, shedding new light on the negative externalities of cyber risk. However, it is also possible that peer insiders' trading improves the price discovery of target and peer firms by making the stock prices of target and peer firms more informative and efficient. We leave the investigation of the positive role of peer insiders' trading for future research.

References

Aboody, David, and Baruch Lev, 2000, Information asymmetry, R&D, and insider gains, *Journal of Finance* 55, 2747-2766.

Ahern, Kenneth R., 2017, Information networks: Evidence from illegal insider trading tips, *Journal of Financial Economics* 125, 26-47.

Alldredge, Dallin M., and David C. Cicero, 2015, Attentive insider trading, *Journal of Financial Economics* 115, 84-101.

Amir, Eli and Levi, Shai and Livne, Tsafrir, 2019, Insider trading and disclosure: The case of cyberattacks, Working paper.

Amir, Eli, Shai Levi, and Tsafrir Livne, 2018, Do firms underreport information on cyber-attacks? Evidence from capital markets, *Review of Accounting Studies* 23, 1177-1206.

Ben-David, Itzhak, Justin Birru, and Andrea Rossi, 2019, Industry familiarity and trading: Evidence from the personal portfolios of industry insiders, *Journal of Financial Economics* 132, 49-75.

Berkman, Henk, Paul Koch, and P. Joakim Westerholm, 2020, Inside the director network: When directors trade or hold inside, interlock, and unconnected stocks, *Journal of Banking & Finance* 118, 105892.

Bettis, J.C, Coles, J.L, and Lemmon, M.L, 2000, Corporate policies restricting trading by insiders, *Journal of Financial Economics*, 57, 191-220.

Bhattacharya, Nilabhra, Frank Ecker, Per Olsson, and Katherine Schipper, 2012, Direct and mediated associations among earnings quality, information asymmetry, and the cost of equity, *Accounting Review* 87, 449-482.

Brochet, Francois, 2010, Information content of insider trades before and after the Sarbanes-Oxley Act, *Accounting Review* 85, 419-446.

Cao,Ying, Dan Dhaliwal, Zengquan Li, and Yong George Yang, 2015, Are all independent directors equally informed? Evidence based on their trading returns and social networks, *Management Science* 61, 795-813.

Carhart, Mark M., 1997, On persistence in mutual fund performance, *Journal of Finance* 52, 57-82.

Chan, Lilian H., Kevin C. W. Chen, and Tai-Yuan Chen, 2013, The effects of firm-initiated clawback provisions on bank loan contracting, *Journal of Financial Economics* 110, 659-679.

Chen, Xi, Gilles Hilary, and Xiaoli (Shaolee) Tian, 2021, Mandatory data breach disclosure and insider trading, Working paper.

Cohen, Lauren, Andrea Frazzini, and Christopher Malloy, 2010, Sell-side school ties, *Journal of Finance* 65, 1409-1437.

Cohen, Lauren, Andrea Frazzini, and Christopher Malloy, 2008, The small world of investing: Board connections and mutual fund returns, *Journal of Political Economy* 116, 951-979.

Dai, Lili, Renhui Fu, Jun-Koo Kang, and Inmoo Lee, 2016, Corporate governance and the profitability of insider trading, *Journal of Corporate Finance* 40, 235-253.

Dechow, Patricia M., Richard G. Sloan, and Amy P. Sweeney, 1995, Detecting earnings management, *Accounting Review* 70, 193-225.

Deuskar, Prachi, Aditi Khatri, and Jayanthi Sunder, 2021, Insider trading restrictions and informed trading in peer stocks, Working paper.

Domhoff, William G., 2009. Who rules America? Challenges to corporate and class dominance, sixth ed. McGraw Hill, New York, NY.

Donelson, Dain C., Rachel W. Flam, and Christopher G. Yust, 2022, Spillover effects in disclosure-related securities litigation, *Accounting Review* 97, 275-299.

Dooley, Peter C., 1969, The interlocking directorate, *American Economic Review* 59, 314-323.

Fracassi, Cesare, and Geoffrey Tate, 2012, External networking and internal firm governance, *Journal of Finance* 67, 153-194.

Frankel, Richard, and Xu Li, 2004, Characteristics of a firm's information environment and the information asymmetry between insiders and outsiders, *Journal of Accounting and Economics* 37, 229-259.

Gosnell, Thomas, Arthur J. Keown, and John M. Pinkerton, 1992, Bankruptcy and insider trading: Differences between exchange-listed and OTC firms, *Journal of Finance* 47, 349-362.

Gu, Feng, and John Q. Li, 2007, The credibility of voluntary disclosure and insider stock transactions, *Journal of Accounting Research* 45, 771-810.

Guay, Wayne R., Kim, Shawn, and Tsui, David, 2022, Determinants of insider trading windows, Working paper.

He, Jie, Jiekun Huang, and Shan Zhao, 2019, Internalizing governance externalities: The role of institutional cross-ownership, *Journal of Financial Economics* 134, 400-418.

Huang, Allen, Kai Wai Hui, and Reeyarn Zhiyang Li, 2019, Federal judge ideology: A new measure of ex ante litigation risk, *Journal of Accounting Research* 57, 431-489.

Huddart, Steven J., and Bin Ke, 2007, Information asymmetry and cross-sectional variation in insider trading, *Contemporary Accounting Research* 24, 195-232.

Ingram, Paul, and Xi Zou, 2008, Business friendships, *Research in Organizational Behavior* 28, 167-184.

Jagolinzer, Alan, David Larcker, and Daniel Taylor, 2011, Corporate governance and the information content of insider trades, *Journal of Accounting Research* 49, 1249-1274.

John, Kose, and H. P. Lang Larry, 1991, Insider trading around dividend announcements: Theory and evidence, *Journal of Finance* 46, 1361-1389.

Kamiya, Shinichi, Jun-Koo Kang, Jungmin Kim, Andreas Milidonis, and René M. Stulz, 2021, Risk management, firm reputation, and the impact of successful cyberattacks on target firms, *Journal of Financial Economics* 139, 719-749.

Kang, Jun-Koo, Juan Luo, and Hyun Seung Na, 2018, Are institutional investors with multiple blockholdings effective monitors?, *Journal of Financial Economics* 128, 576-602.

Karpoff, Jonathan M., D. Scott Lee, and Gerald S. Martin, 2008, The cost to firms of cooking the books, *Journal of Financial and Quantitative Analysis* 43, 581-611.

Ke, Bin, Steven Huddart, and Kathy Petroni, 2003, What insiders know about future earnings and how they use it: Evidence from insider trades, *Journal of Accounting and Economics* 35, 315-346.

Lakonishok, Josef, and Inmoo Lee, 2001, Are insider trades informative?, *Review of Financial Studies* 14, 79-111.

Lin, Zhaoxin, Travis R.A. Sapp, Jackie Rees Ulmer, and Rahul Parsa, 2020, Insider trading ahead of cyber breach announcements, *Journal of Financial Markets* 50, 100527.

Mehta, Mihir N., David M. Reeb, and Wanli Zhao, 2021, Shadow trading, *Accounting Review* 96, 367-404.

Piotroski, Joseph D., and Darren T. Roulstone, 2005, Do insider trades reflect both contrarian beliefs and superior knowledge about future cash flow realizations?, *Journal of Accounting and Economics* 39, 55-81.

Ravina, Enrichetta, and Paola Sapienza, 2010, What do independent directors know? Evidence from their trading, *Review of Financial Studies* 23, 962-1003.

Rogers, Jonathan L., 2008, Disclosure quality and management trading incentives, *Journal of Accounting Research* 46, 1265-1296.

Rogers, Jonathan, L., and Phillip C. Stocken, 2005, Credibility of management forecasts, *Accounting Review* 80, 1233-1260.

Rozeff, Michael S., and Mir A. Zaman, 1998, Overreaction and insider trading: Evidence from growth and value portfolios, *Journal of Finance* 53, 701-716.

Seyhun, H. Nejat, 1986, Insiders' profits, costs of trading, and market efficiency, *Journal of Financial Economics* 16, 189-212.

Seyhun, H. Nejat, and Michael Bradley, 1997, Corporate bankruptcy and insider trading, *Journal of Business* 70, 189-216.

Summers, Scott L., and John T. Sweeney, 1998, Fraudulently misstated financial statements and insider trading: An empirical analysis, *Accounting Review* 73, 131-146.

Thevenot, Maya, 2012, The factors affecting illegal insider trading in firms with violations of GAAP, *Journal of Accounting and Economics* 53, 375-390.

Table 1
Distribution of Cyberattacks by Year and Industry

This table presents the distribution of 266 cyberattacks for a sample of 188 firms covered in Compustat, CRSP, and Thomson Reuters Insider Filing Data over the period 2005 to 2017 by year and industry. We require that information about key variables is not missing. We present the chronological distribution of cyberattacks by calendar year and two-digit SIC code. The numbers in parentheses are the percentages of cyberattacks that occurred in each industry for a given calendar year, and the numbers in brackets in the last row (column) are the percentage of cyberattacks that occurred in each industry (each calendar year) during the sample period.

Calendar year	Agriculture, forestry, fisheries	Mineral, construction	Manufacturing	Transport, communications	Wholesale trade and retail trade	Service	Total
	(01-09)	(10-19)	(20-39)	(40-48)	(50-59)	(70-89)	
2005	0	0	2	0	2	0	4
	(0.00)	(0.00)	(50.00)	(0.00)	(50.00)	(0.00)	[1.50]
2006	0	0	0	1	3	0	4
	(0.00)	(0.00)	(0.00)	(25.00)	(75.00)	(0.00)	[1.50]
2007	0	0	1	1	1	3	6
	(0.00)	(0.00)	(16.67)	(16.67)	(16.67)	(50.00)	[2.26]
2008	0	0	0	1	1	2	4
	(0.00)	(0.00)	(0.00)	(25.00)	(25.00)	(50.00)	[1.50]
2009	0	0	0	1	2	2	5
	(0.00)	(0.00)	(0.00)	(20.00)	(40.00)	(40.00)	[1.88]
2010	0	0	3	1	6	2	12
	(0.00)	(0.00)	(25.00)	(8.33)	(50.00)	(16.67)	[4.51]
2011	1	0	4	5	2	5	17
	(5.88)	(0.00)	(23.53)	(29.41)	(11.76)	(29.41)	[6.39]
2012	1	1	9	3	5	9	28
	(3.57)	(3.57)	(32.14)	(10.71)	(17.86)	(32.14)	[10.53]
2013	1	0	7	3	6	13	30
	(3.33)	(0.00)	(23.33)	(10.00)	(20.00)	(43.33)	[11.28]
2014	1	0	9	4	10	15	39
	(2.56)	(0.00)	(23.08)	(10.26)	(25.64)	(38.46)	[14.66]
2015	0	0	7	4	11	9	31
	(0.00)	(0.00)	(22.58)	(12.90)	(35.48)	(29.03)	[11.65]
2016	0	1	12	7	8	14	42
	(0.00)	(2.38)	(28.57)	(16.67)	(19.05)	(33.33)	[15.79]
2017	0	1	12	8	9	14	44
	(0.00)	(2.27)	(27.27)	(18.18)	(20.45)	(31.82)	[16.54]
Total	4	3	66	39	66	88	266
	[1.50]	[1.13]	[24.81]	[14.66]	[24.81]	[33.08]	[100.00]

Table 2
Summary Statistics

Panel A of this table compares firm characteristics between 188 firms that experience cyberattacks (254 firm-year observations) over the period 2005 to 2017 and their 1,329 industry peer firms (3,021 firm-year observations) over the same period. Panel B compares the characteristics of transactions made by an insider of the peer firm (i.e., a peer insider) between the pre-disclosure period (44,639 transactions made by 5,663 insiders of 1,159 industry peer firms) and the post-disclosure period (48,960 transactions made by 5,801 insiders of 1,166 industry peer firms). Peer firms are industry competitors that have the same four-digit SIC code as the target firm. We require peer firms not to experience cyberattacks in a given year and to have at least one insider transaction during the pre- or post-disclosure period. Pre-disclosure period is defined as the period from 90 to one calendar days before the cyberattack disclosure date. Post-disclosure period is defined as the period from one to 90 calendar days after the cyberattack disclosure date. *All-tie transaction (indicator)* takes the value of one for transactions made by a peer insider who is socially connected to a director or a senior executive of the target firm (i.e., a target insider) through nonworkplace ties (i.e., common educational background, memberships in the same non-business organizations) or workplace ties (i.e., current or prior common employment), and zero otherwise. *Nonworkplace-tie transaction (indicator)* takes the value of one for transactions made by a peer insider who is socially connected to target insiders exclusively through nonworkplace ties, and zero otherwise. *Workplace-tie transaction (indicator)* takes the value of one for transactions made by a peer insider who is socially connected to at least one target insider through workplace ties, and zero otherwise. *Nonboard-tie transaction (indicator)* takes the value of one for transactions made by a peer insider who is socially connected only to nonboard executives of the target firm, and zero otherwise. *Board-tie transaction (indicator)* takes the value of one for transactions made by a peer insider who is socially connected to at least one director of the target firm, and zero otherwise. Appendix A provides detailed descriptions of the construction of the variables. ***, **, and * denote that *t* tests for mean differences and Wilcoxon *z* tests for median differences are significant at the 1%, 5%, and 10% levels, respectively.

Panel A. Comparison of firm characteristics between target firms and peer firms

	Target firm-year observations (N=254): a		Peer firm-year observations (N=3,021): b		Test of difference (a – b): *p*-value	
Variable	Mean	Median	Mean	Median	*t*-test	Wilcoxon *z*-test
Market capitalization ($ billions)	42.418	10.360	6.980	1.028	0.000***	0.000***
Book-to-market	0.372	0.322	0.395	0.305	0.310	0.805
Stock performance	0.030	0.006	0.084	0.020	0.022**	0.398
Stock return volatility	0.020	0.018	0.028	0.025	0.000***	0.000***
Positive R&D (indicator)	0.445	0.000	0.584	1.000	0.000***	0.000***
Missing R&D (indicator)	0.366	0.000	0.282	0.000	0.008***	0.004***
Number of analysts	18.398	18.292	9.374	6.583	0.000***	0.000***
Loss (indicator)	0.118	0.000	0.307	0.000	0.000***	0.000***
Institutional block ownership	0.191	0.182	0.233	0.224	0.000***	0.000***

Panel B. Comparison of peer insiders' transaction characteristics between pre- and post-disclosure periods

	Pre-disclosure period (N=44,639): a		Post-disclosure period (N=48,960): b		Test of difference (a – b): *p*-value	
Variable	Mean	Median	Mean	Median	*t*-test	Wilcoxon *z*-test
Daily trade size (%)	0.067	0.028	0.063	0.028	0.000***	0.331
Recent trade size (%)	0.128	0.029	0.099	0.030	0.000***	0.011**
All-tie transaction (indicator)	0.143	0.000	0.105	0.000	0.000***	0.000***
Nonworkplace-tie transaction (indicator)	0.079	0.000	0.058	0.000	0.000***	0.000***
Workplace-tie transaction (indicator)	0.065	0.000	0.047	0.000	0.000***	0.000***
Nonboard-tie transaction (indicator)	0.045	0.000	0.031	0.000	0.000***	0.000***
Board-tie transaction (indicator)	0.098	0.000	0.073	0.000	0.000***	0.000***

Table 3
Transaction-Level Analyses of Peer Insiders' Trading Profitability

Panel A of this table compares the market-adjusted abnormal buy-and-hold return over the 180 calendar days after the insider trading date (*BHAR180*), measured at the transaction level, of directors and officers of industry peer firms with competitors that become the targets of cyberattacks over the period 2005 to 2017 (i.e., peer insiders) between the pre- and post-disclosure periods. Peer firms are firms that have the same four-digit SIC code as the target firm. Panels B and C present estimates of ordinary least squares (OLS) regressions in which the dependent variable is *BHAR180*. In Panels A and B, the sample consists of 93,599 purchase and sales transactions made by 8,207 insiders of 1,329 industry peer firms. We require peer firms not to experience cyberattacks in a given year and to have at least one transaction during the pre- or post-disclosure period. In Panel C, the samples consist of 89,036 sales transactions made by 7,129 insiders of 1,177 industry peer firms and 4,554 purchase transactions made by 1,405 insiders of 638 industry peer firms. *Pre-disclosure period (indicator)* takes the value of one for transactions made during the period from 90 to one calendar days before the cyberattack disclosure date, and zero for transactions made during the period from one to 90 calendar days after the cyberattack disclosure date (i.e., post-disclosure period). Appendix A provides detailed descriptions of the construction of the variables. In Panel A, the numbers in parentheses are *p*-values for the *t* tests and the Wilcoxon signed-rank *z* tests that the mean and median *BHAR180* are equal to zero, respectively, and the numbers in brackets in the last two columns are *p*-values of the *t* tests for equality of the mean trading profitability and the Wilcoxon z tests for equality of the median *BHAR180*. In Panels B and C, *p*-values reported in parentheses are based on standard errors adjusted for heteroskedasticity and clustering at the peer firm and event level. ***, **, and * denote significance at the 1%, 5%, and 10% levels, respectively.

Panel A. Univariate results of peer insiders' trading profitability: Using the full sample of sales and purchase transactions

	Pre-disclosure period (N=44,639): a		Post-disclosure period (N=48,960): b		Test of difference: (a – b)	
	Mean	Median	Mean	Median	*t*-test	Wilcoxon *z*-test
BHAR180	0.020***	0.033***	-0.034***	-0.010***	0.054***	0.043***
	(0.000)	(0.000)	(0.000)	(0.000)	[0.000]	[0.000]

Panel B. OLS regressions of peer insiders' trading profitability: Using the pooled sample of sales and purchase transactions

	BHAR180		
Independent variable	(1)	(2)	(3)
Pre-disclosure period	0.045***	0.031**	0.034*
	(0.000)	(0.029)	(0.059)
Peer firm characteristics			
Firm size	-0.007	0.172***	0.187***
	(0.412)	(0.000)	(0.000)
Book-to-market	-0.002	-0.080	-0.090
	(0.954)	(0.373)	(0.295)
Prior six-month stock performance	-0.059	0.055	0.075
	(0.372)	(0.461)	(0.310)
Prior six-month stock return volatility	2.822	5.845	6.245
	(0.148)	(0.175)	(0.204)
Positive R&D	-0.011	0.069	0.022
	(0.807)	(0.568)	(0.873)
Missing R&D	-0.028	0.090	0.030
	(0.431)	(0.402)	(0.813)
Analyst coverage	0.032*	0.051	0.033
	(0.050)	(0.206)	(0.392)
Loss	-0.026	-0.028	-0.023
	(0.498)	(0.193)	(0.252)
Institutional block ownership	0.037	0.150	0.142
	(0.600)	(0.102)	(0.181)
Trade characteristics			
Daily trade size (%)	0.070	0.048	0.062
	(0.220)	(0.322)	(0.199)
Recent trade size (%)	-0.001	-0.015	0.002
	(0.954)	(0.545)	(0.931)
Dividend declaration	-0.007	0.000	0.004
	(0.835)	(0.981)	(0.811)
Earnings announcement	-0.009	-0.004	-0.005
	(0.698)	(0.846)	(0.786)
M&A announcement	0.036	0.034**	0.031*

	(0.110)	(0.046)	(0.062)
10K(Q) filing	-0.002	-0.005	-0.009
	(0.931)	(0.809)	(0.612)
Industry fixed effects	Yes	No	No
Firm fixed effects	No	Yes	Yes
Year fixed effects	Yes	Yes	No
Industry-by-year fixed effects	No	No	Yes
Number of observations	93,599	93,504	93,492
Adj. R^2	0.127	0.399	0.434

Panel C. OLS regressions of peer insiders' trading profitability: Using the subsamples of sales and purchase transactions

	BHAR180		
Independent variable	(1)	(2)	(3)
Subsample of sale transactions			
Pre-disclosure period	0.041***	0.026*	0.030*
	(0.001)	(0.059)	(0.081)
Control variables (same as in Panel B)	Yes	Yes	Yes
Industry fixed effects	Yes	No	No
Firm fixed effects	No	Yes	Yes
Year fixed effects	Yes	Yes	No
Industry-by-year fixed effects	No	No	Yes
Number of observations	89,036	88,950	88,939
Adjusted R^2	0.128	0.411	0.451
Subsample of purchase transactions			
Pre-disclosure period	0.059**	0.102***	0.093**
	(0.025)	(0.000)	(0.011)
Control variables (same as in Panel B)	Yes	Yes	Yes
Industry fixed effects	Yes	No	No
Firm fixed effects	No	Yes	Yes
Year fixed effects	Yes	Yes	No
Industry-by-year fixed effects	No	No	Yes
Number of observations	4,554	4,378	4,352
Adj. R^2	0.460	0.802	0.832

Table 4
Cross-Sectional Heterogeneity in Peer Insiders' Trading Profitability: Exposure of Target Firms and Peer Firms to Cyber Risk

This table presents estimates of ordinary least squares (OLS) regressions in which the dependent variable is the market-adjusted abnormal buy-and-hold return over the 180 calendar days after the insider trading date (*BHAR180*). The sample consists of 85,576 transactions (81,185 sales and 4,087 purchase transactions) made by directors and officers of 1,299 industry peer firms with competitors that become the targets of cyberattacks over the period 2005 to 2017 (i.e., peer insiders). Peer firms are firms that have the same four-digit SIC code as the target firm. We require peer firms not to experience cyberattacks in a given year and to have at least one transaction during the pre- or post-disclosure period. We also require that both the cumulative abnormal return for a target firm that experiences a cyberattack from one day before to one day after the cyberattack announcement date (target firm's CAR (-1, 1)) and the cumulative abnormal return for a peer firm from one day before to one day after the target firm's cyberattack announcement date (peer firm's CAR (-1, 1)) are available. *Pre-disclosure period (indicator)* takes the value of one for transactions made during the period from 90 to one calendar days before the cyberattack disclosure date, and zero for transactions made during the period from one to 90 calendar days after the cyberattack disclosure date (i.e., post-disclosure period). *Target firm's low CAR (-1, 1) (indicator)* takes the value of one if the target firm's CAR (-1, 1) is below the target firm's sample median CAR (-1, 1), and zero otherwise. *Peer firm's low CAR (-1, 1) (indicator)* takes the value of one if the peer firm's CAR (-1, 1) is below the peer firm's sample median CAR (-1, 1), and zero otherwise. Appendix A provides detailed descriptions of the construction of the variables. All regressions include controls used in the regression in Panel B of Table 3. We suppress the coefficient estimates on other independent variables to save space. *P*-values reported in parentheses are based on standard errors adjusted for heteroskedasticity and clustering at the peer firm and event level. ***, **, and * denote significance at the 1%, 5%, and 10% levels, respectively. a, b, and c in column (5) indicate significance at the 1%, 5%, and 10% levels, respectively, for the tests of coefficient equality between column (4) and column (5).

Panel A. Using a target firm's CAR (-1, 1) around its cyberattack disclosure date as a measure of the severity of cyberattacks

	BHAR180				
	Pooled sample			Subsample of sales	Subsample of purchases
Independent variable	(1)	(2)	(3)	(4)	(5)
Pre-disclosure period: a	0.016	0.010	0.009	0.004	0.032
	(0.202)	(0.455)	(0.513)	(0.775)	(0.255)
Target firm's low CAR (-1, 1): b	-0.031	0.006	0.064	0.079*	-0.180**
	(0.246)	(0.783)	(0.112)	(0.076)	(0.035)
a × b	0.063***	0.051***	0.054**	0.052*	0.095**
	(0.004)	(0.007)	(0.043)	(0.059)	(0.015)
Industry fixed effects	Yes	No	No	No	No
Firm fixed effects	No	Yes	Yes	Yes	Yes
Year fixed effects	Yes	Yes	No	No	No
Industry-by-year fixed effects	No	No	Yes	Yes	Yes
Number of observations	85,576	85,485	85,473	81,185	4,087
Adj. R^2	0.148	0.413	0.456	0.471	0.811

Panel B. Using a peer firm's CAR (-1, 1) around its rival firm's cyberattack announcement as a measure of its cyber risk exposure

	BHAR180				
	Pooled sample			Subsample of sales	Subsample of purchases
Independent variable	(1)	(2)	(3)	(4)	(5)
Pre-disclosure period: a	-0.007	-0.036	-0.036	-0.050	0.163***
	(0.810)	(0.307)	(0.351)	(0.202)	(0.009)
Peer firm's low CAR (-1, 1): b	0.010	0.014	0.019	0.024	-0.015
	(0.731)	(0.696)	(0.581)	(0.507)	(0.797)
a × b	0.104	0.135*	0.141*	0.156*	-0.137^{**a}
	(0.125)	(0.078)	(0.075)	(0.052)	(0.042)
Industry fixed effects	Yes	No	No	No	No
Firm fixed effects	No	Yes	Yes	Yes	Yes
Year fixed effects	Yes	Yes	No	No	No
Industry-by-year fixed effects	No	No	Yes	Yes	Yes
Number of observations	85,576	85,485	85,473	81,185	4,087
Adj. R^2	0.164	0.432	0.473	0.494	0.812

Table 5
Portfolio-Level Analyses of Peer Insiders' Trading Profitability

Panel A of this table compares the equally weighted average of the market-adjusted abnormal buy-and-hold return over the 180 calendar days after the insider trading date (*Portfolio BHAR180*), measured at the portfolio level, of directors and officers of industry peer firms with competitors that become the targets of cyberattacks over the period 2005 to 2017 (i.e., peer insiders) between the pre- and post-disclosure periods. For each cyberattack event, we construct the equally weighted portfolio of all transactions made by peer insiders in each period. Panel B presents estimates of ordinary least squares (OLS) regressions in which the dependent variable is *Portfolio BHAR180*. The sample consists of 512 portfolios of 1,329 industry peer firms that have the same four-digit SIC code as the target firm. We require peer firms not to experience cyberattacks in a given year and to have at least one transaction during the pre- or post-disclosure period. *Pre-disclosure period (indicator)* takes the value of one for the portfolio of transactions made during the period from 90 to one calendar days before the cyberattack disclosure date, and zero for the portfolio of transactions made during the period from one to 90 calendar days after the cyberattack disclosure date (i.e., post-disclosure period). Appendix A provides detailed descriptions of the construction of the variables. In Panel A, the numbers in parentheses are *p*-values for the *t* tests and the Wilcoxon signed-rank *z* tests that the mean and median trading profitability are equal to zero, respectively, and the numbers in brackets in the last two columns are *p*-values of the *t* tests for equality of the mean trading profitability and the Wilcoxon *z* tests for equality of the median trading profitability, respectively. In Panel B, *p*-values reported in parentheses are based on standard errors adjusted for heteroskedasticity and clustering at the event level. ***, **, and * denote significance at the 1%, 5%, and 10% levels, respectively.

Panel A. Univariate results of peer insiders' trading profitability

	Pre-disclosure period (N=254): a		Post-disclosure period (N=258): b		Test of difference (a - b)	
	Mean	Median	Mean	Median	*t*-test	Wilcoxon z-test
Portfolio BHAR180	0.029***	0.028***	-0.002	-0.001	0.031**	0.029**
	(0.001)	(0.001)	(0.833)	(0.840)	[0.012]	[0.012]

Panel B. OLS regressions of peer insiders' trading profitability

	Portfolio BHAR180	
Independent variable	(1)	(2)
Pre-disclosure period	0.028**	0.028**
	(0.011)	(0.011)
Target firm characteristics		
Firm size		(0.735)
		-0.006
Book-to-market		(0.814)
		-0.019
Prior six-month stock performance		(0.664)
		-0.628
Prior six-month stock return volatility		(0.553)
		0.066*
Positive R&D		(0.097)
		0.067*
Missing R&D		(0.071)
		0.002
Analyst coverage		(0.906)
		-0.007
Loss		(0.786)
		0.057
Institutional block ownership		(0.330)
		(0.735)
Industry (two-digit SIC codes) fixed effects	Yes	Yes
Year fixed effects	Yes	Yes
Number of observations	512	497
Adj. R^2	0.065	0.063

Table 6
Peer Insiders' Trading Profitability and Social Ties to Target Insiders

This table presents estimates of ordinary least squares (OLS) regressions in which the dependent variable is the market-adjusted abnormal buy-and-hold return over the 180 calendar days after the insider trading date (*BHAR180*). The sample consists of 92,689 transactions made by 8,064 directors and officers of 1,325 industry peer firms with competitors that become the targets of cyberattacks over the period 2005 to 2017 (i.e., peer insiders). Peer firms are firms that have the same four-digit SIC code as the target firm. We require peer firms not to experience cyberattacks in a given year and to have at least one transaction during the pre- or post-disclosure period. *Pre-disclosure period (indicator)* takes the value of one for transactions made during the period from 90 to one calendar days before the cyberattack disclosure date, and zero for transactions made during the period from one to 90 calendar days after the cyberattack disclosure date (i.e., post-disclosure period). *All-tie transaction (indicator)* takes the value of one for transactions made by a peer insider who is socially connected to a director or a senior executive of the target firm (i.e., a target insider) through nonworkplace ties (i.e., common educational background, memberships in the same non-business organizations) or workplace ties (i.e., current or prior common employment), and zero otherwise. *Nonworkplace-tie transaction (indicator)* takes the value of one for transactions made by a peer insider who is socially connected to target insiders exclusively through nonworkplace ties, and zero otherwise. *Workplace-tie transaction (indicator)* takes the value of one for transactions made by a peer insider who is socially connected to at least one target insider through workplace ties, and zero otherwise. *Nonboard-tie transaction (indicator)* takes the value of one for transactions made by a peer insider who is socially connected only to nonboard executives of the target firm, and zero otherwise. *Board-tie transaction (indicator)* takes the value of one for transactions made by a peer insider who is socially connected to at least one director of the target firm, and zero otherwise. Appendix A provides detailed descriptions of the construction of the variables. All regressions include controls used in the regression in Panel B of Table 3. We suppress the coefficient estimates on other independent variables to save space. *P*-values reported in parentheses are based on standard errors adjusted for heteroskedasticity and clustering at the peer firm and event level. ***, **, and * denote significance at the 1%, 5%, and 10% levels, respectively.

Panel A. Using *All-tie transactions* as the measure of social ties between peer insiders and target insiders

	BHAR180		
Independent variable	(1)	(2)	(3)
Pre-disclosure period: a	0.042***	0.026*	0.031
	(0.000)	(0.083)	(0.103)
All-tie transaction: b	-0.006	-0.011	-0.017
	(0.782)	(0.557)	(0.259)
a × b	0.020	0.039*	0.028
	(0.468)	(0.052)	(0.138)
Industry fixed effects	Yes	No	No
Firm fixed effects	No	Yes	Yes
Year fixed effects	Yes	Yes	No
Industry-by-year fixed effects	No	No	Yes
Number of observations	92,689	92,592	92,580
Adj. R^2	0.127	0.398	0.434

Panel B. Decomposing *All-tie transaction* according to whether peer and target insiders are connected through workplace ties

	BHAR180		
Independent variable	(1)	(2)	(3)
Pre-disclosure period: a	0.042***	0.026*	0.031*
	(0.000)	(0.076)	(0.098)
Nonworkplace-tie transaction: b	-0.041	-0.044*	-0.043**
	(0.161)	(0.052)	(0.041)
Workplace-tie transaction: c	0.040	0.042	0.026
	(0.203)	(0.152)	(0.312)
a × b	0.057*	0.061**	0.051**
	(0.086)	(0.033)	(0.044)
a × c	-0.026	0.006	-0.005
	(0.322)	(0.790)	(0.807)
F-test for equality of two coefficients (*p*-value): a × b = a × c	0.022**	0.137	0.058*
Industry fixed effects	Yes	No	No
Firm fixed effects	No	Yes	Yes
Year fixed effects	Yes	Yes	No
Industry-by-year fixed effects	No	No	Yes

Number of observations	92,689	92,592	92,580
Adj. R^2	0.128	0.399	0.435

Panel C. Decomposing *All-tie transaction* according to whether target insiders are directors of the target firm

	BHAR180		
Independent variable	(1)	(2)	(3)
Pre-disclosure period: a	0.042***	0.026*	0.031*
	(0.001)	(0.078)	(0.098)
Nonboard-tie transaction: b	-0.095**	-0.073**	-0.072**
	(0.034)	(0.028)	(0.026)
Board-tie transaction: c	0.033	0.018	0.009
	(0.106)	(0.386)	(0.636)
a × b	0.128**	0.125***	0.102***
	(0.013)	(0.001)	(0.001)
a × c	-0.027	-0.002	-0.008
	(0.222)	(0.880)	(0.609)
F-test for equality of two coefficients (*p*-value): a × b = a × c	0.004***	0.003***	0.001***
Industry fixed effects	Yes	No	No
Firm fixed effects	No	Yes	Yes
Year fixed effects	Yes	Yes	No
Industry-by-year fixed effects	No	No	Yes
Number of observations	92,689	92,592	92,580
Adj. R^2	0.129	0.400	0.435

Table 7
Effects of Social Ties and Target Firms' Litigation Risk on Peer Insiders' Trading Profitability

This table presents estimates of ordinary least squares (OLS) regressions in which the dependent variable is the market-adjusted abnormal buy-and-hold return over the 180 calendar days after the insider trading date (*BHAR180*). The sample consists of 92,689 transactions made by 8,064 directors and officers of 1,325 industry peer firms with competitors that become the targets of cyberattacks over the period 2005 to 2017 (i.e., peer insiders). Peer firms are firms that have the same four-digit SIC code as the target firm. We require peer firms not to experience cyberattacks in a given year and to have at least one transaction during the pre- or post-disclosure period. *Pre-disclosure period (indicator)* takes the value of one for transactions made during the period from 90 to one calendar days before the cyberattack disclosure date, and zero for transactions made during the period from one to 90 calendar days after the cyberattack disclosure date (i.e., post-disclosure period). *Nonworkplace-tie transaction (indicator)* takes the value of one for transactions made by a peer insider who is socially connected to target insiders (directors or senior executives of the target firm) exclusively through nonworkplace ties (i.e., common educational background, memberships in the same non-business organizations), and zero otherwise. *Workplace-tie transaction (indicator)* takes the value of one for transactions made by a peer insider who is socially connected to at least one target insider through workplace ties (i.e., current or prior common employment), and zero otherwise. *Nonboard-tie transaction (indicator)* takes the value of one for transactions made by a peer insider who is socially connected only to nonboard executives of the target firm, and zero otherwise. *Board-tie transaction (indicator)* takes the value of one for transactions made by a peer insider who is socially connected to at least one director of the target firm, and zero otherwise. *Common institutional blockholder* is a blockholder that holds shares in both the target firm and its peer firm. *High litigation industry* is a target firm operating in the biotechnology, computer hardware, or computer industry (Rogers and Stocken, 2005). *Liberal court score* is a score measuring the probability that a three-judge panel in the circuit court of the jurisdiction of the target firm's headquarters has at least two Democratic appointees (Huang et al., 2019). Appendix A provides detailed descriptions of the construction of the variables. All regressions include controls used in the regression in Panel B of Table 3. We suppress the coefficient estimates on *pre-disclosure period (indicator)*, *nonworkplace* (*workplace*)*-tie transaction (indicator)*, *nonboard* (*board*)*-tie transaction (indicator)*, and other independent variables to save space. *P*-values reported in parentheses are based on standard errors adjusted for heteroskedasticity and clustering at the peer firm and event level. a, b, and c indicate significance at the 1%, 5%, and 10% levels, respectively, for the tests of coefficient equality between odd and even columns. ***, **, and * denote significance at the 1%, 5%, and 10% levels, respectively.

	Common institutional blockholder				High litigation industry				Liberal court score			
	No	Yes	No	Yes	No	Yes	No	Yes	Low	High	Low	High
Independent variable	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)
Decomposing All-tie transaction according to whether target insiders are connected through workplace ties												
Pre-disclosure period × Nonworkplace-tie transaction	0.118***	-0.030^{b}	0.101***	-0.026^{b}	0.081**	-0.044^{a}	0.066**	-0.032^{b}	0.115**	0.037*	0.102**	0.034*
	(0.002)	(0.430)	(0.006)	(0.458)	(0.011)	(0.224)	(0.018)	(0.289)	(0.030)	(0.085)	(0.039)	(0.063)
Pre-disclosure period × Workplace-tie transaction	0.019	-0.005	0.015	-0.010	-0.007	0.009	-0.009	0.009	0.009	-0.014	0.010	-0.029
	(0.461)	(0.775)	(0.586)	(0.540)	(0.761)	(0.663)	(0.680)	(0.703)	(0.718)	(0.693)	(0.743)	(0.231)
Firm fixed effects	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Year fixed effects	Yes	Yes	No	No	Yes	Yes	No	No	Yes	Yes	No	No
Industry-by-year fixed effects	No	No	Yes	Yes	No	No	Yes	Yes	No	No	Yes	Yes
Number of observations	65,424	27,135	65,413	27,126	77,628	14,964	77,620	14,960	50,705	35,444	50,700	35,434
Adj. R^2	0.447	0.539	0.477	0.582	0.389	0.523	0.417	0.566	0.519	0.477	0.549	0.509
Decomposing All-tie transaction according to whether peer and target insiders are directors of the target firm												
Pre-disclosure period × Nonboard-tie transaction	0.162***	0.057^{*c}	0.140***	0.058*	0.148***	-0.023^{a}	0.120***	-0.024^{a}	0.188***	0.052^{b}	0.159***	0.049^{c}
	(0.000)	(0.099)	(0.000)	(0.095)	(0.000)	(0.327)	(0.001)	(0.269)	(0.000)	(0.120)	(0.001)	(0.118)
Pre-disclosure period × Board-tie transaction	0.031	-0.038^{*c}	0.024	-0.039^{*b}	-0.009	-0.029	-0.009	-0.016	0.001	0.001	0.007	-0.008
	(0.177)	(0.094)	(0.328)	(0.050)	(0.652)	(0.369)	(0.618)	(0.572)	(0.961)	(0.958)	(0.836)	(0.685)
Firm fixed effects	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Year fixed effects	Yes	Yes	No	No	Yes	Yes	No	No	Yes	Yes	No	No
Industry-by-year fixed effects	No	No	Yes	Yes	No	No	Yes	Yes	No	No	Yes	Yes
Number of observations	65,424	27,135	65,413	27,126	77,628	14,964	77,620	14,960	50,705	35,444	50,700	35,434
Adj. R^2	0.447	0.540	0.477	0.583	0.389	0.523	0.418	0.566	0.521	0.477	0.550	0.509

Table 8
Effects of Social Ties and Target Firms' Information Environment on Peer Insiders' Trading Profitability

This table presents estimates of ordinary least squares (OLS) regressions in which the dependent variable is the market-adjusted abnormal buy-and-hold return over the 180 calendar days after the insider trading date (*BHAR180*). The sample consists of 92,689 transactions made by directors and officers of 1,325 industry peer firms with competitors that become the targets of cyberattacks over the period 2005 to 2017 (i.e., peer insiders). Peer firms are firms that have the same four-digit SIC code as the target firm. We require peer firms not to experience cyberattacks in a given year and to have at least one transaction during the pre- or post-disclosure period. *Pre-disclosure period (indicator)* takes the value of one for transactions made during the period from 90 to one calendar days before the cyberattack disclosure date, and zero for transactions made during the period from one to 90 calendar days after the cyberattack disclosure date (i.e., post-disclosure period). *Nonworkplace-tie transaction (indicator)* takes the value of one for transactions made by a peer insider who is socially connected to target insiders (directors or senior executives of the target firm) exclusively through nonworkplace ties (i.e., common educational background, memberships in the same non-business organizations), and zero otherwise. *Workplace-tie transaction (indicator)* takes the value of one for transactions made by a peer insider who is socially connected to at least one target insider through workplace ties (i.e., current or prior common employment), and zero otherwise. *Nonboard-tie transaction (indicator)* takes the value of one for transactions made by a peer insider who is socially connected only to nonboard executives of the target firm, and zero otherwise. *Board-tie transaction (indicator)* takes the value of one for transactions made by a peer insider who is socially connected to at least one director of the target firm, and zero otherwise. *Firm age* is a target firm's age. *Absolute discretionary accrual* is a target firm's absolute discretionary accrual estimated using the modified Jones model (Dechow, Sloan, and Sweeney, 1995). *Positive R&D* is a target firm with positive R&D expenditures. Appendix A provides detailed descriptions of the construction of the variables. All regressions include controls used in the regression in Panel B of Table 3. We suppress the coefficient estimates on *pre-disclosure period (indicator)*, *nonworkplace* (*workplace*)*-tie transaction (indicator)*, *nonboard* (*board*)*-tie transaction (indicator)*, and other independent variables to save space. *P*-values reported in parentheses are based on standard errors adjusted for heteroskedasticity and clustering at the peer firm and event level. a, b, and c indicate significance at the 1%, 5%, and 10% levels, respectively, for the tests of coefficient equality between odd and even columns. ***, **, and * denote significance at the 1%, 5%, and 10% levels, respectively.

	Firm age				Absolute discretionary accruals				Positive R&D			
	Young	Old	Young	Old	High	Low	High	Low	Yes	No	Yes	No
Independent variable	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)
Decomposing All-tie transaction according to whether target insiders are connected through workplace ties												
Pre-disclosure period × Nonworkplace-tie transaction	0.139**	0.000^{b}	0.116**	0.012^{c}	0.186***	0.013^{b}	0.169***	0.015^{a}	0.067**	0.024	0.057**	0.006^{c}
	(0.024)	(0.994)	(0.031)	(0.593)	(0.000)	(0.591)	(0.000)	(0.506)	(0.038)	(0.560)	(0.028)	(0.868)
Pre-disclosure period × Workplace-tie transaction	-0.026	0.019	-0.021	0.002	0.001	0.026	0.002	0.008	-0.030	0.026	-0.029	0.030
	(0.648)	(0.421)	(0.709)	(0.927)	(0.976)	(0.371)	(0.947)	(0.761)	(0.156)	(0.327)	(0.116)	(0.250)
Firm fixed effects	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Year fixed effects	Yes	Yes	No	No	Yes	Yes	No	No	Yes	Yes	No	No
Industry-by-year fixed effects	No	No	Yes	Yes	No	No	Yes	Yes	No	No	Yes	Yes
Number of observations	37,661	48,694	37,660	48,680	41,906	43,926	41,903	43,917	68,583	17,778	68,579	17,769
Adj. R^2	0.393	0.571	0.403	0.607	0.500	0.543	0.514	0.591	0.434	0.602	0.462	0.648
Decomposing All-tie transaction according to whether peer and target insiders are directors of the target firm												
Pre-disclosure period × Nonboard-tie transaction	0.165***	0.038^{b}	0.136***	0.037^{c}	0.239***	0.049^{*a}	0.211***	0.042^{a}	0.137***	0.035^{b}	0.114***	0.002^{a}
	(0.004)	(0.269)	(0.004)	(0.262)	(0.000)	(0.059)	(0.000)	(0.121)	(0.002)	(0.390)	(0.001)	(0.932)
Pre-disclosure period × Board-tie transaction	0.003	0.004	0.005	0.000	0.036	0.005	0.038	-0.002	-0.031	0.019	-0.027	0.020
	(0.967)	(0.846)	(0.946)	(0.989)	(0.432)	(0.819)	(0.400)	(0.906)	(0.107)	(0.582)	(0.141)	(0.543)
Firm fixed effects	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Year fixed effects	Yes	Yes	No	No	Yes	Yes	No	No	Yes	Yes	No	No
Industry-by-year fixed effects	No	No	Yes	Yes	No	No	Yes	Yes	No	No	Yes	Yes
Number of observations	37,661	48,694	37,660	48,680	41,906	43,926	41,903	43,917	68,583	17,778	68,579	17,769
Adj. R^2	0.394	0.571	0.403	0.607	0.500	0.544	0.514	0.591	0.435	0.603	0.463	0.649

Table 9
Effects of Peer Firms' Information Environment on Peer Insiders' Trading Profitability

This table presents estimates of ordinary least squares (OLS) regressions in which the dependent variable is the market-adjusted abnormal buy-and-hold return over the 180 calendar days after the insider trading date (*BHAR180*). The sample consists of 92,689 transactions made by directors and officers of 1,325 industry peer firms with competitors that become the targets of cyberattacks over the period 2005 to 2017 (i.e., peer insiders). Peer firms are firms that have the same four-digit SIC code as the target firm. We require peer firms not to experience cyberattacks in a given year and to have at least one transaction during the pre- or post-disclosure period. *Pre-disclosure period (indicator)* takes the value of one for transactions made during the period from 90 to one calendar days before the cyberattack disclosure date, and zero for transactions made during the period from one to 90 calendar days after the cyberattack disclosure date (i.e., post-disclosure period). *Nonworkplace-tie transaction (indicator)* takes the value of one for transactions made by a peer insider who is socially connected to target insiders (directors or senior executives of the target firm) exclusively through nonworkplace ties (i.e., common educational background, memberships in the same non-business organizations), and zero otherwise. *Workplace-tie transaction (indicator)* takes the value of one for transactions made by a peer insider who is socially connected to at least one target insider through workplace ties (i.e., current or prior common employment), and zero otherwise. *Nonboard-tie transaction (indicator)* takes the value of one for transactions made by a peer insider who is socially connected only to nonboard executives of the target firm, and zero otherwise. *Board-tie transaction (indicator)* takes the value of one for transactions made by a peer insider who is socially connected to at least one director of the target firm, and zero otherwise. *Firm age* is a peer firm's age. *Absolute discretionary accrual* is a peer firm's absolute discretionary accrual estimated using the modified Jones model (Dechow, Sloan, and Sweeney, 1995). *Positive R&D* is a peer firm with positive R&D expenditures. Appendix A provides detailed descriptions of the construction of the variables. All regressions include controls used in the regression in Panel B of Table 3. We suppress the coefficient estimates on *pre-disclosure period (indicator)*, *nonworkplace* (*workplace*)*-tie transaction (indicator)*, *nonboard* (*board*)*-tie transaction (indicator)*, and other independent variables to save space. *P*-values reported in parentheses are based on standard errors adjusted for heteroskedasticity and clustering at the peer firm and event level. a, b, and c indicate significance at the 1%, 5%, and 10% levels, respectively, for the tests of coefficient equality between odd and even columns. ***, **, and * denote significance at the 1%, 5%, and 10% levels, respectively.

	Firm age				Absolute discretionary accruals				Positive R&D			
	Young	Old	Young	Old	High	Low	High	Low	Yes	No	Yes	No
Independent variable	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)
Decomposing All-tie transaction according to whether target insiders are connected through workplace ties												
Pre-disclosure period × Nonworkplace-tie transaction	0.159***	0.004^{b}	0.146***	0.001^{b}	0.124**	0.033	0.107**	0.023	0.052*	0.094	0.065**	0.026
	(0.000)	(0.868)	(0.001)	(0.970)	(0.020)	(0.227)	(0.040)	(0.387)	(0.059)	(0.124)	(0.018)	(0.571)
Pre-disclosure period × Workplace-tie transaction	0.035	0.016	0.021	0.011	0.033	-0.032	0.012	-0.031	-0.035	0.074^{**b}	-0.030	0.066^{*b}
	(0.364)	(0.553)	(0.583)	(0.702)	(0.315)	(0.263)	(0.745)	(0.270)	(0.148)	(0.016)	(0.164)	(0.056)
Firm fixed effects	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Year fixed effects	Yes	Yes	No	No	Yes	Yes	No	No	Yes	Yes	No	No
Industry-by-year fixed effects	No	No	Yes	Yes	No	No	Yes	Yes	No	No	Yes	Yes
Number of observations	44,773	47,801	44,767	47,790	45,872	45,864	45,871	45,852	66,038	26,550	66,031	26,537
Adjusted R^2	0.472	0.445	0.499	0.517	0.429	0.588	0.448	0.638	0.402	0.517	0.427	0.597
Decomposing All-tie transaction according to whether peer and target insiders are directors of the target firm												
Pre-disclosure period × Nonboard-tie transaction	0.255***	0.066^{**a}	0.220***	0.067^{**b}	0.172**	0.091**	0.151**	0.072*	0.081*	0.216***	0.090**	0.143***
	(0.000)	(0.036)	(0.000)	(0.033)	(0.011)	(0.011)	(0.021)	(0.064)	(0.051)	(0.000)	(0.039)	(0.001)
Pre-disclosure period × Board-tie transaction	0.039	-0.012	0.040	-0.021	0.035	-0.025^{c}	0.017	-0.025	-0.015	0.004	-0.005	-0.015
	(0.271)	(0.594)	(0.301)	(0.320)	(0.300)	(0.307)	(0.639)	(0.241)	(0.425)	(0.884)	(0.785)	(0.614)
Firm fixed effects	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Year fixed effects	Yes	Yes	No	No	Yes	Yes	No	No	Yes	Yes	No	No
Industry-by-year fixed effects	No	No	Yes	Yes	No	No	Yes	Yes	No	No	Yes	Yes
Number of observations	44,773	47,801	44,767	47,790	45,872	45,864	45,871	45,852	66,038	26,550	66,031	26,537
Adjusted R^2	0.473	0.444	0.500	0.517	0.430	0.588	0.448	0.638	0.402	0.523	0.427	0.600

Table 10
Peer Insiders' Trading Profitability and SEC's 2011 Guidance on Disclosure of Cybersecurity Risk

The table presents estimates of ordinary least squares (OLS) regressions in which the dependent variable is the market-adjusted abnormal buy-and-hold return over the 180 calendar days after the insider trading date (BHAR180). The sample consists of 93,599 transactions made by directors and officers of 1,329 industry peer firms with competitors that become the targets of cyberattacks over the period 2005 to 2017 (i.e., peer insiders). Peer firms are firms that have the same four-digit SIC code as the target firm. We require peer firms not to experience cyberattacks in a given year and to have at least one transaction during the pre- or post-disclosure period. *Pre-disclosure period (indicator)* takes the value of one for transactions made during the period from 90 to one calendar days before the cyberattack disclosure date, and zero for transactions made during the period from one to 90 calendar days after the cyberattack disclosure date (i.e., post-disclosure period). *Post-SEC guidance (indicator)* takes the value of one for transactions made on October 13, 2011 (the Securities and Exchange Commission's (SEC's) issuance date of the guidance on disclosure obligations relating to cybersecurity risks and incidents) and onward), and zero otherwise. *Nonworkplace-tie transaction (indicator)* takes the value of one for transactions made by a peer insider who is socially connected to target insiders exclusively through nonworkplace ties, and zero otherwise. *Workplace-tie transaction (indicator)* takes the value of one for transactions made by a peer insider who is socially connected to at least one target insider through workplace ties, and zero otherwise. *Nonboard-tie transaction (indicator)* takes the value of one for transactions made by a peer insider who is socially connected only to nonboard executives of the target firm, and zero otherwise. *Board-tie transaction (indicator)* takes the value of one for transactions made by a peer insider who is socially connected to at least one director of the target firm, and zero otherwise. Appendix A provides detailed descriptions of the construction of the variables. All regressions include controls used in the regression in Panel B of Table 3. We suppress the coefficient estimates on other independent variables to save space. *P*-values reported in parentheses are based on standard errors adjusted for heteroskedasticity and clustering at the peer firm and event level. a, b, and c indicate significance at the 1%, 5%, and 10% levels, respectively, for the tests of coefficient equality between odd and even columns. ***, **, and * denote significance at the 1%, 5%, and 10% levels, respectively.

Panel A. Peer insiders' trading profitability and SEC's 2011 guidance on disclosure of cyber-security risk

	BHAR180	
Independent variable	(1)	(2)
Pre-disclosure period: a	0.057***	0.063**
	(0.002)	(0.013)
Post-SEC guidance: b	0.031	0.049
	(0.358)	(0.184)
a × b	-0.045**	-0.052**
	(0.010)	(0.025)
Firm fixed effects	Yes	Yes
Year fixed effects	Yes	No
Industry-by-year fixed effects	No	Yes
Number of observations	93,504	93,492
Adj. R^2	0.400	0.436

Panel B. Effects of social ties on peer insiders' trading profitability in the pre- and post-SEC guidance periods

	BHAR180			
	Pre-guidance	Post-guidance	Pre-guidance	Post-guidance
Independent variable	(1)	(2)	(3)	(4)
Decomposing All-tie transaction according to whether target insiders are connected through workplace ties				
Pre-disclosure period × Nonworkplace-tie transaction	0.156**	0.029c	0.122*	0.029c
	(0.015)	(0.248)	(0.055)	(0.229)
Pre-disclosure period × Workplace-tie transaction	0.027	0.013	0.041	0.002
	(0.470)	(0.615)	(0.296)	(0.928)
Firm fixed effects	Yes	Yes	Yes	Yes
Year fixed effects	Yes	Yes	No	No
Industry-by-year fixed effects	No	No	Yes	Yes
Number of observations	43,773	48,791	43,770	48,782
Adj. R^2	0.497	0.416	0.520	0.459
Decomposing All-tie transaction according to whether peer and target insiders are directors of the target firm				
Pre-disclosure period × Nonboard-tie transaction	0.223***	0.073**b	0.175***	0.069**b
	(0.001)	(0.012)	(0.003)	(0.039)
Pre-disclosure period × Board-tie transaction	0.030	0.001	0.038	-0.003
	(0.480)	(0.980)	(0.387)	(0.856)
Firm fixed effects	Yes	Yes	Yes	Yes
Year fixed effects	Yes	Yes	No	No
Industry-by-year fixed effects	No	No	Yes	Yes
Number of observations	43,773	48,791	43,770	48,782
Adj. R^2	0.498	0.417	0.521	0.459

Table 11
Peer Insider-level Analyses of Trading Volume

This table presents estimates of ordinary least squares (OLS) regressions in which the dependent variables are two measures of transaction volume of directors and officers of industry peer firms with competitors that become the targets of cyberattacks over the period 2005 to 2017 (i.e., peer insiders) in the pre- and post-disclosure periods. Peer firms are firms that have the same four-digit SIC code as the target firm. We require peer firms not to experience cyberattacks in a given year and to have at least one transaction during the pre- or post-disclosure period. In Panels A and B, the dependent variables are the number of shares sold by peer insiders scaled by the number of shares outstanding and the dollar value of shares sold by peer insiders scaled by market capitalization, respectively. We aggregate each peer insider's transaction volume in the pre- and post-disclosure periods separately and use this aggregate volume as a measure of transaction volume. In both panels, column (1) uses a pooled sample of 25,696 aggregate transactions made by 8,207 peer insiders of 1,329 peer firms in the pre- and post-disclosure periods. Column (2) uses a subsample of aggregate transactions made by only *all-tier peer insiders* (i.e., peer insiders who are socially connected to directors or senior executives of the target firm (i.e., a target insider)). Columns (3) and (4) use subsamples of aggregate transactions made by *nonworkplace-tie peer insiders* (i.e., peer insiders who are socially connected to target insiders exclusively through nonworkplace ties (common educational background, memberships in the same nonbusiness organizations)) and *workplace-tie peer insiders* (i.e., peer insiders who are socially connected to at least one target insider through workplace ties (current or prior common employment)), respectively. Columns (5) and (6) use subsamples of aggregate transactions made by *nonboard-tie peer insiders* (i.e., peer insiders who are socially connected only to nonboard executives of the target firm) and board-tie peer insiders (i.e., peer insiders who are socially connected to at least one director of the target firm), respectively. When peer insiders do not make any transactions in the pre-disclosure (post-disclosure period), we set their trading volume in the pre-disclosure (post-disclosure period) to be zero. *Pre-disclosure period (indicator)* takes the value of one for transactions made during the period from 90 to one calendar days before the cyberattack disclosure date, and zero for transactions made during the period from one to 90 calendar days after the cyberattack disclosure date (i.e., post-disclosure period). All regressions include firm-level controls used in the regression in Panel B of Table 3. We suppress the coefficient estimates on other independent variables to save space. *P*-values reported in parentheses are based on standard errors adjusted for heteroskedasticity and clustering at the peer firm and event level. a, b, and c indicate significance at the 1%, 5%, and 10% levels, respectively, for the tests of coefficient equality between odd and even columns. ***, **, and * denote significance at the 1%, 5%, and 10% levels, respectively.

Panel A. Using the number of shares sold by peer insiders scaled by the number of shares outstanding as a measure of transaction volume

	Number of shares sold by peer insiders / number of total shares outstanding (%)					
	Pooled sample	Subsample				
	All peer insiders	All-tie peer insiders	Nonworkplace-tie peer insiders	Workplace-tie peer insiders	Nonboard-tie peer insiders	Board-tie peer insiders
Independent variable	(1)	(2)	(3)	(4)	(5)	(6)
Pre-disclosure period	0.004	0.010*	0.015**	0.004	0.024**	0.006
	(0.149)	(0.059)	(0.033)	(0.571)	(0.027)	(0.323)
Event fixed effects	Yes	Yes	Yes	Yes	Yes	Yes
Firm fixed effects	Yes	Yes	Yes	Yes	Yes	Yes
Year fixed effects	Yes	Yes	Yes	Yes	Yes	Yes
Number of observations	25,696	2,796	1,619	1,169	825	1,969
Adj. R^2	0.065	0.190	0.293	-0.157	0.359	0.155

Panel B. Using dollar value of shares sold by peer insiders scaled by market capitalization as a measure of transaction volume

	Dollar value of shares sold by peer insiders / market capitalization (%)					
	Pooled sample	Subsample				
	All peer insiders	All-tie peer insiders	Nonworkplace-tie peer insiders	Workplace-tie peer insiders	Nonboard-tie peer insiders	Board-tie peer insiders
Independent variable	(1)	(2)	(3)	(4)	(5)	(6)
Pre-disclosure period	0.003	0.012*	0.017*	0.006	0.028**	0.007
	(0.530)	(0.075)	(0.055)	(0.499)	(0.026)	(0.359)
Event fixed effects	Yes	Yes	Yes	Yes	Yes	Yes
Firm fixed effects	Yes	Yes	Yes	Yes	Yes	Yes
Year fixed effects	Yes	Yes	Yes	Yes	Yes	Yes
Number of observations	25,696	2,796	1,619	1,169	825	1,969
Adj. R^2	0.048	0.229	0.322	-0.183	0.395	0.175

Appendix A
Variable Definitions

This appendix provides detailed descriptions of all variables used in the tables.

Variable	Definition	Source
10K(Q) filing (indicator)	One if transactions are made within 30 calendar days prior to 10-K or 10-Q filing dates, and zero otherwise	EDGAR
All-tie peer insider (indicator)	One for a peer insider who is socially connected to target insiders, and zero otherwise. We consider board members and senior executives whose titles include CEO, CFO, CIO, COO, president, executive vice president, senior vice president, managing director, and treasurer to be target insiders.	BoardEx, Thomson Reuters Insider Filing Data
All-tie transaction (indicator)	One for transactions made by a peer insider who is socially connected to a director or a senior executive of the target firm (i.e., a target insider) through nonworkplace ties (i.e., common educational background, memberships in the same non-business organizations) or workplace ties (i.e., current or prior common employment), and zero otherwise	BoardEx, Thomson Reuters Insider Filing Data
Analyst coverage	Natural logarithm of one plus the number of analysts who issue annual earnings per share (EPS) forecasts	I/B/E/S
Board-tie peer insider (indicator)	One for a peer insider who is socially connected to at least one director of the target firm, and zero otherwise	BoardEx, Thomson Reuters Insider Filing Data
Board-tie transaction (indicator)	One for transactions made by a peer insider who is socially connected to at least one director of the target firm, and zero otherwise	BoardEx, Thomson Reuters Insider Filing Data
Book-to-market	Ratio of the book value of equity to the market value of equity	Compustat
Cyberattack (indicator)	One if a firm experiences hacking or malware-electronic entry by an outside party, malware, or spyware, and zero otherwise	PRC, Audit Analytics
Daily trade size	Absolute value of the net number of shares purchased by all insiders of a firm on the transaction date divided by the total number of shares outstanding of the firm (in percentage)	Thomson Reuters Insider Filing Data
Dividend declaration (indicator)	One if transactions are made within 30 calendar days prior to dividend declaration dates, and zero otherwise	CRSP
Earnings announcement (indicator)	One if transactions are made within 30 calendar days prior to earnings announcement dates, and zero otherwise	Compustat
Firm size	Natural logarithm of the market value of equity	Compustat
Institutional block ownership	Number of shares held by institutional shareholders that own more than 5% of an industry peer firm's equity scaled by the total number of shares outstanding	Thomson Reuters 13F Data
Loss (indicator)	One if a firm's net income before extraordinary items is negative, and zero otherwise	Compustat
M&A announcement (indicator)	One if transactions are made within 30 calendar days prior to merger and acquisition (M&A) announcement dates, and zero otherwise	SDC
Missing R&D (indicator)	One if the R&D expenditure is missing, and zero otherwise	Compustat
Nonboard-tie peer insider (indicator)	One for a peer insider who is socially connected only to nonboard executives of the target firm, and zero otherwise	BoardEx, Thomson Reuters Insider Filing Data
Nonboard-tie transaction (indicator)	One for transactions made by a peer insider who is socially connected only to nonboard executives of the target firm, and zero otherwise	BoardEx, Thomson Reuters Insider Filing Data
Nonworkplace-tie peer insider (indicator)	One for a peer insider who is socially connected to target insiders exclusively through nonworkplace ties, and zero otherwise	BoardEx, Thomson Reuters Insider Filing Data
Nonworkplace-tie transaction (indicator)	One for transactions made by a peer insider who is socially connected to target insiders exclusively through nonworkplace ties, and zero otherwise	BoardEx, Thomson Reuters Insider Filing Data
Number of analysts	Number of analysts who cover the firm in a given year	IBES
Peer firm's low CAR (-1, 1) (indicator)	One if the CAR (-1, 1) for an industry peer of the target firm around the cyberattack announcement date is below the sample median, and zero otherwise	CRSP, PRC, Audit Analytics

Variable	Definition	Source
Positive R&D (indicator)	One if the R&D expenditure is positive, and zero otherwise	Compustat
Post-disclosure period (indicator)	One for transactions made during the period from one to 90 calendar days after the cyberattack disclosure date, and zero otherwise	Audit Analytics, Thomson Reuters Insider Filing Data
Post-SEC guidance (indicator)	One for transactions made on October 13, 2011 (the SEC's issuance date of the guidance on disclosure obligations relating to cybersecurity risks and incidents) and onward, and zero otherwise	SEC
Pre-disclosure period (indicator)	One for transactions made during the period from 90 to one calendar days before the cyberattack disclosure date, and zero otherwise.	PRC, Audit Analytics, Thomson Reuters Insider Filing Data
Prior six-month stock performance	Market-adjusted abnormal buy-and-hold return over the 180 calendar days prior to the insider trading date, where the CRSP value-weighted index is used as a proxy for the market portfolio	CRSP
Prior six-month stock return volatility	Standard deviation of daily stock returns over the 180 calendar days prior to the insider trading date	CRSP
Recent trade size	Sum of absolute values of the daily net numbers of shares purchased by all insiders of a firm during the ten days prior to the transaction date, scaled by the number of total shares outstanding (in percentage)	Thomson Reuters Insider Filing Data
Stock performance	Market-adjusted abnormal buy-and-hold return for a given year	CRSP
Stock return volatility	Standard deviation of daily stock returns during a fiscal year	CRSP
Target firm's low CAR (-1, 1) (indicator)	One if the cumulative abnormal returns from one day before to one day after the cyberattack announcement date (CAR (-1, 1)) for a target firm is below the sample median, and zero otherwise. Abnormal returns are computed with the market model that is estimated with 220 trading days of return data beginning 280 days before and ending 61 days before the cyberattack announcement. We use the CRSP value-weighted return as a proxy for the market portfolio return.	CRSP, PRC, Audit Analytics
Workplace-tie insider (indicator)	One for a peer insider who is socially connected to at least one target insider through workplace ties, and zero otherwise	BoardEx, Thomson Reuters Insider Filing Data
Workplace-tie transaction (indicator)	One for transactions made by a peer insider who is socially connected to at least one target insider through workplace ties, and zero otherwise	BoardEx, Thomson Reuters Insider Filing Data

Appendix B
Target Firms' Insider Trading Profitability

Panel A of this table presents descriptive statistics for 116 treated firms that experience a cyberattack over the period 2005 to 2017 and their matched 116 control firms that do not experience a cyberattack over the same period. The propensity score is calculated using a logit regression of *Cyberattack* (an indicator that takes the value of one if a firm becomes a target of cyberattacks, and zero otherwise) on firm size, book-to-market, stock performance, stock return volatility, positive R&D (indicator), missing R&D (indicator), analyst coverage, loss (indicator), and institutional block ownership. We require both treatment and control firms to be in the same industry (i.e., to have the same two-digit SIC code) and in the same fiscal year. We also require these firms to be covered in Compustat and CRSP and to have at least one transaction during the pre- or post-disclosure period. Panel B presents estimates of ordinary least squares (OLS) regressions in which the dependent variable is the market-adjusted abnormal buy-and-hold return over the 180 calendar days after the insider trading date (*BHAR180*). The sample consists of 13,269 transactions made by insiders (i.e., directors and officers) of 116 treatment firms and 116 control firms during the pre- and post-disclosure periods. *Cyberattack (indicator)* takes the value of one if a firm experiences a cyberattack, and zero otherwise. *Pre-disclosure period* (indicator) takes the value of one for transactions made in the period from 90 to one calendar days before the disclosure date, and zero for transactions made in the period from one to 90 calendar days after the cyberattack disclosure date (i.e., post-disclosure period). *Low liberal court score* takes the value of one if the target firm's liberal court score is below the sample median liberal court score, and zero otherwise. The score is measured by the probability that a three-judge panel in the circuit court of the jurisdiction of the target firm's headquarters has at least two Democratic appointees (Huang et al., 2019). All regressions include controls used in the regression in Panel B of Table 3. We suppress the coefficient estimates on other independent variables to save space. Appendix A provides detailed descriptions of the construction of the variables. *P*-values reported in parentheses are based on standard errors clustered at the firm level. ***, **, and * denote significance at the 1%, 5%, and 10% levels, respectively.

Panel A. Descriptive statistics for propensity-score matched sample firms

	Treatment firms with a cyberattack (N=116): a		Control firms without a cyberattack (N=116): b		Test of difference (a − b): *p*-value	
Variable	Mean	Median	Mean	Median	*t*-test	Wilcoxon *z*-test
Firm size	9.840	9.828	9.755	9.818	0.684	0.668
Book-to-market	0.288	0.270	0.318	0.269	0.343	0.882
Stock performance	0.084	0.038	0.077	0.048	0.855	0.843
Stock return volatility	0.018	0.017	0.018	0.017	0.656	0.914
Positive R&D (indicator)	0.526	1.000	0.483	0.000	0.514	0.512
Missing R&D (indicator)	0.379	0.000	0.422	0.000	0.505	0.504
Analyst coverage	2.989	3.121	2.880	3.010	0.148	0.139
Loss (indicator)	0.103	0.000	0.060	0.000	0.233	0.232
Institutional block ownership	0.184	0.163	0.189	0.175	0.792	0.710

Panel B. OLS regressions of target insiders' trading profitability

	BHAR180					
Independent variable	(1)	(2)	(3)	(4)	(5)	(6)
Cyberattack: a	-0.071***	-0.010	0.009	-0.009	-0.019	0.061
	(0.000)	(0.753)	(0.859)	(0.707)	(0.638)	(0.107)
Pre-disclosure period: b	-0.009	0.001	-0.001	0.003	0.009	0.010
	(0.699)	(0.945)	(0.962)	(0.887)	(0.667)	(0.641)
Low liberal court score: c				-0.038	-0.216***	0.030
				(0.310)	(0.000)	(0.458)
a × b	0.134***	0.125***	0.127***	0.045	0.038	0.032
	(0.000)	(0.000)	(0.000)	(0.214)	(0.302)	(0.400)
a × c				-0.139**	-0.005	-0.115
				(0.022)	(0.961)	(0.151)
b × c				-0.050	-0.051*	-0.050
				(0.135)	(0.096)	(0.110)
a × b × c				0.182**	0.185**	0.191**
				(0.021)	(0.026)	(0.022)
Industry fixed effects	Yes	No	No	Yes	No	No
Firm fixed effects	No	Yes	Yes	No	Yes	Yes
Year fixed effects	Yes	Yes	No	Yes	Yes	No
Industry-by-year fixed effects	No	No	Yes	No	No	Yes
Number of observations	13,269	13,269	13,269	13,104	13,104	13,104
Adj. R^2	0.638	0.732	0.748	0.671	0.768	0.782