International Journal of Accounting Information Systems xxx (xxxx) xxx–xxx

Contents lists available at ScienceDirect

International Journal of Accounting Information Systems

journal homepage: www.elsevier.com/locate/accinf

SEC's cybersecurity disclosure guidance and disclosed cybersecurity risk factors

He Li[a], Won Gyun No[b,*], Tawei Wang[c]

[a] Southwestern University of Finance and Economics, 555, Liutai Avenue, Wenjiang District, Chengdu, Sichuan 611130, PR China
[b] Rutgers Business School, Rutgers, the State University of New Jersey, 1 Washington Park, Newark, NJ 07102, United States
[c] Driehaus College of Business, DePaul University, 1 E. Jackson Blvd. Chicago, IL 60604, United States

ARTICLE INFO

Keywords:
Cybersecurity
Cybersecurity risk disclosure
Risk factors
Disclosure guidance
Cybersecurity breach incident

ABSTRACT

Cybersecurity risk disclosure has received great attention in the past several years, especially after the passage of the Securities and Exchange Commission's (SEC's) cybersecurity disclosure guidance published on October 13, 2011. In this study, we examine the usefulness of cybersecurity-related risk factors disclosed in 10-K filings. We document that the presence of these risk factors in the pre-guidance period and length of these risk factors are related to future reported cybersecurity incidents. The association between the presence of cybersecurity risk disclosure and subsequently reported cybersecurity incidents becomes insignificant after the passage of the SEC's cybersecurity disclosure guidance. Our findings, in general, support the SEC's decision on emphasizing cybersecurity risk disclosure. However, SEC's disclosure guidance may unintentionally encourage firms to disclose cybersecurity risks regardless of the level of risks.

1. Introduction

Cybersecurity has attracted a lot of attention in the past ten years.[1] Both the general public and the business world are concerned about the growing cybercrimes that expose sensitive personal information, cause business disruptions, or steal trade secrets, especially after a series of high-profile data breaches such as the ones at Equifax, Sony, and Target.[2] According to a recent Annual Cybersecurity Report, > 20% of the breached firms experienced substantial loss of revenues, customer base, and business opportunities, and most of the breached firms spent millions of dollars improving security solutions and expanding security procedures following the attacks (CISCO, 2017). Due to the potential impact on firm value and operations, cybersecurity is becoming one of the top priorities for the board and executives. For instance, about 88% of U.S. Chief Executive Officers (CEOs) are concerned that cyber threats could hinder the growth of their firms (Loop, 2016). Likewise, investors are clamoring for more information about cybersecurity risks and data breaches, and how firms are addressing those risks (Shumsky, 2016).

To respond to the increasing cyber threats, the Securities and Exchange Commission (SEC) held a roundtable discussion to deliberate on cybersecurity landscape and cybersecurity disclosure issues (SEC, 2014). The Standing Advisory Group of the Public Company Accounting Oversight Board (PCAOB) also discussed the potential implications of cybersecurity on financial reporting and auditing (PCAOB, 2014). Particularly, the SEC's Division of Corporation Finance issued disclosure guidance regarding cybersecurity in 2011 to assist firms in

* Corresponding author at: 1 Washington Park, Room 993, Newark, NJ 07102-3122, United States.
E-mail addresses: lihe_stanley@swufe.edu.cn (H. Li), wgno@business.rutgers.edu (W.G. No), david.wang@depaul.edu (T. Wang).

[1] According to the U.S. Computer Emergency Readiness Team, cybersecurity is "[t]he activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation."

[2] For more detail, please see https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html.

https://doi.org/10.1016/j.accinf.2018.06.003

1467-0895/ Published by Elsevier Inc.

assessing what, if any, disclosures they should provide related to cybersecurity risks (SEC, 2011). Although the guidance is not technically a ruling, the SEC has issued comment letters to several firms pointing out the inadequacies of their cybersecurity risk disclosures by referring to the guidance. Therefore, some have argued that the guidance is becoming a de facto ruling (Grant and Grant, 2014).

In this paper, we investigate the usefulness of cybersecurity risk disclosures in the risk factor section of 10-K filings (hereafter cybersecurity risk disclosure). We define the usefulness of cybersecurity risk disclosures as "*the ability to help stakeholders assess the possibility of the occurrence of future adverse events* (*i.e., cybersecurity breach incidents*)." Understanding the information conveyed by cybersecurity risk disclosures is important as it can help investors assess a firm's cybersecurity risk and provide regulators with information about whether additional legislative rules are necessary to encourage firms to disclose more on their cybersecurity risks. Two aspects of cybersecurity risk disclosure are considered in this study: presence and length. Specifically, we examine whether the presence of cybersecurity risk disclosure in a firm's 10-K filing implies higher cybersecurity risks as measured by subsequent cybersecurity incidents and whether the length of the disclosure is associated with increased likelihood of subsequent cybersecurity incidents. Consistent with Wang et al. (2013a), our results suggest that both the presence and the length of cybersecurity risk disclosure are associated with subsequent cybersecurity incidents. However, the association between the presence of disclosure and cybersecurity incidents becomes insignificant following the SEC's disclosure guidance. The release of the disclosure guidance leads to a substantial increase in the number of firms disclosing cybersecurity risks, suggesting that firms make cybersecurity disclosures regardless of their degree of cybersecurity risk in the post-guidance period.

The findings of this study make several contributions to the existing literature. First, the study contributes to the cybersecurity disclosure literature. Early research in the accounting and information systems domain primarily focuses on the market reaction following cybersecurity incidents and have examined a set of contingency factors such as type of breaches (Gordon et al., 2011; Yayla and Hu, 2011), firm characteristics (Ettredge and Richardson, 2003), and information disclosed through news articles (Wang et al., 2013b) and distribution channels (Benaroch et al., 2012) that could deepen or mitigate the market reaction, while only a few studies consider cybersecurity disclosure. Gordon et al. (2010) find that on average, voluntary disclosure relating to information security increases stock prices by > 6% and that voluntary disclosure concerning proactive security measures has the greatest impact on the firm's stock price, followed by the disclosure of vulnerabilities. This study complements Gordon et al. (2010) by exclusively focusing on the value of cybersecurity disclosures in terms of predicting future cybersecurity incidents. Wang et al. (2013a) examined the ex-post odds of cybersecurity incidents, revealing that firms that disclose information security risk factors in their 10-K filings with actionable information are less likely to be associated with future cybersecurity incidents. The paper complements Wang et al. (2013a) in at least two key ways. First, with the dramatic change in cybersecurity attacking behaviors in the past decade and the high profile breach incidents in recent years, it is worthwhile revisiting the usefulness of cybersecurity risk factor disclosures. More importantly, the sample in this study covers both the pre-guidance period and the post-guidance period, which enables us to examine the changes in disclosure usefulness. Second, our data collection approach enables analyses on a much larger scale to demonstrate that firms facing greater cybersecurity risks devote a greater portion of their disclosures towards describing cybersecurity risks.

Second, this research also contributes to the risk factor disclosure literature. While findings in the study are largely in line with recent accounting literature showing that risk factor disclosure is not boilerplate, we use the actual adverse event (i.e., cybersecurity incident) rather than market-based measures of firm risks (Campbell et al., 2014) or investors' risk perceptions (Kravet and Muslu, 2013) to capture risks that a firm faces. As the objective of providing risk factor disclosures is to discuss "the most significant factors that make the firm risky" (SEC, 2005), our risk measure that focuses on actual risk event is more consistent with the SEC's intention than measures based on the assumption of market efficiency. Our study, therefore, provides more direct evidence that risk disclosures are potentially informative of future operational failures. Furthermore, different from prior studies examining the variation of qualitative disclosures that are already included in risk factor disclosure section, our unique setting allows us to show that the presence or absence of risk disclosures could be informative of the risk.

Third, this paper makes contributions to the textual analysis literature. When examining disclosures related to cybersecurity, prior studies use manual collection (Wang et al., 2013a), take the number of several words around the keywords (Gordon et al., 2010), or simply count the number of predetermined keywords (Hilary et al., 2017). We develop methods that first locate individual risk factors from Item 1A and then identify security-related risk factors. These methods help us to examine the length of cybersecurity risk disclosure more accurately and are also consistent with recent research effort that calls for analysis at the individual risk factor level (Bao and Datta, 2014; Gaulin, 2017). In addition, the topic analysis using word-term patterns helps to obtain a thorough understanding with respect to the consequences of cybersecurity incidents that firms are most concerned about, which is not examined in prior studies.

Fourth, the results can also help the board of directors, executives, and policymakers to determine the benefits and consequences of cybersecurity risk disclosures and disclosure guidance.[3] Our findings support the decision to emphasize cybersecurity risk disclosures, as both the presence in the pre-guidance period and the length of cybersecurity risk disclosures are informative of subsequent cybersecurity incidents. However, the results also reveal that the SEC's disclosure guidance leads to an unintentional consequence that more firms make cybersecurity risk disclosures even though they do not face higher cybersecurity risks. As the SEC warned firms to "avoid generic risk factor disclosure that could apply to any company," the outcome is counter to the SEC' intention.[4] Such outcome arises from the ambiguity in the guidance and comment letters sent by the SEC to force firms to disclose cybersecurity

[3] Studies such as Kwon et al. (2013), Hsu and Wang (2014a), Hsu and Wang (2014b), Hsu and Wang (2015), and Feng and Wang (2017) have investigated various board/executive issues that may be related to information security risk management. Our study does not attempt to provide implications on the composition or characteristics of the board and executives but to highlight the importance of cybersecurity risk disclosures for the board and executives.

[4] This is consistent with the idea that disclosure is an inexpensive insurance policy. That is, firms will disclose their cybersecurity risks since if something happens, they can point to the disclosure and mitigate lawsuits, at least to some extent. We thank an anonymous reviewer for bringing this point out.