# Can Insider Trades Reliably Predict Cybersecurity Hazards in Public Firms?


**Abstract**

The business-ending risks of cybersecurity incidents threaten the interests of a firm and its investors. However, these risks are inflated for investors due to the information asymmetries they have with firm insiders about a firm's vulnerabilities and cybersecurity readiness. To protect the investors against possible information asymmetries, the U.S. Securities and Exchange Commission utilizes two general tools, public reports (e.g., 10-K's and 10-Q's) and disclosures of insider trading, as direct and indirect signals, respectively. This study examines the effectiveness of these two general tools in reducing the specific information asymmetries that exist about the cyber risks of a firm. Utilizing quarterly observations of over 1,900 firms from 2011 to 2017, we show that the firm's disclosure of cyber risks in 10-Q reports, in isolation, does not reliably signal a subsequent cybersecurity incident. In contrast, a firm's heightened levels of insider trading, in the form of selling the firm's securities, can reliably predict the cybersecurity hazard. Moreover, we find that the signals sent via disclosing insiders' trades enhance the reliability of risk disclosures in 10-Q reports in signaling future incidents. Our identification strategy focuses on the utilization of instrumental variables, removing first differences, and verification of the main observational findings in a more controlled and restricted sample. The results remain robust in models with alternative measures and estimations.



**Keywords:** Signaling, cybersecurity incident, information asymmetry, insider trades, public report


## Introduction

The rise in the extent and frequency of cybersecurity incidents, combined with their increasingly business-ending impacts (Deloitte, 2017), has raised concerns for financial markets (e.g., Fazzini, 2018). More critically, uncertainties around such disruptive incidents have exacerbated information asymmetries that exist between a firm and its investors (Amir, Levi, & Livne, 2018). Therefore, the question about how to reduce the information asymmetries about the firm's cybersecurity risks has grown in importance and remains unresolved. In this study, we seek to examine the effectiveness of two corporate reporting tools in the U.S. that could potentially curtail such asymmetries.

Particularly, we focus on transparency tools that exist through the mandates of the U.S. Securities and Exchange Commission (SEC), which is tasked to "protect investors; maintain fair, orderly, and efficient markets; and facilitate capital formation."[1] The SEC is equipped with a set of general transparency tools that have the potential to help in the specific case of reducing the information asymmetry that is related to cybersecurity breach incidents. On the one hand, and through *direct signals*, the public reports (e.g., 10-Q forms) allow firms to directly communicate risk information to outsiders on a regular basis. On the other hand, SEC has long had a policy, through requesting information in forms 3-5, to allow firms to disclose their personal trades, thereby *indirectly* communicating risk information[2] (e.g., managerial perceptions) to the market.

If uncertainties around cybersecurity risks were only faced by investors (i.e., the firm's insiders were fully informed) and firms were fully upfront about all their information, disclosure of cybersecurity risks in public reports would suffice to eliminate the related information asymmetries. The first condition is unrealistic since cybersecurity incidents can even catch insiders off guard. More importantly, direct information, such as the extent of preventive investments and results of internal audits are either insufficient to explain future incidents or firms may take a minimal approach in their disclosure (Amir et al., 2018) out of their fear of losing customers or attracting malicious outsiders to exploit the vulnerabilities hinted in a public report. Therefore, public reports alone are not sufficient to completely eliminate information asymmetries.

Research in accounting and corporate finance has highlighted the effectiveness of another category of SEC reports, i.e., those related to executives' insider trades. These reports have the potential to be similarly effective in reducing cyber-risk asymmetries. Particularly, while research shows that a firm's executives engage in trading their firm's securities when information asymmetries exist between the firm and its investors (Aboody & Baruch, 2000), the literature also provides robust evidence that those executives do so especially in cases where investors are asymmetrically informed about the financial risks to the firm, e.g., in case of financial under-performance (Chen, Martin, & Wang, 2013; Summers & Sweeney, 1998). Thus, suggesting that

[1] https://www.sec.gov/Article/whatwedo.html

[2] By direct information we mean a type of information that can be backed by physical or other robust kinds of evidence. For instance, numbers presenting the financial well-being of the firm or information about new contracts are considered material information. On the contrary, speculations, insights, foresights, and foreknowledge all fall in the category of indirect information. Public firms in the U.S. have a duty to disclose direct information that is material to the public.

executives' trading of firm securities can be used as signals of the heightened risk (e.g., Chung & Charoenwong, 1998).

Given the cyber-risk asymmetries mentioned above, and established evidence about the effectiveness of executives' trading in signaling financial risks, the empirical question is whether or not those executives' trades are also informative in reducing cyber-risk asymmetries. The answer to that question depends largely on: (a) whether executives make trades related to cybersecurity events in the firm, and (b) whether those trades reduce the information gap with investors. There are more expectations for part (a) because there is anecdotal evidence about the relationship between cybersecurity breaches and the dumping of the top manager's shares prior to a public breach announcement[3]. Also, research shows that cybersecurity breach announcements influence a firm's market value and stock prices (Campbell, Gordon, Loeb, & Zhou, 2003; Cavusoglu, Mishra, & Raghunathan, 2004; Goel & Shawky, 2009; Hovav & D'Arcy, 2003). Additionally, in similar cases of imminent bad news, corporate insiders in firms have been known to perform insider trades in the form of selling the firm's securities (Aboody & Baruch, 2000).

However, unlike part (a), part (b) is less clear and is the main target of the current study. Particularly, given the technical complexity of cybersecurity breaches and corrective initiatives that may follow them, *it is not immediately evident that insiders possess superior information relative to investors*. As such, the primary questions in this study pertain to *RQ1: Whether or not firm insiders engage in behavior that is indicative of subsequent (next-quarter) security breach incidents?* Besides, the regulatory instruments are rarely scrutinized together to understand their inter-relationships with respect to cybersecurity breach incidents. Given that the direct and indirect signals to the markets serve different purposes, we tease them apart to clarify the level of synergy that exists between parts of the signals (e.g., quarterly reports and insider trading reporting). As such, the second question is *RQ2: Whether or not any likely insider trading reporting before a security reach incident (announcement) enhances the signaling value of 10-Q reports filed before the incident?*

This paper addresses the above research questions by drawing upon prior literature on insider trading, cybersecurity incidents, and information asymmetry to develop hypotheses. The hypotheses are tested using panel data compiled from multiple sources (Reuters-Thompson, Privacy Rights Clearinghouse, Lexis-Nexis, COMPUSTAT, and the SEC's EDGAR) for a sample

[3] https://www.justice.gov/usao-ndga/pr/former-equifax-employee-sentenced-insider-trading

of 48,312 firm-quarter observations, belonging to 1,914 firms, over 7 years from 2011 to 2017. Our evidence is limited to manufacturing, information, retail, wholesale trading, utilities, transportation and warehousing, and healthcare industries. Despite this limitation, the results of our analysis, after controlling for firm and industry characteristics, show that one standard deviation above-mean trading by executives in a given quarter is indicative of a reliable, albeit modest (9%) increase in the expected hazard of a cybersecurity breach in the subsequent quarter. Moreover, the results indicate that while the informativeness of public reports about cyber risks (e.g., 10-Q's) does not significantly predict an increase in the subsequent hazard of a cybersecurity incident, they have a significantly high impact on the subsequent hazard when accompanied by high levels of executives' selling of the firm's securities. These results indicate that executives' trades enhance the interpretability of risks disclosed in public reports by a firm. These findings are robust to a broad set of alternative specifications and analyses.

**Insider Trading as Indirect Signals of Reducing Information Asymmetries**

Prior literature suggests that individuals make "unusual" returns on their trades in securities of firms in which they are insiders (Chauhan, Chaturvedula, & Iyer, 2014; Finnerty, 1976). Some studies argue that insiders benefit from privileged access to internal information and provide evidence of profits from insider trading in varying contexts and over time (Ahuja, Coff, & Lee, 2005; Cohen, Malloy, & Pomorski, 2012; Finnerty, 1976; Jeng, Metrick, & Zeckhauser, 2003; Lakonishok & Inmoo, 2001; Lorie & Niederhoffer, 1968; Ravina & Sapienza, 2010; Seyhun, 1986).

Insider trading is distinct from market manipulation, disclosure of misleading or false information to the market, and direct expropriation of the firm's wealth by insiders. Moreover, insider trading and similar transactions based on uneven access to information are common and usually legal in labor, commodities, and real estate markets. While routine insider trading in corporate securities is legal, non-routine trading in a firm's securities is sometimes viewed as objectionable because of reasons such as potential violation of the fiduciary duties of corporate managers toward the shareholders (e.g., Coff & Lee, 2003). Also, the economic reason generally offered for prohibiting insider trading is its potential to adversely affect securities markets (Khanna, 1997) or diminish the firm's value (Haft, 1982).

Aside from the legal arguments for or against insider trading, all insiders of a firm – i.e., "a company's officers and directors, and any beneficial owners of more than ten percent of a class

of the company's equity securities registered under Section 12 of the Securities Exchange Act of 1934[4]" are mandated to report their trades (buy or sell), usually within 2 business days from the trade and up to 45 business days after, if trades are subject to SEC exceptions. This mandate enables markets to sense the pulse of the firm as perceived by its executives and major owners. Since insiders are not mandated to disclose the reasons for their trades, a selling (buying) of the firm securities are often interpreted as indirect signals of bad news/heightened risks (good news/lowered risks) to the market.

**The Ineffectiveness of Direct Signals: The Need for Indirect Signals**

With the prevalence of breach incidents, firms are under external pressure to report on the cybersecurity risks and related management activities[5]. There is evidence to suggest that firms voluntarily disclose information regarding their cybersecurity landscape and that such disclosures lead to positive sentiments in markets (Gordon, Loeb, & Sohail, 2010). Still, there remain questions about whether or not those disclosures are effective enough in predicting future incidents. First, the general literature in accounting has documented underreporting negative news in discretionary disclosures, such as those made in annual reports (e.g., Gleason & Mills, 2002; Rice, Weber, & Wu, 2015). Notably, firms are shown to withhold information relevant to their cybersecurity incidents (Amir et al., 2018). Second, per SEC's guidelines (see footnote 5), firms are not mandated to disclose information about their cyber risk when disclosing such information puts them in further danger. Third, given the complexity of cybersecurity incidents and factors leading to it, several factors that are impounded into cybersecurity risk fall outside the clear definition of *direct*, *material* information and therefore are omitted from public reports. The collection of these three reasons significantly reduces the effectiveness of public reports, as direct signals, in reducing cyber risk asymmetries.

Unlike public reports, disclosing executives' trades as indirect signals, designed to reduce information asymmetries with investors, are not impacted by the three conditions noted above. First, the existing literature supports that insiders capitalize on their knowledge gap with investors and engage in beneficial selling or purchasing the firm's securities (e.g., Aboody & Baruch, 2000; Kraft, Lee, & Lopatta, 2014). As such, the mere presence of negative news, in the form of

[4] https://www.sec.gov/fast-answers/answersform345htm.html
[5] https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm

heightened cyber risks, not only does not stifle trades but may also encourage selling the firm's securities. Second, because insiders are not required to disclose the reason for their trades, their selling of the firm's securities do not open their firm to additional cyber risks. Third, armed with their intuition about a likely threat or heightened risks, insiders may engage in personal trade and personal trades that are not bound to or based on direct information. Therefore, the reasons underlying the ineffectiveness of direct signaling tools of SEC are either irrelevant to or increase the effectiveness of insider trades as indirect signaling tools.

While it is easier to explain the effectiveness of insider trades in reducing information asymmetries that exist due to withholding direct information, explaining their effectiveness in reducing asymmetries about cyber risks is less straight-forward. The reason why insiders of a firm can be in possession of indirect information about cyber risks lies in the concept of managerial foresight, as explained by Ahuja et al. (2005).

Ahuja et al. (2005, p. 791) note that " managers possess some degree of strategic foresight" that is accumulated over time. They "demonstrate that when managers have foreknowledge about strategic assets, they may try to use it for personal gain by engaging in insider trading." An example of such foreknowledge account is in the patent domain where "information about patent breakthrough materializes at different times to different stakeholders, where at the onset, such information is tacit and difficult to convey, even within the firm" resulting in information asymmetry between organization insiders and investors (Ahuja et al., 2005, p. 791). In the same way, information about an imminent security breach (due to lax or unpatched systems) in an organization's systems could unfold to different insiders at different times and in various forms, making it difficult to express to others in the firm.

"Managerial foresight is the ability to predict how managers' actions can create a competitive advantage" (Ahuja et al., 2005, p. 792). The assumption is that managers have some foresight about upcoming events that may or may not be advantageous to them. It also argues that if managers played a role in creating those advantages, then they also have foresight on actions that led to those advantages.

Using the managerial foresight argument in the cybersecurity landscape, we argue that it is possible that managers who play a critical role in cybersecurity strategies also have foresight on actions that lead to a well- or ill-secured organization. Such foresight often translates to information asymmetries (Ahuja et al., 2005). For example, insiders of a firm may have, over time,

formed an opinion about the readiness of their firm when and if facing a targeted cybersecurity attack. Especially if this opinion is formed due to the absence of regular internal audits and drills, there is no direct news to share in public disclosures, but the inaction of the firm itself could cause the forming of the assessment of unreadiness. Such an assessment is indirect information that a manager has, and the public will be privy to it, absent information about the manager's trades.

Therefore, both the asymmetric possession of negative direct information, when withheld on the fear of further exposing a firm to cyber risks, and the asymmetric possession of negative indirect information in the form of managerial foreknowledge about cyber risks can incentivize a manager to sell the firm's securities to limit their personal loss. Therefore, we expect that accounting for other observables:

> H1: A firm's increase in selling of insider shares in a period is associated with a higher cybersecurity hazard in the subsequent period.

While we have explained that direct signals sent through public reports (e.g., 10-Q's) are limited in the extent of information disclosed, it is also worth noting that cybersecurity risk disclosures in public reports can also turn into boilerplate statements that do not change much over time. In our sample of SEC reports, we find that, on average, only one sentence out of each 33 sentences related to cybersecurity risks change from one year to another. That said, a close examination of these boilerplate statement changes indicates that firms do change the language of their disclosure in moderate extents immediately prior to the disclosure of cyber incidents. In our sample, a firm is almost three times as likely to increase the extent of information shared about its cyber risk (i.e., its cyber risk informativeness in public reports) in public reports released immediately before the disclosure of a major cybersecurity incident. In isolation, such moderate changes in the language of reports may not be sensed by the investors to alert them about imminent bad news. However, the presence of insider trades and their potential information about the imminent bad news can give more visibility to those moderate changes.

As such, even though we do not expect that boilerplate SEC report statements are informatively associated with an increased hazard of cybersecurity (as it is not clear if the slight changes are due to regular editing of the language in the report or due to actual changes in the cyber risks faced by the firm), we expect that insider trades increase the signaling power of the direct signals, as reflected in public reports. Therefore, we empirically study if:

H2: A firm's increase in selling of insider shares (indirect signals) in a period enhances the association between the informativeness of public reports about cybersecurity risks (direct signals) and the cybersecurity hazard in the subsequent period.

## Methodology

### Data

In creating our initial sample, we followed the guidelines by Gordon et al. (2010), which is a study on the impact of public disclosures about cybersecurity and subsequent market reaction. We obtained SEC disclosures of public firms, from the last quarter of 2011 to the last quarter of 2017. The last quarter of 2011 is the time that SEC released its transformative mandates about the disclosure of cybersecurity direct information and 2017 marks the final year for which we had access to data about the details of cybersecurity investment by firms as reported in the CI Database. A firm was kept in the sample only if: all of the firm's financial information was available, the firm's industry classification was not missing, and the values of the other variables in our empirical estimation (discussed below) were available. Our data exclude foreign firms, including those firms that are listed in the United States as common stock or American Depositary Receipts. We further eliminated firms in banking[6], insurance, and real estate, using Fama and French (1997) industry identifications, and winsorized the data in each 1 percent tail, following the work by Frank and Shen (2012). This process resulted in 48,312 firm-quarter observations belonging to 1,914 firms active mostly in manufacturing, information, retail, wholesale trading, utilities, transportation and warehousing, and healthcare.

Our panel data is compiled from multiple sources. First, we collected insider trading disclosure reports of individuals subject to the disclosure requirements from the Reuters-Thompson database. Quarterly (10-Q) reports are collected from SEC.gov's EDGAR database. Privacy Rights Clearinghouse was used to compile cybersecurity incidents from 2011 to 2017. The breach incidents were cross-referenced with those found in Lexis-Nexis. We also collected data pertinent to firms' financials from COMPUSTAT.

[6] The elimination of the financial industry is due to the different rules for and scrutiny over insider trading in this industry. Therefore, we acknowledge this exclusion as a limitation in our study. That said, the results remain robust when observations from these industries are included in the sample.

## Measures

Insider trading literature, information asymmetry is conceptualized using proxies such as firm size, number of analysts following the firms, the volume of trade, and the volatility of abnormal stock returns (Aboody & Baruch, 2000). **Report informativeness** (RI) is measured by the number of sentences in 10-Q with firm-specific information disclosed in security risk disclosures[7] of SEC filings (normalized by report length). This is an extension to Gordon et al.'s (2010) measure of disclosure.

To do so, paragraphs containing a set of some general keywords pertaining to cybersecurity (listed in Appendix A) were highlighted automatically, by a search engine. This process aides cutting the manual portion of task significantly as it cuts the time required for searching rather larger reports. Then, the task of highlighting particular sentences related to cybersecurity was broken between 214 master's students taking a cybersecurity auditing course in a Southern public university. Each report was assigned to at least 2 students (IRR=0.86). Sentence without disagreement were dropped from both numerator and denominator count in estimating RI.

**Abnormal trading** (AT) is the sales ratio (number of shares sold / (number of shares sold + number of shares bought)) adjusted for the 2-year average of shares sold in the same quarter[8]. We followed Piotroski & Roulstone (2005) in operationalizing this measure.

## Controls

In order to control for the factors contributing to the hazard of a breach in the firm, we consider two very important factors. First, we consider the extent to which an industry has been a target of cybersecurity attacks since that indicates both the extent to which an industry is a lucrative target for malicious outsiders and the extent to which information and knowledge about exploited vulnerabilities in similar firms are accessible to hacking communities. Therefore, we control for the industry-level extent of breach (**Ind-level breach),** which is the number of breaches that occurred in firms in the same 2-digit SIC code. **Investment emphasis** is the extent of cybersecurity investments in each firm based on the firm's business unit investments in 14 categories of

[7] We do not count broad/generic statements about cybersecurity risk or those related to the lack of risk as informative about a subsequent breach because their lack of association with firm-specific risks is rather obvious. We tried to control for declarations of no-risks, but such statements were made very rarely and the measure of the extent of clear no-risk declarations was highly correlated (0.68) with *Investment emphasis*, a control we already have included in our model.

[8] We do so, because some trades may be seasonal and not related to the risks of cybersecurity.

cybersecurity systems/software, as reported in the CI database[9]. For each business unit, we estimate the number of systems/software invested in (divided by the number of technologies surveyed in that given year), and the average value of investment ratio in the firm's business units is treated as the investment emphasis. This control variable intends to remove firm variations in the hazard of cybersecurity breaches due to their exercise of preventive investments (rather than the uncontrolled risk disclosed in public records or reflected in insiders' selling of the firm's securities). We also control for general firm characteristics, including firm size **(log of the number of employees**) and firm's total assets (**log of assets**) from COMPUSTAT, as well as the firm's research and development (**R&D**) budget measured as the R&D/sales from COMPUSTAT. Appendix B presents a summary of sample characteristics.

## Models

### A Cox Proportional Hazard Model

In order to assess the impact of informativeness of SEC reports and insider trades as signals indicating the hazard of a subsequent breach, we use a proportional hazard model, following similar studies in the context of cybersecurity, where both occurrence and timing of cybersecurity breaches are taken into account (e.g., Kwon & Johnson, 2014) . A hazard function, h(t), in the context of our study, pertains to the breach rate of a firm per the unit of time (t; a quarter). The proportional hazard model assumes that the elapsed time to fail, denoted by T, is dependent on a set of explanatory variables, including informativeness of SEC reports and insider trades. T is the time from the beginning of a period of time (quarter) until either a cybersecurity incident is observed or the end of that period of time. In such a case, the hazard ratio manifests the risk of facing a cybersecurity incident in a quarter. The log-likelihood (LL) expression of our models (without and with the interaction term) is as follows:

$$(EQ.1)\ LL_{it} = \beta \cdot RI_{it-1} + \lambda \cdot AT_{it-1} + \phi \cdot Control_{it-1} + Quarter\_Industry + \epsilon_{it} + +c_i$$

[9] The CI database reports the date of installation, as such this measure is time-varying. These 14 categories are: Anti-Virus Software, Network Firewall, Access Management or Identity Management Software, Network Management Software, Asset Management Software, Primary Virtual Private Network (VPN) Provider, Security Information & Event Management Software, Archiving and Backup, Network Management, Disaster Recovery Software, Surveillance Security System, Infrastructure as a Service, Storage Management or Backup and Recovery Software, Cloud Computing. For more information see: https://intermedia-global.co.uk/wp-content/uploads/2015/10/Aberdeen-Group-CITDB-RC.pdf

$$(EQ.2)\ LL_{it} = \beta \cdot RI_{it-1} + \lambda \cdot AT_{it-1} + \xi \cdot RI_{it-1} \cdot AT_{it-1} + \phi \cdot Control_{it-1} + Quarter\_Industry + \epsilon_{it} + +c_i$$

Where *i* subscript signifies the firm unit, *t* signifies the time period, Control is the vector of control variables, and Quarter_Industry is the vector quarter-industry fixed-effect dummies. All explanatory variables are measured at *t*-1[10]. To account for firm-specific variations, a distinct baseline hazard is enforced by stratification around firm ID. Also, standard errors reported are robust standard errors.

**Accounting for Self-Selection into Levels of RI and AT**

It is a stretch to assume that report informativeness and abnormal trading vary randomly in our sample firms. Although, we explicitly assume that both RI and AT are signals of an unobserved cybersecurity risk (this means that if one were able to measure the cyber risk with a reasonably random measurement error, the coefficients of RI and AT should become practically zero), we cannot interpret the coefficients of RI and AT as signals unless variations in RI and AT, due to factors other than the unobserved cybersecurity risks are reasonably accounted for.

To do so, we utilize a control function approach, which models the variations in both RI and AT as a result of variations in some instruments that are related to RI and AT but can be excluded from EQ.1. Because both RI and AT are continuous variables, a simple control function approach, such as the one recommended by Heckman (1977) does not render unbiased estimates. Garen (1984) recommended an extension to the first stage of a Heckman's procedure that allows for the outcome variable to be a continuous variable. In the same fashion as Heckman's procedure, Garen's procedure renders self-selection controls to be included in EQ.1 and EQ.2. These self-selection controls are η and η.RI (controlling for the self-selection of RI), and η* and η*.AT (controlling for the self-selection of AT). All models are estimated while controlling for Garen's self-selection controls in EQ.1 and EQ.2.

As factors explaining the self-selection into the values of RI, we consider two Hausman-type instruments: the industry (firms in the same 2-digit SIC) and geographical (firms with HQs in the same state) averages of RI. Both industry- and geographical-averages of RI can

[10] Among the explanatory variables, number of employees is only reported in annual fundamentals section of COMPUSTAT database. Therefore for quarters in year t, the number of employees in year t-1 is included when measuring the firm size.

institutionally influence the norms of public report disclosure for a firm, and due to their aggregate-level nature are unlikely to impact the hazard of breach directly. Put differently, we expect the impact of the instruments on cybersecurity hazard is absorbed either through the firm-level measure of RI or through the Quarter-Industry level fixed effects.

As factors explaining the self-selection into the values of AT, we follow Piotroski and Roulstone's (2005) model of predicting insiders' trading patterns and consider the firm's contemporaneous return (12-month buy-and-hold) and book to market ratio as both factors encourage trading the firm's securities for purely financial reasons. Moreover, we control for the number of shares of restricted and stock options granted to insiders (GRANTS) and the number of stock options exercised since both factors regulate the holding of firm securities by the insiders. The set of these factors is also unlikely to directly influence the hazard of breach.

## Results

Model 1 in Table 1 presents the estimation of EQ.1. Notably, Ind-level Breach shows the most significant association with the increased hazard of breach. Moreover, the coefficient of investment emphasis is significant and negative, confirming that firms benefit from preventive gains as a result of investing in cybersecurity countermeasures. While the hazard of a cybersecurity incident is not conditioned on the firm size in terms of the number of employees or assets owned, innovative firms (those with higher levels of R&D) show lower levels of vulnerability.

Also, our results show a non-significant association between RI and the hazard of a cybersecurity breach. This is consistent with our expectation that the SEC disclosures may turn into boilerplate statements that do not carry informative signals to investors about the imminent cyber risks. Unlike RI, the coefficient of AT is positive and significant, indicating that more selling of a firm's securities is indeed associated with a higher hazard of a cybersecurity breach (consistent with H1). Specifically, one standard deviation above-mean trading by executives in a given quarter is indicative of an almost 9 percent increase in the expected hazard of a cybersecurity breach in the subsequent quarter.

Moreover, the results of estimating EQ.2, as reported in Model 2 of Table 1, show a positive and significant interaction between RI and AT, suggesting that AT enhances the signaling impact of RI. As such, in firms with higher than average reporting of firm-specific risks, only those with insiders selling their firm's security in amounts in excess of an average firm see a heightened subsequent hazard of a breach. As indicated earlier, this finding suggests that a higher-than-

average disclosure of cybersecurity risks (as proxied by an increase in RI) may not necessarily be due to the firm's intent to relaying the presence of higher-than-average risks or an upcoming, imminent incident. However, in the presence of higher-than-average insiders' selling of firm shares, one can more reliably interpret higher-than-average reporting of cyber risks in SEC reports as signs of an imminent cybersecurity incident.

**Robustness Tests**

In order to test the robustness of our findings to some of the choices in the measurement, we run some additional analyses with alternative measures. First, our original measure of RI builds on the intuition that if public reports are effective tools in forming expectations about cybersecurity hazards, the more risk elements shared by a firm (as impounded into the measure of RI) the more should be its hazard of cybersecurity. That said, disclosures in SEC reports can turn into boilerplate statements and lose their effectiveness as signals over time. That said, a more visible signal about risks relevant to a period might be the changes that a firm makes into the boilerplate disclosures of cybersecurity risks. Tweaking the language of boilerplate statements may be due to the firm's sensing of an imminent threat and the firm's endeavors to take out over-promising/ under-stating language to protect the firm from after-breach litigations due to fraudulent disclosures.

As such, we run a model (Model 1 in Table 2) that considers the ratio of word changes (number of security word reported included in the document at (t-1) and not included in the document at (t-2))/(number of words included in the report at (t-1)) in the cybersecurity risk disclosure section of 10-Q's in a given quarter as the measure of RI. Moreover, while we consider abnormal selling of stock in a period as a measure of AT, Model 2 in Table 2 reports an estimation that considers the un-adjusted value of the selling ratio. Moreover, Model 3 reports an estimate where the raw count of shares sold (instead of the selling ratio based on share sold) is used while estimating AT. Model 4 reports the result when the extent of RI is adjusted for its average extent in the prior two years. Despite differences in the effect sizes, our estimates remain qualitatively unchanged, in Models 1-4, compared to our original estimations.

**Further Identification Remedies**

*First Difference Model*

Although our original estimation considers stratification around firm ID's to account for a varying hazard baseline for each firm, we also run a model that removes the fixed effect of firms by first-

differencing. Model 1 in Table 3 reports the results of this analysis and shows that our findings remain qualitatively similar under this alternative specification.

*A Controlled Sample*

A challenge in identifying the impact of AT as a signal of future cybersecurity incidents is that the insider trades are not earmarked for a specific reason (financial risk, cybersecurity risk, etc.). Our main identification attempt to attenuate this concern is to concurrently control for factors that can give non-cyber reasons to an insider for selling their shares, through the use of a control function approach. That said, the wide window of a quarter to measure AT makes it less likely that any covariate-based approach (such a control function) effectively isolates trades to those that are made in connection to a sense of heightened cybersecurity risk.

In an ideal experimental setting, one could prime executives to consider possible cybersecurity threats they perceive a firm might see in the near future, and then, observe the executives' trades, as well as the subsequent occurrence of a cybersecurity incident, to draw a conclusion. To achieve closer-to-ideal experimental priming of the executives that ensures trades are reasonably related to perceived cybersecurity risks, we consider natural conditions when an external event has directed the insiders' attention to the risks of cybersecurity within their firm. If executives are indeed primed by such an external event, it is more reasonable to expect that their trades made in the proximity of that external event are more likely connected to their perceived risk of cybersecurity.

One such external priming event is the occurrence of a major cybersecurity breach to a firm in the same industry. It is likely that an incident occurred to another firm primes the executives of a focal firm to engage in internal audits that assess the likelihood of a similar adverse event happening to their own firms. As such, the extent and recency of adverse impacts to a rival firm, another firm in the same 4-digit SIC code, can prime the focal firm's executives about their own firm's likelihood of an imminent threat. So, insider trades made in a short window (here, we choose a week) after a major cybersecurity incident in a rival firm can be better identified as related to, or triggered by, cybersecurity risks.

Therefore, we form a restricted sample of 1,256 observations of firm-quarters in which at least one rival of the focal firm is faced with a major cybersecurity incident.[11] Then, we measure

[11] We identify a breach as major if at least five national news agencies in the U.S. have covered the incident.

the AT in the period starting from the same day as the incident until a week later. Similar to our original analysis, we expect this short-window measure of AT in the restricted sample is associated with a higher hazard of a breach in the subsequent quarter. Model 2 in Table 3 reports the results of this estimation. Notably, the stronger coefficients of AT (0.241; $p < 0.001$) and AT*RI (0.117; $p < 0.001$) confirm our expectation that insider trades isolated in a period of heightened attention to cybersecurity risks are far more indicative of a future cybersecurity incident.

*Clarifying the Underlying Mechanism*

Our empirical examination of insider trading as a signal of cybersecurity incidents builds on two premises. First, insiders are expected to trade if they expect that they can benefit from their trades in the presence of information asymmetry with outsiders. As such, abnormal trading in firms with less information asymmetry may be more due to capitalizing on financial trends in the market, such as market momentum (e.g., Piotroski & Roulstone, 2005), rather than due to capitalizing on information gaps with outsiders. Hence, we expect that AT in firms with lower information asymmetry levels is less associated with the hazard of a subsequent incident. We test this boundary condition by examining if the impact of AT on subsequent hazard is lower in firms that are more covered by financial analysts. Analysts are considered as information bridges (Luo, Wang, Raithel, & Zheng, 2015) that reduce the information gaps between a firm and its stakeholders. Therefore, external investors of firms with higher coverage have lower levels of information asymmetry with firm insiders. Model 3 in Table 3 shows a negative and significant coefficient for AT* **Analysts Coverage** (**AC**; ln(1+number of analysts covering a firm's activities as reported in IBES database)), supporting our expectation. This further explains that insider trades become more effective signals as the information asymmetries grow in the market.

The second premise concerns the concept of managerial foreknowledge that supplies insiders of a firm with indirect knowledge about the cyber risks of a firm. While a direct measure of managerial foreknowledge is hard to obtain at this scale, especially in a longitudinal setting that spans several years, we use executives' **tenure** in the firm, in industries with high frequency of breach, and in IT-related positions or in tech firms, as three categories of experience that can elevate the insiders' ability to form a reliable foresight about the cybersecurity risks that a firm faces. As such, we expect the association between AT and hazard of a subsequent incident to be stronger in firms with insiders of higher experience.

Put differently, if all that made insider trades informative to outsiders was their *direct* or *obvious* information about an imminent incident, there should not be any difference between the signaling power of trades made by executives with higher experience and those with less, because direct or obvious information can be reasonably assumed to be circulated among high and low experience executives alike, whereas indirect or less obvious information is probably less likely to be obtained or relayed to newer executives. Models 4, 5, and 6 present the results of the estimation when the executives' tenure (in terms of average number of years in the firm, average number of years in firms in high-breach industries, and average number of years in IT positions/tech firms) and the interaction of tenure with AT is considered. All three models show a positive and significant interaction between tenure and AT, indicating that experience enhances the effectiveness of AT as a signal of subsequent incidents. This provides some indirect evidence supporting the importance of foreknowledge (or access to indirect information) in shaping information asymmetries around the cybersecurity risks of a firm.

**Discussion**

Motivated by the prevalence of information asymmetries related to the uncertainties around cybersecurity incidents, we examined and compared the effectiveness of two corporate reporting tools to reduce these asymmetries. Drawing from the literature on cybersecurity incidents and insider trading, we empirically show that insider trades in the form of selling are associated with higher cybersecurity incidents/hazards. Our results support that the asymmetric possession of information about cybersecurity risks by firms' managers that result in insider selling of shares is also associated with a heightened cybersecurity hazard. This result suggests that insider trades can be indicative of cybersecurity incidents and also complement the effectiveness of disclosing cybersecurity risks in public reports.

Though the literature in accounting and finance highlights the effectiveness of both financial reports and insider trading disclosures to reduce information asymmetries with regards to the financial well-being of the firm, we note a few contrasts that are specific to the cybersecurity landscape and that offer new insights. Unlike financial disclosures, cybersecurity disclosures are limited in their effectiveness to reduce asymmetries. First, the financial disclosures in public reports are recognized as 'boilerplate' with very little changes. This limitation is further compounded by the SEC's corporate finance guidelines, which discourages firms from disclosing cybersecurity risks and incidents if such disclosure would further compromise the firm's

cybersecurity by opening up more vulnerabilities to the public. As such, the effectiveness of the financial disclosures in reducing asymmetries become even more doubtful when it comes to information gaps about the cyber well-being of a firm. So, the informativeness of these reports is then unassociated with increased cybersecurity breach hazards. This suggests that on their own, financial reports have little signaling power on cybersecurity breaches.

However, we find that in conjunction with insider trades, the signaling power of financial reports towards cybersecurity breach hazards increases. This result suggests that there is a synergy between the direct (financial reports disclosure) and indirect signals (insider trades disclosure) in providing outsiders an early indication of a cybersecurity breach in firms. The synergy between the two forms of signals is important because insider trades in isolation are hard to interpret. Insiders' selling of firm securities, in general, only signal the insiders' expectation of some imminent bad news (without a hint about what sort of bad news id expected) or are simply indicative of corrections to the markets' over-optimism. However, when these sell trades are accompanied by a trend in disclosing more cyber risks in public reports, investors can more reliably interpret the two signals to make sense of a firm's cyber risks.

Given the current study's limitations, we advise caution in the interpretation of these results. The sample of firms' cybersecurity breach incidents is only within the years 2011 and 2017, raising the possibility that extending the year range could yield different results. Moreover, and although we provide additional tests pertaining to the importance of indirect information in creating asymmetries with investors, we are unable to test if any of the insider trades observed in our sample are based on direct information. Since withholding direct, material information makes insider trading illegal in the U.S., examining direct evidence of it is cumbersome. Therefore, while we stand with the claim about the effectiveness of insider trading disclosures as tools of reducing information asymmetries with investors, we stop short of arguing what type of information, direct or indirect, is the main reason for their effectiveness. Also, the current analysis does not include the possibility of accounting for other major negative news that may have triggered sales of stocks by executives. Therefore, further ensuring effectiveness of abnormal trading requires additional research. Finally, given our reliance on public sources capturing cybersecurity incidents, our study most likely undercounts these incidents.

Despite these limitations, there are a few theoretical contributions offered by this study. First, this study adds to the literature about cybersecurity disclosures in IS (e.g., Gordon et al.,

2010), which has examined public reports and direct disclosures of cyber risks, by introducing insider trading disclosures as an even more effective indicator of cyber risk, albeit with an indirect nature. Second, this study is, to the best of our knowledge, the first in offering an account of synergistic signaling through two well-studied tools of transparency in financial markets.

We believe that the findings of the study should also be of particular interest to practitioners. A general challenge facing the SEC is that its regulations are somewhat fragmented. That is, regulations based on public reports and insider trading (as well as other various mandated disclosures) are often not presented in a unified setting to investors, neither by the SEC or the analysts covering the activities of a firm. Given this fragmentation in regulations, their associated reports and disclosures are rarely scrutinized together to understand their inter-relationships. Our results show that there is synergetic information to be extracted when utilizing two seemingly unrelated reports mandated by the SEC. Therefore, the study provides empirical evidence that encourages analysts and investors to look beyond a stand-alone interpretation of SEC disclosures.

Particularly, while it is convenient to seek information in public report disclosures only, figures reported in insider filings can significantly increase the usefulness of the said reports. In sum, we encourage investors and analysts to look for clues in the form of selling of a firm's securities by insiders and then scrutinize disclosures related to cybersecurity in public reports to form a better understanding of the likelihood of imminent cyber threats. Also, the evidence from our restricted sample indicates that insiders that are alerted, after an adverse cyber incident has unfolded for a rival, send significantly more reliable signals by their selling trades. As such, not only do the trades by the insiders of impacted firms (which get most of the public press scrutiny) reveal useful information to investors and arbitrageurs but so can the trades by insiders of rival and currently-unimpacted firms.

**Table 1. Main Analysis**

| | **Model 1** | **Model 2** |
|---|---|---|
| | **Main effects** | **Interaction** |
| Report Informativeness (RI) | 0.010 | 0.009 |
| | (0.007) | (0.007) |
| Abnormal Trading (AT) | 0.086** | 0.12*** |
| | (0.03) | (0.026) |
| AT * RI | | 0.061* |
| | | (0.025) |
| Ind-level breach | 0.122*** | 0.119*** |
| | (0.026) | (0.019) |
| Investment emphasis | -0.078* | -0.056* |
| | (0.037) | (0.028) |
| Firm size | 0.001 | -0.021 |
| | (0.001) | (0.018) |
| Assets | 0.008 | 0.008 |
| | (0.006) | (0.005) |
| R&D | -0.085** | -0.069* |
| | (0.026) | (0.035) |
| η | 0.008 | 0.012 |
| | (0.005) | (0.018) |
| η.RI | 0.009 | 0.008 |
| | (0.007) | (0.008) |
| η* | -0.008 | -0.006 |
| | (0.005) | (0.013) |
| η*.AT | -0.005 | 0.013 |
| | (0.210) | (0.244) |
| Industry-Year Fixed Effects | YES | YES |
| ***Wald's Chi*** | ***5701.14*** | ***1943.34*** |
| ***N*** | ***48,312*** | ***48,312*** |

Notes: P-values are represented by # Significant at $p < 0.10$, * Significant at $p < 0.05$, ** Significant at $p < 0.01$, *** Significant at $p < 0.001$. A Cox proportional hazard estimation with stratification around firm id (i.e., distinct baseline hazard for each firm) and a robust standard error estimation are used (reported in parenthesis). The exit condition is set to happen until the next observation about the same firm in another quarter. The year span is 2011 to 2017. All models are run based on quarterly measures (with one quarter lag). Abnormal trading is estimated based on trades made by the CxO's (e.g., CEO, CFO, COO, CIO) as well as the president and chairman of the board in quarter t-1 corrected for the average trades in the same quarter of previous 2 years. Ind-level breach is the average of security breaches reported in the same 2-digit SIC firms in previous quarter.

**Table 2. Robustness Tests**

| | **Model 1** | **Model 2** | **Model 3** | **Model 4** |
|---|---|---|---|---|
| | **ΔWords ratio instead of RI** | **Trading (Unadjusted) instead of AT** | **AT (# of Shares Sold)** | **Adjusted RI** |
| Report Informativeness (RI) | 0.008 | 0.008 | 0.006 | 0.007 |
| | (0.007) | (0.006) | (0.005) | (0.007) |
| Abnormal Trading (AT) | 0.138*** | 0.019 | 0.108** | 0.171*** |
| | (0.019) | (0.013) | (0.038) | (0.038) |
| AT * RI | 0.051* | 0.044# | 0.069* | 0.055* |
| | (0.020) | (0.023) | (0.034) | (0.022) |
| Ind-level breach | 0.139*** | 0.156*** | 0.116*** | 0.131*** |
| | (0.022) | (0.027) | (0.024) | (0.014) |
| Investment emphasis | -0.062** | -0.062* | -0.034# | -0.068* |
| | (0.023) | (0.031) | (0.019) | (0.031) |
| Firm size | -0.011 | -0.017 | -0.022 | -0.019 |
| | (0.011) | (0.014) | (0.018) | (0.013) |
| Assets | 0.008 | 0.007 | 0.008 | 0.008 |
| | (0.009) | (0.005) | (0.005) | (0.003) |
| R&D | -0.063* | -0.083** | -0.071* | -0.077** |
| | (0.028) | (0.03) | (0.03) | (0.024) |
| Industry-Year Fixed Effects | YES | YES | YES | YES |
| ***Wald's Chi*** | ***3819.42*** | ***1983.65*** | ***4876.23*** | ***2336.93*** |
| ***N*** | ***48,312*** | ***48,312*** | ***48,312*** | ***48,312*** |

Notes: P-values are represented by # Significant at $p < 0.10$, * Significant at $p < 0.05$, ** Significant at $p < 0.01$, *** Significant at $p < 0.001$. A Cox proportional hazard estimation with stratification around firm id (i.e., distinct baseline hazard for each firm) and a robust standard error estimation are used (reported in parenthesis). The exit condition is set to happen until the next observation about the same firm in another quarter. The year span is 2011 to 2017. All models are run based on quarterly measures (with one quarter lag). Abnormal trading is estimated based on trades made by the CxO's (e.g., CEO, CFO, COO, CIO) as well as the president and chairman of the board in quarter t-1 corrected for the average trades in the same quarter of previous 2 years. Ind-level breach is the average of security breaches reported in the same 2-digit SIC firms in previous quarter. The coefficients of Garen's $\eta$, $\eta$.RI, $\eta$*, and $\eta$*.AT are omitted from the table for brevity.

**Table 3. Alternative Tests of Identification and Boundary Condition**

| | **Model 1** | **Model 2** | **Model 3** | **Model 4** | **Model 5** | **Model 6** |
|---|---|---|---|---|---|---|
| | **First Differences** | **Restricted Sample** | **Analysts' Coverage** | **Tenure (# of Years in Firm)** | **Tenure (Exp. in High Breach Ind.)** | **Tenure (# Years in IT Positions/ High Tech Firms)** |
| Report Informativeness (RI) | 0.002 | 0.006 | 0.007 | 0.005 | 0.006 | 0.006 |
| | (0.002) | (0.004) | (0.004) | (0.004) | (0.004) | (0.005) |
| Abnormal Trading (AT) | 0.142*** | 0.241*** | 0.100** | 0.102** | 0.098** | 0.020 |
| | (0.022) | (0.038) | (0.037) | (0.039) | (0.031) | (0.017) |
| AT * RI | 0.092** | 0.117*** | 0.044# | 0.058* | 0.047# | 0.052# |
| | (0.033) | (0.021) | (0.024) | (0.026) | (0.028) | (0.028) |
| Analysts' Coverage (AC) | | | 0.016 | | | |
| | | | (0.012) | | | |
| RI*AC | | | 0.005 | | | |
| | | | (0.004) | | | |
| AT*AC | | | -0.038** | | | |
| | | | (0.012) | | | |
| Tenure | | | | 0.007 | 0.007 | 0.009 |
| | | | | (0.005) | (0.005) | (0.008) |
| AT*Tenure | | | | 0.049* | 0.079* | 0.111** |
| | | | | (0.024) | (0.039) | (0.039) |
| RI* Tenure | | | | 0.005 | 0.004 | 0.002 |
| | | | | (0.003) | (0.003) | (0.002) |
| Ind-level breach | 0.159*** | 0.147*** | 0.138*** | 0.14*** | 0.112** | 0.119*** |
| | (0.029) | (0.028) | (0.023) | (0.028) | (0.036) | (0.024) |
| Investment emphasis | -0.062* | -0.058* | -0.027 | -0.035# | -0.034# | -0.045# |
| | (0.024) | (0.029) | (0.024) | (0.019) | (0.02) | (0.024) |
| Firm size | -0.012 | -0.021 | -0.011 | -0.011 | -0.010 | -0.009 |
| | (0.008) | (0.016) | (0.007) | (0.008) | (0.007) | (0.006) |
| Assets | 0.012 | 0.009 | 0.007 | 0.006 | 0.008 | 0.008 |
| | (0.009) | (0.007) | (0.005) | (0.004) | (0.006) | (0.006) |
| R&D | -0.06* | -0.046# | -0.055* | -0.045# | -0.035# | -0.043# |
| | (0.025) | (0.025) | (0.026) | (0.023) | (0.018) | (0.025) |
| Industry-Year Fixed Effects | YES | YES | YES | YES | YES | YES |
| ***Wald's Chi*** | ***3305.54*** | ***6149.06*** | ***5348.16*** | ***6137.76*** | ***4528.8*** | ***5863.32*** |
| ***N*** | ***42,106*** | ***1,256*** | ***48,312*** | ***48,312*** | ***48,312*** | ***48,312*** |

Notes: P-values are represented by # Significant at $p < 0.10$, * Significant at $p < 0.05$, ** Significant at $p < 0.01$, *** Significant at $p < 0.001$. A Cox proportional hazard estimation with stratification around firm id (i.e., distinct baseline hazard for each firm) and a robust standard error estimation are used (reported in parenthesis). The exit condition is set to happen until the next observation about the same firm in another quarter. The year span is 2011 to 2017. All models are run based on quarterly measures (with one quarter lag). Abnormal trading is estimated based on trades made by the CxO's (e.g., CEO, CFO, COO, CIO) as well as the president and chairman of the board in quarter t-1 corrected for the average trades in the same quarter of previous 2 years. Ind-level breach is the average of security breaches reported in the same 2-digit SIC firms in previous quarter. The coefficients of Garen's $\eta$, $\eta$.RI, $\eta$*, and $\eta$*.AT are omitted from the table for brevity.

## References


Aboody, D., & Baruch, L. (2000). Information asymmetry, R&D, and insider gains. *Journal of Finance*, *55*(6), 2747–2766.

Ahuja, G., Coff, R. W., & Lee, P. M. (2005). Managerial foresight and attempted rent appropriation: Insider trading on knowledge of imminent breakthroughs. *Strategic Management Journal*, *26*(9), 791–808. https://doi.org/10.1002/smj.474

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

Campbell, K., Gordon, L. A., Loeb, M. P., & Zhou, L. (2003). The economic cost of publicly announced information security breaches: empirical evidence from the stock market. *Journal of Computer Security*, *11*(3), 431–448.

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

Chauhan, Y., Chaturvedula, C., & Iyer, V. (2014). Insider trading, market efficiency, and regulation. a literature review. *The Review of Finance and Banking*, *06*(1), 7–14.

Chen, C., Martin, X., & Wang, X. (2013). Insider trading, litigation concerns, and auditor going-concern opinions. *Accounting Review*, *88*(2), 365–393.

Chung, K. H., & Charoenwong, C. (1998). Insider trading and the bid-ask spread. *Financial Review*, *33*(3), 1–20.

Coff, R. W., & Lee, P. M. (2003). Insider trading as a vehicle to appropriate rent from R & D. *Strategic Management Journal*, *24*(2), 183–190.

Cohen, L., Malloy, C., & Pomorski, L. (2012). Decoding Inside Information. *Journal of Finance*, *67*(3), 1009–1043.

Deloitte. (2017). *Cyber Insurance a key element of the corporate Risk Management Strategy*. Retrieved from https://www2.deloitte.com/content/dam/Deloitte/cy/Documents/risk/CY_Risk_CyberInsurance_Noexp.PDF

Fama, E., & French, K. (1997). Industry costs of equity. *Journal of Financial Economics*, *43*(2), 153–193.

Fazzini, K. (2018). Moody's to build business hacking risk into credit ratings. Retrieved February 27, 2020, from https://www.cnbc.com/2018/11/12/moodys-to-build-business-hacking-risk-into-credit-ratings.html

Finnerty, J. (1976). Insiders and Market Efficiency. *The Journal of Finance*, *31*(4), 1141–1148.

Frank, M., & Shen, T. (2012). *Investment and the Weighted Average Cost of Capital*. *Journal of Financial Economics*.

Garen, J. (1984). The returns to schooling: A selectivity bias approach with a continuous choice variable. *Econometrica*, 1199.1218.

Gleason, C. A., & Mills, L. F. (2002). Materiality and contingent tax liability reporting. *Accounting Review*, *77*(2), 317–342.

Goel, S., & Shawky, H. A. (2009). Estimating the market impact of security breach announcements on firm values. *Information & Management*, *46*(7), 404–410.

Gordon, L. A., Loeb, M., & Sohail, T. (2010). Market Value of Voluntary Disclosures Concerning Information Security. *MIS Quarterly*, *34*(3), 567–594.

Haft, R. (1982). The effect of insider trading rules on the internal efficiency of the large corporation. *Michigan Law Review*, 1051.

Heckman, J. J. (1977). Sample Selection Bias as a Specification Error (with an Application to the Estimation of Labor Supply Functions). *Econometrica*, *47*, 153–161.

Hovav, A., & D'Arcy, J. (2003). The Impact of Denial of Service Attack Announcements on the Market Value of Firms. *Risk Management and Insurance Review*, *6*, 97–121.

Jeng, L. A., Metrick, A., & Zeckhauser, R. (2003). Estimating the returns to insider trading: A performance-evaluation perspective. *Review of Economics and Statistics*, *85*(2), 453–471.
Khanna, N. (1997). Why both insider trading and non-mandatory disclosures should be prohibited. *Managerial and Decision Economics*, *18*(7/8), 667–679.
Kraft, A., Lee, B. S., & Lopatta, K. (2014). Management earnings forecasts, insider trading, and information asymmetry. *Journal of Corporate Finance*, *26*, 96–123.
Kwon, J., & Johnson, M. E. (2014). Proactive Versus Reactive Security Investments in the Healthcare Sector. *MIS Quarterly*, *38*(2), 451–472.
Lakonishok, J., & Inmoo, L. (2001). Are insider trades informative? *The Review of Financial Studies*, *14*(1), 79–111.
Lorie, J. H., & Niederhoffer, V. (1968). Predictive and Statistical Properties of Insider Trading. *The Journal of Law and Economics*, *11*(1), 35–53.
Luo, X., Wang, H., Raithel, S., & Zheng, Q. (2015, January 1). Corporate social performance, analyst stock recommendations, and firm future returns. *Strategic Management Journal*. John Wiley and Sons Ltd. https://doi.org/10.1002/smj.2219
Piotroski, J., & Roulstone, D. (2005). Do insider trades reflect both contrarian beliefs and superior knowledge about future cash flow realizations? *Journal of Accounting and Economics*, *39*(1), 55–81.
Ravina, E., & Sapienza, P. (2010). What do independent directors know? Evidence from their trading. *The Review of Financial Studies*, *23*(3), 962–1003. Retrieved from https://academic.oup.com/rfs/article-abstract/23/3/962/1594077
Rice, S. C., Weber, D. P., & Wu, B. (2015). Does SOX 404 have teeth? Consequences of the failure to report existing internal control weaknesses. *Accounting Review*, *90*(3), 1169–1200. https://doi.org/10.2308/accr-50974
Seyhun, H. N. (1986). *Empirical Tests of Information Economics Models: Relation Between Expected Value, Cost and Variance of Information, and Market Efficiency*. University of Michigan.
Summers, S., & Sweeney, J. (1998). Fraudulently misstated financial statements and insider trading: An empirical analysis. *The Accounting Review*, *73*(1), 131–146.

# Appendix A: Keywords List

| |
|---|
| Cyber/digital/computer/information/data |
| Authentication |
| Access control |
| Computer security |
| Computer virus |
| Cyber fraud |
| Cyber investigation |
| Cyber operation |
| Cyber/digital/computer break-in |
| Cyber/digital/computer/information/data attack |
| Cyber/digital/computer/information/data defense |
| Cyber/digital/computer/information/data protection |
| Cyber/digital/computer/information/data theft |
| Cyber/digital/computer/information/data threat |
| Cyber/digital/computer/information/data vulnerability |
| Cyber/digital/computer/information/data vulnerability assessment |
| Cyber/digital/computer/network intrusion |
| Cyber/Security assessment |
| Cyber/security investment/expenditure |
| Cybersecurity breach |
| Cyberspace |
| Data breach |
| Denial of service |
| Digital forensics |
| Disaster recovery |
| Encryption |
| Exploitation analysis |
| Firewall |
| Hack |
| Identity theft |
| Information security breach |
| Infosec |
| Phishing |
| Privacy breach |
| Security breach |

# Appendix B: Sample Characteristics

| Industry Breakdown of Firm-Year Observations | | |
|---|---|---|
| | # of Firm-Year Observations | % of Sample |
| Manufacturing (Durable) | 714 | 37.3 |
| Wholesale Trade | 388 | 20.27 |
| Finance, Insurance and Real Estate | 211 | 11.02 |
| Manufacturing (Non-Durable) | 244 | 12.75 |
| Retail Trade | 214 | 11.18 |
| Transportation and Utilities | 84 | 4.39 |
| Services | 54 | 2.82 |
| Construction | 5 | 0.26 |
| *Total* | *1,914* | *100* |

| **Variable** | **Mean** | **S.D.** | **Median** |
|---|---|---|---|
| AT | 0.681 | 0.213 | 0.6256 |
| Sales (million $) | 4392.620 | 20180.200 | 6106.100 |
| Employees (1000) | 20.596 | 53.049 | 32.358 |
| Stock Price ($) | 19.834 | 34.680 | 24.444 |
| Market Share (%)[i] | 5.560 | 13.165 | 3.534 |
| Assets (million $) | 941.160 | 3113.110 | 1217.580 |
| Book-to-Market Ratio | 0.464 | 0.388 | 0.540 |
| Market Beta | 0.892 | 0.463 | 1.132 |
| Momentum (%) | 3.036 | 23.213 | -0.974 |
| Illiquidity | 0.167 | 0.214 | 0.311 |
| Idiosyncratic volatility | 81.274 | 143.608 | 75.082 |
| Capital Investment | 0.113 | 0.350 | 0.093 |
| R&D (% of assets) | 6.441 | 15.911 | 5.154 |
| Investment emphasis | 0.142 | 0.381 | 0.189 |
| Ind-level breach | 2.014 | 3.081 | 3.005 |
| Options Granted[ii] | 0.060 | 0.166 | 0.032 |
| Options Exercised | 0.009 | 0.073 | 0.008 |
| Number of breaches = 971 | | | |
| Number of firms with a single breach = 564 | | | |
| Number of firms with multiple breaches = 112 | | | |

[i] Market share is estimated as the sales ratio to overall sales by the primary industry.

[ii] Options granted (exercised) are estimated as the log of one plus the ratio of the number of shares granted (options exercised) during fiscal year *t* divided by total shares that are outstanding at the end of the fiscal year.