Cybersecurity Awareness and Market Valuations

Henk Berkman
University of Auckland & *University of Sydney*
h.berkman@auckland.ac.nz

Jonathan Jona
The University of Melbourne
jonathan.jona@unimelb.edu.au

Gladys Lee
The University of Melbourne
gladys.lee@unimelb.edu.au

Naomi Soderstrom
The University of Melbourne
naomiss@unimelb.edu.au

Draft Date: 27 August 2018

Abstract

This paper introduces a measure of firm-specific cybersecurity awareness that can be used in empirical research exploring cyber-related issues facing corporations. It extends and updates Gordon, Loeb, and Sohail (2010), who develop an indicator capturing the existence of disclosures related to "information security" and show a positive association between market valuation and their measure. Since publication of their paper, cyber-related events have become more frequent and salient, and disclosure of cybersecurity issues has become more extensive. Increased disclosure is largely due to a 2011 requirement by the Securities and Exchange Commission, which provides guidance for disclosure of cyber-related issues in 10-K filings. Based upon this post-guidance disclosure, we develop a new measure that captures the extent and relevance of cyber disclosures and show that the market positively values cybersecurity awareness. We also show that a more negative tone in cyber disclosures is associated with lower market values. Our results are robust to inclusion of measures of IT governance and controlling for the firm's overall disclosure characteristics.

*Keywords***:** Cybersecurity; Cybersecurity awareness; Cyber breaches; Cyber risks; IT governance; Market valuations; Intangible asset

*Acknowledgements***:** We thank Xinning Xiao for comments and James Kavourakis for research assistance. We are also grateful to Jackie Cook for her help in developing the cybersecurity awareness measure. Jona and Lee acknowledge funding support from the AFAANZ research grant. Jona also acknowledges the financial support provided by the University of Melbourne through the Early Career Researcher grant.

Cybersecurity Awareness and Market Valuations

1. Introduction

In response to the increasing impact of cybersecurity incidents on company customers and investors, the Securities Exchange Commission (SEC) issued *CF Disclosure Guidance: Topic No. 2 Cybersecurity* (SEC 2011) to provide increased transparency regarding material cybersecurity-related issues. This guidance has led to a rapid increase in cybersecurity disclosures by firms in their 10-K reports (Gordon et al. 2015b). In this paper we examine whether these cyber disclosures provide value relevant information, or whether they are merely boilerplate (Hilary et al. 2016; Morse et al. 2018). To perform our tests, we introduce a continuous measure of cybersecurity awareness, employing textual analysis of the language used in cyber disclosures within the entirety of a firm's 10-K (see Appendix A for more details).[1] Our measure and related dictionaries are publicly available, and can be used in further research investigating the impact of cybersecurity awareness at the firm level.[2]

Understanding cybersecurity awareness at the firm level is important because firms are experiencing an increasing number of cyber attacks (Deloitte 2017; PwC 2016). Anecdotal evidence suggests that the costs of these attacks can be significant. In 2013, Target Corporation experienced a data breach that affected approximately 40 million customers with an estimated cost of at least $162 million (Prince 2015). Following Yahoo!'s announcement of a 2014 cyberattack, Verizon Communications, who was at the time seeking to buy Yahoo!, dropped their offer price by $350 million (Athavaley 2017). More recently, Equifax experienced a

[1] Gordon et al. (2010) provide a dichotomous measure of cyber awareness. However, their sample ends in 2004, before introduction of mandatory risk disclosures by the SEC in 2005 (Item 1A) and further guidance on cybersecurity disclosures in 2011 (SEC 2011). Thus, their study relies on voluntary disclosures of cyber-related issues. While Gordon et al. (2010) reported that 86% of firms in their sample did not report any cyber disclosures, we find that only 11% of the observations in our sample did not report any cyber disclosures in the now mandatory regime.

[2] The cybersecurity awareness measure and dictionaries are available from the authors upon request. Using the cybersecurity awareness measure, Berkman, Jona, Lee, et al. (2018) find that trading by privately informed traders is more likely in stocks of firms with lower cybersecurity awareness.

breach, in which the personal financial data of about 143 million U.S. consumers was stolen. The company is facing over 240 class action suits and has already incurred expenses of $87.5 million (Cowley 2017). In addition to compromising personal financial data, cyber attacks have targeted highly-sensitive information and intellectual property (Pentland 2011). Cybercrime has been estimated to cost the global economy approximately $450 billion (Hiscox 2017).

The increase in cyber incidents has drawn the attention of government, both at the state and federal levels. In 2017, the State of New York implemented regulations requiring financial services organizations to implement cybersecurity programs and to file annual certifications that they are in compliance with the regulation (New York 23NYCRR § 500).[3] At the U.S. Federal level, Fischer (2014) identifies 56 federal laws relating to cybersecurity, which address issues both within the Government and entities from regulated industries such as telecommunications and defense. In the European Union (EU), the first cybersecurity law went into effect in May 2018, requiring a broad range of companies to report any breaches they experience. Additional cybersecurity laws are pending in the EU.[4]

Facing pressure from multiple stakeholders, firms are implementing measures to combat growing cybersecurity threats. Some of these initiatives include bringing in directors with IT backgrounds, hiring Chief Information Security Officers,[5] creating IT committees of the Board,[6] purchasing or writing new systems with enhanced security,[7] and purchasing insurance.[8] Development of "cybersecurity awareness" can reduce the threats stemming from cyber security risk and regulatory pressures, potentially resulting in an increase in firm value.

[3] See New York Department of Financial Services' (DFS) Cybersecurity Regulations, 23 NYCRR § 500, eff. Mar. 1, 2017. https://www.dfs.ny.gov/legal/regulations/adoptions/dfsrf500txt.pdf.

[4] https://www.euractiv.com/section/cybersecurity/news/first-eu-cybersecurity-law-brings-fines-for-companies-that-fail-to-report-hacks/

[5] https://www.reuters.com/article/us-usa-companies-cybersecurity-exclusive/exclusive-u-s-companies-seek-cyber-experts-for-top-jobs-board-seats-idUSKBN0EA0BX20140530

[6] https://www2.deloitte.com/content/dam/Deloitte/sg/Documents/risk/sea-risk-cyber-security-changing-role-in-audit-noexp.pdf

[7] https://www.esecurityplanet.com/network-security/86-percent-of-financial-services-firms-to-increase-cyber-security-spend-in-2017.html

[8] http://ww2.cfo.com/risk-management/2016/10/stand-alone-cybersecurity-insurance-becoming-a-must-have/

In this paper, we develop a new measure of cybersecurity awareness and examine its market valuation consequences.

We conjecture that similar to other intangible assets (Barth et al. 1998; Choi et al. 2000; Clarkson et al. 2004), cybersecurity awareness is value relevant. Extant research explores several non-GAAP measures and their association with contemporaneous stock prices, such as order backlog (Lev and Thiagarajan 1993), software capitalization (Aboody and Lev 1998), web usage data (Trueman et al. 2000), information technology capability (Wang and Alam 2007), and firms' patent attributes (Deng et al. 1999; Hirschey and Richardson 2004). We argue that cybersecurity awareness also represents an intangible asset. Due to the qualitative nature of the disclosure (SEC 2011) and complexity of cyber-related issues, managers can report on many dimensions of a firm's cyber security. We argue that rather than providing information about their vulnerabilities, firms with more extensive disclosures are more likely to disclose information related to firm strategies for mitigating cybersecurity risks. This is consistent with Gordon et al. (2015b), who conjecture that government actions such as SEC's 2011 cybersecurity guidance could lead to an increase in cybersecurity investments and in turn, more disclosure of such information. Such disclosure provides investors with information about firms' cybersecurity awareness and should be positively valued by the market.[9]

However, it is possible that cyber-related disclosures in the post-guidance period are merely boiler plate disclosures that are vague or non-specific (Hilary et al. 2016; Morse et al. 2018)[10] and thus, are uninformative to the market and are less value relevant. The lack of clear guidance by the SEC as to what constitutes cyber incidents, issues, and risks has made

[9] Further, given SEC's guidance that "the federal securities laws do not require disclosure that itself would compromise a registrant's cybersecurity" (SEC 2011), firms are unlikely to disclose information that exposes them to additional cyber-related risk from hackers.

[10] Firms have historically been reticent to provide cybersecurity disclosures (Chabrow 2017; Javers 2013; Menn 2012). Reasons for avoiding disclosure include: 1) firms expect the impact of cyber attacks to be immaterial; 2) firms fear that disclosure of weaknesses may expose their vulnerabilities and may hurt their stock value; and/or 3) firms fear that disclosure may result in potential liabilities or may drive away customers (Chabrow 2017; Javers 2013).

identifying such disclosures even more difficult (Ferraro 2014).[11] Under these circumstances, we would fail to find a significant association between our measure of cybersecurity awareness and market valuations.

Consistent with our expectations and the findings in Gordon et al. (2010), we document a positive association between market valuation and cybersecurity awareness. Our results indicate that a one standard deviation increase in our cybersecurity awareness measure (normalized by industry and year) is associated with a $2.3 increase in stock price. This positive association between market valuation and cybersecurity awareness persists after controlling for disclosure tone, with a more negative valuation associated with negative cyber disclosure tone. Our results are also robust to controlling for the tone and length of the overall 10-K filings (Guillamon-Saorin et al. 2017; Huang et al. 2013). In further tests, we consider the effects on market valuations of alternative proxies for cybersecurity awareness, namely, IT governance and firm's prior experience with IT breaches. We also consider inclusion of measures of other types of risks derived from the 10-Ks as proposed in Campbell et al. (2014). We find that while these items are value-relevant, they do not subsume our measure.

In addition to the positive association between market value and our cybersecurity awareness measure, we find that company valuations are higher for firms that have previously experienced a cyber incident. This is consistent with investor expectations that once a firm experiences a breach, management will focus on cyber security, reducing the likelihood of future breaches.[12]

Our study makes several contributions to the literature. First, we provide evidence of benefits stemming from the SEC's guidance on cybersecurity. Our cybersecurity awareness

[11] https://www.auditanalytics.com/blog/when-is-a-cybersecurity-incident-material/

[12] Anecdotal evidence suggests that firms increase cybersecurity spending following a breach, see for example, JP Morgan (https://www.scmagazineuk.com/jpmorgan-to-double-cyber-security-spending-to-310-million-after-hack/article/541128/) or Equifax (https://investor.equifax.com/~/media/Files/E/Equifax-IR/reports-and-presentations/events-and-presentation/investorrelationsqacybersecurityincident.pdf).

measure is based upon firms' cybersecurity disclosures. Our findings of a positive association between our measure of cybersecurity awareness and market valuation, which is not subsumed by other proxies of cybersecurity awareness, suggest that disclosures made by firms following the SEC's cybersecurity guidance are not merely uninformative boilerplate disclosures. Although Li et al. (2018) find that in the post-guidance period, the informativeness of cyber disclosures for breaches declines, they find that the nature of topics disclosed changes. In particular, post-guidance, companies increasingly discuss risks related to intellectual property and reputation. We extend this line of research by more broadly examining market implications of cyber risks. We thus provide evidence that cyber disclosures in the post-guidance period contain additional information that is value relevant to investors. These findings can inform public policy making and should be of interest to the SEC and other regulators. Specifically, policy makers should consider whether more uniform cyber-related disclosures should be required of companies given that cyber information disclosed by companies are value relevant.

Second, we introduce a new measure of cybersecurity awareness. Our cybersecurity awareness score is based upon textual analysis of cyber-related disclosures for a large sample of firms, using a comprehensive dictionary. This measure can be used in future research to further explore the impact of cybersecurity awareness at the firm level. We show that cybersecurity awareness, tone of cyber-related disclosures and other proxies of cybersecurity awareness (IT governance and prior experience with cyber breaches) are all positively associated with market valuations. This evidence of capital market effects of cybersecurity awareness and tone of cyber-related disclosures should be of particular interest to management.

Third, our results contribute to the literature on risk disclosures and valuations. Studies in this area typically find that more extensive risk disclosures indicate higher risk and thus lower firm valuation (e.g., Berkman, Jona, and Soderstrom 2018; Matsumura et al. 2014). In contrast, our study finds that firms that disclose more on cyber issues are valued higher by the

market. Our study also contributes to the literature on the valuation of intangible assets, which are typically not recognized in financial statements because their value is difficult to estimate, such as brands, commitment by employees and technology (Aboody and Lev 1998; Barth et al. 1998; Choi et al. 2000).

2. Literature review and theoretical development

2.1 Prior literature on cybersecurity

Research on cyber-related issues has largely focused on the impact of cybersecurity events or incidents.[13] Investment in information security can help to protect firms against negative cybersecurity events (Gordon and Loeb 2002). Studies show that positive cybersecurity-related events such as investments in IT security (Bose and Leung 2013; Chai et al. 2011; Im et al. 2001), or the creation of a Chief Information Officer position (Chatterjee et al. 2001) are associated with higher stock prices. On the other hand, negative cybersecurity-related events such announcements of software vulnerability (Telang and Wattal 2007), announcements of IT products containing viruses (Hovav and D'arcy 2005) and cybersecurity breaches and incidents are associated with negative market reactions (Acquisti et al. 2006; Amir et al. 2018; Cavusoglu et al. 2004; Garg et al. 2003; Gatzlaff and McCullough 2010; Goel and Shawky 2009; Gordon et al. 2011; Hinz et al. 2015; Malhotra and Kubowicz Malhotra 2011; Modi et al. 2015; Morse et al. 2011; Pirounias et al. 2014; Yayla and Hu 2011). The effect of a cybersecurity breach or incident on market reaction depends on the nature of the event (Campbell et al. 2003; Wang, Kannan, et al. 2013; Yayla and Hu 2011). For example, compared to non-confidential information, security breaches involving confidential information are associated with a negative market reaction (Campbell et al. 2003). Technology firms suffer higher costs from security breaches than non-technology firms (Cavusoglu et al.

[13] See Spanos and Angelis (2016) for a comprehensive review of the impact of security events on the stock market.

2004; Pirounias et al. 2014; Yayla and Hu 2011). Wang, Ulmer, et al. (2013) further show that market reaction to a security breach event depends on the specificity of information about the incident. The market reacts negatively when the textual content of the breach report provides more detailed information about the breach.

Cyber attacks and security breaches have spillover effects. Cyber attacks or breaches not only negatively affects the affected firm, but also on the firm's peers/rivals (Ettredge and Richardson 2003; Hinz et al. 2015; Kashmiri et al. 2017; Martin et al. 2017). This is due to the perception that the root cause of a breach is systematic across peer firms (Martin et al. 2017). Martin et al. (2017) further show that the effect of a data breach on peer firms depends on the severity of the breach. While data breaches of low severity have a negative effect on a rival firm's performance, the effect is positive when data breaches are of higher severity. This is because in such cases, customers of the breached firm are more likely to switch over to a rival firm. Kashmiri et al. (2017) show that the effect of a data breach on a peer firm is moderated by the IT ability of the peer firm to prevent a similar breach, its corporate social responsibility, and its ability to respond effectively in the aftermath of a breach though marketing. While cyber attacks and security breaches negatively affect peer firms, such events are associated with higher market value for providers of information security, such as internet internet security products and services (Cavusoglu et al. 2004; Ettredge and Richardson 2003) and IT consulting firms (Chen et al. 2012).

Research that investigates corporate governance and cybersecurity provides evidence of governance mechanism effectiveness. Firms with a more established technology committee, as compared to a relatively younger committee, are less likely to be breached (Higgs et al. 2016). Strong support from the board or top management on information security also enhances the relationship quality between the internal audit and information security function (Steinbart et al. 2018) and is associated with a greater extent of cybersecurity audits (Islam et al. 2018).

Taking a different approach, Westland (2018) examines results of audits stemming from the Sarbanes-Oxley Act and finds that there are fewer security breaches when firms have stronger internal controls. Other studies investigate changes in corporate governance following a cyber-related event. Zafar et al. (2016) find that following a security breach incident, firms perform better when they have a Chief Information Officer in their top management team. In the audit literature, Li et al. (2016) find that audit fees increase following cyber incidents.

Research has also investigated the effect of cybersecurity related information sharing among firms. Such studies show that sharing cybersecurity related information among firms helps to reduce information security costs and raise social welfare (Gordon et al. 2003) and reduces the tendency of firms to defer cybersecurity investment until a cyber breach (Gordon et al. 2015a). Together, the above studies underscore the importance of cyber awareness and the need to manage cyber risk in a firm.

Our study is most closely related to Gordon et al. (2010) who examine market valuation and voluntary disclosure of information security between years 2000 and 2004 and find a positive association between market value and voluntary disclosure of information security. Their sample period is prior to both the SEC's requirements for mandatory reporting of risks (which occurred in 2005) and the SEC's 2011 supplementary guidance on cybersecurity disclosures. Gordon et al. (2010) view voluntary disclosure of cyber-related information in 10-Ks as a signal of firms' commitment to addressing cybersecurity risks and find higher market valuations for disclosing firms. Whereas Gordon et al. (2010) focus on the presence or absence of information security disclosures, we construct a continuous measure that captures a broader notion of cybersecurity awareness through the use of a comprehensive dictionary and textual analysis of 10-Ks, identifying both the length of relevant disclosures and the relevance of the language used.

It is possible that the results of our investigation of the value relevance of cyber disclosures following the SEC's 2011 supplementary guidance on cybersecurity disclosures could differ from those of Gordon et al. (2010). Li et al. (2018) find that while the presence and length of cybersecurity risk disclosures are positively associated with the likelihood of subsequently reported cybersecurity incident, this relationship only holds prior to the SEC's 2011 guidance on cybersecurity disclosures. They argue that disclosures in the pre-guidance period were informative because such disclosures predicted cybersecurity incidents. However, perhaps because of an increase in disclosure non-material cybersecurity risks, cyber disclosures in the post-guidance period are no longer predictive of cyber security events (Li et al. 2018). These findings question the informativeness of cyber disclosures in the post-guidance regime. However, given the broader nature of cyber disclosures, it is possible that the informativeness documented by Gordon et al. (2010) continues post-guidance, albeit through a broader impact on market valuation beyond prediction of cybersecurity events.

2.2 SEC Guidance on Cybersecurity Disclosures

Section 1A disclosures were mandated in 2005 through Regulation S-K Item 503(c) (SEC 2005), in which companies are required to disclose and describe company-specific risk factors. While companies are required to disclose all material risks, this guidance did not explicitly address disclosure of cyber risks and incidents (SEC 2011).[14]

In an effort to provide increased transparency regarding material cyber-related issues, in 2011, SEC issued *CF Disclosure Guidance: Topic No. 2 Cybersecurity* (SEC 2011). The guidance highlights that firms facing material cyber-related issues have a duty to disclose information regarding material cybersecurity issues (SEC 2011). The primary areas of the 10-

[14] The passage of Sarbanes-Oxley (SOX) Act in 2002 increased the need for firms to invest more in information security, however, neither SOX nor the SEC in 2002 required firms to publicly disclose their information security activities (Gordon et al. 2006).

K where firms must provide disclosure of risks and opportunities related to cybersecurity include management's discussion and analysis of financial condition and results of operation (MD&A), description of business, description of legal proceedings, and in Item 1A, Risk Factors. The guidance indicates that firms should disclose the most significant factors related to the riskiness of investing in a company (SEC 2011). The SEC reminds firms to avoid generic boilerplate disclosures, but rather to provide sufficient and appropriate disclosures that are tailored to their circumstances, such that users can appreciate the nature of the risks faced by the firm. In 2018, SEC provided an update to the 2011 cybersecurity guidance to assist public companies in preparing disclosures about cybersecurity risks and incidents (SEC 2018).

It is important to note that managers are strategic in their disclosure behavior (Dye 1985; Jorgensen and Kirschenheiter 2003). If companies have specific cyber risks, disclosing too much or too specific information about the risks may make the firm more vulnerable to cyber attacks (Rogers and Van Buskirk 2009), although increased disclosure may reduce litigation risk that follows from a breach (Francis et al. 1994; Gordon et al. 2010). Thus, when identifying material risks, management may only briefly and vaguely discuss areas of weakness. For example, managers could avoid providing proprietary information about their risks by using boilerplate language that does not actually provide incremental information (Dye 2010), or they could focus their discussion on material risks that the firms are already addressing. For example, Gordon et al. (2015b) conjecture that the increased reporting of cybersecurity related activities following SEC's 2011 guidance are accompanied by an increase in cybersecurity investments. Firms are thus more likely to focus their discussion on such positive related aspects of cybersecurity. The qualitative nature of risk disclosures makes it easier for managers to be strategic in their disclosures. Given the substantial risks associated with disclosure of vulnerabilities, we view cyber-related disclosures as relating to the firm's cybersecurity awareness.

2.3 Cybersecurity awareness and market valuations

Information assets in a firm, such as its data, information on server-based devices and websites, are highly valuable.[15] These assets could be compromised because of an unintentional (accidental) mistake or an intentional cyber attack. Cyber incidents or attacks are costly to a firm because they can result in litigation and regulatory costs,[16] and firms may also suffer from other damages such as to its reputation, business operations[17] and customer base[18] (Deloitte 2016). Firms with greater cybersecurity awareness are likely to be more cognizant of their vulnerabilities to cyber risks and threats (both accidental or intentional). Such firms can be expected to be more proactive in their management of cyber risks by adopting appropriate cybersecurity policies and measures, implementing effective threat detection, and ensuring there is proper and adequate response capability. Firms with better cybersecurity awareness are thus in a better position to prevent a cyber incident from occurring or to minimize the cost of a cyber incident.

In addition, there is increasing regulation on data privacy and cybersecurity related matters such as cyber risk disclosures.[19] Firms with higher cybersecurity awareness should be aware of cyber-related issues in relation to regulatory demands (such as the need for cyber disclosures or notification of data breaches).[20] Hence, such firms are more likely to comply and adhere with existing regulation and avoid incurring potential regulatory costs.

---

[15] Data is a highly valuable asset and can account for as much as 80% of the market value of firms (AISA 2017; Durbin 2016).

[16] For example, Yahoo (now known as Altaba) has entered into a US$80 million proposed class action settlement (https://www.databreaches.net/yahoo-enters-80-million-securities-class-action-settlement-after-data-breach/) and has agreed to pay a US$35 million penalty imposed by the SEC (https://www.sec.gov/news/press-release/2018-71) for failing to adequate disclose their 2013 and 2014 data breaches.

[17] The car maker, Chrysler, recalled 1.4 million vehicles following the exposure of a hackable software vulnerability in the vehicles' dashboard computers (https://www.wired.com/2015/07/jeep-hack-chrysler-recalls-1-4m-vehicles-bug-fix/).

[18] TalkTalk reported losing more than 100,000 customers as a result of a cyber attack in October 2015, while rivals Sky and BT reported an increase in subscribers in the last three months of 2015 (https://uk.reuters.com/article/uk-talktalk-tlcm-gp-results/talktalk-lost-more-than-100000-customers-after-cyber-attack-idUKKCN0VB0I7).

[19] In the U.S., there are presently 47 states that have enacted data breach notification laws.

[20] Target paid US$18.5 million to 47 states after state attorneys general took action against Target for their 2013 data breach.

Based on the above discussion, we expect that a firm's market value will be positively associated with its cybersecurity awareness.[21]

3. Research method and sample

3.1 Cybersecurity awareness measures

Our firm-specific cybersecurity awareness measure is based upon a score (*SCORE*), obtained from textual analysis of 10-K disclosures.[22] Specifically, we measure a firm's cybersecurity awareness by considering both the length of relevant disclosures as well as the relevance of the language used. *SCORE* is higher when the language is more directly relevant to cybersecurity, as opposed to when the language is indirectly relevant. We determine the language relevance through a self-developed dictionary, which is based upon a glossary of common cybersecurity terminology from the National Initiative for Cybersecurity Careers and Studies (NICCS). We supplement the NICCS list by including cyber-related legislative Acts, which we obtained from a report on laws relating to cybersecurity prepared by the Congressional Research Service (Fischer 2014).[23] Appendix A provides a description of our method for deriving *SCORE*.

Cyber-related disclosures in 10-Ks are largely qualitative, which gives managers the opportunity to be strategically optimistic/pessimistic in the way that they discuss cyber issues. We thus consider the tone of cyber disclosures in our analysis. We capture negative (positive)

[21] Presumably, the market can discern and value a firm's level of cybersecurity awareness. This is in line with prior research which has documented that the market recognizes the value of IT-related investments. For example, Bharadwaj et al. (1999) find that IT investments are associated with higher Tobin's Q. Using an event study methodology, Im et al. (2001) document higher market returns following a firm's announcement of IT initiatives.

[22] Li et al. (2018) capture cyber disclosures using Item 1A of the 10-K. Given that cyber disclosures are provided throughout the 10-K and are not restricted to Item 1A or the MD&A section (Gordon et al. 2015b; SEC 2018), we use the entire 10-K to construct our cyber disclosure measure.

[23] Because industries vary in their degree of cyber risk exposure, in addition to examining results based upon *SCORE*, we derive *NSCORE*, which is an industry-normalized version of the score (based upon Fama-French 48 industries). Specifically, for each year, we subtract the industry mean from *SCORE* and divide by the standard deviation across the firms in each industry. This industry-year normalized cyber awareness measure is labelled *NSCORE*. Our inferences do not change when we employ the standardized measure in our models.

tone using word lists from Loughran and McDonald (2011), which are restricted to words that have negative (positive) implications in a financial sense. The variable *Neg_Tone* (*Pos_Tone*) captures the number of words that are negative (positive), divided by the total number of words in a given 10-K disclosure. In further sensitivity tests, we include measures based upon the Loughran and McDonald (2011) dictionary to capture the negative (*10K_Neg*) and positive (*10K_Pos*) tone of the entire 10-K, along with the wordcount for the entire 10-K (*10K_WC*).

3.2 Model

We examine the effect of cybersecurity awareness on market valuation using the Ohlson model (Ohlson 1995). Starting with the standard Ohlson (1995) model, we follow earlier work on the valuation of intangible assets and include our measure of cybersecurity awareness as an additional regressor. We scale all variables in the standard Ohlson model by common shares outstanding (Barth and Clinch 2009). We estimate the following regression, clustering standards errors by firm and year.

$$MVE_{i,t} = \beta_0 + \beta_1 SCORE_{i,t} + \beta_2 BVE_{i,t} + \beta_3 EARN_{i,t} + \beta_3 EARN\_Neg_{i,t} + \sum Year\ FE + \sum Industry\ FE + \varepsilon_{i,t} \quad (1)$$

where *SCORE* is our cybersecurity awareness proxy; *MVE* is the share price three months after the end of the fiscal year; *BVE* is the book value of equity per share; *EARN* is earnings per share; *EARN_Neg* is earnings per share if earnings are equal or less than zero, 0 otherwise; *Year FE* represents year fixed effects and *Industry FE* represents industry fixed effects, which are based on the Fama-French 48 industry classification.

3.3 Sample

Our sample is drawn from the Russell 3000 firms for the period 2012-2016. We begin our investigation in 2012 because this is the first year following the SEC's issuance of guidance on cyber risk disclosure. We obtain all financial data from the Compustat and CRSP databases. We exclude financial institutions and insurance companies (i.e., those with SIC codes of 6000-

6999). All continuous variables are winsorized at the 1 and 99 percent level to minimize the effect of outliers.

Our sample selection is reported in Table 1. We obtain 13,592 firm-year observations of cybersecurity awareness scores from 3,084 unique firms for the period 2012–2016. We exclude 3,423 observations of firms from the financial services industry, 489 observations where firms have negative book values, and another 3 observations with missing financial data. Our final sample comprises 9,677 observations for 2,264 unique firms.

(Insert Table 1 here)

Panel A of Table 2 reports our sample distribution by year. The vast majority of firms in our sample (88.75%) disclosed cyber-related issues. This is in stark contrast to Gordon et al. (2010), where only 13.81% of firms provided cyber-related disclosures. This difference is almost certainly related to the changes in the regulatory environment stemming from the SEC's mandatory risk disclosure and guidance on cyber disclosures. We further observe an increase in the number of firms providing cyber-related disclosures across time. In 2012, 77.3% of our sample provided disclosures. This figure increased to 96.16% by 2016. Consistent with increasing importance of cyber-related issues, cybersecurity awareness has been monotonically increasing over time. The mean cybersecurity awareness score increased from 15.38 in 2012, to 27.66 in 2016.

Panel B of Table 2 reports the sample distribution by industry. Unsurprisingly, the industry with the highest mean cybersecurity awareness raw score is Computers (industry mean cybersecurity awareness score = 52). The largest industry representation is Business Services (14% of all firm-year observations), which has the second highest mean cybersecurity awareness score (industry mean cybersecurity awareness score = 43). Industries with the lowest mean cybersecurity awareness scores are Coal (industry mean cybersecurity awareness score = 6) and Textiles (industry mean cybersecurity awareness score = 4).

(Insert Table 2 here)

3.4 Descriptive statistics

Panel A of Table 3 presents sample descriptive statistics. The mean cybersecurity awareness score (*SCORE*) is 21.93.[24] Negative words (*Neg_Tone*) comprise an average of 5% of cyber disclosures and positive words (*Pos_Tone*) comprise an average of 0.5% of cyber disclosures.[25] Similarly, in overall 10-K disclosures, we observe a more negative tone. Negative words (*10K_Neg*) comprise an average of 1.88% of disclosures in 10-Ks and positive words (*10K_Pos*) comprise an average of 0.85% of 10-Ks disclosures.

We present pairwise correlations among the variables in our sample in Table 3, Panel B. Unsurprisingly, our measures of cybersecurity awareness are significantly correlated. Consistent with the notion that cyber awareness is higher in firms with more intangible assets, *SCORE* is positively correlated with *RnD* and *Advert*, and negatively correlated with *CapInt* and *CapExp*. This provides preliminary evidence that the market values firms with higher cybersecurity awareness more positively.

(Insert Table 3 here)

4. Results

4.1 Cybersecurity awareness and firm value

Table 4 presents results of estimating the association between cybersecurity awareness and market valuation.[26] Column (1) presents results for the standard Ohlson model augmented with our measure of cybersecurity awareness, which is the base model (Equation 1). Consistent with prior literature, we find a positive coefficient of book value of equity (*BVE*), earnings per

[24] Our measure of cybersecurity awareness (*SCORE*) ranges from 0 to 616 and is positively skewed. We test the sensitivity of our results to outliers by excluding the top 10% of firms with the highest cybersecurity awareness score. Our results remain robust. Our results are also robust to excluding observations with a cybersecurity awareness score of zero.

[25] Note that all word frequencies in Table 3 are multiplied by 100. Also note that there are fewer observations for *Neg_Tone* and *Pos_Tone* than *SCORE* because we lose observations when the word count of cyber disclosures is zero (i.e., when *SCORE* is zero).

[26] Our results are robust to the inclusion of firm fixed effects to the models.

share (*EARN*) and a negative coefficient of negative earnings (*EARN_Neg*). Consistent with Gordon et al. (2010), the coefficient of *SCORE* is positive and significant ($p < 0.01$), indicating a positive market valuation of cybersecurity awareness. A one-standard deviation increase in *SCORE* is associated with a $1.619 higher stock price.

We next consider the tone of cybersecurity awareness disclosures. This helps differentiate our cybersecurity awareness score from disclosure of cybersecurity awareness that represents firm vulnerabilities (in the case of negative tone, *Neg_Tone*), or providing an optimistic view of the firm's risk exposure and/or awareness (in the case of positive tone, *Pos_Tone*). Results in Table 4, Column (2), indicate that although positive tone of cyber disclosure does not explain market value, negative cyber disclosure tone is negatively associated with market valuations. After controlling for cyber disclosure tone, our cybersecurity awareness proxy (*SCORE*) remains significantly positive at the one percent level.

In Column (3) of Table 4, we further control for tone of overall 10-K disclosures (*10K_Neg* and *10K_Pos*) and the length of 10-K (*10K_WC*). *10K_Pos* (*10K_Neg*) is positive (negative) and significant (both at $p < 0.01$), indicating a positive (negative) market valuation of positive (negative) tone of overall disclosures. Length of 10-K does not affect market valuations. Importantly, after controlling for tone and length of general disclosures and tone of cyber disclosures, the coefficient of *SCORE* continues to be positive and significant ($p < 0.01$).

Because industries vary in their degree of cyber risk exposure, we also examine *NSCORE,* an industry-normalized version of *SCORE* (based upon Fama-French 48 industries). We construct *NSCORE,* by subtracting the industry mean from *SCORE* and dividing by the standard deviation across the firms in each industry for each year. As we report in Column (4), we continue to find a significant and positive coefficient of *NSCORE* ($p < 0.01$). A one standard deviation increase in *NSCORE* is associated with a $2.309 increase in stock price. Taken

together, these results indicate that the market value is positively associated with cybersecurity awareness.

(Insert Table 4 here)

5. Additional analyses and robustness tests

5.1 Alternative measures of cybersecurity awareness

Our measure of cybersecurity awareness is granular, allowing for a wide range of cybersecurity awareness levels. In further tests, we explore additional measures that could proxy for cybersecurity awareness, namely, if the firm has an IT executive or director (CIO, CTO, or CISO) (*IT_Dum*), or if the firm has a technology committee of the Board of Directors (*Tech_Com*). Further, a firm's level of cybersecurity awareness is likely to be affected by their prior experience of cyber breaches. In a survey by Cisco (2017), 90 percent of security professionals reported that a security breach resulted in improvements in cybersecurity defense technologies and processes. We thus consider firm's experience with cyber breaches as another proxy for cybersecurity awareness and examine the impact of breaches on market valuations. We obtain data on cyber incidents from the Privacy Rights Clearinghouse database (https://www.privacyrights.org/data-breaches). We capture a firm's history of cyber incidents by coding an indicator variable *BREACH* as 1 if a firm has experienced a cyber incident as reported in the Privacy Rights Clearinghouse database, 0 otherwise.[27]

As we report in Panel A of Table 3, only 3% of firms in our sample have an IT executive or director, and only 1% of firms have a Technology committee. Based upon the Privacy Rights Clearinghouse database, 4% of the observations in our sample have previously experienced a cyber breach. As we report in Panel B of Table 3, these alternative measures of cybersecurity awareness are positively correlated with our cybersecurity awareness measure.

[27] The first available year in which a cyber incident was recorded to have occurred on the Privacy Rights Clearinghouse database is 2004.

Panel A of Table 5 (Columns 1-3) reports results employing these alternative measures of cybersecurity awareness.[28] In all cases, the alternative measures have significantly positive associations with market valuation ($p < 0.10$ or better). In Column (4), when we include all the alternative measures and *SCORE*, we continue to find a significant positive association between our cybersecurity awareness measure and market valuation ($p < 0.01$). This suggests that our measure provides a broader measure of cybersecurity awareness than the alternatives. We also examine the sensitivity of our results to additional controls that relate to the tone of cyber disclosures (*Neg_Tone* and *Pos_Tone*) and tone and length of general 10-K disclosures (*10K_Neg*, *10K_Pos* and *10K_WC*). As we report in Panel B of Table 5, our results remain qualitatively similar, except that *BREACH* is no longer significant.

(Insert Table 5 here)

5.2 Other risks in 10-K disclosures

A possible concern is that our measure of cybersecurity awareness serves as a proxy for firms' general risk disclosure behavior rather than their cyber disclosures. To address this concern, we use the dictionary provided in Campbell et al. (2014) to capture other types of risks disclosed in 10-Ks and test whether our results are robust to their inclusion in the model. Panel A of Table 6 presents pairwise correlations among these other types of risks. The additional risk factors are highly correlated among each other and some of these risk factors are marginally correlated with *SCORE*.

Panel B of Table 6 presents results of re-estimating Equation (1) including the risks documented in Campbell et al. (2014). We find that greater disclosure of financial risks is associated with more negative market valuations (Column 1), although greater disclosure of tax risks is associated with higher market valuations (Column 5). We do not find evidence that other risks are significantly related to market valuations. Importantly in all model specifications

[28] Our results are robust to including firm fixed effects to the models.

(Columns 1-7), our measure of cybersecurity awareness (*SCORE*) remains positive and significant ($p < 0.01$).

(Insert Table 6 here)

5.3 Alternative valuation model

In this section, we employ Tobin's Q (*Q*) as an alternative measure of market valuation and examine its association with cybersecurity awareness. As we report in Table 7 Column (1), we find a positive and significant coefficient on *SCORE* ($p < 0.01$), indicating that greater cybersecurity awareness is associated with higher Tobin's Q. We next introduce the tone of cybersecurity awareness disclosures (Column 2). In contrast to Table 4, we find no evidence that cybersecurity awareness disclosure tone affects Tobin's Q, but we continue to find a positive and significant coefficient of *SCORE* ($p < 0.01$).

We next control for the tone and length of general 10-K disclosures (Column 3). We find that negative (positive) tone of 10-K disclosures and lengthier 10-K disclosures are associated with lower (higher) firm valuations. After controlling for the tone and length of general 10-K disclosures, the coefficient on *SCORE* remains significantly positive ($p < 0.01$). In Column (4), we report results using the normalized measure of our cybersecurity awareness score (*NSCORE*). We continue to find a positive and significant coefficient of *NSCORE* ($p < 0.01$). Collectively, our results indicate that greater cybersecurity awareness is associated with higher firm valuations as proxied by Tobin's Q.

(Insert Table 7 here)

5.4 Comparison to the information security measure by Gordon et al. (2010)

As we have noted, our study extends Gordon et al. (2010) by developing a new and updated cyber security measure, which is based upon increased disclosures following the 2011 SEC cybersecurity guidance and upon a more comprehensive dictionary that considers both the length and relevance of cyber disclosures. To test if our measure captures incremental

information about a firm's cyber awareness relative to the information security disclosure measure developed by Gordon et al. (2010), we re-estimate our model including Gordon et al.'s information security measure. Examining the voluntary disclosure on information security, Gordon et al. (2010) used a dichotomous variable based on 24 information security keywords to capture the presence or absence of disclosures. Our sample covers the post-guidance period, so the majority of firm-years in our sample provide cyber-related disclosures. As a result, using the dichotomous measure in Gordon et al. (2010) is less meaningful. We thus adapt the measure in Gordon et al. (2010) by constructing a continuous variable (*CYBER_GLS*), which is the total count of keywords in a firm's 10-K based on the information security dictionary of Gordon et al. (2010).

Unsurprisingly, our measure of cyber awareness (*SCORE*) is strongly correlated with *CYBER_GLS* ($\rho = 0.459$, $p < 0.01$). To examine whether our measure of cyber awareness provides incremental value relevant cyber-related information, we include *CYBER_GLS* in model 1. The results (untabulated) show that, consistent with Gordon et al. (2010), the coefficient on *CYBER_GLS* is positive and significant at the one percent level. These results suggest that greater information security disclosures are associated with higher market valuations. Importantly, our measure of cyber awareness (*SCORE*) remains positively significant at the one percent level. These results hold after controlling for disclosure tone and other 10-K characteristics.

Results using the normalized score of cyber awareness (*NSCORE*) are qualitatively similar; the coefficient of *NSCORE* remains positively significant at the one percent level after controlling for *CYBER_GLS*, disclosure tone and other characteristics of the 10-K. Together, these results provide evidence that our cyber awareness score captures information that is incremental to the measure constructed by Gordon et al. (2010), and that such information continues to be value relevant to the market after the SEC's 2011 cybersecurity guidance.

6. Conclusion

In light of the growing number of cyber attacks on corporations, there is heightened concern about firms' cybersecurity awareness. This concern is reflected in increased media coverage of cyber-related issues as well as increased regulation at multiple levels of government. In this paper, we develop a novel firm-specific measure of cybersecurity awareness and examine its impact on market valuations. Our measure of cybersecurity awareness considers both the relevance and length of cyber disclosures in 10-K filings. This measure can be used in future research regarding cybersecurity awareness.

Our empirical results indicate a positive association between cybersecurity awareness and market value. This association persists after controlling for disclosure tone, and we find negative tone to be negatively valued by the market. Our results are robust to a number of sensitivity tests, including using an industry-adjusted cybersecurity awareness measure, using an alternative valuation model, controlling for the tone and length of 10-K disclosures and controlling for other types of risk disclosures in 10-Ks. In addition, we provide evidence that our cybersecurity awareness measure captures value relevant information about a firm's cyber awareness that is incremental to the pre-guidance, disclosure-based measure developed by Gordon et al. (2010). Our results are consistent with the increased cyber disclosures providing information about a firm's cyber awareness, which is valued by the market. Thus, expanding the measure of cybersecurity awareness to take advantage of increased disclosure following SEC (2011) can help investors and other market participants to incorporate cyber awareness in their decision-making. These findings should be of interest to regulators and management.

We also investigate the market valuation impact of two other proxies of cybersecurity awareness, namely, IT corporate governance and firm's prior experience with IT breaches. We find that firms with better IT corporate governance enjoy higher market valuations and that company valuations are higher for firms which have previously experienced a cyber breach

incident. This latter result might indicate that once a firm experiences a breach, management will take measures to minimize the likelihood of future breaches and that investors consider these actions as value-enhancing. Collectively, our results reinforce our prior findings that cybersecurity awareness is positively valued by the market.

Overall, we provide strong evidence that in the post-cybersecurity guidance period, 10-K disclosures reflect cybersecurity awareness and not merely boilerplate disclosure. These disclosures allow us to develop a comprehensive measure of cybersecurity awareness that captures the ways in which firms address cyber-related issues. Given the increased interest in cyber security and cybersecurity awareness in both academia and in practice, our measure provides a promising means of investigating many different ways that cybersecurity awareness reflects and affects firm behavior.

References

Aboody, D., and B. Lev. 1998. The value relevance of intangibles: The case of software capitalization. *Journal of Accounting Research* 36: 161-191.

Acquisti, A., A. Friedman, and R. Telang. 2006. Is there a cost to privacy breaches? An event study. In *Proceedings of the Twenty Seventh International Conference on Information Systems, Wilwaukee, WI*.

AISA. 2017. Trust - the new face of cyber security. *Australian Cyber Security Magazine. Available at: https://australiancybersecuritymagazine.com.au/trust-the-new-face-of-cyber-security/*.

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

Athavaley, A. 2017. Verizon sought $925 million discount for Yahoo merger, got $350 million. *Reuters*.

Barth, M. E., M. B. Clement, G. Foster, and R. Kasznik. 1998. Brand values and capital market valuation. *Review of Accounting Studies* 3 (1-2): 41-68.

Barth, M. E., and G. Clinch. 2009. Scale effects in capital markets-based accounting research. *Journal of Business Finance & Accounting* 36 (3-4): 253-288.

Berkman, H., J. Jona, G. Lee, and N. S. Soderstrom. 2018. Cybersecurity awareness and the cost of liquidity, working paper.

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

Bharadwaj, A. S., S. G. Bharadwaj, and B. R. Konsynski. 1999. Information technology effects on firm performance as measured by tobin's q. *Management Science* 45 (7): 1008-1024.

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.

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.

Campbell, K., L. A. Gordon, M. P. Loeb, and L. Zhou. 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., 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.

Chabrow, E. 2017. SEC chair wants more cyber risk disclosure from public firms. *Available at: https://www.bankinfosecurity.com/sec-chair-more-cyber-risk-disclosure-from-public-firms-a-10336*.

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.

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, J. V., H.-C. Li, D. C. Yen, and K. V. Bata. 2012. Did it consulting firms gain when their clients were breached? *Computers in Human Behavior* 28 (2): 456-464.

Choi, W. W., S. S. Kwon, and G. J. Lobo. 2000. Market valuation of intangible assets. *Journal of Business Research* 49 (1): 35-45.

Cisco. 2017. 2017 annual cybersecurity report.

Clarkson, P. M., Y. Li, and G. D. Richardson. 2004. The market valuation of environmental capital expenditures by pulp and paper companies. *The Accounting Review* 79 (2): 329-353.

Cowley, S. 2017. Equifax faces mounting costs and investigations from breach. *Available at: https://www.nytimes.com/2017/11/09/business/equifax-data-breach.html*.

Deloitte. 2016. Beneath the surface of a cyberattack. *Available at: https://www2.deloitte.com/us/en/pages/risk/articles/hidden-business-impact-of-cyberattack.html*.

———. 2017. Cyber reporting survey. Available at: Https://www.Deloitteacademy.Co.Uk/media/823595/deloitte-uk-governance-in-focus-cyber-risk-reporting.Pdf.

Deng, Z., B. Lev, and F. Narin. 1999. Science and technology as predictors of stock performance. *Financial Analysts Journal* 55 (3): 20-32.

Durbin, S. 2016. Security vs. Privacy: Securing your critical information assets. *Available at: http://www.infosecisland.com/blogview/24846-Security-vs-Privacy-Securing-Your-Critical-Information-Assets.html*.

Dye, R. A. 1985. Disclosure of nonproprietary information. *Journal of Accounting Research* 23 (1): 123-145.

———. 2010. Disclosure "bunching". *Journal of Accounting Research* 48 (3): 489-530.

Ettredge, M. L., and V. J. Richardson. 2003. Information transfer among internet firms: The case of hacker attacks. *Journal of Information Systems* 17 (2): 71-82.

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.

Francis, J., D. Philbrick, and K. Schipper. 1994. Shareholder litigation and corporate disclosures. *Journal of Accounting Research* 32 (2): 137-164.

Garg, A., J. Curtis, and H. Halper. 2003. The financial impact of it security breaches: What do investors think? *Information Systems Security* 12 (1): 22-33.

Gatzlaff, K. M., and K. A. McCullough. 2010. The effect of data breaches on shareholder wealth. *Risk Management and Insurance Review* 13 (1): 61-83.

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

Gordon, L. A., and M. P. Loeb. 2002. The economics of information security investment. *ACM Transactions on Information and System Security (TISSEC)* 5 (4): 438-457.

Gordon, L. A., M. P. Loeb, and W. Lucyshyn. 2003. Sharing information on computer systems security: An economic analysis. *Journal of Accounting and Public Policy* 22 (6): 461-485.

Gordon, L. A., M. P. Loeb, W. Lucyshyn, and T. Sohail. 2006. The impact of the Sarbanes-Oxley Act on the corporate disclosures of information security activities. *Journal of Accounting and Public Policy* 25 (5): 503-530.

Gordon, L. A., M. P. Loeb, W. Lucyshyn, and L. Zhou. 2015a. The impact of information sharing on cybersecurity underinvestment: A real options perspective. *Journal of Accounting and Public Policy* 34 (5): 509-519.

———. 2015b. 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* 34 (3): 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.

Guillamon-Saorin, E., H. Isidro, and A. Marques. 2017. Impression management and non-GAAP disclosure in earnings announcements. *Journal of Business Finance & Accounting* 44 (3-4): 448-479.

Higgs, J. L., R. E. Pinsker, T. J. Smith, and G. R. Young. 2016. The relationship between board-level technology committees and reported security breaches. *Journal of Information Systems* 30 (3): 79-98.

Hilary, G., B. Segal, and M. H. Zhang. 2016. Cyber-risk disclosure: Who cares?

Hinz, O., M. Nofer, D. Schiereck, and J. Trillig. 2015. The influence of data theft on the share prices and systematic risk of consumer electronics companies. *Information & Management* 52 (3): 337-347.

Hirschey, M., and V. J. Richardson. 2004. Are scientific indicators of patent quality useful to investors? *Journal of Empirical Finance* 11 (1): 91-107.

Hiscox. 2017. Hiscox cyber readiness report 2017. Available at: Https://www.Hiscox.Co.Uk/cyber-readiness-report/docs/cyber-readiness-report-2017.Pdf.

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, X., S. H. Teoh, and Y. Zhang. 2013. Tone management. *The Accounting Review* 89 (3): 1083-1113.

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.

Islam, M. S., N. Farah, and T. F. Stafford. 2018. Factors associated with security/cybersecurity audit by internal audit function: An international study. *Managerial Auditing Journal*.

Javers, E. 2013. Cyberattacks: Why companies keep quiet. *Available at: https://www.cnbc.com/id/100491610*.

Jorgensen, B. N., and M. T. Kirschenheiter. 2003. Discretionary risk disclosures. *The Accounting Review* 78 (2): 449-469.

Kashmiri, S., C. D. Nicol, and L. Hsu. 2017. Birds of a feather: Intra-industry spillover of the target customer data breach and the shielding role of it, marketing, and CSR. *Journal of the Academy of Marketing Science* 45 (2): 208-228.

Lev, B., and S. R. Thiagarajan. 1993. Fundamental information analysis. *Journal of Accounting Research* 31 (2): 190-215.

Li, H., W. G. No, and J. E. Boritz. 2016. Are external auditors concerned about cyber incidents? Evidence from audit fees. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2880928.

Li, H., W. G. No, and T. Wang. 2018. SEC's cybersecurity disclosure guidance and disclosed cybersecurity risk factors. *International Journal of Accounting Information Systems*.

Loughran, T., and B. McDonald. 2011. When is a liability not a liability? Textual analysis, dictionaries, and 10-ks. *The Journal of Finance* 66 (1): 35-65.

Malhotra, A., and C. Kubowicz Malhotra. 2011. Evaluating customer information breaches as service failures: An event study approach. *Journal of Service Research* 14 (1): 44-59.

Martin, K. D., A. Borah, and R. W. Palmatier. 2017. Data privacy: Effects on customer and firm performance. *Journal of Marketing* 81 (1): 36-58.

Matsumura, E. M., R. Prakash, and S. C. Vera-Muñoz. 2014. Firm-value effects of carbon emissions and carbon disclosures. *The Accounting Review* 89 (2): 695-724.

Menn, J. 2012. Hacked companies still not telling investors. *Available at: https://www.reuters.com/article/us-hacking-disclosures/exclusive-hacked-companies-still-not-telling-investors-idUSTRE8110YW20120202*.

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.

Morse, E., V. Raval, and J. Wingender. 2018. SEC cybersecurity guidelines: Insights into the utility of risk factor disclosures for investors. *Business Lawyer* 73 (1-33).

Morse, E. A., V. Raval, and J. R. Wingender Jr. 2011. Market price effects of data security breaches. *Information Security Journal: A Global Perspective* 20 (6): 263-273.

Ohlson, J. A. 1995. Earnings, book values, and dividends in equity valuation. *Contemporary Accounting Research* 11 (2): 661-687.

Pentland, W. 2011. Night dragon attacks target technology in energy industry. *Available at: https://www.forbes.com/sites/williampentland/2011/02/19/night-dragon-attacks-target-technology-in-energy-industry/#7f2f7bd61d49*.

Pirounias, S., D. Mermigas, and C. Patsakis. 2014. The relation between information security events and firm market value, empirical evidence on recent disclosures: An extension of the glz study. *Journal of Information Security and Applications* 19 (4-5): 257-271.

Prince, B. 2015. Target data breach tally hits $162 million in net costs, available at: Http://www.Securityweek.Com/target-data-breach-tally-hits-162-million-net-costs.

PwC. 2016. The global state of information security survey 2016. Available at: Http://www.Pwc.Com/sg/en/publications/assets/pwc-global-state-of-information-security-survey-2016.Pdf.

Rogers, J. L., and A. Van Buskirk. 2009. Shareholder litigation and changes in disclosure behavior. *Journal of Accounting and Economics* 47 (1): 136-156.

SEC. 2005. Securities and exchange commission final rule, release no. 33–8591 (fr-75). edited by http://www.sec.gov/rules/final/33-8591.pdf.

———. 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.

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*.

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.

Trueman, B., M. F. Wong, and X.-J. Zhang. 2000. The eyeballs have it: Searching for the value in internet stocks. *Journal of Accounting Research*: 137-162.

Wang, L., and P. Alam. 2007. Information technology capability: Firm valuation, earnings uncertainty, and forecast accuracy. *Journal of Information Systems* 21 (2): 27-48.

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.

Wang, T., J. R. Ulmer, and K. Kannan. 2013. The textual contents of media reports of information security breaches and profitable short-term investment opportunities. *Journal of Organizational Computing and Electronic Commerce* 23 (3): 200-223.

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.

Zafar, H., M. S. Ko, and K.-M. Osei-Bryson. 2016. The value of the CIO in the top management team on performance in the case of information security breaches. *Information Systems Frontiers* 18 (6): 1205-1215.

Appendix A. Cybersecurity awareness measure

A.1 Domain mapping methodology and general approach to identifying, categorizing and ranking cybersecurity disclosures.

Cyber-related disclosures in firm's 10-Ks were identified, categorized and ranked using the rules-based text analysis algorithms. We developed a keyword list from a core set of keywords contained in a list provided by a glossary of common cybersecurity terminology from the National Initiative for Cybersecurity Careers and Studies (NICCS). We supplemented the NICCS list by including cyber-related legislative Acts, which we obtained from a report on laws relating to cybersecurity prepared by the Congressional Research Service (Fischer 2014). These keywords and phrases were then incorporated into the disclosure mapping logic to develop an initial corpus of cyber-security disclosures.

The keyword dictionary is structured around a core keyword or keyword phrase and 0 or more additional terms that qualify that core keyword or keyword phrase. The dictionary was refined through an iterative process of testing this original list against samples of disclosures from a variety of industry groupings. As the domain was refined, an effort was made to prune false positives while minimizing the risk of false negatives.

Each excerpt was assigned a relevance score. This score is a function of amount of relevant language contained within the excerpt as well as a weighting on this language that reflects how directly it addresses the domain of cybersecurity. Specifically, the relevance score reflects the amount of language contained within an excerpt that is relevant to the domain. Some keywords and phrases are relevant wherever they are found in a text (e.g. 'cyber security' or 'digital information'). Some are only relevant only within context (e.g. 'network security' or 'personal information'). The score is derived by the number of times a relevant keyword or keyword phrase occurs within an excerpt, as well as whether it is independently relevant to the domain or contextually relevant, the former being awarded a higher score. Within this logic, language specificity (e.g. 'Advancing America's Networking and Information Technology Research And Development Act') is rewarded with a higher key phrase score.

The scores are derived by summing the individual relevance values assigned to each keyword phrase found within the excerpt. Scores are tallied across all excerpts identified as true positives within a particular filing to compute at total score for the whole filing.

This process is similar, except for the textual adjustments for cyber-risk disclosures, to the Climate Risk Disclosure project that was developed by CookESG Research and available through Ceres. The excerpts identified as cybersecurity disclosures can be found at www.climateriskdisclosure.com (select “Show advanced options” and select Cyber Security under the Disclosure Category).

A.2 Examples of cybersecurity awareness scores

1. Hawaiian Electric Industries, Inc. 2016 10-K

Cybersecurity awareness score:	Percentage positive tone:	Percentage negative tone:
68	0.31	3.5

Relevant excerpts:

The Company may be subject to information technology system failures, network disruptions, cyber attacks and breaches in data security that could adversely affect its businesses and reputation. The Utilities rely on networks, information systems and other technologies, including the Internet and third-party hosted services to support a variety of business processes and activities, including procurement and supply chain, invoicing and collection of payments, customer relationship management, human resource management, the acquisition, generation and delivery of electrical service to customers, and to process financial information and results of operations for internal reporting purposes and to comply with regulatory financial reporting and legal and tax requirements. The Utilities use their systems and infrastructure to create, collect, store, and process sensitive information, including personal information regarding customers, employees and their dependents, retirees, and other individuals.

In addition, the Utilities are pursuing complex business transformation initiatives, which include establishing common processes across Hawaiian Electric, Hawaii Electric Light and Maui Electric and the upgrade or replacement of existing systems. Significant system changes increase the risk of system interruptions. Although the Utilities maintain change management processes to mitigate this risk, system interruptions may occur. Further, delay or failure to complete the integration of information systems and processes may result in delays in regulatory cost recovery, increased service interruptions of aging legacy systems, or the failure to realize the cost savings anticipated to be derived from these initiatives.

As noted by the U.S. Department of Homeland Security, the utility industry is continuing to experience an increase in the frequency and sophistication of cyber security incidents. The Utilities' systems have been, and will likely continue to be, a target of attacks. Although the Utilities have not experienced a material cyber security breach to date, such incidents may occur and may have a material adverse effect on the Company in the future. In order to address cyber security risks to their information systems, the Utilities maintain security measures designed to protect their information technology systems, network infrastructure and other assets. The Utilities actively monitor developments in the area of cyber security and are involved in various related government and industry groups.

Although the Utilities continue to make investments in their cyber security program, including personnel, technologies, cyber insurance and training of Utilities personnel, there can be no assurance that these systems or their expected functionality will be implemented, maintained, or

expanded effectively; nor can security measures completely eliminate the possibility of a cyber security breach. If the Utilities' cyber security measures were to be breached, the Utilities could suffer financial loss, business disruptions, liability to customers, regulatory intervention or damage to their reputation.

2. WGL Holdings 2016 10-K

Cybersecurity awareness score:	Percentage positive tone:	Percentage negative tone:
24	0.47	3.18

Relevant excerpts:

Cyber attacks, including cyber-terrorism or other information technology security breaches, or information technology failures may disrupt our business operations, increase our costs, lead to the disclosure of confidential information and damage our reputation. Security breaches of our information technology infrastructure, including cyber attacks and cyber-terrorism, or other failures of our information technology infrastructure could lead to disruptions of our natural gas distribution operations and otherwise adversely impact our ability to safely and effectively operate our pipeline and distributed generation systems and serve our customers. In addition, an attack on or failure of information technology systems could result in the unauthorized release of customer, employee or Company data that is crucial to our operational security or could adversely affect our ability to deliver and collect on customer bills. Such security breaches of our information technology infrastructure could adversely affect WGL Holdings, Inc… We have implemented preventive, detective and remediation measures to manage these risks, and we maintain cyber risk insurance to mitigate the effects of these events. Nevertheless, these may not effectively protect all of our systems all of the time. To the extent that the occurrence of any of these cyber events is not fully covered by insurance, it could adversely affect WGL's financial condition and results of operations.

3. El Paso Electric 2013 10-K

Cybersecurity awareness score:	Percentage positive tone:	Percentage negative tone:
8	0	7.80

Relevant excerpts:

We rely upon our infrastructure to manage or support a variety of business processes and activities, including the generation, transmission and distribution of electricity, supply chain functions, and the invoicing and collection of payments from our customers. We also use information technology systems for internal accounting purposes and to comply with financial reporting, legal and tax requirements. Our information technology networks and infrastructure may be vulnerable to damage, disruptions or shutdowns due to attacks by hackers, breaches due to employee error or malfeasance, system failures, natural disasters, a physical attack on our facilities, or other catastrophic events.

Appendix B. Variable definitions

Variable	Definition	Source
SCORE	Raw scores for cyber disclosure extensiveness	CookESG Research
NSCORE	*SCORE*, normalized to industry and year	CookESG Research
Cyber_GLS	Total count of information security keywords in the 10-K based on the information security dictionary in Gordon et al. (2010).	10-K
IT_Dum	Indicator variable coded one if the firm has an IT executive or director, zero otherwise	BoardEx
Tech_Com	Indicator variable coded one if the firm has a technology board committee, zero otherwise	BoardEx
BREACH	Indicator variable coded one if the firm previously experienced a cyber breach, zero otherwise	Privacy Rights Clearinghouse database
Neg_Tone	The ratio of negative words to total words in the cyber extracts multiplied by 100 (based on Loughran and McDonald 2011).	CookESG Research
Pos_Tone	The ratio of positive words to total words in the cyber extracts multiplied by 100 (based on Loughran and McDonald 2011).	CookESG Research
10K_Neg	The ratio of negative words to total words in the 10-Ks (based on Loughran and McDonald 2011), multiplied by 100	WRDS SEC Analytics Suite
10K_Pos	The ratio of positive words to total words in the 10-Ks (based on Loughran and McDonald 2011) , multiplied by 100	WRDS SEC Analytics Suite
10K_WC	Natural logarithm of the total number of words in the 10-Ks	WRDS SEC Analytics Suite
MVE	Stock price at three months after fiscal year-end (prcc_q)	The merged CRSP - COMPUSTAT
BVE	Book value of equity per share ((ceq- pstk)/cshoq)	The merged CRSP - COMPUSTAT
EARN	Earnings per share ((epspx*csho)/cshoq)	The merged CRSP - COMPUSTAT
EARN_Neg	Earnings per share to common equity earnings ≤0, zero otherwise	The merged CRSP - COMPUSTAT
Q	Tobin's Q, the sum of market capitalization and the book value of debt, divided by the book value of total assets (at-ceq-txdb+ csho*prcc_f)/at	The merged CRSP - COMPUSTAT
LEV	The short term and long-term debt scaled by market value of common equity ((dltt+dlc)/(dltt+dlc+ceq))	The merged CRSP - COMPUSTAT
ROA	Return on Assets is earnings divided by the book value of total assets (ib/at)	The merged CRSP - COMPUSTAT
SIZE	The log of total assets (at)	
CapInt	Capital intensity is gross property, plant and equipment scaled by total assets (ppegt/at)	The merged CRSP - COMPUSTAT
CapExp	Capital expenditure is capital expenditure on property plant and equipment scaled by total assets (capx/at)	The merged CRSP - COMPUSTAT
RnD	Research and Development is research and development expense scaled by total assets (xrd/at)	The merged CRSP - COMPUSTAT
Advert	Advertising is advertising expense scaled by total assets (xad/at)	The merged CRSP - COMPUSTAT
Div_Dum	Dividends is 1 if the firm paid dividends in the fiscal year, 0 otherwise	The merged CRSP - COMPUSTAT

Table 1
Sample Selection

	Observations	Number of Firms
Cyber-Related Disclosure data	**13,592**	**3,084**
Less observations:		
For financial services firms	(3,423)	
Negative book value	(489)	
Missing financial data	(3)	
Final Valuation Sample	**9,677**	**2,264**

This table presents the sample development process. The sample is based on Russell 3000 firms in the period 2012–2016.

Table 2
Sample Distribution

Panel A: Sample by Year

Year	Total firms	Mean cybersecurity awareness score	Number of firms without any cyber disclosures	% of firms without any cyber disclosures
2012	1,771	15.38	402	22.70%
2013	1,900	18.13	308	16.21%
2014	2,072	22.08	182	8.78%
2015	2,084	25.73	126	6.05%
2016	1,850	27.66	71	3.84%
Total	9,677	21.93	1,089	11.25%

This panel reports the sample by year. The sample is based on Russell 3000 firms in the period 2012–2016.

Panel B: Industry Classification and Distribution

Industry Classification	(1) *N*	(2) *Mean SCORE*
Agriculture	34	**14**
Aircraft	57	**22**
Apparel	125	**22**
Automobiles and Truck	193	**9**
Beer & Liquor	34	**13**
Business Services	1,384	**43**
Business Supplies	116	**10**
Candy & Soda	33	**14**
Chemicals	268	**11**
Coal	24	**6**
Communication	289	**31**
Computers	306	**52**
Construction	202	**10**
Construction Material	214	**9**
Consumer Goods	140	**15**
Defense	27	**22**
Electrical Equipment	145	**13**
Electronic Equipment	550	**24**
Entertainment	128	**18**
Fabricated Products	24	**10**
Food Products	214	**14**
Healthcare	163	**25**
Machinery	384	**10**
Measuring and Control	197	**15**
Medical Equipment	362	**21**
Non-Metallic	58	**11**
Personal Services	133	**25**
Petroleum and Natural	463	**11**
Pharmaceutical	1,076	**14**
Precious Metals	20	**13**
Printing and Publishing	52	**30**
Recreation	44	**24**
Restaurants, Hotels,	219	**22**
Retail	594	**25**
Rubber and Plastic	57	**9**
Shipbuilding, Railroads	42	**12**
Shipping Containers	45	**11**
Steel Works	109	**9**
Textiles	25	**4**
Tobacco Products	11	**13**
Transportation	302	**17**
Utilities	396	**21**
Wholesale	315	**18**
Other	103	**15**
Total	**9,677**	

Notes: The table presents the full sample firm-year observations across the Fama-French 48 Industry Classification. Column 1 reports the total number of firm-year observations for each industry in the sample. Column 2 provides the industry mean cybersecurity awareness score (*SCORE*).

Table 3
Descriptive Statistics for Regression Model Variables

Panel A: Descriptive Statistics

Variables	N	mean	sd	p25	p50	p75	min	max
Cybersecurity awareness variables								
SCORE	9,677	21.93	28.91	8.00	16.00	27.00	0.00	616.00
IT_Dum	7,716	0.03	0.18	0.00	0.00	0.00	0.00	1.00
Tech_Com	7,713	0.01	0.08	0.00	0.00	0.00	0.00	1.00
BREACH	9,677	0.04	0.21	0.00	0.00	0.00	0.00	1.00
Textual analysis variables								
Neg_Tone	8,584	4.55	2.03	3.27	4.42	5.74	0.00	17.86
Pos_Tone	8,584	0.52	0.52	0.20	0.43	0.71	0.00	10.00
10K_Neg	9,446	1.88	0.39	1.61	1.87	2.12	0.38	4.76
10K_Pos	9,446	0.85	0.18	0.72	0.83	0.94	0.27	2.35
10K_WC	9,446	10.82	0.41	10.56	10.80	11.05	8.39	12.97
Dependent variables								
MVE	9,677	37.91	35.76	13.93	27.75	50.29	1.76	216.24
Q	9,677	0.66	0.54	0.25	0.55	0.97	-0.27	2.25
Control variables								
BVE	9,677	14.11	12.78	4.87	10.53	19.34	0.22	67.31
EARN	9,677	1.20	2.69	-0.16	0.99	2.45	-7.54	11.32
EARN_Neg	9,677	-0.45	1.19	-0.16	0.00	0.00	-7.54	0.00
ROA	9,677	-0.01	0.17	-0.01	0.04	0.07	-0.80	0.26
LEV	9,628	0.32	0.26	0.04	0.31	0.51	0.00	0.95
SIZE	9,677	7.20	1.75	5.88	7.10	8.39	3.56	11.57
CapInt	9,620	0.48	0.40	0.16	0.35	0.75	0.01	1.70
CapExp	9,673	0.05	0.05	0.02	0.03	0.06	0.00	0.31
RnD	9,677	0.05	0.10	0.00	0.00	0.06	0.00	0.58
Advert	9,677	0.01	0.03	0.00	0.00	0.01	0.00	0.17
Div_Dum	9,677	0.48	0.50	0.00	0.00	1.00	0.00	1.00

Panel B: Pearson Pair-Wise Correlations Matrix

		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	20	21	22
1	***SCORE***																					
2	***IT_Dum***	0.10***																				
3	***Tech_Com***	0.02	0.04**																			
4	***BREACH***	0.14***	0.07***	0.03**																		
5	***Neg_Tone***	-0.21***	-0.06***	-0.01	-0.07***																	
6	***Pos_Tone***	0.01	0.00	0.01	0.01	-0.17***																
7	***10K_Neg***	0.20***	0.01	0.02*	0.00	0.01	0.03**															
8	***10K_Pos***	0.01	0.00	0.05***	0.01	-0.04***	0.11***	0.07***														
9	***10K_WC***	0.16***	-0.00	0.00	0.08***	-0.11***	0.03*	0.17***	-0.02													
10	***MVE***	0.03**	0.08***	0.03**	0.10***	-0.03*	-0.01	-0.16***	-0.05***	0.01												
11	***Q***	0.08***	0.08***	0.03*	-0.01	-0.04**	0.03**	0.11***	0.25***	-0.08***	0.17***											
12	***BVE***	-0.06***	0.01	0.02	0.05***	0.01	-0.03**	-0.19***	-0.20***	0.02	0.64***	-0.30***										
13	***EARN***	-0.04***	0.03*	0.01	0.09***	0.02	-0.03*	-0.27***	-0.09***	-0.14***	0.61***	0.00	0.52***									
14	***EARN_Neg***	-0.00	-0.02	-0.01	0.03**	0.02*	-0.02	-0.20***	-0.06***	-0.19***	0.09***	-0.00	0.08***	0.67***								
15	***ROA***	0.00	-0.00	-0.00	0.07***	0.05***	-0.03**	-0.26***	-0.24***	-0.20***	0.30***	-0.13***	0.28***	0.59***	0.58***							
16	***LEV***	0.00	-0.01	0.00	0.07***	-0.02	-0.03**	-0.12***	-0.15***	0.26***	0.09***	-0.28***	0.02	0.07***	-0.02*	0.10***						
17	***SIZE***	0.06***	0.10***	0.03***	0.06***	-0.02	0.03***	0.01***	-0.18***	0.26***	0.45***	-0.32***	0.15***	0.05***	-0.01	0.39***	0.48***					
18	***CapInt***	-0.16***	-0.03*	-0.03*	-0.01	0.07***	-0.05***	-0.24***	-0.26***	-0.04***	0.02	-0.29***	0.15***	0.05***	-0.01	0.15***	0.24***	0.22***				
20	***CapExp***	-0.08***	-0.01	-0.02	-0.02*	0.04***	-0.04**	-0.14***	-0.24***	-0.01	0.05***	-0.10***	0.09***	0.03*	-0.03*	0.10***	0.10***	-0.10***	0.65***			
21	***RnD***	0.04***	0.03*	0.03**	-0.05***	-0.07***	0.04***	0.27***	0.40***	0.12***	-0.18***	0.39***	-0.33***	-0.32***	-0.25***	-0.70***	-0.31***	-0.44***	-0.34***	-0.21***		
22	***Advert***	0.10***	-0.01	-0.01	0.03***	0.01	0.01	0.05***	0.02	-0.06***	0.02*	0.11***	-0.10***	0.02*	0.04***	0.09***	-0.08***	-0.05***	0.01	0.04***	-0.07***	
23	***Div_Dum***	-0.10***	0.00	0.00	0.07***	0.05***	-0.01	-0.29***	-0.14***	-0.09***	0.22***	-0.17***	0.28***	0.32***	0.17***	0.31***	0.17***	0.41***	0.25***	0.04***	-0.34***	-0.03**

This table presents descriptive information for the full sample. Panel A presents descriptive statistics and Panel B presents Pearson pair-wise correlations for variables in the various regression models used in the study based on Russell 3000 firms in the period 2012-2016.

Variable definitions: *SCORE* is the raw score for extensiveness of total cyber risk disclosure in the 10-K; *IT_Dum* is an indicator variable coded one if the firm has an IT executive or director, zero otherwise; *Tech_Com* is an indicator variable coded one if the firm has a technology board committee, zero otherwise; *BREACH* is an indicator variable coded one if the firm previously experienced a cyber breach, zero otherwise; *Neg_Tone* and *Pos_Tone* are the ratios of negative and positive words to total words in the cyber extracts (based on Loughran and McDonald 2011), respectively; *10K_Neg* and *10K_Pos* are the ratios of negative and positive words to total words in the 10-K disclosures (based on Loughran and McDonald 2011), respectively; *10K_WC* is the natural logarithm of the total number of words in the 10-K filing; *MVE* is the stock price three months after the end of fiscal year; *Q* is Tobin's Q, the sum of market capitalization and the book value of debt, divided by the book value of total assets; *BVE* is book value per share of common equity; *EARN* is earnings per share to common equity; *EARN_Neg* is earnings per share to common equity if earnings ≤0, 0 otherwise; *ROA* is return on assets; *LEV* is long-term debt scaled by market value of common equity. *,**,*** denote correlations that are significant at the 0.10, 0.05 and 0.01 level, respectively. See Appendix B for detailed variable definitions.

Table 4
Regression Model Results for Market Value and Cybersecurity Awareness

	(1) Base model	(2) Inclusion of tone of cyber disclosures	(3) Inclusion of general tone disclosures	(4) Normalized cyber score
SCORE	0.056***	0.046***	0.051***	
	(0.000)	(0.000)	(0.000)	
NSCORE				2.309***
				(0.000)
BVE	0.920***	0.936***	0.937***	0.938***
	(0.000)	(0.000)	(0.000)	(0.000)
EARN	9.874***	9.814***	9.608***	9.572***
	(0.000)	(0.000)	(0.000)	(0.000)
EARN_Neg	-12.692***	-12.661***	-12.565***	-12.589***
	(0.000)	(0.000)	(0.000)	(0.000)
Neg_Tone		-0.344***	-0.260**	-0.201*
		(0.002)	(0.021)	(0.069)
Pos_Tone		0.122	0.103	0.155
		(0.763)	(0.799)	(0.702)
10K_Neg			-3.730***	-4.297***
			(0.000)	(0.000)
10K_Pos			4.926***	4.735***
			(0.002)	(0.003)
10K_WC			0.892	0.223
			(0.203)	(0.753)
Year FE	Yes	Yes	Yes	Yes
Industry FE	Yes	Yes	Yes	Yes
N	9,677	8,584	8,365	8,365
Adj R^2	0.640	0.630	0.628	0.630

The table presents results of regression models that examine the effect of cybersecurity awareness on market value, scaled by shares (*MVE*). The sample period is 2012 to 2016. Column 1 reports the results for the base model. *SCORE* is the cybersecurity awareness score. *BVE* is book value per share of common equity; *EARN* is earnings per share to common equity; *EARN_Neg* is earnings per share to common equity if earnings ≤0, 0 otherwise. Column 2 reports the results for the market valuation model including tone of cyber disclosures (*Neg_Tone* and *Pos_Tone*. Column 3 reports the results for the market valuation model including general tone of disclosures in the 10-Ks (*10K_Neg* and *10K_Pos*) and the length of 10-K disclosures *(10K_WC)* in the 10-Ks. Column 4 reports the results using normalized cyber score (*NSCORE*). Two-tailed *p*-Values are given in parentheses and are based on firm cluster-adjusted standard errors. *, **, *** denote differences that are significant at the 0.10, 0.05 and 0.01 level, respectively.

Table 5
Regression Model Results for Other Cybersecurity Awareness Measures

Panel A: Main models

	(1) IT executive or director	(2) Technology committee	(3) Previous cyber breach experience	(4) Inclusion of *SCORE*
IT_Dum	9.681***			9.109***
	(0.000)			(0.000)
Tech_Com		7.483**		6.478*
		(0.041)		(0.085)
BREACH			2.362*	1.764
			(0.066)	(0.273)
SCORE				0.045***
				(0.000)
BVE	0.934***	0.929***	0.918***	0.935***
	(0.000)	(0.000)	(0.000)	(0.000)
EARN	9.715***	9.784***	9.856***	9.698***
	(0.000)	(0.000)	(0.000)	(0.000)
EARN_Neg	-12.884***	-13.033***	-12.695***	-12.826***
	(0.000)	(0.000)	(0.000)	(0.000)
Year FE	Yes	Yes	Yes	Yes
Industry FE	Yes	Yes	Yes	Yes
N	7,716	7,713	9,677	7,713
Adj R^2	0.643	0.641	0.640	0.645

The table presents results of regression models that examine the effect of other cybersecurity awareness measures on market valuations. The dependent variable is market value, scaled by shares (*MVE*). The sample period is 2012 to 2016. Column 1 reports the results with inclusion of a variable that captures whether the firm has an IT executive or director (*IT_Dum*). *SCORE* is the cybersecurity awareness score. *BVE* is book value per share of common equity; *EARN* is earnings per share to common equity; *EARN_Neg* is earnings per share to common equity if earnings ≤0, 0 otherwise. Column 2 reports the results with inclusion of a variable that captures whether the firm has an IT committee (*Tech_Com*). Column 3 reports the results with inclusion of a variable that captures whether the firm previously experienced a cyber breach (*BREACH*). Column 4 reports the results including *SCORE*, *IT_Dum*, *Tech_Com*, and *BREACH*. Two-tailed *p*-Values are given in parentheses and are based on firm cluster-adjusted standard errors. *, **, *** denote differences that are significant at the 0.10, 0.05 and 0.01 level, respectively.

Panel B: Main Models with Additional Controls

	(1) IT executive or director	(2) Technology committee	(3) Previous cyber breach experience	(4) Inclusion of *SCORE*
IT_Dum	10.298***			9.872***
	(0.000)			(0.000)
Tech_Com		7.781**		6.959*
		(0.046)		(0.081)
BREACH			1.856	1.721
			(0.160)	(0.299)
SCORE				0.044***
				(0.000)
BVE	0.950***	0.944***	0.934***	0.950***
	(0.000)	(0.000)	(0.000)	(0.000)
EARN	9.488***	9.562***	9.601***	9.464***
	(0.000)	(0.000)	(0.000)	(0.000)
EARN_Neg	-12.723***	-12.871***	-12.526***	-12.711***
	(0.000)	(0.000)	(0.000)	(0.000)
Neg_Tone	-0.273**	-0.312**	-0.369***	-0.165
	(0.024)	(0.010)	(0.001)	(0.176)
Pos_Tone	0.169	0.135	0.059	0.194
	(0.698)	(0.758)	(0.884)	(0.657)
10K_Neg	-3.836***	-3.859***	-3.022***	-4.463***
	(0.000)	(0.000)	(0.000)	(0.000)
10K_Pos	5.411***	5.425***	5.024***	5.098***
	(0.003)	(0.003)	(0.002)	(0.005)
10K_WC	1.239	1.287*	1.238*	0.745
	(0.109)	(0.098)	(0.078)	(0.345)
Year FE	Yes	Yes	Yes	Yes
Industry FE	Yes	Yes	Yes	Yes
N	6,657	6,654	8,365	6,654
Adj R^2	0.629	0.627	0.627	0.631

The table presents results of regression models that examine the effect of other cybersecurity awareness measures on market valuations described in panel A, with the inclusion of controls for disclosure tone (*Neg_Tone*, *Pos_Tone*, *10K_Neg*, and *10K_Pos*) and length of disclosures (*10K_WC*). Two-tailed *p*-Values are given in parentheses and are based on firm cluster-adjusted standard errors. *, **, *** denote differences that are significant at the 0.10, 0.05 and 0.01 level, respectively.

Table 6
Market Value and Different Types of Risks

Panel A: Correlations between *SCORE* and types of risks

		1	2	3	4	5	6	7
1	***SCORE***							
2	***Financial***	0.07**						
3	***Idiosyn***	0.28***	0.34***					
4	***Legal_Reg***	0.11***	0.37***	0.82***				
5	***Sys***	0.03*	0.65***	0.36***	0.44***			
6	***Tax***	0.15***	0.59***	0.65***	0.64***	0.63***		
7	***All_Risks***	0.19***	0.64***	0.87***	0.87***	0.73***	0.83***	
8	***All_Words***	0.23***	0.53***	0.93***	0.86***	0.51***	0.77***	0.93***

Panel A presents pairwise correlations between our cybersecurity awareness measure (*SCORE*) and other 10-K risk disclosures based on Campbell et al. (2014). The sample period is 2012 to 2016. *Financial* is the key word count in the risk factor section referring to financial risk exposure; *Idiosyn* is the key word count in the risk factor section referring to "other-idiosyncratic" risk exposure; *Legal_Reg* is the key word count in the risk factor section referring to legal and regulatory risk exposure; *Sys* is the key word count in the risk factor section referring to "other-systematic" risk exposure; *Tax* is the key word count in the risk factor section referring to tax risk exposure; *All_Risks* is the key word count in the risk factor section referring to financial, idiosyncratic, systematic, tax and legal and regulatory risk exposure; and *All_Words* is the natural logarithm of the total number of words in the firm's risk factor disclosure section. *,**,*** denote differences that are significant at the 0.10, 0.05 and 0.01 level, respectively.

Panel B: Regression Model Results for Market Value and Types of Risks

	(1) *Financial*	(2) *Idiosyn*	(3) *Legal_Reg*	(4) *Sys*	(5) *Tax*	(6) *All_Risks*	(7) *All_Words*
SCORE	0.062***	0.052***	0.054***	0.054***	0.052***	0.055***	0.056***
	(0.000)	(0.000)	(0.000)	(0.000)	(0.000)	(0.000)	(0.000)
Financial	-0.041***						
	(0.000)						
Idiosyn		0.003					
		(0.309)					
Legal_Reg			0.003				
			(0.426)				
Sys				0.005			
				(0.119)			
Tax					0.012*		
					(0.072)		
All_Risks						0.000	
						(0.732)	
All_Words							-0.000
							(0.963)
BVE	0.969***	0.973***	0.972***	0.972***	0.971***	0.972***	0.972***
	(0.000)	(0.000)	(0.000)	(0.000)	(0.000)	(0.000)	(0.000)
EARN	9.527***	9.645***	9.635***	9.648***	9.642***	9.632***	9.626***
	(0.000)	(0.000)	(0.000)	(0.000)	(0.000)	(0.000)	(0.000)
EARN_Neg	-12.741***	-12.655***	-12.656***	-12.663***	-12.637***	-12.671***	-12.681***
	(0.000)	(0.000)	(0.000)	(0.000)	(0.000)	(0.000)	(0.000)
Year FE	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Industry FE	Yes	Yes	Yes	Yes	Yes	Yes	Yes
N	7,430	7,430	7,430	7,430	7,430	7,430	7,430
Adj R^2	0.635	0.633	0.633	0.633	0.633	0.633	0.633

Panel B presents results of regression models that examine the robustness of our results to the inclusion of different types of risks based on Campbell et al. (2014). The sample period is 2012 to 2016. The dependent variable is market value, scaled by shares (*MVE*). Column 1 reports the results with inclusion of financial risks, *Financial* is the key word count in the risk factor section referring to financial risk exposure. Column 2 reports the results with inclusion of idiosyncratic risks, where *Idiosyn* is the key word count in the risk factor section referring to "other-idiosyncratic" risk exposure. Column 3 reports the results with inclusion of legal and regulatory risks, where *Legal_Reg* is the key word count in the risk factor section referring to legal and regulatory risk exposure. Column 4 reports the results with inclusion of systematic risks, where *Sys* is the key word count in the risk factor section referring to "other-systematic" risk exposure. Column 5 reports the results with inclusion of tax risks, *Tax* is the key word count in the risk factor section referring to tax risk exposure. Column 6 reports the results with inclusion of all the earlier mentioned risks, *All_Risks* is the key word count in the risk factor section referring to financial, idiosyncratic, systematic, tax and legal and regulatory risk exposure. Column 6 reports the results with inclusion of the length of discussion of all risks, where *All_Words* is the natural logarithm of the total number of words in the firm's risk factor disclosure section. Two-tailed *p*-Values are given in parentheses and are based on firm cluster-adjusted standard errors. *,**,*** denote differences that are significant at the 0.10, 0.05 and 0.01 level, respectively.

Table 7
Regression Model Results for Market Value (Tobin's Q) and Cybersecurity Awareness

	(1) Base model	(2) Inclusion of tone of cyber disclosures	(3) Inclusion of general tone disclosures	(4) Normalized cyber score
SCORE	0.001***	0.001***	0.001***	
	(0.003)	(0.005)	(0.000)	
NSCORE				0.033***
				(0.000)
ROA	1.030***	1.086***	0.979***	0.971***
	(0.000)	(0.000)	(0.000)	(0.000)
LEV	-0.071***	-0.073***	-0.052**	-0.051**
	(0.001)	(0.001)	(0.023)	(0.025)
SIZE	-0.037***	-0.034***	-0.027***	-0.029***
	(0.000)	(0.000)	(0.000)	(0.000)
CapInt	-0.251***	-0.239***	-0.259***	-0.258***
	(0.000)	(0.000)	(0.000)	(0.000)
CapExp	1.527***	1.671***	1.732***	1.729***
	(0.000)	(0.000)	(0.000)	(0.000)
RnD	2.486***	2.559***	2.438***	2.440***
	(0.000)	(0.000)	(0.000)	(0.000)
Advert	1.733***	1.505***	1.657***	1.622***
	(0.000)	(0.000)	(0.000)	(0.000)
Div_Dum	0.064***	0.051***	0.032***	0.032***
	(0.000)	(0.000)	(0.003)	(0.003)
Neg_Tone		-0.003	-0.002	-0.001
		(0.272)	(0.514)	(0.590)
Pos_Tone		-0.002	-0.001	-0.001
		(0.803)	(0.873)	(0.926)
10K_Neg			-0.095***	-0.100***
			(0.000)	(0.000)
10K_Pos			0.184***	0.182***
			(0.000)	(0.000)
10K_WC			-0.093***	-0.099***
			(0.000)	(0.000)
Year FE	Yes	Yes	Yes	Yes
Industry FE	Yes	Yes	Yes	Yes
N	9,567	8,487	8,270	8,270
Adj R^2	0.391	0.390	0.401	0.402

The table presents results of regression models that examine the effect of cybersecurity awareness on Tobin'Q (*Q*). The sample period is 2012 to 2016. Column 1 reports the results for the base model. *SCORE* is the cybersecurity awareness score. *BVE* is book value per share of common equity; *EARN* is earnings per share to common equity; *EARN_Neg* is earnings per share to common equity if earnings ≤0, 0 otherwise. Column 2 reports the results for the market valuation model including tone of cyber disclosures (*Neg_Tone* and *Pos_Tone*. Column 3 reports the results for the market valuation model including general tone of disclosures in the 10-Ks (*10K_Neg* and *10K_Pos*) and the length of 10-K disclosures *(10K_WC)* in the 10-

Ks. Column 4 reports the results using normalized cyber score (*NSCORE*). Two-tailed *p*-Values are given in parentheses and are based on firm cluster-adjusted standard errors. *,**,*** denote differences that are significant at the 0.10, 0.05 and 0.01 level, respectively.