Digital Insiders and Informed Trading Before Earnings Announcements

Henk Berkman [a]
Jonathan Jona [b*]
Gladys Lee [c]
Naomi Soderstrom [d]

Draft date: 28 November 2019

[a] The University of Auckland & The University of Sydney, Owen G Glenn Building, Auckland 1010, New Zealand. Email: h.berkman@auckland.ac.nz
[b] Freeman School of Business, Tulane University. 7 McAlister Dr, S, New Orleans, LA 70118. Email: jjona@tulane.edu
[c] The University of Melbourne, 198 Berkeley Street, Parkville, 3010, Victoria Melbourne. Email: gladys.lee@unimelb.edu.au
[d] The University of Melbourne, 198 Berkeley Street, Parkville, 3010, Victoria Melbourne. Email: naomiss@unimelb.edu.au

[*] Corresponding author.
We are grateful to Jackie Cook from CookESG Research for her help in extracting the cybersecurity excerpts. We also thank Angelo Angelis, Mary Barth, Kasper Jønsson, Katherine Schipper and workshop participants at Aarhus University, Copenhagen Business School, Lingnan University, [illegible] dney for their valuable insights. We thank Marco Lugstei, James Kavourakis, and Rachel Soderstrom for research assistance.

Funding: Jona acknowledges the financial support provided by the University of Melbourne through an Early Career Researcher grant.

Provided by ScholarSpace at University of Hawai'i at Manoa
CORE
Metadata, citation and similar papers at core.ac.uk

Digital Insiders and Informed Trading Before Earnings Announcements

Abstract

While it is widely acknowledged that companies face increasing cybersecurity risk stemming from hackers stealing customer information, a relatively unknown cybersecurity risk is from information leakage and subsequent trading by digital insiders – hackers who target corporations to obtain non-public corporate information for illegal trading. We use a firm-specific measure of cybersecurity risk mitigation based on textual analysis of 10-Ks to proxy for the organization's ability to reduce the probability of digital insider trading. We find that a larger share of new earnings information is incorporated into prices prior to earnings announcements for firms with low cybersecurity risk mitigation scores. We also find that pre-announcement trading by short sellers is more predictive of earnings surprises for firms with low cybersecurity risk mitigation. Further, on days closer to earnings announcements, firms with relatively low cybersecurity risk mitigation scores experience a larger increase in bid-ask spreads, particularly the adverse selection component. These results suggest that weak cybersecurity risk mitigation provides opportunities for acquisition of private information and that trading by privately informed traders is more likely in stocks of firms with higher exposure to cybercrimes.

JEL classification: G14, G18, K24, M48, M41

*Keywords***:** liquidity, cybersecurity, cybersecurity risk disclosure, adverse selection, bid ask spread, probability of informed trading, private information, hacking, cybersecurity risk mitigation, price jump ratio, textual analysis, short selling.

Digital Insiders and Informed Trading Before Earnings Announcements

1. Introduction

There is an increasing number of cases where "hackers" of corporate information systems obtain proprietary firm data and use this information to conduct illegal stock market trades.[1] Fin4, which is a group of hackers that has been operating since at least 2013, is a prominent example. Fin4 hackers illegally obtained data for trading purposes from more than 100 companies, systematically targeting employees such as C-level executives, legal counsel, and risk and compliance personnel, who might possess value-relevant non-public information.[2] Rather than installing malware or ransomware to get a payout, these 'digital insiders' (Carson 2017) steal identities (e.g., through phishing emails) to obtain access to privileged accounts. Once the cybercriminals insinuate themselves into the firm's system, they install hidden surveillance tools to gather valuable undisclosed information, which can subsequently be exploited in the stock market.[3] While these activities are potentially very damaging to the integrity of financial markets, it is difficult to establish their impact due to their secretive nature. In this paper, we examine whether firm cybersecurity risk mitigation affects differences in the extent to which private information is traded on and is reflected in prices prior to earnings announcements.

---

[1] https://www.sec.gov/news/public-statement/statement-clayton-2017-09-20 .

[2] https://www.computerworld.com/article/2853697/fireeye-suspects-fin4-hackers-are-americans-after-insider-info-to-game-stock-market.html and http://securityaffairs.co/wordpress/38118/cyber-crime/sec-investigates-fin4-hackers.html. In a similar incident in 2016, a former Expedia IT specialist remotely hacked into computers and email accounts of senior Expedia executives and made highly profitable trades in Expedia securities ahead of company announcements (https://www.sec.gov/news/pressrelease/2016-280.html) Cyber criminals have also successfully targeted media firms (https://www.sec.gov/news/pressrelease/2015-163.html), law firms, (https://www.welivesecurity.com/2017/05/11/hackers-stole-information-law-firms-made-millions-insider-trading-fined-9-million/) and advisory firms (https://www.theguardian.com/business/2017/sep/25/deloitte-hit-by-cyber-attack-revealing-clients-secret-emails) to steal non-public information about mergers and acquisitions or earnings announcements. We note that trades based upon hacked information can be made by the hackers themselves or by others who receive the information derived from hacking.

[3] Cybercriminals often try to hack the credentials of key employees to get access to valuable information that is shared via emails, or in files with limited security (https://www.forbes.com/sites/robertadams/2017/04/04/top-online-threats-to-your-cybersecurity-and-how-to-deal-with-them/#5e28979e31be). This threat becomes amplified as technology and communication networks and systems become more interconnected (Hamm 2019).

We develop a cybersecurity risk mitigation measure based on textual analysis of 10-K disclosures starting in 2011. This timeframe is driven by SEC guidance in 2011, which requires companies to include material information related to cybersecurity risk in their periodic filings (*CF Disclosure Guidance: Topic No. 2 Cybersecurity*). We argue that 10-K disclosures contain information about how firms address and mitigate cybersecurity risks and are unlikely to provide information that exposes them to additional cyber-related risk from hackers.[4] Our measure counts the number of words and phrases that relate to risk mitigation within cybersecurity-related excerpts from the 10-K reports.[5] These excerpts comprise paragraphs in the 10-K that we identify by searching for use of cybersecurity-related words. The word search is based on a dictionary of cybersecurity terminology that we developed from the glossary of the National Initiative for Cybersecurity Careers and Studies (NICCS) and a report on laws relating to cybersecurity prepared by the Congressional Research Service (Fischer 2014). Our cybersecurity risk mitigation dictionary aims to capture strategies relating to hardware and software solutions that address cybersecurity risks, as well as management systems to improve employee awareness and to hold third parties such as auditors and legal advisers to higher cybersecurity standards.

We test the prediction that firms with higher cybersecurity risk mitigation scores are less likely to experience leakage of inside information due to the activities of cyber criminals. Our empirical tests examine the impact of cybersecurity risk mitigation on the probability that private information will be traded on and reflected in prices before earnings announcements.[6] We focus on earnings announcements because of the documented trading activity of hackers preceding earnings announcements (see footnote 2). Our first test employs the price jump ratio (Weller 2017) to investigate the relative pre-announcement

[4] SEC (2011) states that, "federal securities laws do not require disclosure that itself would compromise a registrant's cybersecurity." This interpretation is consistent with result in Berkman et al. (2018a), who find positive market valuations for a broader cybersecurity measure based upon 10-K disclosures.

[5] It might be possible to obtain firm-specific measures of cybersecurity from trawling dark web marketplaces. However, the most valuable inside information cannot be advertised openly online, since doing so would cause the information to lose its value. There are specialized dark web sites such as 'The Stock Insider' that solve this problem by employing strict access restrictions, thus providing sellers and buyers of inside information with a sense of protection. See also: https://www.securityweek.com/financial-industry-insiders-put-keys-kingdom-risk.

[6] Akey et al. (2019) find that private information traded upon by digital insiders is impounded in price prior to public release of the information.

information content of prices. The price jump ratio divides the return at the time of the earnings information's public disclosure by the total return over a longer pre-announcement period. Consistent with our expectation, we find that firms with high cybersecurity risk mitigation scores have a high price jump ratio, indicating that a relatively large proportion of earnings information is not discovered until the earnings announcement.

Our second test examines the impact of a firm's cybersecurity risk mitigation on the relative amount of short selling before earnings announcements due to informed trading. This test is motivated by several charges brought by the SEC, where hackers short-sold stocks just before firm disclosure of disappointing earnings news.[7] Consistent with our hypothesis, we find that pre-announcement trading by short sellers for firms with lower cybersecurity risk mitigation scores is more negatively related to earnings surprises. This implies that the ability of informed traders (proxied by the relative trading activity of short sellers) to predict earnings surprises is greater for firms with lower levels of cybersecurity risk mitigation.

The first two tests suggest that there is a greater incidence of informed trading in the pre-announcement period for firms with low cybersecurity risk mitigation scores. In our third test, we exploit the increased information asymmetry during the period just before earnings announcements (Bhattacharya et al. 2013; Chae 2005; Lee et al. 1993). We provide evidence that relative to other pre-announcement days, in the days leading up to earnings announcements, firms with lower cybersecurity risk mitigation scores experience a larger increase in the adverse selection component of the bid-ask spread. These results are consistent with the idea that liquidity providers will require more *ex-ante* compensation for firms with low cybersecurity risk mitigation scores in periods of increased exposure to informed trading (e.g., Glosten and Harris 1988).

Our study makes several contributions to the literature. Many studies examine the impact of specific groups of potentially informed market participants on price formation (some examples are insiders (Schnitzlein 2002; Seyhun 1986), short sellers (Chen and Singal 2003; Saffi and Sigurdsson 2010), analysts

[7] For example https://www.nbcnews.com/business/business-news/u-s-charges-9-insider-trading-based-hacked-press-releases-n407771.

(Brennan and Subrahmanyam 1995; Gleason and Lee 2003), and institutional investors (Piotroski and Roulstone 2004; Lakonishok et al. 1992)). We add hackers and their associates to this list of potentially informed market participants. We provide evidence suggesting that firms trying to manage their exposure to cybercrime can reduce the probability that private information will be traded on before disclosure. We also find that the association between a firm's cybersecurity risk mitigation score and the cost of liquidity – in particular the adverse selection component – is significantly more negative on days with a high probability of trading with informed traders. Given increasing recognition of risks associated with hackers infiltrating firms and obtaining private information for illegal trading (SEC 2018), our findings are timely and should be of interest to regulators, management, and investors.

We also contribute to the literature on cybersecurity risk disclosures by providing evidence that cybersecurity disclosures in 10-K filings provide useful insight into firm exposure to cybersecurity risks and help explain variation in the probability of private information leakage. As such, we contribute to the literature that examines implications of increased requirements for risk disclosures (Miihkinen 2012; Kravet and Muslu 2013; Campbell et al. 2014; Berkman et al. 2018b; Hope et al. 2016). Our findings should be informative to regulators (who are facing calls for improved cybersecurity disclosure requirements from within the SEC),[8] auditors (who are charged with understanding potential weaknesses in the systems that support the financial reporting process (Hamm 2019), academics (Gordon et al. 2015; Ferraro 2014; Selznick and LaMacchia 2016), and other market participants.[9]

Finally, our paper contributes to the literature on the relation between earnings and returns by showing a new channel through which earnings information gets impounded into prices in the period before it is released (e.g., Ball and Shivakumar 2008; Bushee et al. 2010; Huang and Skantz 2016). Ball and Shivakumar (2008) find that at the time of earnings announcement, most information is already impounded

[8] See the statements from Commissioner Kara M. Stein (https://www.sec.gov/news/public-statement/statement-stein-2018-02-21) and Commissioner Robert J. Jackson Jr (https://www.sec.gov/news/public-statement/statement-jackson-2018-02-21), who argue that existing cybersecurity disclosure requirements are not sufficient.
[9] https://www.csoonline.com/article/3260006/data-breach/secs-new-cybersecurity-guidance-falls-short.html, https://www.nytimes.com/2018/03/05/business/dealbook/sec-cybersecurity-guidance.html.

into prices. We contribute to this literature on information asymmetry in the pre-earnings announcement period and price formation by showing that price discovery in the pre-announcement period differs among firms based upon their cybersecurity risk management. Our results thus suggest that a firm's management of its cybersecurity risk is important to its information environment.

2. Literature review and hypothesis development

In this section we review prior research on cybersecurity. We then develop our hypotheses on the relation between cybersecurity risk mitigation, the probability of leakage of private information and the cost of liquidity.

2.1 Prior literature on cybersecurity

Research on cybersecurity in accounting and finance can be split into two streams. The first stream provides evidence on the impact of cybersecurity disclosures on market valuations. In the period before the SEC guidance on disclosure of cybersecurity risk (SEC 2011), Gordon et al. (2010) find higher market valuations for the small proportion of firms that voluntarily disclosed cybersecurity risks. Following the SEC guidance and using a broad sample of firms, Berkman et al. (2018a) find that more informative cyber disclosures are associated with higher market valuations.

The second stream of research examines the consequences of cybersecurity events. Several articles find evidence that positive cybersecurity events such as IT security investments (Im et al. 2001; Chai et al. 2011; Bose and Leung 2013) and/or creation of a Chief Information Officer position (Chatterjee et al. 2001) are associated with higher stock prices. Relatedly, Kwon et al. (2012) find that greater total IT executive compensation is associated with a lower likelihood of information security breaches. Firms also suffer fewer security breaches when they have stronger internal controls (Westland 2018) and when there is a higher quality relationship between the internal audit and the information security function (Steinbart et al. 2018).

Studies that examine the consequences of negative cybersecurity events generally find evidence of negative market reactions to the events.[10] For example, research indicates that announcements of software vulnerability (Telang and Wattal 2007), IT products containing viruses (Hovav and D'arcy 2005), and cybersecurity breaches are associated with negative market reactions (Cavusoglu et al. 2004; Yayla and Hu 2011; Gordon et al. 2011; Amir et al. 2018; Modi et al. 2015; Kamiya et al. 2018). Such events also negatively affect the performance and liquidity of a firm. Bianchi and Tosun (2019) find that firms experience a decrease in liquidity and that daily excess returns are lower following the revelation of a first-time corporate hacking event. Mitts and Talley (2018) find evidence consistent with arbitrageurs obtaining early notice of impending breach announcements and profiting from short-selling. Akey et al. (2019) provide direct evidence that prior to its public release, private information traded upon by digital insiders is impounded in price.

While the above studies highlight the need for firms to actively mitigate cybersecurity risks, there is comparatively little research on cybersecurity risk mitigation. One exception is a study by Wang et al. (2013) who find that firms disclosing security risk factors with risk-mitigation themes are less likely to have future breach announcements. We extend this literature by providing evidence that firm cybersecurity risk mitigation strategies reduce the probability of informed trading by digital insiders prior to earnings announcements.

2.2 Hypotheses development

2.2.1 Price discovery and information acquisition

A key aspect of our study is investigating whether cybersecurity risk mitigation impacts how earnings-related information is impounded into price. Early research on price formation employs a measure of intra-period timeliness (IPT) to investigate the speed with which information is impounded into prices during an earnings quarter (Ball and Brown 1968; McNichols 1984; Butler et al. 2007; Alford et al. 1993).

[10] Spanos and Angelis (2016) provide a comprehensive review of the stock market impacts of security events.

Fast price discovery implies that the end-of-quarter perfect foresight price level is attained early in the quarter.

Weller (2017) extends the literature by introducing the price jump ratio (PJR). The price jump ratio measures the share of information incorporated into the price before the earnings announcement of a specific stock. The PJR is defined as the cumulative abnormal return in a short window around the earnings announcement relative to the cumulative abnormal return for the same stock over a longer pre-announcement window ending on the same day as the short earnings announcement window. A high PJR, indicating a large announcement price change relative to the pre-announcement price change, is consistent with little pre-announcement informed trading. In contrast, a low PJR, indicating a small announcement price change relative to the pre-announcement price change, suggests aggressive informed trading in the pre-announcement period.

Based on the conjecture that firms providing more extensive cybersecurity risk-mitigating disclosure are more likely to have taken measures to manage that risk, we hypothesize that informed trading by hackers is more likely in firms with low cybersecurity risk mitigation scores. For these firms, we expect relatively less discovery of new earnings information upon announcement, resulting in a lower price jump ratio.

HYPOTHESIS 1. *Earnings announcement price jump ratios are positively associated with cybersecurity risk mitigation.*

2.2.2 Probability of information leakage

Digital insiders gain access to information that may relate to positive or negative earnings surprise. Informed traders can benefit from this information through either long or short selling in advance of the earnings announcement. We focus on short selling because there is no daily data on trading by a group of equally well-informed long-side investors. In a wide variety of settings, research provides evidence consistent with short sellers anticipating future information releases by exploiting private information. For example, there is greater short selling activity in the days leading up to downgrades by analysts (Christophe

et al. 2010) and insider sales (Chakrabarty and Shkilko 2013; Khan and Lu 2013). Karpoff and Lou (2010) find that abnormal short selling increases in the period before disclosure of misrepresentations. In a cybersecurity-related setting, Mitts and Talley (2018) find evidence that prior to firm breach announcements, informed traders take short positions against the hacked firms. Studies also show that short interest increases prior to the announcement of private placements in which hedge funds are involved (Berkman et al. 2016) and that short sellers are able to profitably exploit material non-public information arising from the syndicated lending process (Massoud et al. 2011).

Weak cybersecurity risk mitigation by firms should increase the probability that hackers can obtain (and exploit or sell) private information related to earnings. As a result, with a higher probability of information leakage, pre-announcement trading by short sellers should be more negatively associated with earnings surprises for firms with lower cybersecurity risk mitigation scores.

HYPOTHESIS 2. *Short selling in the days before earnings announcements is more predictive of earnings surprises for firms with low scores on cybersecurity risk mitigation.*

2.2.3 The cost of liquidity and informed trading

Theoretical models of the cost of liquidity typically assume that one set of traders provides liquidity via quotes or limit orders and another set of traders initiates trades for liquidity or for informational reasons (Holden et al. 2014; Huang and Stoll 1996). These models typically posit that the spread provides suppliers of liquidity with compensation for: 1) adverse selection costs (Glosten and Milgrom 1985; Kyle 1985; Easley and O'Hara 1987); 2) order processing costs (Roll 1984); and 3) inventory holding costs (Amihud and Mendelson 1980; Ho and Stoll 1981; Ho and Stoll 1983). Building on these models, several papers attempt to measure components of the bid-ask spread, in particular the component related to adverse selection risk (e.g., Glosten and Harris 1988; Stoll 1989; Hasbrouck 1991; Lin et al. 1995).

Using measures derived from trade and quote data, several empirical studies examine the association between firm or ownership characteristics that might proxy for information asymmetry and the cost of liquidity and adverse selection. For example, Loughran and Schultz (2005) find that rural stocks,

which are more likely to be held by better-informed local investors, have lower turnover and higher quoted and effective spreads than urban stocks (see also Ivković and Weisbenner 2005). Berkman et al. (2014) find that underaged account holders (whose trades are likely to be controlled by informed guardians) outperform older investors and that stocks have higher bid-ask spreads if there is a higher proportion of underaged trading. In the accounting literature, using earnings quality as a measure of information asymmetry, Bhattacharya et al. (2013) find that poor earnings quality is associated with adverse selection risk as measured by the price impact of trade, and that poor earnings quality is associated with increased information asymmetry around earnings announcements.[11]

Our study builds on prior research findings that information asymmetry increases and liquidity deteriorates around earnings announcements (Lee et al. 1993; Bhattacharya et al. 2013). Firms with low cybersecurity mitigation are more susceptible to being hacked, with a concomitant higher likelihood of digital insiders trading on information about forthcoming earnings news. If suppliers of liquidity anticipate this increased probability of facing informed traders prior to earnings announcements, then the bid-ask spread, particularly the adverse selection component, should widen. We conjecture that in the days shortly before earnings releases, the cost of liquidity increases relatively more for firms with low cybersecurity risk mitigation.

HYPOTHESIS 3. *In the days leading up to earnings announcements, the cost of liquidity becomes negatively associated with firm cybersecurity risk mitigation.*

3. Sample, variables and descriptive statistics

3.1 Sample

Our sample period starts with fiscal year 2012, the first fiscal year subsequent to the SEC guidance on cybersecurity risk disclosure. For fiscal years 2012–2016, we construct a cybersecurity risk mitigation

[11] In contrast to studies that suggest microstructure measures of adverse selection are positively related to information asymmetry, Collin-Dufresne and Fos (2015) find that when informed traders have a relatively long period to select when and how to trade, standard measures of adverse selection may fail to capture the presence of informed trading.

measure using cybersecurity-related excerpts from 10-Ks of Russell 3000 firms. After merging the cybersecurity risk mitigation data with Compustat and CRSP, our sample is reduced to 13,187 firm-year observations, with cybersecurity risk mitigation scores for 3,096 firms. To identify 'event day 0', the first day after the quarterly earnings announcement that the closing price reflects the new earnings information, we use earnings announcement date and time from the I/B/E/S database. We adjust event day 0 for after-hours earnings announcements. In addition, after merging I/B/E/S and Compustat databases using the linking table in WRDS and requiring the best match score, we require that the earnings announcement date be the same in both databases. As a result of these requirements, our sample drops to 9,720 firm-years for 2,316 firms. Our final sample requirement is the availability of trade and quote data in DTAQ. To merge with the DTAQ database we use the linking table provided in WRDS, resulting in a final sample of 30,187 quarterly earnings announcements for 2,059 firms.

3.2 Variables of interest

3.2.1 Cybersecurity risk mitigation measure

Our cybersecurity risk mitigation measure is constructed using cybersecurity-related excerpts from 10-Ks for Russell 3000 firms for fiscal years 2012–2016.[12] Cybersecurity-related excerpts comprise paragraphs from 10-K disclosures containing words or phrases that directly relate to cybersecurity themes. Our dictionary of cybersecurity terminology is based upon the glossary from the National Initiative for Cybersecurity Careers and Studies (NICCS) and the Congressional Research Service report on laws relating to cybersecurity (Fischer 2014). Our cybersecurity risk mitigation measure, *MitigationWords*, is the number of words or phrases in the cybersecurity-related excerpts that we identify as describing risk mitigation themes. Appendix A.1 provides the terms included in the dictionary for this measure. Although many of these words (e.g., insurance and training) are not uniquely related to cybersecurity and thus could be generalized to other themes, we examine usage of these words solely within the context of cybersecurity

[12] See Appendix A for a more in-depth description of our score development. The score was produced in conjunction with CookESG (cookesg.com/g.com/).

(i.e., in the cybersecurity-related excerpts). This provides confidence that the disclosed mitigation measures relate specifically to cybersecurity and not to a more general risk management strategy by the firm. Appendix A.2 provides examples of 10-K excerpts containing cybersecurity risk mitigation themes. Additional tests in Section 5 indicate that our results are robust to inclusion of controls for firms' overall risk mitigation strategy.

3.2.2 Price Jump Ratio

For our test of Hypothesis 1, the measure of PJR for the earnings announcement of stock *i* in quarter *t* is defined as:

$$PJR_{it} = CAR_{it}\left(0,2\right) / CAR_{it}(-21,2) \tag{1}$$

Similar to Weller (2017), we estimate cumulative abnormal returns (*CAR)* relative to a Fama and French (1992) three-factor model, using daily returns over a 365-calendar day window ending 90 days before the earnings announcement (we require at least 63 valid preceding trading days). The pre-announcement period starts on trading day -21 (about 1 month) and to ensure that prices fully reflect the new information, the total window ends 2 trading days after the earnings announcement. Our announcement return window starts on day 0 and ends 2 days after the earnings announcement.[13]

To address the problem of a near-zero denominator in the PJR, we exclude events in the lowest decile of absolute value *CAR*(-21,+2). By excluding observations with small denominators (i.e., *CAR*(-21,+2) is close to 0), we exclude observations with low signal-to-noise ratios that are also non-events from the perspective of informed traders (see Weller 2017). In robustness tests, we also present results that use different exclusion cut-offs for *CAR*(-21,+2).

[13] In sensitivity tests, we present results for different windows. Note that our earnings announcement window starts on day 0 rather than day -1 as in Weller (2017). We adjust earnings announcement dates for after-hours announcements, whereas Weller (2017) uses Compustat earnings announcement dates, which are not adjusted for after-hours announcements.

3.2.3 Abnormal short-selling measure

For our test of Hypothesis 2, following prior literature (Christophe et al. 2004; Engelberg et al. 2012) we measure the level of daily short selling for firm *i* on day *t* as the daily number of shares sold short as a proportion (in percent) of total volume traded:

$$SHVOL_{i,t} = \frac{\text{Number of shares sold short}_{i,t}}{\text{Trading volume}_{i,t}} \times 100 \qquad (2)$$

To measure abnormal short selling for a specific stock on a given day, we calculate the deviation of the level of short selling on that day from a "normal" benchmark level for that stock. We define normal short selling separately for every event (i.e., earnings announcement) as the mean short sales over event days -40 to -11 for that stock. Abnormal short volume, *ASHVOL*, is calculated as:

$$ASHVOL_{i,t} = SHVOL_{i,t} - \overline{SHVOL(-40,-11)}_i \qquad (3)$$

3.2.4 Liquidity measures

Our tests of Hypothesis 3 for the relation between the cost of liquidity and cybersecurity risk mitigation focus on the dollar-weighted average percentage effective spread (*ESPREAD*), Kyle's (1985) lambda (*LAMBDA*), and the Amihud (2002) illiquidity measure (*AMI*). Our data source for *ESPREAD* and *LAMBDA* is the daily TAQ database (DTAQ). We use SAS code available on Craig Holden's website (https://kelley.iu.edu/cholden/) and follow the trade-signing approach of Lee and Ready (1991), using contemporaneous quotes to sign trades (e.g., Bessembinder 2003). Calculation of *AMI* employs daily CRSP data.

The effective spread is the difference between an estimate of the true value of the security (the midpoint of the bid and ask) and the actual transaction price, and is computed by comparing the trade price to the prevailing quote midpoint (Huang and Stoll 1996; Bessembinder and Kaufman 1997). For each stock in each day, we calculate the dollar-weighted average percentage effective spread, based on the following definition of the effective spread for a trade at time *t*:

$$Percent\ Effective\ Spread_t = 2 \times D_t \left(Ln\left(P_t\right) - Ln\left(M_t\right)\right) \quad (4)$$

where D_t is an indicator variable that equals +1 if the trade at time t is buyer-initiated and −1 if the trade at time t is seller-initiated. M_t is the midpoint of the consolidated best bid and offer at the moment of the trade.

Kyle's (1985) lambda, *LAMBDA*, is a measure of adverse selection through price impact. It represents the extent to which signed order flow affects a security's price. We follow Hasbrouck (2009) and define *LAMBDA* as the slope of the following regression:

$$r_n = \lambda S_n + \varepsilon_n \quad (5)$$

where r_n is the security's log price change in the nth five-minute period, S_n is the signed square-root of dollar volume in the nth five-minute period, and ε_n is the error term. S_n is defined by

$$S_n = \sum sign(v_{kn} \times SQRT\left(|v_{kn}|\right) \quad (6)$$

where v_{nk} is the signed dollar volume of the *k*th trade in the *n*th five-minute period.

Our second measure of adverse selection through price impact is the measure proposed by Amihud (2002). The Amihud (2002) illiquidity measure, *AMI*, is the ratio of absolute value of daily stock return to the daily dollar trading volume.

3.3 Descriptive statistics

Table 1 Panel A presents descriptive statistics of our measures. The number of cybersecurity risk mitigation words (*MitigationWords*), ranges from 0 to 305 and the average (median) number of cybersecurity risk mitigation words in the cybersecurity-related excerpts is 6.5 (3). Based upon the distribution of *MitigationWords*, in our subsequent empirical tests, we use the natural log of number of cybersecurity risk mitigation words plus one, *LMitigationWords*.

We winsorize *PJR* and the liquidity measures at the 1st and 99th percent levels to reduce the effect of outliers. *PJR* has a mean value of 0.51, indicating that a substantial amount of total price discovery in

the period from 1 month before the earnings announcement to 2 days after the earnings announcement takes place in the last 3 days. The number of observations for *PJR* is lower than for the other variables in table 1 because we exclude the decile of observations with the lowest absolute value of *CAR*(-21,+2). The average effective spread (*ESPREAD*) in our sample is 0.21% of the bid-ask spread mid-price. After multiplying by a factor 100,000, the average lambda (*LAMBDA*) equals 0.249, and after multiplying by a factor 1,000,000, the average Amihud measure (*AMI*) is 10.1. Apart from *PJR*, all market-based variables in Table 1 are measured over trading days -42 to -22 before each earnings announcement.

In Table 1, Panel B we report the Pearson correlations between *PJR*, the liquidity measures, the cybersecurity risk mitigation measure and control variables. Correlations between *PJR* and our cybersecurity risk mitigation measure, price, institutional ownership, and the liquidity measures are statistically significant, but low in magnitude (all correlations < |0.05|). As expected, liquidity measures are lower for larger firms and for higher-priced firms. Firms with higher volatility have higher values for our liquidity measures. Firms with more mitigation words also tend to have longer cybersecurity-related discussions in their 10-Ks (the correlation between *LMitigationWords* and *LCyberWords* is 0.68).

(Insert Table 1 here)

4 Empirical method and results

4.1 Information leakage and pre-announcement price discovery.

In this section we test our first hypothesis, that privately informed trading by hackers is more likely in firms with low cybersecurity risk mitigation, resulting in relatively fast discovery of new earnings information for these firms. Based on Weller (2017) and using *PJR* as the dependent variable, we estimate the following model:

$$\begin{aligned} PJR_{i,t} = a + \beta_1 LMitigationWords_{i,t} + \beta_2 LCyberWords_{i,t} + \beta_3 LNMV_{i,t} + \beta_4 LN(PRC)_{i,t} + \\ \beta_5 BIDASK_{i,t} + \beta_6 LN(STDRET)_{i,t} + \beta_7 ANALYST_{i,t} + \beta_8 IO_{i,t} + YEARFE + \varepsilon_{i,t} \end{aligned} \quad (7)$$

The model contains the same control variables as Weller (2017), including the natural log of market capitalization (*LNMV*), the natural log of the standard deviation of daily returns (*LN(STDRET*), average share price (*LN(PRC)*) and bid ask spread (*BIDASK*), all of which are computed over the period from event day -42 through event day -22. We also control for the number of analysts covering stock *i* in quarter *t-1* (*ANALYST*), from I/B/E/S, and the institutional ownership ratio at the end of the preceding quarter from 13-F filings (*IO*). Standard errors are two-way clustered by stock and quarter.

Table 2 presents the results from estimating equation (7). Column (1) presents results for the base model. In column (2), we include the number of words or phrases in all cybersecurity-related excerpts in a firm's disclosures in the entire 10-K filing for a given year (*LCyberWords*) as an addition control to ensure that our results are not driven merely by the amount of cybersecurity disclosures provided by a firm. Column (3) reports results when we exclude the first percentile of observations with the smallest absolute *CAR*(-21,+2) instead of the decile of observations with the smallest absolute *CAR*(-21,+2). Column (4) provides results when we drop the quartile of observations with the smallest absolute *CAR*(-21,+2). Columns (5) and (6) repeat the analysis in the third column, but use *CAR*(-10,+2) and *CAR*(-3,+2) in the denominator of *PJR*.

(Insert Table 2 here)

Similar to Weller (2017), we find that the price jump at the earnings announcement is higher (or equivalently, that information leakage before the earnings announcement is lower) for firms covered by a larger number of analysts and higher institutional ownership. Further, the price jump at the earnings announcement decreases with firm size, quoted spread and volatility. For our test of Hypothesis 1, in column (1), the coefficient of *LMitigationWords* is positive and significant at the one percent level. This result indicates that a one-standard deviation increase in *LMitigationWords* increases the *PJR* by 0.0293. The average PJR for this sample is 0.51, implying that a one standard deviation increase in *LMitigationWords* corresponds to a 6 percent increase in the fraction of the price discovery that occurs at the time of the public announcement. Results in column (2) indicate that *LMitigationWords* continues to have explanatory power even when *LCyberWords* is included in the model. These results provide evidence

that 1) company cybersecurity risk mitigation disclosures are not boilerplate; and 2) the extensiveness of disclosures about cybersecurity risk mitigation is not simply indicative of more extensive cybersecurity risk disclosures.

Results reported in the third column are based on a sample where only the first percentile of observations with the smallest absolute *CAR*(-21,+2) are trimmed from the sample. Consistent with our expectations, the coefficient of our cybersecurity risk mitigation measure becomes insignificant. This result supports our initial exclusion of observations with small denominators (i.e., where *CAR*(-21,+2) is close to 0), due to the low signal-to-noise ratios for these observations. When we trim the quartile of observations with the smallest absolute *CAR*(-21,+2) from the sample, the magnitude and significance of the *LMitigationWords* coefficient increases (column (4)). Results in the last two columns indicate that *LMitigationWords* is positively associated with the *PJR* if the *PJR* is based on a pre-announcement window that is limited to the last 10 days before the earnings announcement (column (5)), or the last 3 days before the earnings announcement (column (6)). Overall our results consistently indicate that more price discovery takes place in the pre-announcement period for firms with lower cybersecurity risk mitigation.

4.2 Cybersecurity risk mitigation and short selling

In this section we test our second hypothesis, that relatively low cybersecurity risk mitigation is associated with more informative short selling in the days before earnings announcements. We obtain data on short sales transactions from the Financial Industry Regulatory Authority (FINRA) website.[14] Beginning in August 2009, FINRA provides data of short sale transactions that include transaction times, prices, and sizes for all short sales of National Market System stocks.

[14] The FINRA short transactions data have been used in prior studies (e.g., Jain et al. 2013; Jain et al. 2012; Berkman and Eugster 2017). For more information on the short sales transactions on FINRA, see http://www.finra.org/sites/default/files/NoticeDocument/p120044.pdf .

To test if short sellers have an ability to predict earnings surprises, we estimate a model where the dependent variable is *RSURPRISE*, and specify the following model:

$$\begin{aligned} RSURPRISE_{i,t} = {} & \alpha + \beta_1 LMitigationWords_{i,t} + \beta_2 ASHVOL(-5,-1)_{i,t} + \beta_3 LMitigationWords_{i,t} \times ASHVOL(-5,-1)_{i,t} + \\ & \beta_4 LCyberWords_{i,t} + \beta_5 LNMV_{i,t} + \beta_6 BM_{i,t} + \beta_7 LN(PRC)_{i,t} + \beta_8 BIDASK_{i,t} + \beta_9 TURN_{i,t} + \\ & \beta_{10} STDRET_{i,t} + \beta_{11} CAR(-40,-6)_{i,t} + \beta_{12} CAR(-5,-1)_{i,t} + YearFE + \varepsilon_{i,t} \end{aligned} \quad (8)$$

where *RSURPRISE* is defined as the quarterly rank decile of the earnings surprise with earnings surprise defined as the difference between the actual earnings per share and the most recent average earnings per share forecast from I/B/E/S, scaled by the absolute value of this most recent average earnings per share forecast.

Control variables are based on prior studies in the short sales literature (e.g., Christophe et al. 2004; Christophe et al. 2010; Blau and Wade 2012; Henry et al. 2015). *LNMV* is the natural logarithm of the stock's market capitalization averaged over event day -40 to -11. The firm's book-to-market equity ratio, *BM*, is calculated as at the latest quarter-end prior to the announcement. *LN(PRC)* is the natural logarithm of the stock's closing price and *BIDASK* is the percentage difference between the closing bid and ask price. *TURN* is the number of shares traded during the day as a proportion of shares outstanding. These last three variables are calculated as the average over event day -40 through -11. We include two measures of cumulative abnormal returns: over event days -40 to -6, *CAR*(-40,-6), and over the last week, *CAR*(-5,-1). Finally, we also control for return volatility, *STDRET*, defined as the standard deviation of daily stock returns over event days -40 through -11. $\overline{ASHVOL(-5,-1)}$ is the average daily abnormal short volume over the week before the earnings announcement.[15] Standard errors are clustered at both the firm and quarter levels.

[15] We follow Berkman and Eugster (2017) and use abnormal short selling measured over the last five trading days before the earnings announcement in our base case model.

The key independent variable in the regression is the interaction term for *LMitigationWords* and $\overline{ASHVOL(-5,-1)}$. Our main hypothesis is that pre-announcement informed short sales are more likely in firms with low cybersecurity risk mitigation. If informed short selling prior to the announcement of earnings surprises is higher for firms with weak cybersecurity risk mitigation, we expect a significant positive coefficient of the interaction term between our cybersecurity risk mitigation measures and pre-announcement short selling. That is, the relation between earnings surprise and pre-announcement short selling is more negative for firms with relatively low scores on *LMitigationWords*.

Results of this analysis in Table 3 indicate that negative earnings surprises are more prevalent at firms with high volatility, low stock price and low book-to-market ratios. We also find that the abnormal stock return before the earnings announcement is positively associated with the forthcoming earnings news for both pre-announcement windows (-40,-6) and (-5,-1). In line with our prediction, the interaction term between *LMitigationWords* and *ASHVOL* has a positive coefficient, which is significant at the one percent level. Consistent with our analysis of *PJR* in the previous section, the results in the second column show that our inferences remain robust after including *LCyberWords* as well as the interaction term between *LCyberWords* and *ASHVOL*.

Columns (3) - (6) in Table 3 present the results of several alternative specifications, each model making one change relative to the specification in column (2). The model in column (3) employs the actual earnings surprise (winsorized at 1% and 99%) rather than the decile rank as dependent variable. Results in column (4) are based on abnormal short selling on the day before the earnings announcement rather than the week before the earnings announcement. Column (5) presents results when the earnings surprise measure is calculated as the difference between the actual earnings per share and the most recent average earnings per share estimate across analysts, scaled by the standard deviation across analyst estimates.

Finally, column (6) presents results using the median earnings per share forecast across analysts instead of the mean earnings per share forecast to calculate the earnings surprise measure. Results of robustness tests in columns (3) - (6) are all consistent with the specification in column (2) and consistently

show a positive and significant association between earnings surprise and the interaction variable between our cybersecurity risk mitigation variable and abnormal short selling.

(Insert Table 3 here)

4.3 Cybersecurity and the cost of liquidity around earnings announcements

In this section, we test the third hypothesis, which predicts that during days closer to earnings announcements, liquidity suppliers require relatively higher compensation for stocks where there is a higher probability of trading by digital insiders. To test this hypothesis, we select the 35 trading days before each earnings announcement for our sample stocks. For each earnings announcement, we calculate abnormal values for each liquidity measure for day -10 through day -1, using the mean and standard deviation based on the 25 trading days from day -35 to day -11. We use three commonly used measures of liquidity: (1) effective spread (*ESPREAD*), (2) Kyle's (1985) lambda (*LAMBDA*), and (3) Amihud (2002) illiquidity measure (*AMI*). The abnormal value of each liquidity measure (1-3) on day *t* relative to the earnings announcement day for quarter *q* for stock *i* is defined as follows:

$$A_LM_{1-3,i,\,q,\,t} = \left(LM_{1-3,i,\,q,\,t} - M_LM_{1-3,i,\,q}\right) \;/\; S_LM_{1-3,i,\,q} \qquad (9)$$

Where:

$A_LM_{1-3,i,\,q,\,t}$	=	the abnormal value for liquidity measure 1, 2, or 3, on day *t* relative to quarter *q*'s earnings announcement day (day 0) for stock *i*.
$LM_{1-3,i,\,q,\,t}$	=	the actual value for liquidity measure 1, 2, or 3, on day *t* relative to quarter *q*'s earnings announcement day for stock *i*.
$M_LM_{1-3,i,\,q}$	=	the mean value for liquidity measure 1, 2, or 3, measured over the 25-day period from day -35 to day -11 relative to quarter *q*'s earnings announcement day for stock *i*.
$S_LM_{1-3,i,\,q}$	=	the standard deviation of liquidity measure 1, 2, or 3, measured over the 25-day period from day -35 to day -11 relative to quarter *q*'s earnings announcement day for stock *i*.

Next, we estimate the following model for each of the 10 days before earnings announcement, for *t* = -10 through *t* = -1:

$$A_LM_{1-3,i,q,t} = a + \beta_1 LMitigationWords_{i,q} + \beta_2 LCyberWords_{i,q} + \beta_3 LNMV_{i,q} + \beta_4 TURN_{i,q} + \beta_5 STDRET_{i,q} + YearFE + \varepsilon_{i,q,t} \quad (10)$$

Based on the literature we use the log of market capitalization (*LNMV*), turnover defined as the daily number of shares traded divided by the number of shares outstanding (*TURN*), the closing price (*LN(PRC)*) and the standard deviation of daily returns (*STDRET*) as control variables (e.g. Stoll, 1989). The first three control variables are averaged over the period from day -35 to day -11 relative to the quarterly earnings announcement day (day 0), and the standard deviation is based on daily returns during this period. *LMitigationWords* is as previously defined.

We expect that in the days leading up to the earnings announcement date, stocks with a relatively high probability of trading by hackers experience a relatively high cost of liquidity. For example, on day -10, suppliers of liquidity might still be relatively unconcerned about trading on hacked information about the forthcoming earnings announcement. We therefore would not expect the coefficient of *LMitigationWords* to be significantly different from zero for the sample of day -10 observations. In contrast, for the sample of day -1 observations, we predict that the coefficient of *LMitigationWords* is significantly negative. This is because relative to suppliers of liquidity for firms with high cybersecurity risk mitigation, suppliers of liquidity for firms with low cybersecurity risk mitigation are more likely to be concerned about digital insiders trading on information about the forthcoming earnings announcement. Facing a higher probability of trading with hackers, suppliers of liquidity to low cybersecurity risk mitigation firms will require higher compensation to recoup the (expected) losses incurred by trading with these informed traders.

Panel A of Table 4 reports the coefficient of *LMitigationWords*, where equation (10) is estimated for each of the 10 trading days preceding quarterly earnings announcements, including *LMitigationWords* but not *LCyberWords*. We find that the effective spread is significantly negatively related to the firm's score on *LMitigationWords* on the four days immediately before earnings announcements. For measures of the adverse selection component of the spread, *LAMBDA* and *AMI*, we find that both measures are significantly

negatively related to a firm's score on *LMitigationWords* on the three days immediately before earnings announcements.

Panel B presents the results of equation (10) after including *LCyberWords* as an additional control and reports the coefficients of *LCyberWords* and *LMitigationWords*. On the three days immediately before earnings announcements, the effective spread is significantly negatively related to a firm's value for *LMitigationWords*. In contrast, the coefficient of *LCyberWords* is not significantly related to the effective spread on any of the ten days preceding the earnings announcements. We find similar results for both measures of the adverse selection component of the spread: the coefficients of both *LAMBDA* and *AMI* are significantly negatively related to a firm's score on *LMitigationWords* in the three days before earnings announcements, whereas *LCyberWords* is not significantly related to these measures of liquidity.

Overall, we conclude that the results in Table 4 are consistent with our conjecture that for days when it is more likely that digital insiders might exploit illegally acquired inside information, the cost of liquidity, and in particular the measures of adverse selection, increases more for firms with lower cybersecurity risk mitigation relative to firms with higher cybersecurity risk mitigation.

(Insert Table 4 here)

5 Robustness tests

We examine the sensitivity of our results to a firm's more general level of disclosure and overall focus on risk mitigation by controlling for 10-K characteristics. We augment equations (7) and (8) by including *L10KWords,* which captures the natural log of the number of words in the 10-K plus one, and *L10KMitigationWords,* which captures the occurrences of risk mitigation words across the entire 10-K (excluding the cybersecurity related excerpts) plus one. In addition, we continue to include *LCyberWords* as an additional control variable.

Table 5 presents results of these tests. In panel A, the relation between *LMitigationWords* and the price jump ratio continues to hold after including controls for 10-K disclosure characteristics. Similarly, in panel B, after controlling for 10-K characteristics, the relation between the earnings surprise and pre-

announcement short selling continues to be more negative for firms with relatively low scores on *LMitigationWords*.

(Insert Table 5 here)

6 Conclusion

There is growing awareness that hackers target corporations to obtain non-public corporate information for illegal trading. Spurred by growing concerns about hacking activities, this study examines whether a firm's cybersecurity risk mitigation affects the extent to which its private information is traded on and is reflected in prices before earnings announcements. We capture a firm's cybersecurity risk mitigation by assessing and scoring cyber-related disclosures in their 10-Ks, with a particular focus on discussion related to cybersecurity risk mitigation.

We first provide evidence that firms with higher cybersecurity risk mitigation experience relatively large price changes at the time of the earnings announcement, i.e., a high price jump ratio, indicating that a greater amount of information remains undiscovered until it is publicly revealed. Further tests show that pre-announcement trading by short sellers is more predictive of earnings announcement surprises for firms with low cybersecurity risk mitigation scores. Finally, we exploit increased information asymmetry in the period just before earnings announcements and demonstrate that relative to other pre-announcement days, firms with lower cybersecurity risk mitigation scores experience a larger increase in the adverse selection component of the bid-ask spread shortly before earnings announcements. Collectively, these findings indicate firms with better cybersecurity risk mitigation are associated with a lower extent to which private information is traded on and reflected in prices before publication of new earnings information.

We identify hacking as a new source of information for informed trading. Based upon measures of cybersecurity risk mitigation as disclosed in 10-Ks, we find evidence consistent with leakage of information through hacking prior to earnings announcements. Further, these leaks appear to be anticipated by market makers and other suppliers of liquidity, who charge a premium based upon the expectation of facing

informed traders prior to earnings announcements. We also find evidence that this information leads to more profitable short selling around earnings announcements. Overall, we find that weak cybersecurity risk mitigation increases exposure to cybercrimes, resulting in opportunities for acquisition of private information and trading by privately informed traders.

References

Akey, P., V. Gregoire, and C. Martineau. 2019. Retail insider trading and market price efficiency: Evidence from hacked earnings news. *Available at SSRN. https://ssrn.com/abstract=3365024*.

Alford, A., J. Jones, R. Leftwich, and M. Zmijewski. 1993. The relative informativeness of accounting disclosures in different countries. *Journal of Accounting Research* 31:183-223.

Amihud, Y. 2002. Illiquidity and stock returns: Cross-section and time-series effects. *Journal of financial markets* 5 (1):31-56.

Amihud, Y., and H. Mendelson. 1980. Dealership market: Market-making with inventory. *Journal of Financial Economics* 8 (1):31-53.

Amir, E., S. Levi, and T. Livne. 2018. Do firms underreport information on cyber-attacks? Evidence from capital markets. *Review of Accounting Studies, Forthcoming*.

Ball, R., and P. Brown. 1968. An empirical evaluation of accounting income numbers. *Journal of Accounting Research* 6 (2):159-178.

Ball, R., and L. Shivakumar. 2008. How much new information is there in earnings? *Journal of Accounting Research* 46 (5):975-1016.

Berkman, H., and M. Eugster. 2017. Short on drugs: Short selling during the drug development process. *Journal of financial markets* 33:102-123.

Berkman, H., J. Jona, G. Lee, and N. S. Soderstrom. 2018a. Cybersecurity awareness and market valuations. *Journal of Accounting and Public Policy, Forthcoming*.

Berkman, H., J. Jona, and N. S. Soderstrom. 2018b. Do market valuations incorporate climate risk?, working paper.

Berkman, H., P. D. Koch, and P. J. Westerholm. 2014. Informed trading through the accounts of children. *The Journal of Finance* 69 (1):363-404.

Berkman, H., M. D. McKenzie, and P. Verwijmeren. 2016. Hole in the wall: Informed short selling ahead of private placements. *Review of Finance* 21 (3):1047-1091.

Bessembinder, H. 2003. Issues in assessing trade execution costs. *Journal of financial markets* 6 (3):233-257.

Bessembinder, H., and H. M. Kaufman. 1997. A comparison of trade execution costs for nyse and nasdaq-listed stocks. *Journal of Financial and Quantitative Analysis* 32 (3):287-310.

Bhattacharya, N., H. Desai, and K. Venkataraman. 2013. Does earnings quality affect information asymmetry? Evidence from trading costs. *Contemporary Accounting Research* 30 (2):482-516.

Bianchi, D., and O. K. Tosun. 2019. Cyber attacks and stock market activity. *Available at SSRN 3190454*.

Blau, B. M., and C. Wade. 2012. Informed or speculative: Short selling analyst recommendations. *Journal of Banking & Finance* 36 (1):14-25.

Bose, I., and A. C. M. Leung. 2013. The impact of adoption of identity theft countermeasures on firm value. *Decision Support Systems* 55 (3):753-763.

Brennan, M. J., and A. Subrahmanyam. 1995. Investment analysis and price formation in securities markets. *Journal of Financial Economics* 38 (3):361-381.

Bushee, B. J., J. E. Core, W. Guay, and S. J. Hamm. 2010. The role of the business press as an information intermediary. *Journal of Accounting Research* 48 (1):1-19.

Butler, M., A. Kraft, and I. S. Weiss. 2007. The effect of reporting frequency on the timeliness of earnings: The cases of voluntary and mandatory interim reports. *Journal of Accounting and Economics* 43 (2-3):181-217.

Campbell, J. L., H. Chen, D. S. Dhaliwal, H.-m. Lu, and L. B. Steele. 2014. The information content of mandatory risk factor disclosures in corporate filings. *Review of Accounting Studies* 19 (1):396-455.

Carson, J. 2017. The evolution of the digital insider trader. *Computer Fraud & Security* (8):12-15.

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

Chae, J. 2005. Trading volume, information asymmetry, and timing information. *The Journal of Finance* 60 (1):413-442.

Chai, S., M. Kim, and H. R. Rao. 2011. Firms' information security investment decisions: Stock market evidence of investors' behavior. *Decision Support Systems* 50 (4):651-661.

Chakrabarty, B., and A. Shkilko. 2013. Information transfers and learning in financial markets: Evidence from short selling around insider sales. *Journal of Banking & Finance* 37 (5):1560-1572.

Chatterjee, D., V. J. Richardson, and R. W. Zmud. 2001. Examining the shareholder wealth effects of announcements of newly created cio positions. *MIS quarterly*:43-70.

Chen, H., and V. Singal. 2003. Role of speculative short sales in price formation: The case of the weekend effect. *The Journal of Finance* 58 (2):685-705.

Christophe, S. E., M. G. Ferri, and J. J. Angel. 2004. Short-selling prior to earnings announcements. *The Journal of Finance* 59 (4):1845-1876.

Christophe, S. E., M. G. Ferri, and J. Hsieh. 2010. Informed trading before analyst downgrades: Evidence from short sellers. *Journal of Financial Economics* 95 (1):85-106.

Collin-Dufresne, P., and V. Fos. 2015. Do prices reveal the presence of informed trading? *The Journal of Finance* 70 (4):1555-1582.

Easley, D., and M. O'Hara. 1987. Price, trade size, and information in securities markets. *Journal of Financial Economics* 19 (1):69-90.

Engelberg, J. E., A. V. Reed, and M. C. Ringgenberg. 2012. How are shorts informed?: Short sellers, news, and information processing. *Journal of Financial Economics* 105 (2):260-278.

Fama, E. F., and K. R. French. 1992. The cross-section of expected stock returns. *The Journal of Finance* 47 (2):427-465.

Ferraro, M. F. 2014. Groundbreaking or broken; an analysis of SEC cybersecurity disclosure guidance, its effectiveness, and implications. *Albany Law Review* 77:297-347.

Fischer, E. A. 2014. Federal laws relating to cybersecurity: Overview of major issues, current laws, and proposed legislation: Congressional Research Service.

Gleason, C. A., and C. M. Lee. 2003. Analyst forecast revisions and market price discovery. *The Accounting Review* 78 (1):193-225.

Glosten, L. R., and L. E. Harris. 1988. Estimating the components of the bid/ask spread. *Journal of Financial Economics* 21 (1):123-142.

Glosten, L. R., and P. R. Milgrom. 1985. Bid, ask and transaction prices in a specialist market with heterogeneously informed traders. *Journal of Financial Economics* 14 (1):71-100.

Gordon, L. A., M. P. Loeb, W. Lucyshyn, and L. Zhou. 2015. Increasing cybersecurity investments in private sector firms. *Journal of Cybersecurity* 1 (1):3-17.

Gordon, L. A., M. P. Loeb, and T. Sohail. 2010. Market value of voluntary disclosures concerning information security. *MIS quarterly*:567-594.

Gordon, L. A., M. P. Loeb, and L. Zhou. 2011. The impact of information security breaches: Has there been a downward shift in costs? *Journal of Computer Security* 19 (1):33-56.

Hamm, K. M. *Cybersecurity: Where we are; what more can be done? A call for auditors to lean in*. PCAOB 2019 [cited 05/11/2019. Available from https://pcaobus.org/News/Speech/Pages/hamm-cybersecurity-where-we-are-what-more-can-be-done.aspx.

Hasbrouck, J. 1991. Measuring the information content of stock trades. *The Journal of Finance* 46 (1):179-207.

———. 2009. Trading costs and returns for us equities: Estimating effective costs from daily data. *The Journal of Finance* 64 (3):1445-1477.

Henry, T. R., D. J. Kisgen, and J. J. Wu. 2015. Equity short selling and bond rating downgrades. *Journal of Financial Intermediation* 24 (1):89-111.

Ho, T., and H. R. Stoll. 1981. Optimal dealer pricing under transactions and return uncertainty. *Journal of Financial Economics* 9 (1):47-73.

Ho, T. S., and H. R. Stoll. 1983. The dynamics of dealer markets under competition. *The Journal of Finance* 38 (4):1053-1074.

Holden, C. W., S. Jacobsen, and A. Subrahmanyam. 2014. The empirical analysis of liquidity. *Foundations and Trends in Finance* 8 (4):263-365.

Hope, O.-K., D. Hu, and H. Lu. 2016. The benefits of specific risk-factor disclosures. *Review of Accounting Studies* 21 (4):1005-1045.

Hovav, A., and J. D'arcy. 2005. Capital market reaction to defective it products: The case of computer viruses. *Computers & Security* 24 (5):409-424.

Huang, Q., and T. R. Skantz. 2016. The informativeness of pro forma and street earnings: An examination of information asymmetry around earnings announcements. *Review of Accounting Studies* 21 (1):198-250.

Huang, R. D., and H. R. Stoll. 1996. Dealer versus auction markets: A paired comparison of execution costs on nasdaq and the nyse. *Journal of Financial Economics* 41 (3):313-357.

Im, K. S., K. E. Dow, and V. Grover. 2001. A reexamination of it investment and the market value of the firm—an event study methodology. *Information systems research* 12 (1):103-117.

Ivković, Z., and S. Weisbenner. 2005. Local does as local is: Information content of the geography of individual investors' common stock investments. *The Journal of Finance* 60 (1):267-306.

Jain, A., P. K. Jain, T. H. McInish, and M. McKenzie. 2013. Worldwide reach of short selling regulations. *Journal of Financial Economics* 109 (1):177-197.

Jain, C., P. Jain, and T. H. McInish. 2012. Short selling: The impact of SEC rule 201 of 2010. *Financial Review* 47 (1):37-64.

Kamiya, S., J.-K. Kang, J. Kim, A. Milidonis, and R. M. Stulz. 2018. What is the impact of successful cyberattacks on target firms?: National Bureau of Economic Research.

Karpoff, J. M., and X. Lou. 2010. Short sellers and financial misconduct. *The Journal of Finance* 65 (5):1879-1913.

Khan, M., and H. Lu. 2013. Do short sellers front-run insider sales? *The Accounting Review* 88 (5):1743-1768.

Kravet, T., and V. Muslu. 2013. Textual risk disclosures and investors' risk perceptions. *Review of Accounting Studies* 18 (4):1088-1122.

Kwon, J., J. R. Ulmer, and T. Wang. 2012. The association between top management involvement and compensation and information security breaches. *Journal of Information Systems* 27 (1):219-236.

Kyle, A. S. 1985. Continuous auctions and insider trading. *Econometrica: Journal of the Econometric Society*:1315-1335.

Lakonishok, J., A. Shleifer, and R. W. Vishny. 1992. The impact of institutional trading on stock prices. *Journal of Financial Economics* 32 (1):23-43.

Lee, C., and M. J. Ready. 1991. Inferring trade direction from intraday data. *The Journal of Finance* 46 (2):733-746.

Lee, C. M., B. Mucklow, and M. J. Ready. 1993. Spreads, depths, and the impact of earnings information: An intraday analysis. *The Review of Financial Studies* 6 (2):345-374.

Lin, J.-C., G. C. Sanger, and G. G. Booth. 1995. Trade size and components of the bid-ask spread. *The Review of Financial Studies* 8 (4):1153-1183.

Loughran, T., and P. Schultz. 2005. Liquidity: Urban versus rural firms. *Journal of Financial Economics* 78 (2):341-374.

Massoud, N., D. Nandy, A. Saunders, and K. Song. 2011. Do hedge funds trade on private information? Evidence from syndicated lending and short-selling. *Journal of Financial Economics* 99 (3):477-499.

McNichols, M. 1984. *The anticipation of earnings in securities markets*: University of California, Los Angeles--Management.

Miihkinen, A. 2012. What drives quality of firm risk disclosure?: The impact of a national disclosure standard and reporting incentives under ifrs. *The International Journal of Accounting* 47 (4):437-468.

Mitts, J., and E. L. Talley. 2018. Informed trading and cybersecurity breaches. *Available at SSRN: https://ssrn.com/abstract=3107123*.

Modi, S. B., M. A. Wiles, and S. Mishra. 2015. Shareholder value implications of service failures in triads: The case of customer information security breaches. *Journal of Operations Management* 35:21-39.

Piotroski, J. D., and D. T. Roulstone. 2004. The influence of analysts, institutional investors, and insiders on the incorporation of market, industry, and firm-specific information into stock prices. *The Accounting Review* 79 (4):1119-1151.

Roll, R. 1984. A simple implicit measure of the effective bid-ask spread in an efficient market. *The Journal of Finance* 39 (4):1127-1139.

Saffi, P. A., and K. Sigurdsson. 2010. Price efficiency and short selling. *The Review of Financial Studies* 24 (3):821-852.

Schnitzlein, C. R. 2002. Price formation and market quality when the number and presence of insiders is unknown. *The Review of Financial Studies* 15 (4):1077-1109.

SEC. 2011. Cf disclosure guidance: Topic no. 2. Available at: Https://www.Sec.Gov/divisions/corpfin/guidance/cfguidance-topic2.Htm.

———. 2018. Commission statement and guidance on public company cybersecurity disclosures, available at: Https://www.Sec.Gov/rules/interp/2018/33-10459.Pdf.

Selznick, L. F., and C. LaMacchia. 2016. Cybersecurity: Should the SEC be sticking its nose under this tent. *Journal of Law, Technology & Policy* 16 (1):35-70.

Seyhun, H. N. 1986. Insiders' profits, costs of trading, and market efficiency. *Journal of Financial Economics* 16 (2):189-212.

Spanos, G., and L. Angelis. 2016. The impact of information security events to the stock market: A systematic literature review. *Computers & Security* 58:216-229.

Steinbart, P. J., R. L. Raschke, G. Gal, and W. N. Dilla. 2018. The influence of a good relationship between the internal audit and information security functions on information security outcomes. *Accounting, Organizations and Society*.

Stoll, H. R. 1989. Inferring the components of the bid-ask spread: Theory and empirical tests. *The Journal of Finance* 44 (1):115-134.

Telang, R., and S. Wattal. 2007. An empirical analysis of the impact of software vulnerability announcements on firm stock price. *IEEE Transactions on Software Engineering* (8):544-557.

Wang, T., K. N. Kannan, and J. R. Ulmer. 2013. The association between the disclosure and the realization of information security risk factors. *Information systems research* 24 (2):201-218.

Weller, B. M. 2017. Does algorithmic trading reduce information acquisition? *The Review of Financial Studies* 31 (6):2184-2226.

Westland, J. C. 2018. The information content of sarbanes-oxley in predicting security breaches. *Management Science* Forthcoming (Manuscript ID: MS-17-00363).

Yayla, A. A., and Q. Hu. 2011. The impact of information security events on the stock value of firms: The effect of contingency factors. *Journal of Information Technology* 26 (1):60-77.

Appendix A

A1. Construction of Cybersecurity risk Mitigation Scores

Cybersecurity risk mitigation scores are calculated based on cyber-related disclosures in firm's 10-Ks. To identify cyber-related disclosures, we developed a keyword list using a glossary of common cybersecurity terminology from the National Initiative for Cybersecurity Careers and Studies (NICCS) and a report on laws relating to cybersecurity prepared by the Congressional Research Service (Fischer 2014). Cyber-related keywords and phrases were incorporated into the disclosure mapping logic to develop an initial corpus of cyber-security disclosures. This dictionary was refined through an iterative process of testing the original list against samples of disclosures from a variety of industry groupings. In this process, an effort was made to prune false positives while minimizing the risk of false negatives.

Each cyber excerpt was assigned a score (*CyberWords*) which is the word count of the cyber excerpt. Next, we identify a list of mitigation-related words to create a score that reflects cybersecurity risk mitigation (*MitigationWords*). The dictionary of mitigation words was developed by a team consisting of one of the authors on this project and two other independent research assistants. The team independently went through cyber excerpts and identified mitigation-related words and phrases. The team then resolved any discrepancies and refined the dictionary. Each mitigation word / phrase found within the excerpt is given a score of one and scores are tallied across all excerpts identified as true positives within a particular filing to compute a total score for the whole filing.

A2. Cybersecurity Risk Mitigation Wordlist

actionable
address the risk
analysis of our security
analysis of our technologies
ciso
compliance
confidentiality agreement
consult
data management
detect
develop new polic(y|ies)
encrypt
enhancement
expert
hardened firewall
implement
independent analysis
independent review
insur
mitigat
monitor
monitoring solution
personnel
polic(y|ies) review
policies procedures and controls
policy solution
pre(| |\\-)emptive
predict
prevent
privacy and security management
privacy program
project(i|e)
protect
protocol
remedi
risk and fraud management
security analysis
security brief
security capabil
security enhancement
security process
security program
security protocol
security review
security solution
security tool
self(|\\-)regulatory
standards review
strategy
tak(e|ing) step
train
validat
verif
voluntary self(|\\-)disclosure
vulnerability assessment
vulnerability management

A3. Examples of Cyber Excerpts Containing Risk Mitigation Themes

1. Ellie Mae (FY 2015, reporting date: Feb 25, 2016)

16 cybersecurity-related excerpts were identified with a total *MitigationWords* score of 51. Below is an example for 1 out of the 16 excerpts.

"All sensitive data transmitted over public networks is **encrypt**ed using industry standard **encrypt**ion **protocol**s in order to **protect** sensitive data against third-party disclosure in transit. Servers and network components are secured with access control mechanisms and **protect**ed by **hardened firewall**s, virus **protect**ion, and intrusion **prevent**ion/**detect**ion systems. Security services are **monitor**ed and updated in order to address emerging vulnerabilities. Even with our current security **monitor**ing and **detect**ion systems, we cannot guarantee that our security measures will **prevent** security breaches. We are committing significant resources to **protect** against and remedy any potential security breaches and their consequences and intend to keep doing so in the future. New threats and vulnerabilities are identified frequently and there are often time lags before our vendors deploy **mitigat**ions. In 2015 we made substantial investment in our network security infrastructure, including headcount and third party tools and systems. In 2016 and beyond we will continue to make substantial investments in our network security infrastructure to **protect** the confidentiality of the information stored in our data centers."
For this excerpt MitigationWords: 16

The full disclosure is available in:
https://cookesg.com/abstract.php?analysis=cybersecurity&year=2016&cocik=1122388&filingtype=10-K&relevance_filter=1&risk=2#

2. Capella Education Company (FY 2015, reporting date: Feb 18, 2016)

4 cybersecurity-related excerpts were identified with a total *MitigationWords* score of 15. Below is an example for 1 out of the 4 excerpts.

"Capella has an information **security program** that includes leadership, tools, processes, and **train**ing. To **protect** our information assets, Capella's information security practices are designed to reduce information security and IT risks, respond to incidents, establish appropriate standards and controls, and establish, **implement**, and maintain information security policies and procedures. These practices include an education and **train**ing program on information security and privacy matters for employees and external stakeholders."
For this excerpt MitigationWords: 5

The full disclosure is available in:
https://cookesg.com/abstract.php?isabstract=1&year=2015&analysis=6&filename=0001104349-15-000009

3. Fossil Group (FY 2016, reporting date: Feb 29, 2016)

6 cybersecurity-related excerpts were identified with a total *MitigationWords* score of 7. Below is an example for 1 out of the 4 excerpts.

"We may experience operational problems with our information systems as a result of system failures, viruses, computer "hackers" or other causes. Any material disruption or slowdown of our systems could cause information, including data related to customer orders, to be lost or delayed which could result in delays in the delivery of merchandise to our stores and customers or lost sales, which could reduce demand for our merchandise and cause our sales to decline. Moreover, the failure to maintain, or a disruption in, financial and management control systems could have a material adverse effect on our ability to respond to trends in our target markets, market our products and meet our customers' requirements."

For this excerpt MitigationWords: 0

The full disclosure is available in:
https://cookesg.com/abstract.php?isabstract=1&year=2016&analysis=6&filename=0000883569-16-000005

Appendix B: Variable Definitions

Variable	Definition	Source
Cybersecurity risk mitigation score		
MitigationWords	Number of cyber mitigation words or phrases in all cyber-related excerpts in a firm's disclosures in the entire 10-K filing for a given year.	10-Ks
LMitigationWords	Natural logarithm of *MitigationWords* plus one.	10-Ks
Liquidity measures		
ESPREAD	Effective spread. The difference between an estimate of the true value of the security (the midpoint of the bid and ask) and the actual transaction price.	DTAQ
LAMBDA	Kyle's lambda.	DTAQ
AMI	Amihud (2002) illiquidity measure, computed as the ratio of absolute value of daily stock return to the daily dollar trading volume	CRSP
PJR, Earnings surprise and short selling measures		
PJR	Price Jump Ratio, computed as abnormal returns relative to a Fama and French (1992) three-factor model using daily returns over a 365-calendar day window ending 90 days before the earnings announcement. The pre-announcement window starts on day -21 and ends 2 trading days after the earnings announcement. The announcement return window starts on day 0 and ends 2 days after the earnings announcement.	CRSP
RSURPRISE	The quarterly rank decile of the earnings surprise, where earnings surprise is defined as the difference between the actual earnings per share and the most recent average earnings per share forecast from I/B/E/S, scaled by the absolute value of this most recent average earnings per share forecast.	I/B/E/S
$\overline{ASHVOL(-5,-1)}$	Average daily abnormal short volume over the week before the earnings announcement.	FINRA
Firm controls		
CyberWords	Number of words or phrases in all cyber-related excerpts in a firm's disclosures in the entire 10-K filing for a given year.	CookESG
LCyberWords	Natural logarithm of *CyberWords* plus one.	CookESG
LNMV	The natural logarithm of the stock's market capitalization.	The merged CRSP - COMPUSTAT
IO	Institutional ownership ratio at the end of the preceding quarter.	Thomson Reuters
ANALYST	Number of analysts covering the stock.	I/B/E/S
LN(PRC)	Natural logarithm of the closing share price.	CRSP
TURN	Number of shares traded as a proportion of shares outstanding (in thousands)	CRSP
BM	Book to market equity ratio.	The merged CRSP - COMPUSTAT
BIDASK	Percentage difference between the closing bid and share price.	CRSP
STDRET	Standard deviation of daily stock	CRSP
CAR(-40,-6)	Cumulative abnormal return over event dates -40 to -6.	CRSP
CAR(-5,-1)	Cumulative abnormal return over event dates -5 to -1.	CRSP

Table 1: Descriptive Statistics

Panel A: Cybersecurity risk mitigation score and controls

	N	Mean	Median	Std Dev	Min.	Max.
MitigationWords	30,187	6.469	3.000	13.000	0.000	305.000
LMitigationWords	30,187	1.338	1.386	1.125	0.000	5.724
PJR	27,168	0.511	0.507	1.041	-3.201	4.288
ESPREAD	30,187	0.002	0.001	0.002	0.000	0.014
LAMBDA	30,187	0.249	0.101	0.407	0.005	2.558
AMI	30,187	10.071	3.329	20.218	0.067	137.945
ASHVOL(-5,-1)	30,187	0.013	0.009	0.038	-0.077	0.139
RSURPRISE	30,187	4.496	4.000	2.868	0.000	9.000
LCyberWords	30,187	5.241	5.886	2.272	0.000	9.712
LNMV	30,187	14.419	14.275	1.628	11.383	18.792
LN(PRC)	30,187	3.297	3.395	0.970	0.598	5.409
LN(STDRET)	30,187	-4.030	-4.069	0.513	-5.110	-2.652
ANALYST	30,187	9.680	7.000	7.304	1.000	33.000
IO	30,187	0.598	0.677	0.276	0.000	1.000

Panel A reports descriptive statistics of the cybersecurity risk mitigation scores measure and firm control variables in our sample. The sample period is between 2012 to 2016. All variables are defined in the Appendix B.

Panel B: Pearson correlations

		1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*
1	***MitigationWords***												
2	***LMitigationWords***	0.72											
3	***PJR***	0.02	0.03										
4	***ESPREAD***	-0.02	-0.02	-0.03									
5	***LAMBDA***	0.00	0.00	0.00	0.00								
6	***AMI***	-0.01	-0.01	0.00	0.14	0.01							
7	***ASHVOL(-5,-1)***	-0.01	0.01	0.00	0.10	0.02	0.06						
8	***RSURPRISE***	0.06	0.06	0.02	0.00	0.01	0.00	0.00					
9	***LCyberWords***	0.42	0.68	0.02	-0.11	0.00	0.00	-0.01	0.05				
10	***LNMV***	-0.04	-0.11	0.01	-0.63	-0.01	-0.06	-0.11	-0.01	0.18			
11	***LN(PRC)***	-0.04	-0.05	0.03	-0.51	-0.01	-0.02	-0.08	-0.04	0.09	0.69		
12	***LN(STDRET)***	0.04	0.05	-0.03	0.34	0.01	0.00	0.01	0.01	-0.06	-0.48	-0.51	
13	***ANALYST***	0.07	0.00	0.01	-0.42	0.00	-0.04	-0.07	0.02	0.17	0.69	0.39	-0.20

This table reports Pearson correlations between the liquidity measures and the independent and control variables in our sample. The sample period is 2012 to 2016, and there are 30,187 firm-year observations. All correlations with an absolute value larger than 0.012 are significant at the 5% level and all correlations with an absolute value larger than 0.015 are significant at the 1% level. All variables are defined in Appendix B.

Table 2: Cybersecurity Risk Mitigation and the Price Jump Ratio

	(1)		(2)		(3)		(4)		(5)		(6)	
	Est.	**t-stat**	**Est.**	**t-stat**	**Est.**	**t-stat**	**Est.**	**t-stat**	**Est.**	**t-stat**	**Est.**	**t-stat**
Intercept	0.644	6.04	0.658	6.06	0.840	4.94	0.574	6.11	0.621	5.79	0.768	9.25
LMitigationWords	0.026	3.79	0.020	2.21	0.012	0.84	0.028	4.22	0.028	3.82	0.015	2.64
LCyberWords			0.004	1.03	0.005	0.84	0.002	0.42	-0.004	-1.06	0.001	0.32
LNMV	-0.044	-5.86	-0.046	-5.86	-0.051	-3.48	-0.042	-5.65	-0.023	-2.37	-0.010	-1.65
LN(PRC)	0.041	3.23	0.042	3.23	0.038	2.26	0.024	2.27	-0.004	-0.38	0.002	0.26
BIDASK	-0.142	-2.59	-0.145	-2.63	-0.230	-2.96	-0.179	-3.69	-0.245	-5.09	-0.135	-3.69
LN(STDRET)	-0.059	-2.74	-0.059	-2.76	-0.045	-1.34	-0.085	-5.06	-0.079	-5.37	-0.041	-3.07
ANALYST	0.003	2.23	0.003	2.25	0.004	1.41	0.002	1.30	0.003	1.73	0.001	1.49
IO	0.127	5.34	0.127	5.37	0.072	1.50	0.135	5.59	0.138	5.20	0.079	3.69
Year FE	YES		YES		YES		YES		YES		YES	
N	26,284		26,284		28,918		21,909		26,333		26,373	
Adj R2	0.005		0.005		0.001		0.013		0.007		0.004	

$$PJR_{i,t} = a + \beta_1 LMitigationWords_{i,t} + \beta_2 LCyberWords_{i,t} + \beta_3 LNMV_{i,t} + \beta_4 LN(PRC)_{i,t} + \beta_5 BIDASK_{i,t} + \beta_6 LN(STDRET)_{i,t} + \beta_7 ANALYST_{i,t} + \beta_8 IO_{i,t} + \varepsilon_{i,t}$$

This table presents the results of cybersecurity risk mitigation and the price jump ratio. Column (1) presents the base model. Column (2) reports the base model including both *LMitigationWords* and *LCyberWords*. Column (3) reports results when we only exclude the percentile of observations with the lowest absolute *CAR*(-21,+2) instead of the decile of observations with the smallest absolute *CAR*(-21,+2). Column (4) presents results when we drop the quartile of observations with the lowest absolute *CAR*(-21,+2). Columns (5) and (6) repeat the analysis in the third column but employ *CAR*(-10,+2) and *CAR*(-3,+2) in the denominator of the PJR, respectively.

Table 3: Cybersecurity Risk Mitigation and Informativeness of Short Selling

	(1)		(2)		(3)		(4)		(5)		(6)	
	Est.	**t-stat**	**Est.**	**t-stat**	**Est.**	**t-stat**	**Est.**	**t-stat**	**Est.**	**t-stat**	**Est.**	**t-stat**
Intercept	4.83	10.06	4.96	10.01	-0.05	-0.46	4.94	10.10	3.26	6.31	4.95	9.71
LMitigationWords	0.18	7.36	0.13	3.83	0.03	3.32	0.13	3.90	0.15	3.76	0.13	3.67
LMitigationWords × ASHVOL (-5,-1)	1.21	2.73	1.41	2.45	0.35	2.50	0.78	2.10	1.44	2.26	1.52	2.69
ASHVOL (-5,-1)	-2.37	-3.24	-1.86	-1.62	0.01	0.04	-0.88	-1.09	-2.44	-2.15	-1.87	-1.64
LCyberWords			0.03	1.92	0.00	0.94	0.03	1.94	0.03	1.60	0.03	1.72
LCyberWords × ASHVOL (-5,-1)			-0.15	-0.56	-0.07	-1.01	-0.09	-0.48	-0.05	-0.17	-0.22	-0.84
LNMV	0.02	0.64	0.00	0.07	0.01	1.51	0.00	0.10	0.08	2.13	0.00	0.09
BM	-0.22	-2.28	-0.23	-2.32	-0.07	-2.07	-0.23	-2.34	-0.35	-4.50	-0.22	-2.25
LN(PRC)	-0.17	-3.76	-0.16	-3.65	-0.02	-1.69	-0.16	-3.64	0.06	1.28	-0.16	-3.78
BIDASK	-3.58	-0.16	-6.75	-0.30	4.17	0.72	-7.74	-0.35	25.19	1.08	-13.76	-0.61
TURN	0.10	1.82	0.11	1.93	0.00	-0.12	0.10	1.90	0.02	0.41	0.12	2.16
STDRET	-10.89	-3.93	-11.09	-3.97	-2.05	-1.83	-10.86	-3.89	-13.88	-3.99	-10.50	-3.46
CAR(-40,-6)	52.68	5.49	52.73	5.52	10.73	5.88	52.98	5.53	50.98	4.89	54.04	5.14
CAR(-5,-1)	20.88	5.39	20.84	5.36	4.59	4.79	20.67	5.30	21.32	6.28	21.35	5.69
Year FE	YES		YES		YES		YES		YES		YES	
N	29,639		29,639		29,639		29,639		27,075		29,639	
Adj R2	0.017		0.017		0.001		0.017		0.030		0.017	

$$RSURPRISE_{i,t} = \alpha + \beta_1 LMitigationWords_{i,t} + \beta_2 ASHVOL(-5,-1)_{i,t} + \beta_3 LMitigationWords_{i,t} \times ASHVOL(-5,-1)_{i,t} + \beta_4 LNMV_{i,t} +$$
$$\beta_5 BM_{i,t} + \beta_6 LN(PRC)_{i,t} + \beta_7 BIDASK_{i,t} + \beta_8 TURN_{i,t} + \beta_9 STDRET_{i,t} + \beta_{10} CAR(-40,-6)_{i,t} + \beta_{11} CAR(-5,-1)_{i,t} + YearFE + \varepsilon_{i,t}$$

This table presents the results of cybersecurity risk mitigation and the informativeness of short selling. Column (1) presents the base model. Column (2) reports the base model including both *LCyberWords* and *LMitigationWords*. Column (3) reports the results when we use the actual earnings surprise instead of decile rank as the dependent variable. Column (4) presents the results when we capture abnormal short selling based on the day before the earnings announcement rather than the week before the earnings announcement. Column (5) reports the results when the earnings surprise

measure is calculated as the difference between the actual earnings per share and the most recent average earnings per share estimate across analysts, scaled by the standard deviation across analyst estimates. Column (6) presents the results using the median earnings per share forecast across analysts instead of the mean earnings per share forecast to calculate the earnings surprise measure.

Table 4: Cybersecurity Risk Mitigation and Liquidity in Pre-Earnings Announcements

Panel A: Cybersecurity risk mitigation and liquidity leading up to earnings announcements

	(1)		(2)		(3)	
	ESPREAD		***LAMBDA***		***AMI***	
day	**Est.**	**t-stat**	**Est.**	**t-stat**	**Est.**	**t-stat**
-10	-0.006	-0.50	-0.007	-1.10	-0.007	-0.88
-9	-0.010	-0.98	-0.009	-1.33	0.003	0.33
-8	-0.003	-0.28	-0.010	-1.45	-0.010	-1.18
-7	-0.008	-0.68	0.002	0.26	-0.003	-0.41
-6	-0.007	-0.67	-0.007	-1.05	-0.015	-2.10
-5	0.004	0.40	-0.007	-1.04	-0.012	-1.65
-4	-0.024	-2.38	-0.012	-1.89	-0.012	-1.71
-3	-0.020	-1.95	-0.037	-5.63	-0.030	-3.98
-2	-0.030	-3.22	-0.027	-3.98	-0.025	-3.71
-1	-0.027	-3.11	-0.041	-6.33	-0.040	-6.60

Panel B: Cybersecurity risk mitigation and liquidity leading up to earnings announcements including *LCyberWords*

	(1)		(2)		(3)		(4)		(5)		(6)	
	ESPREAD				***LAMBDA***				***AMI***			
	LMitigationWords		***LCyberWords***		***LMitigationWords***		***LCyberWords***		***LMitigationWords***		***LCyberWords***	
day	**Est.**	**t-stat**	**Est.**	**t-stat**	**Est.**	**t-stat**	**Est.**	**t-stat**	**Est.**	**t-stat**	**Est.**	**t-stat**
-10	0.003	0.23	-0.006	-0.69	-0.014	-1.57	0.005	0.99	-0.007	-0.79	0.000	0.01
-9	0.008	0.59	-0.013	-1.62	0.005	0.58	-0.010	-2.15	-0.004	-0.38	0.005	0.94
-8	-0.004	-0.29	0.001	0.13	-0.006	-0.64	-0.003	-0.62	-0.006	-0.66	-0.002	-0.44
-7	0.002	0.10	-0.007	-0.67	0.009	0.95	-0.005	-1.06	-0.007	-0.79	0.003	0.61
-6	-0.014	-0.85	0.005	0.63	0.005	0.49	-0.008	-1.72	-0.017	-1.79	0.001	0.25
-5	0.001	0.05	0.002	0.35	-0.002	-0.22	-0.004	-0.78	-0.019	-2.13	0.005	1.09
-4	-0.023	-1.68	-0.001	-0.10	-0.006	-0.72	-0.004	-0.93	-0.016	-1.88	0.003	0.70
-3	-0.031	-2.05	0.008	1.10	-0.028	-3.17	-0.006	-1.32	-0.036	-4.06	0.004	0.85
-2	-0.038	-2.88	0.005	0.82	-0.030	-3.44	0.002	0.55	-0.028	-3.37	0.002	0.47
-1	-0.031	-2.19	0.003	0.40	-0.042	-5.10	0.001	0.15	-0.042	-6.01	0.002	0.41

The table presents the results of the coefficients of interest for each of the 10 days preceding earnings announcements (day 0) based on the following regression model:

$$A_LM_{1-3,i,q,t} = a + \beta_1 LMitigationWords_{i,q} + \beta_2 LCyberWords_{i,q} + \beta_3 LNMV_{i,q} + \beta_4 TURN_{i,q} + \beta_5 STDRET_{i,q} + YearFE + \varepsilon_{i,q,t}$$

Panel A reports the estimated coefficients of models including only mitigation words *LMitigationWords*; and results in Panel B are for models including both *LMitigationWords* and *LCyberWords*.

Liquidity is measured as: the quoted spread (*QSPREAD*), effective spread (*ESPREAD*), realized spread (*RSPREAD*), price impact (*PI*), lambda (*LAMBDA*) and Amihud's illiquidity measure (*AMI*). All variables are defined in Appendix B. Standard errors are clustered by firm and quarter-year. The sample period is 2012 to 2016 and there are 28,345 earnings announcements in our sample. *,**,*** represent significance significant at the 0.10, 0.05 and 0.01 level, respectively.

Table 5: Controlling for 10-K Characteristics

Panel A: Cybersecurity risk mitigation and Price Jump Ratio

	(1)		(2)		(3)		(4)		(5)	
	Est.	**t-stat**	**Est.**	**t-stat**	**Est.**	**t-stat**	**Est.**	**t-stat**	**Est.**	**t-stat**
Intercept	0.708	5.32	0.938	4.90	0.628	5.96	0.612	5.54	0.815	9.28
LMitigationWords	0.023	2.54	0.019	0.94	0.028	4.24	0.028	4.03	0.018	3.10
LCyberWords	0.004	1.21	0.003	0.36	0.002	0.58	-0.003	-0.78	0.000	-0.14
L10KWords	-0.007	-1.47	-0.007	-0.72	-0.005	-1.39	0.001	0.18	-0.004	-1.10
L10KMitigationWords	-0.006	-2.41	-0.011	-1.87	-0.002	-0.98	-0.001	-0.33	0.000	-0.23
LNMV	0.040	3.20	0.039	2.01	0.024	2.44	-0.001	-0.10	0.002	0.19
LN(PRC)	-0.145	-2.55	-0.286	-3.32	-0.181	-3.75	-0.247	-4.97	-0.128	-3.32
BIDASK	-0.043	-5.46	-0.048	-2.88	-0.040	-5.54	-0.025	-2.51	-0.010	-1.59
STDRET	-0.057	-2.76	-0.043	-1.10	-0.079	-4.65	-0.082	-4.80	-0.038	-2.71
ANALYST	0.003	1.89	0.004	1.39	0.001	1.20	0.002	1.58	0.002	1.79
IO	0.155	6.76	0.060	1.12	0.146	5.45	0.137	4.96	0.087	4.33
N	26,284		28,918		21,909		26,333		26,373	
Adj R2	0.005		0.001		0.013		0.007		0.004	

Panel A presents the results of cybersecurity risk mitigation and the price jump ratio after controlling for 10-K characteristics (*L10KWords* and *L10KMitigationWords*). Columns (1) reports the base model including both *LCyberWords* and *LMitigationWords*. Column (2) reports the results when we only exclude the percentile of observations with the lowest absolute *CAR*(-21,+2) instead of the decile of observations with the smallest absolute *CAR*(-21,+2). Column (3) presents the results when we drop the quartile of observations with the lowest absolute *CAR*(-21,+2). Columns (4) and (5) repeat the analysis in the first column but uses *CAR*(-10,+2) and *CAR*(-3,+2) in the denominator of the PJR, respectively.

Panel B: Cybersecurity risk mitigation and short selling activity

	(1)		(2)		(3)		(4)	
	Est.	**t-stat**	**Est.**	**t-stat**	**Est.**	**t-stat**	**Est.**	**t-stat**
Intercept	4.909	10.79	-0.020	-0.18	3.291	7.15	4.885	10.57
LMitigationWords	0.140	4.02	0.029	3.40	0.149	3.89	0.135	3.82
LCyberWords	0.029	1.68	0.004	0.80	0.024	1.34	0.025	1.46
L10KWordcount	0.000	0.05	0.000	0.01	-0.001	-0.14	0.000	0.03
L10KMitigationWords	-0.005	-0.62	-0.002	-1.14	0.004	0.37	-0.006	-0.74
ASHVOL (-5,-1)	-1.882	-1.19	0.281	0.55	-1.872	-1.50	-2.014	-1.33
LCyberWords × ASHVOL (-5,-1)	-0.154	-0.60	-0.090	-1.18	-0.121	-0.45	-0.215	-0.81
LMitigationWords × ASHVOL (-5,-1)	1.368	2.49	0.369	2.86	1.478	2.43	1.469	2.67
L10KCyberWords × ASHVOL (-5,-1)	-0.011	-0.11	-0.035	-1.58	-0.073	-0.78	-0.007	-0.07
L10KMitigationWords × ASHVOL (-5,-1)	0.026	0.16	0.004	0.11	0.023	0.17	0.054	0.34
LNMV	0.011	0.36	0.011	1.46	0.074	2.24	0.014	0.45
BM	-0.248	-2.46	-0.082	-2.32	-0.365	-4.64	-0.233	-2.39
LN(PRC)	-0.174	-3.94	-0.023	-1.75	0.075	1.49	-0.180	-4.09
BIDASK	-0.032	-0.14	0.027	0.47	0.344	1.60	-0.106	-0.47
TURN	0.120	2.31	-0.003	-0.19	0.020	0.41	0.138	2.60
STDRET	-11.898	-4.06	-2.202	-1.92	-13.861	-4.00	-11.392	-3.56
CAR(-40,-6)	53.405	5.59	11.212	6.3	51.517	4.82	54.684	5.18
CAR(-5,-1)	21.350	5.33	4.611	4.72	21.417	6.08	21.801	5.68
N	29,639		29,639		27,075		29,639	
Adj R2	0.017		0.001		0.030		0.017	

Panel B presents the results of cybersecurity risk mitigation and the informativeness of short selling after controlling for 10-K characteristics (*L10KWords* and *L10KMitigationWords*). Column (1) reports the results using ranked decile rank earnings surprise as the dependent variable. Column (2) reports the results when we use the actual earnings surprise instead of decile rank as the dependent variable. Column (3) reports the results when the earnings surprise measure is calculated as the difference between the actual earnings per share and the most recent average earnings per share estimate across analysts, scaled by the standard deviation across analyst estimates. Column (4) presents the results using the median earnings per share forecast across analysts instead of the mean earnings per share forecast to calculate the earnings surprise measure.