Communications of the Association for Information Systems

Volume 50 Article 26

6-8-2022

Talk too much? The Impact of Cybersecurity Disclosures on Investment Decisions

Xu Cheng
Auburn University, joycecheng@auburn.edu

Carol Hsu
University of Sydney Business School, Carol.hsu@sydney.edu.au

Tawei (David) Wang
DePaul University, david.wang@depaul.edu

Recommended Citation
Cheng, X., Hsu, C., & Wang, T. (2022). Talk too much? The Impact of Cybersecurity Disclosures on Investment Decisions. Communications of the Association for Information Systems, 50, pp-pp.
https://doi.org/10.17705/1CAIS.05022

Communications of the Association for Information Systems

Research Article DOI: 10.17705/1CAIS.05022 ISSN: 1529-3181

Talk too much? The Impact of Cybersecurity Disclosures on Investment Decisions

Xu Cheng
School of Accountancy, Auburn University, USA,
joycecheng@auburn.edu

Carol Hsu
University of Sydney Business School, Australia,
carol.hsu@sydney.edu.au

Tawei Wang
School of Accountancy and MIS, DePaul University, USA,
david.wang@depaul.edu

Abstract:

High-profile cybersecurity breaches have raised concerns regarding how organizations disclose security management information to the public. The American Institute of Certified Public Accountants (AICPA) developed a cybersecurity risk management (CSRM) reporting framework to better help organizations convey their cybersecurity programs to the public. In this article, we attempt to provide evidence of how cybersecurity disclosures, as developed by AICPA, affect investment decisions. Our findings suggest that nonprofessional investors are less likely to invest in breached firms with the disclosure of CSRM reports alone. Disclosing the risk management report with an independent assurance report does not result in the mitigation of the negative impact of security breach news. We discuss the corresponding implications.

Keywords: Cybersecurity Disclosures, Cybersecurity Risk Management Program, Investment Judgments, Nonprofessional Investors.

This manuscript underwent peer review. It was received 10/28/2020 and was with the authors for 11 months for one revision. Alvin Leung served as Associate Editor.

1 Introduction

High-profile cybersecurity incidents, such as those involving Equifax, Target, and Sony's PlayStation, have attracted the attention of regulators and professional organizations regarding what companies should convey to the public about cybersecurity. For instance, the Chairman of the Securities and Exchange Commission (SEC) states that "[i]ssuers should consider whether their publicly filed reports adequately disclose information about their risk management governance and cybersecurity risks, in light of developments in their operations and the nature of current and evolving cyber threats" (Securities and Exchange Commission, 2017, p. 1).

Efforts have therefore been made to improve publicly traded firms' disclosure of risk management practices or the incidence of cybersecurity breaches. For instance, several states in the US have enacted security breach notification laws requiring the mandatory disclosure of any security breach incidents (Goel & Shawky, 2014). More recently, the American Institute of Certified Public Accountants (AICPA) developed a cybersecurity risk management (CSRM) reporting framework that helps organizations communicate relevant and useful cybersecurity information (American Institute of Certified Public Accountants, 2017a). The AICPA framework includes management's description of how organizations manage sensitive information and management's assertion about whether controls are effective in meeting cybersecurity objectives (American Institute of Certified Public Accountants, 2018). The framework further suggests that organizations disclose their CSRM programs potentially with an attestation issued by an independent accountant. However, several comment letters (e.g., Deloitte, 2016; PricewaterhouseCoopers, 2016) about the AICPA's framework have raised concerns about whether the detailed CSRM program is helpful for interested stakeholders in light of its ambiguity.

Thus, consistent with broad information security research interests on firms' voluntary disclosures concerning information security (Gordon et al., 2010; Goel & Shawky, 2014), in this article, we examine how cybersecurity disclosures affect investment judgments and we provide policy implications for AICPA's framework. Specifically, we explore whether cybersecurity disclosures, to which investors have previously been exposed, aggravate or mitigate the negative impact of security[1] breaches. We focus on nonprofessional investors' judgments because they constitute a large portion of the stock market. More than 41 million nonprofessional investors invest in the stock market and own about 34 percent of shares outstanding (Cheng & Walton, 2019; Tadesse & Murthy, 2018). Additionally, a survey from the Center for Audit Quality (2016) indicates that nonprofessional investors value cybersecurity management and take cybersecurity concerns into consideration when making investment judgments.

To address our research question, we developed our main hypothesis based on the notion of blame from social psychology and the literature on blame in corporate failure (Gibson & Schroeder, 2003; Pal et al., 2011; Shaver, 1985; Shaver, 2012; Tsang, 2002). The notion of blame explains how people assign blame to negative outcomes. It suggests that people often search for the causes of negative outcomes and attempt to consider how the negative outcomes could have been avoided (Shaver, 2012). The literature blaming corporate failure on corporations also suggests that people tend to link businesses or organizations with corporate failure (Gibson & Schroeder, 2003; Pal et al., 2011). In the cybersecurity disclosure context, investors may attribute more blame to a company that claimed the effectiveness of its CSRM or controls initially (via the CSRM report) but later experienced security breaches. In this case, investors may further reason how a company's security breach could have been avoided and question whether the evaluations of controls were performed effectively or adequately, thus reducing their willingness to invest in the company.

To test the hypotheses of this study, we used a 3 × 2 mixed experimental design manipulating cybersecurity disclosure and security breach news. Cybersecurity disclosure, the between-participant variable, is manipulated at three levels: no disclosure, CSRM report, or CSRM report with the independent accountant (IA) report[2]. Security breach news, the within-participant variable, is manipulated by the

[1] Security or information technology (IT) security refers to the process of implementing measures to protect information using various forms of technology (Paulsen & Byers, 2019). Cybersecurity refers to the precautions taken to guard against crime that involves the Internet, especially unauthorized access to computer systems and data connected to the Internet. Cybersecurity is often considered a part of IT security. In this study, we used these two terms interchangeably, with a focus particularly on cybersecurity.

[2] The CSRM report and Independent Accountant (IA) report were developed based on AICPA's cybersecurity risk management reporting framework (American Institute of Certified Public Accountants, 2017b).

presence or absence of security breach news regarding a hypothetical company. All participants in our study provided their investment judgments before and after viewing the security breach news.

The findings of this study indicate that nonprofessional investors are less likely to invest in a company after learning that the company has been affected by a security breach. The results further suggest that compared with a no (prior) disclosure condition, nonprofessional investors are less likely to invest in a company that has previously disclosed a CSRM report after learning that the company has been affected by a security breach. Furthermore, the results show that disclosing an additional IA report with a CSRM report does not result in the mitigation of the negative impact of security breach news. Additional analysis shows that investors are more likely to blame companies claiming the effectiveness of CSRM first but experience a security breach later.

This study has contributed to the cybersecurity literature by experimentally investigating the influence of cybersecurity disclosures on investment judgments. Our findings have practical and policy implications regarding cybersecurity disclosures. Although disclosing a CSRM report provides additional information on a company's CSRM program, it can reduce investors' interest after the company experiences security breaches. Additionally, we note that investors are more likely to question the quality of CSRM and assign more blame to companies that claimed the effectiveness of CSRM but later experienced a security breach, compared to companies that do not initially provide any cybersecurity information. The findings of this study suggest that making assertions about the effectiveness of the CSRM program of a company that later experiences security breaches could lead to more severe consequences. Companies facing a higher security breach risk may take the findings of this study into account when exploring their different cybersecurity disclosures.

The remainder of this paper is organized as follows. We provide the research background and develop the hypotheses in Section 2. We present the research methodology and findings in Sections 3 and 4. Finally, we discuss the practical implications and contributions in Section 5.

2 Background and Hypothesis Development

2.1 Research Background

More and more organizations are facing data breaches in recent years. Because of their potential impact, the assurance and communication of an organization's CSRM efforts have therefore become more critical. Executive Vice President of AICPA, Susan Coffey, stated that "[w]hile there are many methods, controls and frameworks for developing cybersecurity risk management programs, until now there hasn't been a common language for companies to communicate about, and report on, these efforts" (Tysiac, 2017, p.1). AICPA developed a voluntary CSRM reporting framework (American Institute of Certified Public Accountants, 2017b) that aims to assist organizations in better communicating the effectiveness of their CSRM program. The framework has also been discussed by the Center for Audit Quality as part of a tool that can be used by board members to understand cybersecurity risk oversight. In addition to the information disclosed regarding CSRM, the framework introduces system and organization controls for cybersecurity attestation services for CPAs to report the control effectiveness of an organization's CSRM. The resulting report includes the following three major components:

(1) Management's description: Management's description provides information "about how the entity identifies its most sensitive information, the ways in which the entity manages the cybersecurity risks that threaten it, and the key security policies and processes implemented and operated to protect the entity's information assets against those risks" (American Institute of Certified Public Accountants, 2018, p.1).

(2) Management's assertion: The assertion is about whether the description meets the description criteria[3] and whether the controls are effective[4] to meet the organization's cybersecurity objectives (American Institute of Certified Public Accountants, 2018).

[3] AICPA's Assurance Services Executive Committee publishes description criteria. These criteria can be used to evaluate the description of the organization's cybersecurity risk management.

[4] The 2017 Trust Service Criteria can be used to evaluate the effectiveness of the corresponding controls. The trust services criteria are as follows: the entity internally communicates information, including objectives and responsibilities for internal control; the entity communicates with external parties regarding matters affecting the functioning of internal control; the entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate; and the entity identifies, develops, and implements activities to recover from identified security incidents.

(3) The practitioner's opinion, often referred to as an IA report: This is the CPA's opinion on the description and effectiveness of the controls (American Institute of Certified Public Accountants, 2018).

The framework allows management to disclose a CSRM report that includes not only a narrative description of the company's CSRM program but also an assertion about the effectiveness of controls within the program to achieve the company's cybersecurity objectives. Additionally, the practitioner's opinion or an IA report, which provides a CPA's opinion on the description of the CSRM program and the effectiveness of the controls within that program, can be added to the CSRM report.

2.2 Related Studies

Prior research has examined a wide variety of issues in the context of cybersecurity (e.g., Backhouse et al., 2006; Feng & Wang, 2019; Hsu & Wang, 2014; Kwon et al., 2013; Li et al., 2018). One stream of research has largely devoted efforts to understanding the factors influencing employees' computer abuse intention (e.g., D'Arcy et al., 2009; Lowry et al., 2015; Willison et al., 2018), information security policy compliance and violation (e.g., Bulgurcu et al., 2010; Cram et al., 2019; Siponen & Vance, 2010), and whistle-blowing intention to report security policy violations and breaches (Li, 2020; Wei et al., 2016). The other stream of information security research focuses on investors' reactions to various organizational security issues. For instance, several studies have looked at organizational stock market performance after reported information technology (IT) incidences and breaches (Campbell et al., 2003; Cavusoglu et al., 2004; Goel & Shawky, 2009). Most found a negative market reaction when an organization is reported to have cybersecurity breach incidents. The study of Chai and Rao (2011) investigates the relationship between market value and security investment announcements. Their results show favorable reactions from investors to a firm's security investment decisions. Interestingly, focusing on security management certification, the paper of Hsu, Wand, and Lu (2016) finds no evidence that an ISO 27001 certification leads to a positive impact in terms of financial and stock market performance. Kamiya, Kang, Kim, Milidonis, and Stulz (2021) propose a model to examine the economic implications of successful security breaches and find that breaches with personal financial information loss show adverse information about the security risk toward breached companies, their stakeholders, and their competitors.

More recently, studies have emerged to analyze the financial impact of either mandatory or voluntary disclosure on organizations' security risk management or security breaches. The study of Gordon, Loeb, Lucyshyn, and Sohail (2006) shows that the Sarbanes-Oxley Act has a positive impact on companies' disclosures regarding security activities. In another study, they further examined the relationship between firms' voluntary disclosure concerning information security practices and their market value. Based on their event study of annual reports filed with the SEC, the results show that voluntary disclosures on information security are positively and significantly related to the market value of firms. The paper of Goel and Shawky (2014) examines the impact of security breach announcements on the stock prices of publicly traded firms during the period before and after the enactment of security breach notification laws in the US. Their empirical results reveal that the negative effects of security breach announcements on market value are reduced significantly after the enactment of the laws. Our paper is different from prior studies in that we test how investors react when a company initially claims the effectiveness of its CSRM or controls but later experiences security breaches. This experimental approach is important because our findings can help organizations evaluate the outcomes of disclosing detailed cybersecurity risk programs and consider whether adding an IA report to a CSRM report is beneficial.

2.3 Hypotheses Development

Studies, such as that of Wang, Rees, and Karthik (2013), argue that news articles about security breaches are the information set that may change investors' assessments about how a security breach may affect the breached company's business value. This is because news articles may change market participants' expectations about the breached firm's future cash flows, reputation loss, and compliance/litigation costs, which, in turn, affect the breached firm's business value. For example, Equifax had a security breach in 2017. About a year later, the firm identified another $2.4 million loss that resulted from the breach (Andriotis, 2018). It also has class action lawsuits in all 50 states (Swaminatha, 2017), with an outlook downgrade by Moody's in 2019 (O'Flaherty, 2019). Additionally, prior archival and experimental studies that examined investment judgments documented that investments are less favorable when there is negative news and a high degree of uncertainty and risks, including risks associated with internal controls (Cheng & Walton, 2019; Easley & O'Hara, 2010; Tadesse & Murthy, 2018). Therefore, building upon the

prior literature, our first hypothesis states that investor judgment is less favorable after a security breach is publicized.

Hypothesis 1: Investors are less likely to invest in a company after learning that the company has been affected by a security breach.

When there is no news indicating a company is affected by a security breach, the financial performance of the company is the more influential factor that impacts investment judgments and decisions. However, when there is news on security breaches, investors can react differently depending on which cybersecurity disclosure they were previously exposed to. Hence, we further examine the impact of cybersecurity disclosures on investment judgments. In particular, we investigate whether a cybersecurity disclosure that investors are previously exposed to will aggravate or mitigate the negative impact of security breaches.

Prior studies provide very limited guidance on this issue, except for the discussion on action-oriented versus general security risk factors disclosed in 10-K filings in the paper of Wang, Kannan, and Ulmer (2013a). Action-oriented risk factors disclosed in 10-K filings can mitigate the negative effect of security breaches on business value (Wang et al., 2013a). The study of Wang et al. (2013a) focuses on the textual content of risk factors, whereas the present article, using an experimental approach, investigates how disclosing or not disclosing a CSRM report can affect investment decisions.

We use the notion of blame from social psychology and the literature on blame in corporate failure to develop our hypotheses (Pal et al., 2011; Shaver, 1985; Shaver, 2012). According to the notion of blame, people often assign blame by first searching for the causes of negative outcomes and reason how these negative outcomes could have been avoided (Kahneman & Miller, 1986; Shaver, 1985; Shaver, 2012). Recall that the CSRM report includes not only a narrative description of the company's CSRM program but also an assertion about the effectiveness of controls within the program to achieve the company's cybersecurity objectives. When a company discloses a CSRM report first and later experiences a security breach, there could be two possible outcomes. The public may interpret that the company has made efforts to manage cybersecurity risks and prevent security breaches from happening, hence mitigating the negative impact of security breaches. Alternatively, the public may think that the company does not effectively manage its cybersecurity risks, and additional actions should have been taken to avoid the occurrence of security breaches, thus aggravating the negative influence of these breaches.

We argue that the second outcome is more relevant to the setting of disclosing the CSRM report. Pal, Medway and Byrom's (2011) paper suggests that human nature links culpability to businesses or companies for corporate failure. In the context of cybersecurity disclosures, nonprofessional investors attribute more blame to management or companies that initially claim the effectiveness of the CSRM of the breached company (in the CSRM report) but later experience security breaches. This is because when a CSRM report is provided, investors are more likely to expect the company to effectively manage cybersecurity risks and less likely to link the company with the occurrence of a security breach. After learning that the company has been affected by a security breach, investors who were previously exposed to the CSRM report are more likely to reason how a security breach could have been avoided and question the quality of the CSRM conducted and whether management has performed evaluations of controls effectively or adequately. Comparably, when the breached company did not provide information or assertions related to the effectiveness of managing cybersecurity risks, investors have no prior information (anchor) as a reference to make an investment judgment.[5] Hence, investors are less likely to question the quality of the CSRM conducted or blame the breached company for poor CSRM program. Therefore, we expect that the investment judgment is less favorable when a company discloses the CSRM report initially but experiences a security breach later, compared with when the breached company made no prior cybersecurity disclosure. We formally propose our second hypothesis as follows:

Hypothesis 2: Investors are less likely to invest in a company after learning that the company has been affected by a security breach given the company's disclosed CSRM report, compared with when the breached company made no prior cybersecurity disclosures.

The practitioner's opinion, known as an IA report, can be added to the CSRM report. We are also interested in understanding how a CSRM report with an IA report can influence investment judgments. An

[5] Psychologists have found that individuals have the tendency to rely heavily on the first piece of information they learn, which can have a greater impact on the final decision making. This cognitive bias is known as the anchoring bias or anchoring effect (Kahneman 1992).

IA report is a third party's opinion on the description of a CSRM program and the effectiveness of controls within that program. When there is a reliable and independent report by a third party on the effectiveness of the CSRM of the breached company, concerns related to whether the company makes cybersecurity assertions based on effective or adequate evaluations of controls may be reduced. Nonprofessional investors can also interpret that management has made enough effort to manage cybersecurity risks by showing that a third party has also agreed on the effectiveness of the CSRM program of the breached company, thus reducing the blame attributed to the breached company. However, how much concern or blame would be reduced and whether the disclosure of a CSRM report with an IA report can lead to the mitigation of the negative impact of security breaches are not clear. Therefore, rather than providing a formal directional hypothesis, we explore the research question: *after learning that a company has been affected by a security breach, are investors more likely to invest in the company that disclosed a CSRM report with an IA report or the company made no cybersecurity disclosure or that only disclosed a CSRM report?*

3 Methodology

3.1 Participants

We recruited participants from Amazon Mechanical Turk (M-Turk).[6] M-Turk is an online platform that allows users to create human intelligence tasks and hire participants to complete tasks. Researchers have documented that the subject group of M-Turk is large and more representative than more traditional student pools; thus, M-Turk workers are appropriate proxies for nonprofessional investors (Brandon et al., 2013; Owens & Hawkins, 2019; Rennekamp, 2012). Several studies have recruited non-professional investors using M-Turk (Cheng & Walton, 2019; Farkas & Murthy, 2014; Grenier et al., 2015; Kelton & Murthy, 2015; Rennekamp, 2012).

As a baseline requirement, we recruited M-Turk workers who reside in the US and have completed at least 100 tasks with at least 99% acceptance rate. To further reduce concerns regarding the appropriateness of the M-Turk participant pool, we also required participants to answer four qualification questions prior to accessing the experiment.[7] Participants were automatically excluded from the study if they were under 18 or had no investment experience.

3.2 Experimental Design and Dependent Variable

This study used a 3 x 2 mixed experimental design manipulating cybersecurity disclosure and security breach news. Cybersecurity disclosure, the between-participant variable, was manipulated at three levels: no disclosure, CSRM report, or CSRM report with an IA report. In the CSRM report condition, the participants read the CSRM report. The report shows management's descriptions of the company's CSRM program and assertions about the effectiveness of the controls within the program to achieve the company's cybersecurity objectives. In the CSRM report with an IA report condition, the participants read the same CSRM report and were then given an IA report. This IA report provides a CPA's opinions on the description of the CSRM program and the effectiveness of controls within that program. The CSRM and IA reports used in the experiment are based on sample reports issued by AICPA (2017a). The detailed discussions related to the company's CSRM are the same for all reports.

Security breach news, the within-participant variable, was manipulated at two levels: presence or absence of security breach news. All participants were asked to provide their initial investment judgment (pre-investment judgment) after viewing the background and financial performance information and cybersecurity disclosure of XYZ Stores, a hypothetical company used in the experiment.[8] Next, the participants read the security breach news and learned that the breach at XYZ Stores had affected the stores' payment system, potentially exposing millions of credit and debit cards. Then, the participants indicated their post-investment judgments after learning about the security breach news that impacted XYZ Stores.

[6] We obtained Institutional Review Board approval prior to recruiting the participants or collecting data.
[7] M-Turk workers were asked to indicate their ages, whether they had made personal investments in the common stock of a company, the number of years of personal investment experience they have, and the number of times they have purchased common stock as a personal investment.
[8] The participants make their initial investment judgments without knowing the security breach news that affects XYZ Stores.

The main dependent variable of this study is investment judgment after learning the security breach news (post-investment judgment). Two questions were used to measure investment judgment: the attractiveness of XYZ Stores as a potential investment and the likelihood that the participants would consider the company as a potential investment.[9] Responses were collected on an 11-point Likert scale ranging from 0–Not At All Attractive (Likely) to 10–Extremely Attractive (Likely). As the two investment judgment measures are highly correlated (Pearson correlation = 0.90, $p < 0.001$, and Cronbach's alpha = 0.92), we averaged the two measures into a single variable for data analysis purposes.[10]

3.3 Procedure

The participants first read a brief description of the experimental task after accessing the experimental website through M-Turk. They were then asked to assume the role of investors and make investment judgments for XYZ Stores. The experiment was conducted in two stages. In stage 1, all participants were provided XYZ Stores' background and financial performance information and were exposed to one of the cybersecurity disclosures: 1) no disclosure, 2) CSRM report, and 3) CSRM report and an IA report. The participants made their initial investment judgments (hereafter, pre-investment judgment) based on the financial information and the cybersecurity disclosure provided.

In stage 2, all participants read the same security breach news and provided their investment judgment (hereafter, post-investment judgment). Then, they answered manipulation check questions and a series of post-experimental questions, including their views about XYZ Stores' financial performance, cybersecurity disclosure, and security breach news. We also asked the participants to rate the quality of XYZ Stores' CSRM and the likelihood they are to blame XYZ Stores for the breach. Lastly, the participants provided their demographic information, including their investment experience, academic training, gender, and age.

4 Results

4.1 Manipulation Check Questions

Manipulation checks were used to ensure that the participants understood the manipulations of this study as intended. They were first asked to indicate whether XYZ Stores disclosed any information about cybersecurity risk. For those participants who chose "Yes," we provided them with screenshots of the different cybersecurity disclosures. The participants selected the disclosure they viewed earlier.

We also added one attention check question in the experiment to identify whether the participants paid enough attention to the text of the measures in the online survey. We recruited a total of 114 participants from M-Turk and removed two for incorrectly answering the attention and manipulation check questions.[11] Therefore, the final data set included 112 participants.

4.2 Participant Demographics

Of the 112 participants, 61 (54%) were male and 51 (46%) were female. These participants were from 39 different states. Most participants had at least three years of investment experience and had completed at least two accounting and finance courses. Participants indicated that they have some experience with analyzing company performance via financial statements. Based on the demographic information, we believe that our sample of participants should have sufficient knowledge and experience to act as non-professional investors, to read financial information and security breach news, and to provide investment judgments based on the experimental task provided.

Table 1 presents the demographic information of the study's 112 participants by treatment. Untabulated one-way ANOVA testing reveals no significant difference in demographic variables across treatments ($p > 0.10$, two tailed). Additionally, we did not find any difference in personal investment experience and prior financial statement experience across treatments ($p > 0.10$, two tailed). We also conducted several additional analyses to test the robustness of the results. Variables, including manipulation checks, prior investment experience, prior financial statements experience, gender, and age, were added as control

[9] The same two questions were used to measure pre- and post-investment judgments.
[10] The results do not change if investment attractiveness and likelihood of investment are separately tested as the dependent variable.
[11] Participants were removed from the final sample if they failed both manipulation check questions and the attention check question. The results do not change when we include participants who failed the attention or manipulation check questions.

variables into the model. None of these variables are significant, and there is no change in the pattern of significance in our main results.

Table 1. Participant Demographics

	Cybersecurity Disclosure			Total
	No Disclosure	CSRM Report	CSRM Report with an IA Report	
Sample Size	38	38	36	112
Age:				
Below 18	0	0	0	0
18-25	0	2	3	5
26-30	10	6	4	20
31-35	8	10	5	23
36-40	9	4	5	18
41-45	3	5	7	15
45-50	4	3	8	15
Above 50	4	8	4	16
Gender:				
Male	21	23	17	61
Female	17	15	19	51
Number of times company performance has been analyzed via financial statements:				
This is the first time	0	1	1	2
1-5 times	13	14	8	35
6-10 times	9	4	14	27
More than 10 times	16	19	13	48
Have bought or sold common stock or debt securities?				
Yes	38	38	36	112
No	0	0	0	0
Years of personal investment experience				
0	0	0	0	0
1-3	9	14	9	32
4-7	14	9	13	36
8-10	5	3	5	13
More than 10 years	10	12	9	31

4.3 Hypothesis testing

Table 2 presents the sample size, mean, and standard deviations for investment judgment under each experimental condition. We first analyzed the pre-investment judgments. Although we do not have a formal hypothesis on them, we expect that before the security breach news is viewed, the investment judgments will not differ when there is no cybersecurity disclosure, CSRM report, or CSRM report with an IA report.[12] We used one-way ANOVA to test this expectation. As shown in Panel A of Table 3, there are no differences in investment judgments when the participants were exposed to different cybersecurity disclosures ($F = 0.644$, $p = 0.527$). This finding suggests that investors mainly use the company's financial performance information to make investment judgments, and cybersecurity disclosure does not significantly influence investment judgments when there is no security breach news.

[12] We note that, without the information of security breaches, some prior studies suggest positive market reactions toward voluntary cybersecurity disclosure (e.g., Bose & Leung 2019, Gordon et al. 2010). However, our finding is consistent with Wang et al. (2013a, p. 212) that without the information of security breaches, they did not observe any differences in market valuation given different types of disclosures regarding information security risks.

Table 2. Descriptive Statistics for Pre- and Post-Investment Judgments

Descriptive statistics: Mean (standard deviation)				
Condition	Cybersecurity Disclosure			Overall
	No Disclosure	CSRM Report	CSRM Report with an IA Report	
	n = 38	*n = 38*	*n = 36*	*n = 112*
Absence of security breach news	5.80 (2.78)	5.42 (2.16)	5.58 (2.43)	5.60 (2.28)
Presence of security breach news	4.08 (2.38)	2.71 (2.49)	2.83 (2.06)	2.31 (2.38)

Table 3. Pre- and Post-Investment Judgments

Panel A: Results of the ANOVA for Pre-Investment Judgments				
Factor	*df*	*MS*	*F*	*p* (two-tailed)
Cybersecurity Disclosure	2	3.382	0.644	0.527
Error	109	5.248		

Panel B: Results of the T-Test for Pre- and Post-Investment Judgments (H1)			
	t	*df*	*p* (two-tailed)
Pre- vs. Post-Investment Judgments	12.658	111	0.000

We then used *t*-test to compare pre- and post-investment judgments. We predicted in Hypothesis 1 that investors are less likely to invest in the breached company after learning the security breach news. As presented in Panel B of Table 3, the findings from the *t*-test ($t = 12.658$, $p < 0.001$) support Hypothesis 1, indicating that investors make less favorable investment judgments after learning about the negative news related to the security breach. This finding is consistent with prior literature that shows investors are less likely to invest in a company that has experienced a security breach.

We used two-way mixed ANOVA to test the impact of cybersecurity disclosure and security breach news on post-investment judgments. Hypothesis 1 states that investors make less favorable investments after knowing the security breach news. The results, as shown in Panel A of Table 4, indicate that there is a significant main effect of security breach news on investment judgments ($F = 163.653$, $p < 0.001$), which provides additional support to Hypothesis 1. The result also shows that the interaction between security breach news and cybersecurity disclosure is not significant ($F = 1.986$, $p = 0.142$). Even though the interaction is not significant, we can use planned contracts to test the predicted ordinal interaction. Figure 1 provides the plot of the means by condition.

Hypothesis 2 predicts that compared with the no cybersecurity disclosure condition, investors are less likely to invest in a company that has disclosed a CSRM report after learning that the company has been affected by a security breach. We used a contrast coding of (1, −1, 0) to test whether the CSRM report has a lower investment judgment compared with the no disclosure condition. As indicated in Panel B of Table 4, our findings from the planned contrasts support Hypothesis 2 ($t = 2.569$, $p = 0.006$), suggesting that investors make less favorable investment judgments when the breached company disclosed a CSRM report compared with not disclosing any cybersecurity information. The multiple comparisons technique can also be used to test the mean differences between the CSRM report condition and the no disclosure condition ($p = 0.006$). The findings further confirm our prediction and suggest that the disclosing choice, a CSRM report that investors previously were exposed to, can aggravate the negative impact of security breach news.

Table 4. Post-Investment Judgments

Panel A: Results of the Mixed ANOVA for Post-Investment Judgments				
Factor	*df*	*MS*	*F*	*p* (two-tailed)
Breach News	1	338.814	163.653	0.000
Breach News × Cybersecurity Disclosure	2	4.112	1.986	0.142
Error	109	2.070		

Panel B: Planned Contrast (H2)			
	Contrast Coding	*t*	*p* (one-tailed)
CSRM Report vs. No Disclosure	1, −1, 0	2.569	0.006

Panel C: Multiple Comparisons (Research Question)			
	Mean Diff.	Std. Err	*p* (two-tailed)
CSRM Report with an IA Report vs. No Disclosure	−1.246	0.540	0.023
CSRM Report with an IA Report vs. CSRM Report	0.123	0.540	0.821

We next turned our attention to the impact of disclosing a CSRM report with an IA report on investment judgments. We used multiple comparisons to answer this question. We observed from Table 2 that the mean score of post-investment judgment under the CSRM report with an IA report condition is 2.83, which is higher than that of the CSRM report condition (2.71) but lower than that of the no disclosure condition (4.08). The findings from multiple comparisons, as reported in Panel C of Table 4, suggest that compared with the no-disclosure condition (p = 0.023), investors make less favorable investment judgments when the breached company disclosed a CSRM report with an IA report. This finding implies that a CSRM report with an IA report does not mitigate the negative influence of security breach news.

We also compared the investment judgments between the CSRM report condition and the CSRM report with an IA report condition. The result, reported in Panel C of Table 4, does not suggest that there are significant differences in investment judgments when the breached company discloses the CSRM report along with an IA report and when the company discloses the CSRM report alone. This finding further supports the finding that adding an independent IA report evaluating the description of the CSRM program and the effectiveness of controls for the breached company does not mitigate the negative impact of security breach news.

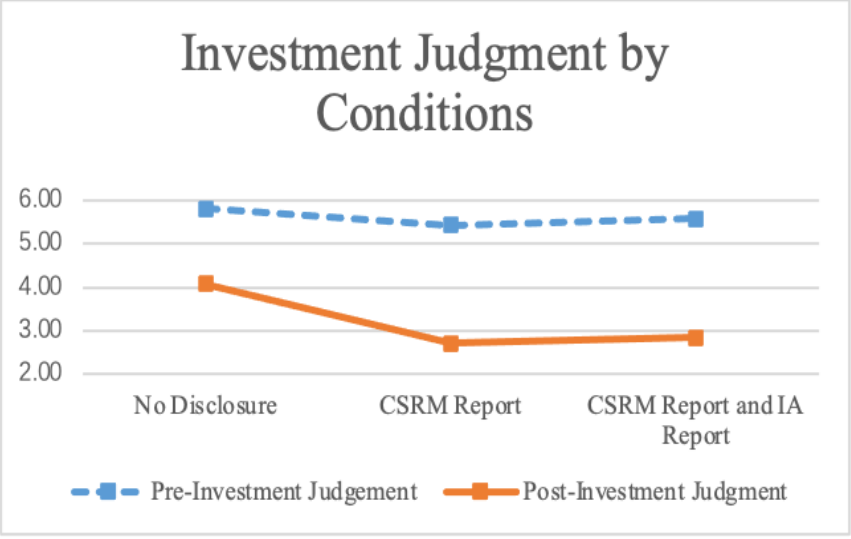

Figure 1. Plots of the Means by Condition

4.4 Additional Analyses

4.4.1 Blame Measures

The participants rated the quality of XYZ Stores' CSRM (1–Very low quality to 7–Very high quality) and the likelihood that they were to blame XYZ Stores for the breach (1–Extremely unlikely to 7–Extremely likely).[13] These two questions were adapted from the papers of Kadous and Mercer (2014) and Gimbar, Hansen, and Ozlanski (2016) to measure the blame assigned to organizations with negative outcomes. From Panel B of Table 5, we note that the quality rating was the lowest when the participants were exposed to a CSRM report that made assertions about the effectiveness of the CSRM program (t = 3.559, p = 0.001). The results of multiple comparisons show that the quality rating of CSRM in the no disclosure condition is higher than those of the CSRM report condition ($p < 0.001$) and the CSRM report along with an IA report condition (p = 0.057). Moreover, the quality rating in the CSRM report along with an IA report condition is higher than that in the CSRM report only condition (p = 0.039). These findings are interesting because investors actually rated the quality of XYZ Stores' CSRM the highest, although no detailed CSRM program was introduced in the experiment. This implies that investors are more likely to perceive that, for breached firms that claim the effectiveness of its CSRM program, management did not effectively manage cybersecurity risks. Adding an IA report seems to help increase the quality rating, but the rating is still lower than that of the no disclosure scenario.

We then analyzed the likelihood that the participants were to blame XYZ Stores for the breach. The findings, as presented in Panel B of Table 6, indicate that the participants were the most likely to assign blame to XYZ Stores when they were exposed to a CSRM report that claimed the effectiveness of a CSRM program (t = 2.793, p = 0.006). The results also provide marginally significant support that the participants in the CRSM report only condition assigned more blame to XYZ Stores compared with the CRSM report along with an IA report condition (p = 0.078). However, there is no evidence to show that the participants assigned less blame when they were provided with a CSRM report along with an IA report compared with the no-disclosure condition (p = 0.400).

Table 5. Blame Measures – Quality of Cybersecurity Risk Management

Panel A: Descriptive Statistics

Descriptive statistics: Mean (standard deviation)			
Quality of Cybersecurity Risk Management			Overall
No Disclosure	CSRM Report	CSRM Report with an IA Report	
n = 38	n = 38	n = 36	n = 112
3.55 (1.50)	2.34 (1.30)	2.97 (1.38)	2.96 (1.38)

Panel B: Planned Contrast and Multiple Comparisons

Planned Contrast			
	Contrast Coding	t	p (two-tailed)
CSRM Report vs. No Disclosure and CSRM Report with an IA Report	1, −2, 1	3.559	0.001

[13] The results are qualitatively similar when we include or exclude blame measures as covariates.

Multiple Comparisons			
	Mean Diff.	Std. Err	*p* (two-tailed)
No Disclosure vs. CSRM Report	1.211	0.297	0.000
No Disclosure vs. CSRM Report with an IA Report	0.580	0.301	0.057
CSRM Report vs. CSRM Report with an IA Report	−0.630	0.301	0.039

Table 6. Blame Measures – Blame Likelihood

Panel A: Descriptive statistics

Descriptive Statistics: Mean (standard deviation)			
Blame Likelihood			Overall
No Disclosure	CSRM Report	CSRM Report with an IA Report	
n = 38	*n = 38*	*n = 36*	*n = 112*
4.78 (1.89)	5.79 (1.36)	5.11 (1.62)	5.23 (1.68)

Panel B: Planned Contrast and Multiple Comparisons

Planned Contrast			
	Contrast Coding	*t*	*p* (two-tailed)
CSRM Report vs. No Disclosure and CSRM Report with an IA Report	−1, 2, −1	2.793	0.006

Multiple Comparisons			
	Mean Diff.	Std. Err	*p* (two-tailed)
No Disclosure vs. CSRM Report	−1.000	0.376	0.009
No Disclosure vs. CSRM Report with an IA Report	−0.322	0.381	0.400
CSRM Report vs. CSRM Report with an IA Report	0.678	0.381	0.078

The results from the two blame measures provide support for our assumption that investors question the quality of CSRM and assign more blame to companies that claimed the effectiveness of CSRM but later experienced a security breach.

4.4.2 Additional Measures

We also collected additional measures to understand participants' views on cybersecurity disclosure, IA report, and companies' actions toward preventing security breaches. Participants in the CSRM report condition and CSRM report with an IA report condition provided their responses after reading the cybersecurity disclosure but before making their pre-investment judgments. The Panel A of Table 7 shows the descriptive statistics related to these measures.

Participants in the CSRM report condition and CSRM report with an IA report condition rated the favorableness of cybersecurity disclosure. Only participants in the CSRM report with an IA report condition rated the favorableness of an IA report. Both responses were collected on 7-point Likert scales, anchored on 1 (Very unfavorable) and 7 (Very favorable). As shown in Panel A of Table 7, the mean of favorableness of IA report is 5.66, indicating participant views of the IA report about the cybersecurity risk

management are slightly favorable. The results of t-test in Panel B of Table 7 indicate that participants in the CSRM report with an IA report condition view the company more favorably than participants in the CSRM report condition (t = 7.603, p = 0.008).

Participants in the CSRM report condition and CSRM report with an IA report condition indicated their agreement/disagreement of the two statements related to XYZ Stores' actions to prevent security breaches. The statements are "XYZ does enough to prevent data breaches" and "XYZ does little to prevent data breaches." The response was collected on a 7-point Likert scale, anchored on 1 (Strongly disagree) and 7 (Strongly agree). As indicated in Panel C and D of Table 7, participants in the CSRM report and an IA report condition are more likely to agree that the company does enough to prevent data breaches and less likely to agree that the company does little to prevent data breaches.

These findings are interesting because we do not note the pre-investment judgment differ, although the results from the additional measures indicate that participants in the CSRM report with an IA report condition are more likely to view the cybersecurity disclosure more favorable and rate the company does enough to prevent data breaches. This pattern may be due to the fact that when there is no news indicating a company is affected by a security breach and the financial performance is favorable, the financial performance of the company is the more influential factor that impacts investment judgments and decisions.

The findings related to the additional measure can potentially be used to explain the quality rating and blame likelihood results. That is, participants in the CSRM report with an IA report condition are likely to agree that the company provides more favorable cybersecurity disclosure and that the company does enough to prevent data breaches. Hence, we found in 4.4.1 that the quality rating (blame likelihood) is higher (lower) in the CSRM report along with an IA report condition than that in the CSRM report only condition.

Table 7. Additional Measures

Panel A: Descriptive statistics: Mean (standard deviation)			
	CSRM Report	**CSRM Report with an IA Report**	
Favorableness of Cybersecurity disclosure	4.42 (1.80)	5.48 (1.18)	4.88 (1.64)
Favorableness of IA report	-	5.66 (1.20)	-
Enough to prevent data breaches	4.39 (1.46)	5.34 (1.17)	4.81 (1.42)
Little to prevent data breaches	3.58 (1.50)	2.72 (1.31)	3.21 (1.47)

Panel B: Results of the T-Test for Favorableness of Cybersecurity Disclosure		
	t	p (two-tailed)
CSRM report vs. CSRM report with an IA report	7.603	0.008

Panel C: Results of the T-Test for Enough to Prevent Data Breaches		
	t	p (two-tailed)
CSRM report vs. CSRM report with an IA report	8.204	0.006

Panel D: Results of the T-Test for Little to Prevent Data Breaches		
	t	p (two-tailed)
CSRM report vs. CSRM report with an IA report	5.961	0.017

5 Discussion and Conclusions

Cybersecurity breaches are becoming prevalent (Audit Analytics, 2020; Ponemon Institute, 2017; PricewaterhouseCoopers, 2017). However, currently, companies are only required to disclose limited information on CSRM programs (Newman, 2017; Securities and Exchange Commission, 2018) even when the SEC and the AICPA have provided additional guidance on cybersecurity disclosures. This study examines the impact of different cybersecurity disclosures on investment judgments before and after the public is aware of security breach news. We find that when there is no security breach news, investor judgments do not differ across different conditions, including no cybersecurity disclosure, CSRM report, and CSRM report with an IA report. This implies that nonprofessional investors primarily use the financial performance information of a company to make judgments when there is no negative news related to the breach. We also find that nonprofessional investors are less likely to invest in a company after knowing that the company has been affected by a security breach. This finding is consistent with some of the prior results of studies examining the impact of security breaches on business value (e.g., Campbell et al., 2003). We then investigate whether the cybersecurity disclosure (chosen before the public breach announcement) aggravates or mitigates the negative impact of security breach news. We note that after knowing about the security breach news, nonprofessional investors are less likely to invest in a breached company if the company provided a CSRM report compared with the case when the breached company made no cybersecurity disclosure. This finding indicates that disclosing additional information on the cybersecurity program of a company that later experienced a security breach can lead to negative outcomes, thus aggravating the negative impact of security breach news. We further show that disclosing a CSRM program with an IA report does not necessarily mitigate the negative impact of security breaches, even if a third party also agreed on the effectiveness of the CSRM program within the breached company.

Our study has made several contributions. First, it has contributed to the literature on cybersecurity disclosures. As mentioned in Section 2, while there is an increasing interest in studying the impact of voluntary and mandatory disclosure concerning information security, most studies have taken the approach of applying event-study methodology to analyze either the announcement of security breaches or the disclosure of information security items in annual reports filed with the SEC, and the effect on market value. Instead, this study focuses on a new initiative—the CSRM report—by experimentally examining whether and how different cybersecurity disclosures influence investment judgments before and after the public announcement of security breaches.

Second, this study has contributed to the understanding of nonprofessional investors' decision-making process. The findings of our study suggest that nonprofessional investors rely on the financial performance information of companies to make investing judgments; however, they value cybersecurity disclosures when there is security breach news. We use the notion of blame from social psychology and the literature on blame in corporate failure to enhance our understanding of nonprofessional investors' judgments. We note that nonprofessional investors are likely to assign more blame to companies that claim the effectiveness of CSRM but later experience a security breach. While prior studies suggest that nonprofessional or retail investors are less sophisticated (Barber & Odean, 2013), this study shows that nonprofessional investors are also capable of dissecting nonfinancial disclosure. Further, consistent with the survey from the Center for Audit Quality (2016), nonprofessional investors value cybersecurity management and take cybersecurity concerns into consideration when making investment judgments.

Third, this study has informed policy makers regarding the possible negative effect of detailed cybersecurity disclosures on business value. The results of our study show that disclosing a CSRM report can lead to less favorable investment judgments after the announcement of security breaches. Detailed cybersecurity disclosures are useful pieces of information not only to customers whose personal information could be compromised but also to investors who need valuable cybersecurity information to make investment decisions. However, the market may punish firms that initially claimed the effectiveness of their CSRM but later experienced security breaches.

Fourth, this study should also interest companies that are considering disclosing a detailed CSRM program. This study notes that disclosing a CSRM report leads to lower investment attractiveness and likelihood to invest than not disclosing any cybersecurity information, while disclosing a CSRM report with an IA report does not necessarily result in higher investment judgment. Compared to companies that do not initially provide any cybersecurity information, investors are more likely to question the quality of CSRM and assign more blame to companies that claimed the effectiveness of CSRM but later experience a security breach. Thus, breached companies with cybersecurity disclosure may be under-valued and

breached companies without cybersecurity disclosure could be over-valued. Although this study shows that *talking too much* could have negative impacts on investment decisions, it does not suggest that companies should avoid making voluntary management disclosures. Instead, we argue that making assertions about the effectiveness of the CSRM program of a company that still experiences security breaches later could lead to more severe consequences. Companies may include more details related to their effort in CSRM to signal the public that they have made every effort possible, or more effort than competitors, to manage cybersecurity risk. Companies facing a higher breach risk may take the findings of this study into account when evaluating the outcomes of disclosing detailed cybersecurity risk information.

All studies are subject to limitations, which can provide opportunities for future research. First, the CSRM report in our study includes management's descriptions of the company's CSRM program and assertions about the effectiveness of the controls within the program to achieve the company's cybersecurity objectives. While it is more common for companies to include assertions about the effectiveness of controls in management reports, future studies can examine how investors react to a CSRM report with no assertions or an assertion about the ineffectiveness of the controls. Second, we develop the CSRM an IA reports based on the AICPA's CSRM reporting framework. Since the AICPA does not mandate specific formats for most of the information to be presented, companies are likely to create their own disclosing format. Our study aims to examine how the CSRM and IA reports developed based on the AICPA's framework influence investment judgments, therefore, we adapt the standardized reports which contain all the required components of CSRM reporting framework. Companies are likely to update or modify such report to meet their reporting needs. Future studies can examine whether and how the different types of CSRM disclosure affect investment judgments. Additionally, our results suggest adding an IA report, a third party's opinion, does not necessarily reduce the negative impact of security breaches. However, future research can examine the extent to which investors will appreciate companies' efforts in CSRM when more detailed CSRM actions are disclosed (e.g., advanced technology employed to prevent and identify firm/industry specific threats).

Third, the retail industry and payment system-related breaches were chosen in this study to provide a salient setting to the participants. Future research could investigate whether investor judgments will differ if a company in another industry experiences security breaches or if other types of confidential information are compromised. Fourth, we recruited nonprofessional investors from M-Turk as participants. The experiment was not conducted in a controlled lab. Prior studies have shown that M-Turk workers are motivated, more representative than more traditional student pools, and appropriate proxies for nonprofessional investors, thereby reducing the concerns about using M-Turk. Future research could examine how student pools or professional investors, who have more sophisticated knowledge about companies and the consequences stemming from a security breach, evaluate the impact of different cybersecurity disclosures. Fifth, participants were shown the prior cybersecurity disclosures before the data breach was publicized. We employ this research design because this paper aims to examine how such prior disclosure can influence investor judgments. It is likely that a data breach is publicized a few weeks or months after the cybersecurity disclosure. Future research can examine whether the lag between cybersecurity disclosure and a data breach can affect investor decisions. Lastly, when more data becomes available, it will be interesting to use secondary data to investigate how the market reacts to breached firms with or without CSRM and IA reports.

Acknowledgments

The authors are grateful for the financial support of Auburn University, DePaul University, and Tongji University. The authors are also thankful for the helpful suggestions of the participants of the 2019 UWCISA 11th Biennial Symposium on Information Integrity and Information Systems Assurance.

References

American Institute of Certified Public Accountants. (2017a). *Illustrative cybersecurity risk management report*. Retrieved from https://us.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/illustrative-cybersercurity-risk-management-report.pdf

American Institute of Certified Public Accountants. (2017b). *SOC for cybersecurity*. Retrieved from https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/soc-for-cybersecurity-brochure.pdf

American Institute of Certified Public Accountants. (2018). *Cybersecurity risk management reporting fact sheet*. Retrieved from https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/cybersecurity-fact-sheet.pdf

Andriotis, A. (2018). Equifax identifies additional 2.4 million affected by 2017 breach. *WSJ*. Retrieved from https://www.wsj.com/articles/equifax-identifies-additional-2-4-million-affected-by-2017-breach-1519918282

Audit Analytics. (2020). Trends in cybersecurity breach disclosures. Retrieved from https://go.auditanalytics.com/cybersecurityreport

Backhouse, J., Hsu, C. W., & Silva, L. (2006). Circuits of power in creating de jure standards: Shaping an international information systems security standard. *MIS Quarterly*, *3*0(SI), 413-438.

Barber, B. M., & Odean, T. (2013). The behavior of individual investors (pp. 1533-1570). *Handbook of the Economics of Finance.* Elsevier.

Bose, I., & Leung, A. C. M. (2019). Adoption of identity theft countermeasures and its short-and long- term impact on firm value. *MIS Quarterly, 43*(1), 313-327.

Brandon, D. M., Long, J. H., Loraas, T. M., Mueller-Phillips, J., & Vansant, B. (2013). Online instrument delivery and participant recruitment services: Emerging opportunities for behavioral accounting research. *Behavioral Research in Accounting*, *26*(1), 1-23.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, *34*(3), 523-548.

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

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). The effect of internet security breach announcements on market value of breached firms and internet security developers. *International Journal of Electronic Commerce*, *9*(1), 69-105.

Center for Audit Quality. (2016). *2016 Main street investor survey*. Center for Audit Quality.

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

Cheng, X., & Walton, S. (2019). Do nonprofessional investors care about how and when data breaches are disclosed? *Journal of Information Systems*, *33*(3), 163-182.

Cram, W. A., D'Arcy, J., & Proudfoot, J. G. (2019). Seeing the forest and the trees: A meta-analysis of the antecedents to information security policy compliance. *MIS Quarterly*, *43*(2), 525-554.

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach, *Information Systems Research*, *20*(1), 79-98.

Deloitte. (2016). Response to the proposed description criteria for management's description of an entity's cybersecurity risk management program. Retrieved from https://dart.deloitte.com/USDART/ov-resource/139e0012-c07f-11e6-a391-2b48717272bf.pdf

Easley, D., & O'Hara, M. (2010). Liquidity and valuation in an uncertain world. *Journal of Financial Economics*, *97*, 1-11.

Farkas, M., & Murthy, U. S. (2014). Nonprofessional investors' perceptions of the incremental value of continuous auditing and continuous controls monitoring: An experimental investigation. *International Journal of Accounting Information Systems*, *15*(2), 102-121.

Feng, Q., & Wang, T. (2019). Does CIO risk appetite matter? Evidence from information security breach incidents. *International Journal of Accounting Information Systems*, *32*, 59-75.

Gibson, D. E., & Schroeder, S. J. (2003). Who ought to be blamed? The effect of organizational roles on blame and credit attributions. *International Journal of Conflict Management*, *14*(2), 95-117.

Gimbar, C., Hansen, B., & Ozlanski, M. E. (2016). The effects of critical audit matter paragraphs and accounting standard precision on auditor liability. *The Accounting Review*, *91*(6), 1629-1646.

Goel, S., & Shawky, H. A. (2014). The impact of federal and state notification laws on security breach announcements. *Communications of the Association for Information Systems*, *34(1)*, 37-50.

Gordon, L. A., Loeb, M. P., & Sohail, T. (2010). Market value of voluntary disclosures concerning information security. *MIS Quarterly*, *34*(3), 567-594.

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

Grenier, J. H., Pomeroy, B., & Stern, M. T. (2015). The effects of accounting standard precision, auditor task expertise, and judgment frameworks on audit firm litigation exposure. *Contemporary Accounting Research*, *32*(1), 336-357.

Hsu, C., & Wang, T. (2014). Exploring the association between board structure and information security breaches. *Asia Pacific Journal of Information Systems*, *24*(4), 531-557.

Hsu, C., Wang, T., & Lu, A. (2016). The impact of ISO 27001 certification on firm performance. *49th Hawaii International Conference on System Sciences*.

Kadous, K., & Mercer, M. (2014). Are juries more likely to second-guess auditors under imprecise accounting standards? *Auditing: A Journal of Practice & Theory*, *35*(1), 101-117.

Kahneman, D. (1992). Reference points, anchors, norms, and mixed feelings. *Organizational Behavior and Human Decision Processes*, *51*(2), 296-312.

Kahneman, D., & Miller, D. (1986). Norm theory: Comparing reality to its alternatives. *Psychological Review*, *93*(2), 136-153.

Kamiya, S., Kang, J.-K., Kim, J., Milidonis, A., & Stulz, R. M. (2021). Risk management, firm reputation, and the impact of successful cyberattacks on target firms. *Journal of Financial Economics*, *139*(3), 719-749.

Kelton, A. S., & Murthy, U. S. (2015). The effects of information disaggregation and financial statement interactivity on judgments and decisions of nonprofessional investors. *Journal of Information Systems*, *30*(3), 99-118.

Kwon, J., Rees, J., & Wang, T. (2013). The association between top management involvement and compensation and information security breaches. *Journal of Information Systems*, *27*(1), 219-236.

Li, H., No, W. G., & Wang, T. (2018). SEC's cybersecurity disclosure guidance and disclosed cybersecurity risk factors. *International Journal of Accounting Information Systems*, *30*, 40-55.

Li, W. (2020). Understanding the whistle-blowing intention to report breach of confidentiality. *Communications of the Association for Information Systems*, *47*, 72-94.

Lowry, P. B., Posey, C., Bennett, R. B. J., & Roberts, T. L. (2015). Leveraging fairness and reactance theories to deter reactive computer abuse following enhanced organisational information security policies: An empirical study of the influence of counterfactual reasoning and organisational trust. *Information Systems Journal*, *25*(3), 193-273.

Newman, L. H. (2017). The biggest cybersecurity incidents of 2017 so far. Retrieved from https://www.wired.com/story/2017-biggest-hacks-so-far/

O'Flaherty, K. (2019). Equifax becomes first firm to see its outlook downgraded due to a cyber-attack. Retrieved from https://www.forbes.com/sites/kateoflahertyuk/2019/05/28/equifax-becomes-first-firm-to-see-its-outlook-downgraded-due-to-a-cyber-attack/#98064695671d

Owens, J., & Hawkins, E. M. (2019). Using online labor market participants for nonprofessional investor research: A comparison of MTurk and Qualtrics samples. *Journal of Information Systems*, *33*(1), 113-128.

Pal, J., Medway, D., & Byrom, J. (2011). Deconstructing the notion of blame in corporate failure. *Journal of Business Research*, *64*(10), 1043-1051.

Paulsen, C., & Byers, R. (2019). Glossary of key information security terms. National Institute of Standards and Technology. *U.S. Department of Commerce*. Retrieved from https://csrc.nist.gov/publications/detail/nistir/7298/rev-3/final

Ponemon Institute. (2017). 2017 Cost of cyber crime study. Retrieved from https://www.ponemon.org/blog/2017-cost-of-cyber-crime-study

PricewaterhouseCoopers. (2016). PwC comments on ASEC's proposed revision of its trust services criteria. Retrieved from https://www.pwc.com/us/en/cfodirect/publications/comment-letter-aicpa/aicpa-asec-proposed-revision-trust-services-criteria.html

PricewaterhouseCoopers. (2017). The Global State of Information Security® survey 2018. Retrieved from https://www.pwc.com/us/en/services/consulting/cybersecurity/library/information-security-survey.html

Rennekamp, K. (2012). Processing fluency and investors' reactions to disclosure readability. *Journal of Accounting Research*, *50*(5), 1319-1354.

Securities and Exchange Commission. (2017). *Statement on cybersecurity*. Securities and Exchange Commission. Retrieved from https://www.sec.gov/news/public-statement/statement-clayton-2017-09-20

Securities and Exchange Commission. (2018). Commission statement and guidance on public company cybersecurity disclosures. Retrieved from https://www.sec.gov/rules/interp/2018/33-10459.pdf

Shaver, K. (1985). *The attribution of blame: Causality, responsibility and blameworthiness.* Springer.

Shaver, K. G. (2012). *The attribution of blame: Causality, responsibility, and blameworthiness.* Springer.

Siponen, M., & Vance, A. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. *MIS Quarterly*, *34*(3), 487-502.

Swaminatha, T. (2017). Equifax now hit with a rare 50-state class-action lawsuit. Retrieved from https://www.csoonline.com/article/3238076/equifax-now-hit-with-a-rare-50-state-class-action-lawsuit.html

Tadesse, A. F., & Murthy, U. S. (2018). Nonprofessional investor perceptions of the partial remediation of IT and non-IT control weaknesses: An experimental investigation. *International Journal of Accounting Information Systems*, *28*, 14-30.

Tsang, E. W. (2002). Self-serving attributions in corporate annual reports: A replicated study. *Journal of Management Studies*, *39*(1), 51-65.

Tysiac, K. (2017). A new cybersecurity risk management reporting framework for management and CPAs. *Journal of Accountancy*, Retrieved from https://www.journalofaccountancy.com/news/2017/apr/cybersecurity-risk-management-reporting-framework-201716483.html.

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

Wang, T., Rees, J., & Karthik, K. (2013b). 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.

Wei, L.-C., Hsu, C., & Wang, K. (2016). Intentions of employees to whistleblowing information security policy violations in the organization. *Asia Pacific Journal of Information Systems*, *26*(1), 163-188.

Willison, R., Warkentin, M., & Johnston, A. C. (2018). Examining employee computer abuse intentions: Insights from justice, deterrence and neutralization perspectives. *Information Systems Journal*, *28*(2), 266-293.

About the Authors

Xu (Joyce) Cheng is an Assistant Professor at Auburn University. She received her Ph.D. from the Lynn Pippenger School of Accountancy, University of South Florida in 2017. She has a wide array of research interests in experimental based accounting research, including accounting information systems and judgment decision making. Her primary teaching interests include accounting information systems, data analytics, and IT Auditing. She currently teaches accounting information systems and accounting analytics at the undergraduate level. She is a member of the American Accounting Association and the Canadian Academic Accounting Association.

Tawei (David) Wang is currently an associate professor and Driehaus Fellow at DePaul University. He received his Ph.D. from Purdue University in 2009. His research interests are information security management and IT management. His papers have appeared in several leading journals, including *Information Systems Research*, *Accounting Horizons*, *Decision Support Systems*, *European Journal of Information Systems*, *Information and Management*, *Information Systems Journal*, *International Journal of Accounting Information Systems*, *Journal of Accounting and Public Policy*, *Journal of Banking and Finance*, and *Journal of Information Systems*, among others. He was a panelist on cyber risk in a workshop hosted by the Federal Reserve Bank, Charlotte. He was selected as the KPMG James Marwick Professor-in-Residence in 2018.

Carol Hsu is a Professor at the University of Sydney Business School. She received her Ph.D. in Information Systems from the London School of Economics and Political Science. Her research interests focus on information security management, information technology adoption and digital transformation. Her work has been published in *MIS Quarterly*, *Information Systems Research*, *Journal of Management Information Systems*, *Information Systems Journal*, and other outlets. She has received the Sandra Slaughter Service Award from the Association of Information Systems. She currently serves as Senior Editor at the *Journal of Strategic Information Systems* and *Information Systems Journal*, and on the editorial board of the *Journal of the Association for Information Systems*, and the *IEEE Transactions on Engineering Management*.