STARS

University of Central Florida
STARS

Electronic Theses and Dissertations, 2004-2019

2019

Three Studies on Cybersecurity Disclosure and Assurance

Patricia Navarro Vekez
University of Central Florida

 Part of the Accounting Commons
Find similar works at: https://stars.library.ucf.edu/etd
University of Central Florida Libraries http://library.ucf.edu

This Doctoral Dissertation (Open Access) is brought to you for free and open access by STARS. It has been accepted for inclusion in Electronic Theses and Dissertations, 2004-2019 by an authorized administrator of STARS. For more information, please contact STARS@ucf.edu.

STARS Citation
Navarro Vekez, Patricia, "Three Studies on Cybersecurity Disclosure and Assurance" (2019). *Electronic Theses and Dissertations, 2004-2019*. 6541.
https://stars.library.ucf.edu/etd/6541

University of Central Florida
STARS
Showcase of Text, Archives, Research & Scholarship

THREE STUDIES ON CYBERSECURITY DISCLOSURE AND ASSURANCE

by

PATRICIA NAVARRO VELEZ
B.B.A. University of Puerto Rico, Ponce PR, 2007
M.Acc. Bowling Green State University, Bowling Green, OH, 2008

A dissertation submitted in partial fulfillment of the requirements
for the degree of Doctor of Philosophy
in the Kenneth G. Dixon School of Accounting
in the College of Business Administration
at the University of Central Florida
Orlando, Florida

Summer Term
2019

Major Professor: Steve G. Sutton

ABSTRACT

This dissertation comprises three experimental studies that explore how management's financial disclosure behavior and security strategies influence the costs associated with cybersecurity breaches. The first study examines the cost of litigation in connection with cybersecurity incidents. The purpose of this study is to determine how the characteristics and content of cybersecurity incidents' disclosure affects jurors' liability assessments. Specifically, this study explores how jurors react to management timeliness in disclosing the incident and the plausibility of the explanations provided to justify the disclosure strategy. The second and third studies explore the value relevance of cybersecurity risk management (CRM) assurance. In particular, the second study examines whether engagement in voluntary assurance over CRM before the occurrence of an incident affects investors' reactions after the incident, and whether these reactions differ based on whether assurance is expected or not expected based on industry norms. The third study scrutinizes how perceptions of disclosure timeliness affect investor decisions and explores the use of CRM assurance as a potential tool to mitigate the deleterious effects of delayed disclosures of cybersecurity incidents. Overall, the results reported in this dissertation suggest that timely disclosure of a cybersecurity breach reduces liability, improves management credibility assessments, and results in higher valuation judgments. Moreover, the findings reveal that CRM assurance further leads to enhanced management credibility assessments and valuation judgments and that the impact of CRM assurance is particularly beneficial when not necessarily expected for the industry. In combination, these three studies address calls for research exploring the costs of cybersecurity and inform regulators currently engaged in developing both cybersecurity disclosure requirements and voluntary assurance services designed to address stakeholders' information needs regarding companies' cybersecurity

activities. These studies also add to the literature and theory documenting the link between disclosure timeliness and litigation risk, and the value of voluntary assurance services.

ACKNOWLEDGMENTS

Completion of this dissertation would not have been possible without the support, mentoring, and guidance from several individuals. I would like to express my deepest appreciation to my committee members, Dr. Steve Sutton, Dr. Elizabeth Altiero, Dr. Sean Robb, and Dr. David Wood, for their comments and feedback throughout the dissertation process. I am extremely grateful for your time and guidance. Special thanks to Dr. Steve Sutton, my dissertation chair, for all the invaluable advice, mentoring, and time since I started the Ph.D. program. I consider myself fortunate to have you as my advisor and chair and will always be grateful for your support. Moreover, I would like to thank Dr. Lisa Baudot, Dr. Khim Kelley, Enrique Guerra, Irina Malaescu, Nadra Pencle, Wioleta Olckzak, Natalia Ardasheva, Gregory Stone, and Jacob Lennard for specific feedback on my studies and experimental materials, and Dr. Jeff Reinking, Dr. Dana Wallace, and Enrique Guerra for allowing me to recruit students for my research.

I also would like to thank Dr. Vicky Arnold, Dr. Jesse Dillard, Dr. Robin Roberts, and Dr. Steve Sutton, for sharing your knowledge and experience and for all the lessons learned during our Ph.D. seminars. I appreciate the generosity of the Dixon School of Accounting for providing resources for data collection and to the UCF College of Graduate Studies for their Doctoral Research Support Award. I am also thankful with the AICPA, KPMG, and the McKnight Doctoral Fellowship Program for their financial support during the PhD Program.

Finally, I would specially like to thank my family and friends for the continued love, support, and encouragement. I especially wish to thank my kids, Armando, Deliana, Gian, and Isadora, for providing me with the motivation and strength to overcome every challenge on my way. Thanks to my dear husband, David, for holding my hand throughout this journey and for all

the love, support, and sacrifices made to help me get to this point. Thanks to my sisters and brother for all the love and encouragement and mostly, thanks to my parents for a lifetime of love, hard-work, and sacrifices to build our family and for always reminding us that the sky is the limit. Last, thanks to my friend and mentor, Dr. Jose Gonzalez Taboada, for his continued advice, encouragement, and support before and throughout my journey through the Ph.D. program.

TABLE OF CONTENTS

LIST OF FIGURES ix

LIST OF TABLES x

GENERAL INTRODUCTION 1

Study One: Jurors' Liability Assessments After Cybersecurity Breaches: The Impact of Disclosure Timeliness and the Plausibility of Management Justifications 1

Study Two: Investors' Judgments and Decisions After a Cybersecurity Breach: Understanding the Value Relevance of Cybersecurity Risk Management Assurance 3

Study Three: The Impact of Disclosure Timeliness and Cybersecurity Risk Management Assurance on Investors Judgments and Decisions 4

Overall Contribution 6

References 7

STUDY ONE: JURORS' LIABILITY ASSESSMENTS AFTER CYBERSECURITY BREACHES: THE IMPACT OF DISCLOSURE TIMELINESS AND THE PLAUSIBILITY OF MANAGEMENT JUSTIFICATIONS 8

Introduction 8

Background, Theory, and Hypothesis 13

Information Security Disclosures 13

Disclosure Timeliness and Litigation Risk 15

Causal Attribution and Generalization of Inferences 17

The Plausibility of Justifications 19

Methods 21

Participants 21

Task 23

Independent Variables 24

Dependent Variables 26

Results 27

Manipulation Checks and Review Questions 27

Testing of Hypotheses 28

Additional Analysis 30

Perceived Plausibility 30

Perceived Timeliness 31
Conclusion 33
References 35
STUDY TWO: INVESTORS' JUDGMENTS AND DECISIONS AFTER A CYBERSECURITY BREACH: UNDERSTANDING THE VALUE RELEVANCE OF CYBERSECURITY RISK MANAGEMENT ASSURANCE 39
Introduction 39
Background, Theory, and Hypothesis 44
The Cost of Cybersecurity Breaches 44
Cyber-risk Management 45
Assurance over Information Security 48
Theoretical Model 52
Methods 56
Participants 57
Task 58
Independent Variables 59
Dependent Variables 60
Results 61
Manipulation Checks and Comprehension Questions 61
Testing of Hypotheses 62
Additional Analysis 65
Perceived Benefits of Assurance-as-Insurance – The Insurance Hypothesis 65
Perceived Accountant's Cyber-expertise 67
Disclosure of Cyber-risk Management Practices 69
Conclusion 70
References 73
STUDY THREE: THE IMPACT OF DISCLOSURE TIMELINESS AND CYBERSECURITY RISK MANAGEMENT ASSURANCE ON INVESTORS JUDGMENTS AND DECISIONS. 79
Introduction 79
Background, Theory, and Hypothesis 83
Disclosure Timeliness and Investment Decisions 83
Disclosure Timeliness and Management Credibility 86

Voluntary Assurance and the Insurance Hypothesis 87
Methods 89
Design and Participants 89
Task 90
Independent Variables 90
Dependent Variables 91
Results 92
Manipulation Checks 92
Testing of Hypothesis 93
Additional Analysis 95
Perceived Timeliness 95
Conclusion 96
References 99
GENERAL CONCLUSION 102
APPENDIX A: STUDY ONE FIGURES 105
APPENDIX B: STUDY ONE TABLES 112
APPENDIX C: STUDY TWO FIGURES 117
APPENDIX D: STUDY TWO TABLES 125
APPENDIX E: STUDY THREE FIGURES 130
APPENDIX F: STUDY THREE TABLES 133
APPENDIX G: STUDY ONE EXPERIMENTAL MATERIALS 139
APPENDIX H: STUDY TWO EXPERIMENTAL MATERIALS 179
APPENDIX I: STUDY THREE EXPERIMENTAL MATERIALS 203
APPENDIX J: IRB APPROVALS 230

LIST OF FIGURES

Figure 1 - Study 1: Model Predictions 106

Figure 2 - Study 1: Experimental Conditions 107

Figure 3 - Study 1: Operationalization of Plausibility 110

Figure 4 - Study 1: Additional Analysis 111

Figure 5 - Study 2: Model Predictions 118

Figure 6 - Study 2: Test of H1 119

Figure 7 - Study 2: Test of H2 120

Figure 8 - Study 2: Test of H3 121

Figure 9 - Study 2: Additional Analysis 122

Figure 10 - Study 2: Additional Analysis 123

Figure 11 - Study 2: Additional Analysis 124

Figure 12 - Study 3: Model Predictions 131

Figure 13 - Study 3: Test of H1 and H3 132

LIST OF TABLES

Table 1 - Study 1: Test of H1 113

Table 2 - Study 1: Test of H2a and H3 114

Table 3 - Study 1: Test of H2b and H3 115

Table 4 - Study 1: Additional Analysis 116

Table 5 - Study 2: Test of H1 126

Table 6 - Study 2: Test of H2a and H3a 127

Table 7 - Study 2: Test of H2b 128

Table 8 - Study 2: Test of H3b 129

Table 9 - Study 3: Test of H1 134

Table 10 - Study 3: Test of H2a and H3 135

Table 11 - Study 3: Test of H2b and H3 136

Table 12 - Study 3: Additional Analysis 138

GENERAL INTRODUCTION

Cyber-attacks have continued increasing in size, frequency, and cost to companies (Ponemon 2018). Therefore, regulators, accounting standard setters and practitioners are interested in understanding how companies are addressing cybersecurity risks and are engaged in several initiatives to promote the adoption of cybersecurity risk management (CRM) practices in organizations and to increase voluntary disclosure of CRM and security breach events. The three studies in this dissertation answer a call for research on the cost of cybersecurity attacks (AAA 2017) and explore the impact of cybersecurity disclosure and CRM assurance on judgments and decision making in accounting.

This dissertation comprises three experiments that explore the cost of cybersecurity incidents. Specifically, in the first study I investigate how management's disclosures and remedial tactics in connection with a cybersecurity incident impact jurors' assessment of a company's liability. The second and third studies explore how the disclosure of a cybersecurity incident and a company's engagement in CRM assurance influence investors' perceptions and valuation judgments. The following subsections provide additional detail on the motivation for each study, the research method employed, the main findings and contributions to practice, theory, and accounting literature. The overall contribution of this dissertation is discussed in the last subsection.

Study One: Jurors' Liability Assessments After Cybersecurity Breaches: The Impact of Disclosure Timeliness and the Plausibility of Management Justifications

In study one, I explore the impact of a cybersecurity breach disclosure timeliness and the plausibility of management justifications for the disclosure timing on jurors' assessments of

causal attribution and liability. Studying the cost of liability associated with cyber-attacks is important given that post-data breach costs, including legal costs, are considered one of the main cost drivers of cyber-attacks (Ponemon 2018). Research on the impact of disclosure timeliness suggests that timely disclosures reduce the cost of litigation (Skinner 1994, 1997). Based on this evidence, timely disclosure of cyber-attacks would be desirable. However, evidence of major recent breaches (e.g., Yahoo, Equifax) suggests that companies delay the disclosure of cyber-attacks (Fung 2017; Haselton and Lee 2017). It is possible that firms elect to delay the disclosure of cyber-attacks given management career incentives to delay the disclosure of bad news (Kothari, Li, and Short 2009). However, firms may have valid reasons to delay these disclosures given the complexities associated with discovering the breach and conducting subsequent investigations. As such, it is important to explore how the use of plausible and implausible justification for a cyber-attack disclosure's timeliness impacts jurors' judgment and decision making.

I use a 2 x 3 experiment and manipulate disclosure timeliness (more or less timely) and the plausibility of management justifications (plausible, implausible, or control) between-subjects. The dependent variables are participants' assessment of causal attribution (mediator) and liability assessments. As predicted, I find that more timely disclosures result in more favorable assessments of causal attribution and liability. I also find that causal attribution mediates the relationship between disclosure timeliness and liability assessments. However, I am unable to find support for the predicted interaction of timeliness and plausibility on causal attribution. Additional analysis reveals that timeliness of disclosures and participants disclosure preferences drive perceptions of plausibility.

This study informs companies and market participants about the cost of delayed disclosure of cyber-attacks. The findings have implications for regulators and standard setters interested in developing more disclosure requirements over cybersecurity. This study also contributes to the literature and theory on the impact of disclosure timeliness and the literature on remedial tactics to reduce liability by providing initial insights into the importance of disclosing cyber-attacks on a timely manner and showing that the benefits of remedial tactics, as documented in prior research, may be context specific.

Study Two: Investors' Judgments and Decisions After a Cybersecurity Breach: Understanding the Value Relevance of Cybersecurity Risk Management Assurance

In study two, I investigate how voluntary CRM assurance affects non-professional investors' judgments and decisions. The study also examines how the value relevance of CRM assurance is altered when such assurance violates or conforms to users' expectations. The AICPA developed in 2017 a CRM reporting framework and is promoting its use for voluntary disclosure of cybersecurity. The AICPA is also promoting assurance services through a Systems and Organization Controls (SOC) for cybersecurity engagement. Although there are known benefits of engaging in voluntary assurance, prior attempts of the accounting profession to promote assurance over information technology have largely failed (Gendron and Barrett 2004; Barett and Gendron 2006; Boulianne and Cho 2009). As such, investigating the impact of CRM assurance after cyber-attacks and understanding how investors' expectancies of influence their judgments and decision could help shed light on the value relevance of CRM assurance.

This study employs a 2 x 2 between-subjects experiment. The independent variables are CRM assurance (present or absent) and expectancies of assurance (conform to or violate expectancies). The dependent variables are valuation judgments and management credibility

assessments (mediator). I predict and find that companies that engage in voluntary CRM assurance receive higher stock price valuations and more favorable investor assessments of management credibility. Moreover, I find that investors' assessments of management credibility and stock price valuations are more extreme in the presence of positive and negative expectancy violations. Additional analysis reveals that investors' perceived benefits of assurance-as-insurance and perceived accountants' cyber-expertise are important determinants of investors' decision behavior. Further analysis also sheds light on the benefits and potential penalties associated with a firm's in-house CRM practices.

Evidence of the benefits of CRM assurance have implications for regulators, accounting professionals, and market participants and may help promote the use of CRM assurance to mitigate the negative impact of cyber-attacks. This study also adds to the literature and theory exploring the value relevance of voluntary assurance by identifying expectancy violations as a relevant variable that influences investors' judgments and decisions.

Study Three: The Impact of Disclosure Timeliness and Cybersecurity Risk Management Assurance on Investors Judgments and Decisions

Study three explores the impact of a cybersecurity breach disclosure's timeliness in the context of investors' judgment and decision making. This study also explores whether voluntary CRM assurance could help mitigate the negative impact of delayed disclosures. The market reaction to disclosure timeliness has been studied in the context of bad earnings news and restatement disclosure. Research find that the market negatively reacts to delayed disclosure of restatements (BenYousset and Khan 2016). However, no such negative reaction is found in the context of delayed disclosure of bad earnings (Givoly and Palmon 1982; Kalay and Loewenstein 1986). These results suggest that the impact of disclosure timeliness is context specific.

Therefore, studying the impact of a cyber-attack disclosure's timeliness on investors' judgment and decision making is central to further understand the cost and implications of cybersecurity breaches.

To conduct this study, I use a 2 x 2 experiment in which disclosure timeliness (more or less timely) and the CRM assurance (present or absent) are manipulated between-subjects. The dependent variables are valuation judgments and assessments of management credibility (mediator). I find that more timely disclosures lead to more favorable valuation judgments and more favorable assessments of management credibility. I also find that management credibility mediates the relationship between disclosure timeliness and valuation judgments. Nevertheless, although I find that the interaction of timeliness and CRM assurance is significant and impacts credibility assessments, the results are in the opposite direction predicted. This finding suggests that CRM assurance significantly influences credibility assessments only when the breach is disclosed in a timely manner. Additional analysis reveals that perceptions of disclosure timeliness are context specific and influenced by users' perceptions of cybersecurity disclosures.

The findings of this study inform companies and market participants about the negative implications of delayed disclosure of cyber-attacks, in particular the impact on firm value and credibility. The results are also relevant for regulators and standard setters promoting CRM disclosure and assurance and highlights the importance of timely disclosure of security events as part of a company's CRM program. This study also adds to the literature and theory on the market implications of disclosure timeliness by identifying context specific determinants of perceived timeliness which could help further understand mixed results from prior research.

Overall Contribution

The three studies in this dissertation aim to answer a call for research on the cost of cybersecurity to companies and shareholders (AAA 2017). These studies look at the cost of litigation and firm value which are important cost drivers after a cyber-attack. Moreover, these studies investigate the impact of disclosure timeliness and voluntary CRM assurance which makes the insights from these studies timely and relevant for regulators and standard setters currently engage in CRM disclosure and assurance initiatives.

Results from the three studies support several of the predictions. Overall, findings from Study One and Study Three sheds light on the cost of delayed disclosure of cyber-attacks and show that delayed disclosures increase liability and reduce perceptions of management credibility and stock price value. The results suggest that disclosure timeliness is a strong determinant of liability and valuation judgments and that the use of remedial tactics to reduce liability and voluntary CRM assurance do not effectively mitigate the effects of delayed disclosure of a cyber-attack. CRM assurance, however, enhances credibility and firm value when a cyber-attack is timely disclosed. Results from Study Two sheds light on the potential use of CRM assurance to mitigate the negative market reaction to cyber-attacks and suggests that market expectancies could help drive the demand for voluntary CRM assurance. Altogether, these studies help further our understanding of how cybersecurity disclosure and assurance affect judgment and decision-making and suggest that timely disclosure and voluntary CRM could help reduce the cost of cyber-attacks.

References

American Accounting Association (AAA). 2017. Cybersecurity Risk Management Program Examination Engagements; Panelists: Chris Halterman, Amy Pawlicki, and Paul Steinbart. AAA Mid-Year Meeting of the AIS and SET Sections, January 19, 2017, Orlando, FL.

Barrett, M., and Y. Gendron. (2006). WebTrust and the "commercialistic auditor" The unrealized vision of developing auditor trustworthiness in cyberspace. *Accounting, Auditing & Accountability Journal*, 19(5), 631-662.

BenYoussef, N., and S. Khan. 2016. Timing of earnings restatements: CEO equity compensation and market reaction. *Accounting & Finance*.

Boulianne, E., and C.H. Cho. 2009. The rise and fall of WebTrust. *International Journal of Accounting Information Systems*, 10(4), 229-244.

Fung, B. 2017. The SEC is reportedly probing Yahoo over its data breaches. *The Washington Post*, January 23, 2017.Gendron and Barrett 2004

Gendron, Y., and M. Barrett. 2004. Professionalization in action: Accountants' attempt at building a network of support for the WebTrust seal of assurance. *Contemporary Accounting Research*, 21(3), 563-602.

Givoly, D., and D. Palmon. 1982. Timeliness of annual earnings announcements: Some empirical evidence. *The Accounting Review*, 486-508.

Haselton T, and Y.N. Lee. 2017. Three Equifax executives sold $2 million worth of shares days after cyberattack. CNBC. Available at: https://www.cnbc.com/2017/09/07/equifax-cyberattack-three-executives-sold-shares-worth-nearly-2-million-days-after-data-breach.html

Kalay, A., and U. Loewenstein. 1986. The informational content of the timing of dividend announcements. *Journal of Financial Economics*, *16*(3), 373-388.

Kothari, S. P., X. Li, and J.E. Short. 2009. The effect of disclosures by management, analysts, and business press on cost of capital, return volatility, and analyst forecasts: A study using content analysis. *The Accounting Review*, *84*(5), 1639-1670.

Ponemon Institute. 2018. 2018 Cost of Data Breach Study: Global Overview. *Ponemon Institute Research Report*, July 2018.

Skinner, D. J. 1994. Why firms voluntarily disclose bad news. *Journal of accounting research*, *32*(1), 38-60.

Skinner, D. J. 1997. Earnings disclosures and stockholder lawsuits. *Journal of Accounting and Economics*, *23*(3), 249-282.

STUDY ONE: JURORS' LIABILITY ASSESSMENTS AFTER CYBERSECURITY BREACHES: THE IMPACT OF DISCLOSURE TIMELINESS AND THE PLAUSIBILITY OF MANAGEMENT JUSTIFICATIONS

Introduction

There are competing incentives for companies required to publicly disclose cybersecurity incidents. The Litigation Reduction Hypothesis suggests that companies may have incentives to timely disclose bad news to reduce the associated litigation risk and reduce expected legal costs (Skinner 1994, 1997). On the other hand, companies may also have incentives to strategically time the disclosure of bad news either due to management's career incentives (Kothari, Li, and Short 2009) or due to a desire to first collect all the relevant facts, as prior research suggests that investors reward accurate estimates (Hirst, Jackson, and Koonce 2003; Rupar 2017). Although prior research shows that timelier disclosures lower the likelihood of litigation (Donelson, McInnis, Mergenthaler, and Yu 2012), little is known about how the disclosure timeliness impacts jurors' liability assessments when remedial tactics are opportunistically employed to obfuscate managers' self-serving intentions.

Accordingly, in this study, I explore the impact of disclosure timeliness on jurors' liability assessments in the context of cybersecurity incidents. The purpose of this study is to determine how the characteristics and content of cybersecurity incidents' disclosures impact jurors' liability assessments. Specifically, this study explores how jurors react to management forthcomingness (i.e., timeliness) in disclosing the incident and to the plausibility of the explanations provided to justify the disclosure strategy (i.e., timing). This study is relevant in light of the increased incidence of cybersecurity attacks and their associated cost[1]. Moreover,

[1]The 2018 Ponemon Institute report on the cost of data breaches indicates that the average cost of a data breach is around $3.86 million, about $148 for each lost or stolen record containing sensitive information (Ponemon 2018). The report shows that the U.S. is the country with the highest average cost of a data breach ($7.91 million). These costs include detection and escalation costs, notification costs, and post data breach costs (including help desk

studying the litigation risk associated with companies' disclosures of cybersecurity incidents is timely considering recent media attention to high profile cybersecurity incidents, such as the Yahoo! Inc. (Yahoo) and Equifax breaches. For instance, Yahoo is undergoing the first securities class action lawsuit in connection with two cybersecurity incidents that, Yahoo's alleges, occurred in 2013 and 2014 but were discovered and announced in 2016. [2] [3] The timeliness aspect has gained media attention after the SEC announced an investigation into the timing of the disclosures (Fung 2017). Moreover, early in September 2017, Equifax announced a massive data breach and the announcement was made six weeks after the breach was discovered. The timing of the disclosure is being questioned following reports that three Equifax executives, including the Chief Financial Officer (CFO), engaged in insider trading after the breach was discovered but before the announcement (Haselton and Lee 2017).

Drawing on Skinner's (1994, 1997) Litigation Reduction Hypothesis, which suggest that earlier financial disclosures reduce expected legal costs, I predict that more (less) timely disclosures will decrease (increase) jurors' liability assessments. Moreover, I further explore the impact of disclosure timeliness on jurors' liability assessments drawing on Correspondence Inference Theory (CIT), which posits that individuals assess whether the behavior is intentional (internal attribution) or accidental (external attribution) based on the most likely alternative, after weighing all the potential choices. Accordingly, I predict that more (less) timely disclosures

activities, investigative activities, legal expenditure, and identity protection services, among others). The average cost of detection and escalation costs, notification costs, and post data breach costs in the U.S. are $1.21 million, $0.74 million, and $1.76 million, respectively. Also, the average lost business costs in the U.S. is $4.20 million; the U.S. being the country with the highest average notification costs, post data breach costs, and lost business costs.

[2] Studying the potential consequences of securities class action litigation is also important considering the spike in the volume of securities class action cases in 2016. According to a report on recent trends in securities class action litigation released by NERA Economic Consulting, is the highest number of filings since the 2000 dot-com crash (NERA Economic Consulting 2017).

[3] Yahoo's shareholders filed a securities class action lawsuit against Yahoo alleging that they failed to disclose that users' data was not encrypted with an up-to-date and secure encryption scheme.

result in weaker (stronger) correspondence of inferences about a company's intention to act opportunistically, hereafter referred as causal attributions. [4] I also predict that stronger causal attribution towards a company's intent to act opportunistically lead jurors to generalize their inferences about the company and, in turn, mediate the relationship between disclosure timeliness and jurors' liability assessments. Lastly, I predict that the relationship between disclosure timeliness and causal attributions is moderated by the plausibility of management justifications for their disclosure strategy.

To test my predictions, I use a 2 x 3 between-subjects experiment in which participants are required to assess a company's liability after a cybersecurity incident. The independent variables of interest are the timeliness of the disclosure (more timely versus less timely) and the plausibility of management's justification for the company's disclosure strategy (plausible, implausible, and control group with no justification). Specifically, the timeliness of the disclosure is manipulated by informing participants that the incident was disclosed *three days*, for the more timely condition, or *three months*, for the less timely condition, after the company became aware of the incident. The plausibility of management's justifications is manipulated by including a quote in which the defendant's attorney justifies the company's disclosure strategy. Specifically, in justifying less timely disclosures, plausible justifications include allegations that the delay was necessary to disclose accurate facts, while implausible justifications include allegations that the delay was required to disclose accurate facts but the initial facts released were not accurate. In contrast, in justifying less timely disclosures, plausible justifications include allegations that the company traded-off accuracy for timeliness and that accurate

[4] Correspondence is defined as "the extent that the act and the underlying characteristics or attributes are similarly described by the inference" (Jones and Davis 1965, 223). Accordingly, in this study correspondence of inference is operationalized as the degree to which an individual believes that behavior was intentional or unintentional.

information was provided in subsequent disclosures, while implausible justifications include allegations that the delay was timely and accurate, which considering the complexities of the event may be perceived as “too good to be true”. After being provided with the case information, participants indicate their perceived causal attributions and evaluate the company’s liability toward the plaintiff.

I find that more (less) timely disclosures decrease (increase) jurors’ liability assessments and weaker (stronger) assessments of causal attributions. I also find that assessments of causal attribution mediate the relationship between disclosure timeliness and jurors' liability assessments. However, the predicted interaction between disclosure timeliness and plausibility is not significant. Evaluation of participants' assessments suggests that more timely disclosures result in weaker assessments of causal attributions, regardless of the plausibility of justifications. Moreover, in contrast with prior research that suggests that the use of remedial tactics results in lower negligence verdicts (Cornell, Warne, and Eining 2009; Reffett 2010), the results suggest that in the context of disclosure timeliness justifications have no such effect. Additional analysis reveal that disclosure timeliness and participants’ preferences (for timeliness or accuracy) drives perceptions of plausibility and that, in turn, perceived plausibility influences assessments of causal attribution and liability.

This study has several practical implications. First, results of this study shed light on the cost of cybersecurity disclosures and inform companies, investors, and analysts. In particular, this study provides evidence that timely disclosures are desirable and help reduce the cost of liability associated with cyber-attacks. Evidence from this study is particularly interesting considering that participants have strong negative reaction to a disclosure delay of three months

while there are known cases of longer delayed disclosures.[5] This study also informs regulators that are currently evaluating disclosure requirements over cybersecurity. In particular, although the findings suggest that justifications are not helpful in reducing liability assessments for companies that delay the disclosure of cyber-attacks, the findings also indicate that jurors are unable to detect when timely disclosures are implausible.

This study adds to the accounting literature on the use of justifications to reduce legal liability and shows that the benefits of justifications are context specific and are not helpful in reducing liability associated with delayed disclosures of cyber-attacks. Last, this study contributes to the literature and theory that documents the link between disclosure timeliness and litigation risk. In particular, this study uses an experimental approach to test and build on the Litigation Reduction Hypothesis and help address limitations from prior archival research that relied on various proxies for timeliness given the lack of concrete data available regarding the timing of bad news disclosures (e.g. Francis, Philbrick, and Schipper 1994; Skinner 1994; Skinner 1997; Donelson, Mc Innis, Mergenthaler, and Yu 2012). An experimental setting provides the means for a cleaner operationalization of this important variable and helps further our understanding of the implications of disclosure timeliness, such as the link of disclosure timeliness and perceived plausibility, causal attributions, and liability.

The remainder of the paper continues as follows. The next section includes a discussion of the background and the theoretical motivations driving the predictions. Section III discusses the methods, including a description of the participants, the task, and the main variables in the

[5] There are known high-profile cyber-attacks for which disclosures were delayed for over a year (e.g. Yahoo, Uber). Also, I obtained data from Audit Analytics from 169 cyber-attacks disclosed between 2007 to 2018. On average disclosures of cyber-attacks are delayed for 55 days. The delay in disclosure range from zero (0) to 1,104 days. About 20% of the disclosure in the data set were disclosed over 60 days after learning about the attack.

analysis. Section IV discusses the results of the hypotheses, and additional analysis and Section V concludes.

Background, Theory, and Hypothesis

Information Security Disclosures

The requirements of the Sarbanes-Oxley Act (SOX) of 2002 for companies to establish and maintain an adequate system of internal controls, which includes the identification and testing of relevant information technology controls, contributed to the increased voluntary disclosure of information security activities by organizations (Gordon, Loeb, Lucyshyn, and Sohail 2006). Research in this area shows that voluntary disclosures concerning information security are positively associated with a company's market value and that disclosures of proactive security measures have the greatest impact (Gordon, Loeb, and Sohail 2010).

More recent debates about the threat of cybersecurity incidents as a national security concern have motivated further actions from the U.S. Congress. For instance, in March 2017 the U.S. Senate Bill 536 (2017) was introduced to create the Cybersecurity Disclosure Act of 2017. This Act will require disclosure of cybersecurity expertise on the board of directors and the nature of such expertise or, in the absence of this expertise in the board, companies should disclose steps that are taken to incorporate a cybersecurity expert onto the board. Further regulation has been enforced at the state level, such as New York State's Cybersecurity Requirements for Financial Service Companies (NYSDFS 2017). This regulation requires financial service companies to implement a cybersecurity program based on the entity's assessment of cybersecurity risks, and that is designed to detect and prevent incidents. The regulation also requires these companies to submit a certification of compliance with the New York State's Department of Financial Services. Companies are also required to maintain a

written cybersecurity policy, to appoint a CISO, to evaluate the qualifications of cybersecurity personnel and provide relevant training, and to maintain and test relevant controls for cybersecurity.

Despite these efforts to promote more transparency regarding how companies manage and control cybersecurity risks and recent efforts to enforce more transparency regarding companies' cybersecurity practices, there is little guidance and concrete requirements regarding disclosure of actual cybersecurity incidents. Although enforcement has not been released by the Securities and Exchange Commission (SEC), their "Corporate Finance Disclosure Guidance: Topic No. 2" (U.S. 2011) provides guidance on the disclosure of cybersecurity risks and cybersecurity incidents by highlighting other mandated disclosures that may require a discussion of cybersecurity. For instance, requirements of Regulation S-K Item 503(c) for risk factor disclosure would apply to the disclosure of cybersecurity if the risks make an investment speculative or risky (SEC 2011). Furthermore, cybersecurity risks or incidents should be disclosed in the Management Discussion and Analysis (MD&A) section of the annual report in instances in which the costs or consequences represent a material event. The SEC also highlights other areas for companies to determine whether disclosures are necessary, such as in the registrant's "Description of Business," the disclosure of "Legal Proceedings" when applicable, and as part of the disclosures to the financial statements. The SEC's "Corporate Finance Disclosure Guidance: Topic No. 2" also provides a reference to applicable accounting standards for guidance on the proper recognition of losses and estimates in the event of a cyber incident. Still, the guidelines furnished by the SEC do not specifically address critical aspects of the disclosure of cybersecurity incidents, such as the timeliness of disclosures.

Current regulatory enforcement that refers to the timeliness of disclosures is only applicable to the disclosure of incidents that result in the breach of personally identifiable information. This is further complicated by the fact that there is not a set of uniform compliance requirements as associated laws are individually enacted by the states. In general, U.S. companies are allowed to delay the disclosure of cybersecurity incidents. In most states, the wording of data breach notification laws, as it relates to time limits and allowed reporting delays, is ambiguous as it prompts for reasonableness at the time of selecting a disclosure strategy. For instance, Arizona requires the disclosure to be made “in the most expedient manner possible, " and Texas requires it "as quickly as possible." Even the compliance requirements in the state of California, which is known for the severity of penalties regarding privacy and consumer protection laws, do not specify time limits. To illustrate, the requirements of the article 7, 1798.29 in the California Information Practices Act of 1977 requires that “the disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.”. Consistent with regulations from other states, California allows for delayed disclosure when this is requested by enforcement agencies: “(c) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made after the law enforcement agency determines that it will not compromise the investigation”.

Disclosure Timeliness and Litigation Risk

The lack of time limit requirements for the disclosure of cybersecurity incidents creates an opportunity for companies to strategically delay such disclosures considering the decision is,

most of the time, at a company's discretion. Nonetheless, unreasonable delays in disclosing cybersecurity incidents may have significant liability implications. Prior literature on voluntary disclosures of bad news finds that these disclosures have an impact on a company's stock market returns and identifies the timeliness of disclosure as a relevant factor that may explain the market behavior (e.g., Skinner 1994). This body of literature documents the potential consequences of delaying the disclosure of bad news and also identifies competing incentives. For instance, sudden stock price declines on earning announcement days may lead investors to perceive that management failed to disclose the bad earnings news promptly and this may result in litigation and loss of reputation (Skinner 1994). Skinner (1994) argues that although timelier disclosures may not prevent litigation, these will undercut the plaintiff arguments about management's failure to disclose the news promptly and will result in a smaller plaintiff class as there will be fewer investors completing transactions during the non-disclosure period. In contrast, there is also an argument that weighs the potential incentives for managers to delay the disclosure of bad news due to career concerns (e.g., performance-based compensation tied to annual results) or given concerns about disruptions in operations (e.g., impact on seasonal sales).

There is archival evidence supporting the legal liability argument about managers' incentive to pre-disclose bad news early. Skinner (1994) reported that companies voluntarily disclose bad news to a greater extent than good news which suggests that management pre-discloses bad news to alleviate liability concerns. This finding is consistent with subsequent research that revealed that managers have a strong tendency to pre-disclose bad news and that more timely disclosures of bad earnings news resulted in lower settlement amounts (Skinner 1997). Similarly, evidence from a sample of securities class-action lawsuits disclosing bad news showed that more timely disclosure of bad news deterred litigation (Donelson et al. 2012).

Despite the apparent evidence suggesting that managers have an incentive to pre-disclose bad earnings, there is conflicting evidence that contradicts the liability argument for voluntary disclosure of bad news given a lack of evidence that companies disclose bad earnings news before the formal earnings announcement date (Francis at al. 1994).

In this study, I draw on the Litigation Reduction Hypothesis (LRH) to develop baseline expectations regarding the impact of disclosure timeliness on jurors' liability assessments. Skinner's (1994, 1997) LRH uses two main arguments to establish that timelier disclosures reduce expected legal costs. First, the LRH explains that timelier disclosures shorten the nondisclosure period and result in a smaller class period. This suggests that there is an economic component to the relationship between disclosure timeliness and litigation risk and that a larger economic impact, given the size of the class period, results in higher litigation risk. Second, LRH explains that timelier disclosures weaken arguments regarding management's failure to disclose on time. This second component of the relationship between disclosure timeliness and litigation risk suggests there is a process by which individuals assign blame or responsibility and that this, in turn, influences the assessment of a company's legal liability. Thus, LRH posits that, regardless of the context of the lawsuit and the arguments of the plaintiff (e.g., regardless of the motivations for the lawsuit), disclosure timeliness will influence jurors' liability assessments. This leads to the first hypothesis:

> **H1**: Less (more) timely disclosure of a cybersecurity incident leads to a greater (lower) likelihood that jurors will find the company liable.

Causal Attribution and Generalization of Inferences

To complement the assumptions of LRH, Jones and Davis' (1965) CIT develops additional expectations that aid in better understanding the relationship between disclosure timeliness and litigation risk as depicted in Figure 1. CIT is a theory within the body of

attribution theories which describes two conditions in the inference process: the assumptions about the actor's (1) knowledge and (2) ability to execute an action. These two conditions help an individual judge whether an act was intentional or whether it was accidental or incidental (also referred to as internal or external attributions, respectively). Correspondence is defined as *"the extent that the act and the underlying characteristic or attribute are similarly described by the inference"* (Jones and Davis 1965, 223). For instance, in the context of delayed disclosure of bad news, the most correspondent inference may be that which assumes with high confidence that the delayed disclosure is a result of the inherent uncertainty of the event (external attribution). Alternatively, the most correspondent inference may be that which assumes with high confidence that the delayed disclosure is a result of management's intention to behave opportunistically (internal attribution). In this study, the term ***causal attribution*** refers to a participant's correspondence of inference about the cause of behavior, such that if a behavior is perceived as intentional (incidental or accidental) the assessment of causal attribution will be higher (lower).

CIT posits that individuals make inferences based on expectations about the behavior of an average person in the same circumstances and that in the existence of competing explanations (intentions) for behavior, an individual will indicate extreme confidence in the causal attribution when one of the intentions is perceived to be much more likely than others (Jones and Davis 1965). I argue that perceiving the delayed disclosure of a cybersecurity incident as an intentional act is more than likely. Prior research shows that managers have career incentives to obfuscate the disclosure of bad news and to strategically time such disclosures (Kothari, Li, and Short 2009). Moreover, the delayed disclosures of high-profile cybersecurity incidents, such as the Target and Neiman Marcus data breaches, have been highlighted in media articles and the media

suggests that these disclosures may have been strategically timed to maintain sales over the holiday's season (e.g., Freifeld 2014).

Consistent with CIT, in the context of delayed disclosures, I argue that jurors will perceive the plaintiff inferences as highly correspondent with the company's behavior and will assume with high confidence that the delayed disclosure is a result of management's intention to behave opportunistically. Accordingly, I expect that less timely disclosures will lead to extreme assessments of causal attribution. Besides, CIT establishes that if the consequences of an act are positive (negative), a perceiver will have more favorable (unfavorable) dispositions toward the actor. Accordingly, I argue that causal attributions should mediate the relationship between disclosure timeliness and liability assessments, such that stronger (weaker) jurors' assessments of causal attribution will increase (decrease) jurors' liability assessments. Based on the above discussion, the second set of hypotheses are stated as:

> **H2a:** Less (more) timely disclosure of a cybersecurity incident leads to stronger (weaker) jurors' assessments of causal attribution.
> **H2b:** Jurors liability assessments will increase (decrease) as jurors' assessment of causal attribution is stronger (weaker).

The Plausibility of Justifications

Considering the complexity of cybersecurity incidents and the challenges that companies face to be able to disclosure accurate and comprehensive information on a timely manner, I argue that companies may be able to use remedial tactics to mitigate the potential negative impact of their disclosure strategy. The literature on the use of justifications for reducing jurors' liability assessments suggests that jurors are less likely to issue negligence verdicts when the defendant apologizes or uses first-person justifications as a remedial tactic (Cornell et al. 2009). Prior literature suggests that remedial tactics may be used to mitigate the negative impact of jurors' affective reactions toward negative outcome information (Reffett 2010). Nevertheless, this

literature also highlights that the use of remedial tactics is only effective when they are perceived as credible (Grenier, Pomeroy, and Reffett 2012). Grenier et al. (2012) studied the credibility of remedial tactics by manipulating the source of internal inspections used as remedial tactics in cases of undetected fraud. The broader theoretical concept of interest is the plausibility of the justifications as a source of credibility.

Plausibility refers to "the credibility or believability of an assertion within the context of a larger argument" (Mitroff and Mason 1983, 199). Prior research suggests that companies' stakeholders are able to identify instances in which management uses self-serving disclosure and blame poor performance on external factors (Barton and Mercer 2005; Kimbrough and Wang 2014). Specifically, Barton and Mercer (2005) in an experimental study found that plausible explanations result in higher analyst's earnings forecast while implausible explanations harm management reputation and result in lower earnings forecast. Moreover, using archival data, Kimbrough and Wang (2014) document that investors use consensus industry and company-specific information to assess the plausibility of management explanations and that companies that provide implausible (plausible) explanations experience significant market penalties (rewards).

From a theory perspective, Kelley's (1973) attribution theory (that extends CIT) explains that one's internal causes (desirable behaviors) are discounted when there is high external justification for an action. Thus, a plausible justification about a company's disclosure strategy should moderate the impact of disclosure timeliness on jurors' assessments of causal attribution such that a plausible justification mitigates the negative impact of less timely disclosure. In contrast, an implausible justification should "backfire" and lead to stronger negative assessments of causal attribution (Barton and Mercer 2005). This leads to the third hypothesis:

H3: The plausibility of justifications moderates the strength of the effect of the timeliness of disclosure on jurors' assessment of causal attribution, such that implausible (plausible) justifications lead to stronger (weaker) jurors' assessment of causal attribution.

Methods

This study employs a 2 x 3 experimental design in which the timeliness of the disclosure (more timely versus less timely) and the plausibility of management's justification for the company's disclosure strategy (plausible, implausible, and no justifications) is manipulated between-participants. Using a sample of jury-eligible participants as a proxy for jurors, I test whether the timeliness of disclosures and the plausibility of justifications impact jurors perceived causal attribution and liability assessments.

Participants

To test the hypotheses, participants that represent jury-eligible individuals who represent eligible jurors in an actual court case similar to that used in the experiment are desired. As such, I recruited 168 participants through Amazon Mechanical Turk (MTurk).[6] Prior research using MTurk workers have found them to be a good proxy for actual jurors (Grenier, Pomeroy, Stern 2014; Gimbar, Hansen, and Ozlanski 2015; Grenier, Lowe, Reffett, and Warne 2015; Brasel et al. 2016; Maksymov and Nelson 2017). Research generally finds that MTurk workers are demographically diverse and are a source of reliable data (Paolacci, Chandler, and Ipeirotis 2010; Buhrmester, Kwang, and Gosling 2011). Screening procedures were conducted to assure participants meet basic criteria for juror eligibility such as being at least 18 years of age and a

[6] The desired sample size was 180 (30 participants per cell) participants. To achieve equal cell sizes, the Qualtrics survey was set-up to randomly assign participants to one of the six experimental conditions and a quota was set-up in Qualtrics to stop collecting data once the desired cell-size was achieved for each experimental condition. There were 432 attempts to complete this study. From the 432 attempts, there were 168 usable responses (28 per cell), 95 incomplete surveys, 82 surveys in which participants failed to meet the qualification criteria, 55incomplete surveys given that participants failed to pass the review questions, and 32 surveys with either a duplicate IP address or Mturk ID.

United States citizen. Also, Grenier, Reffett, Simon, and Warne (2017) encourage the use of additional screening to ensure that the participants are appropriate. Thus, additional screening excluded participants that may have a potential bias toward the case facts including participants that have worked for an insurance company or health provider, lawyers or employees in a law firm, and individuals that have suffered financial loss due to identity theft.

Participants were compensated $2.50 for completing the 20 to 25 minutes task[7]; however, only those that answer all the review questions (including the attention check question) accurately were allowed to complete the study. Access to the experimental materials is restricted to avoid duplicate responses from the same Mturk ID and the same IP address to alleviate issues of repeated participation (Arnold and Triki 2017). [8] As an additional control measure for the quality of the participant pool, only MTurk workers with the "Masters"[9] designation were recruited for this study.

On average, participants are 29 to 38 years old, with slightly liberal political views, and full-time employed. About 52 percent of the participants are female, 99 percent of participants have at least a high school degree and about 50 percent of the participants have at least a bachelor's degree. About 17 percent of the participants have previously served on a jury, 16 percent of participants have been a victim of a cybersecurity attack, and 50 percent of the participants have made personal investments in the common stock of a company.

[7] Compensation is deemed reasonable, considering MTurk workers' average wage of $3.00 (Rennekamp, Rupar, and Seybert 2015).
[8] Consistent with suggestions provided by Arnold and Triki (2017), a reminder about the importance of scientific research was also be presented to discourage participants from participating a second time.
[9] MTurk "Masters" have higher approval rates and low number of abandoned HITs (Farrell et al. 2017).

Task

The experimental materials follow the format used in prior research examining jurors' assessment of auditor's liability. Specifically, consistent with Brasel et al. (2016), participants are first provided background information to educate them on disclosures of cybersecurity risks and practices along with review questions on the material.[10] Participants subsequently received general information about the defendant, Aplus Insurance, which is portrayed as a successful and leading health and well-being company headquartered in California, together with general case facts, such as the date of the data breach, the date the company became aware of the breach, the extent of the breach, the impact of the breach on the company's stock price, and information about an investigation announced by the SEC into the timing of the breach disclosure. [11]

After the provision of summarized case facts, I present the case allegations and the defendant's arguments. The allegations against the defendant resemble those that Yahoo is currently facing. Specifically, the plaintiff arguments claim that the defendant made false and misleading statements by failing to disclose the lack of appropriate encryption of its customers' information. Participants are also informed that the plaintiff presented evidence to support their allegations, which shows that the lack of encryption was not disclosed, and that the timeliness of the disclosure is brought as an allegation of negligence, as it took them eight months to uncover the breach and an additional three months to disclose the breach (only for the not-timely condition). Participants are informed about the defense arguments and evidence provided about

[10] Brasel et al. (2015) also provide background information on additional concepts, such as material misstatements, reasonable assurance, auditor negligence, critical audit matters, and due professional care, relevant to their study. However, my experimental materials are adapted to fit the context of this study such that only background information about financial statements and additional information regarding cybersecurity is presented to participants.

[11] Participants are informed that the attacker gained access to personal information from customers and employees, such as names, birthdays, social security numbers, street addresses, email addresses, and employment information. This is consistent with information frequently targeted by attackers.

actions taken to notify about the breach and to protect affected customers and employees. Also, as part of the arguments from the defense, the defendant's apologies are displayed followed by the defendant's justification for the timeliness of the disclosure. After receiving the judge's instructions, participants are required to answer case questions and to complete a demographics' survey. The case materials were subjected to review and validation by a lawyer with experience in this area of business law.

Independent Variables

The first independent variable is the timeliness of the disclosure. Timeliness is operationalized as the difference between the date when the company learned of the breach and the date the breach was disclosed. Participants are informed about the timeliness of the disclosure when provided with the case facts and the arguments from the plaintiff. Participants in the more timely condition are notified that the company disclosed the incident in three days, while in the less timely conditions participants are notified that the company disclosed the incident in three months.

The second independent variable is plausibility. Plausibility is operationalized as the extent to which the defendant's attorney justifications are more or less plausible. As illustrated in Figure 2, this variable is manipulated at three levels: 1) plausible, 2) implausible, and 3) no justification. Given that the plausibility of an assertion is assessed within the context of a larger argument (Mitroff and Mason 1983), I operationalize plausibility in the context of other relevant case facts and manipulate the accuracy of management disclosures between-subjects to build plausible and implausible conditions. [12] Specifically, given that the case facts state that the

[12] The company, industry, the details about the company's financial condition, and facts about the breach, such as the economic impact and the breach data and discovery date, are fixed between participants. This is consistent with

breach was discovered eight months after the event, it is plausible that the investigation would be complicated and will impede companies' ability to release accurate information about the impact of the breach in a timely manner. In justifying less timely disclosures, plausible justifications include allegations that the delay was necessary to disclose comprehensive and accurate information about the extent of the breach. In contrast, implausible justifications for less timely disclosures, include allegations that the delay was required to disclose all relevant facts but also a caveat to notify that it was later determined that the magnitude of the incident was greater than what was initially disclosed. Participants in the less timely condition are also presented with a timeline of the disclosure timelines that shows that on average, it takes 47 days for a company to disclose a cybersecurity breach of a similar magnitude and argues that the disclosure was made 44 days later than the average disclosure.

Plausible justifications for more timely disclosures include allegations that the company released the news in a timely manner to notify customers and employees about the breach, so they could take actions to protect their identities, and that accurate facts were subsequently disclosed. In contrast, implausible justifications for timely disclosures take the position that the breach was disclosed promptly and that all the facts released were accurate. Considering the complexity of the event and that it went unnoticed for eight months, the timely and accurate release of information may be perceived as "too good to be true." Also, participants in the timely condition are presented with a timeline of the disclosure timelines that shows that on average, it takes 47 days for a company to disclose a cybersecurity breach of a similar magnitude and argues that the disclosure was made 44 days earlier than the average disclosure. See Figure 3 for details. Prior research suggests that it is difficult for unsophisticated users to detect when companies

Barton and Mercer's (2005) operationalization of plausibility in which they manipulated the location of an incident to convey a plausible and an implausible condition.

behave opportunistically (Koonce, Williamson, and Winchel 2010). Similarly, jurors may be unable to detect implausible explanations on their own, and the plaintiff may need to highlight such allegations. Thus, within each experimental condition I include an argument in which the plaintiff implies that the justifications provided by the defendant are not plausible.

Dependent Variables

The first dependent variable of interest is the jurors' liability assessments. In this study, the primary measure of liability assessment is the likelihood that participants find the defendant liable using a 7-point, fully labeled, scale that ranges from "extremely unlikely" (equal to 1) to "extremely likely" (equal to 7).[13]

The second dependent variable is causal attribution. Causal attribution represents the participants' level of confidence in their assessment of causal attribution. The measure of causal attributions is adapted from Koonce et al. (2010). In assessing the causal attribution, participants are first informed about two potential reasons for the timing of the disclosure: 1) that the delay was caused by the company's intent to strategically disclose the cyber-attack to portray the company in a favorable light, or 2) that the delay was caused by the company's difficulty in estimating the extent of the breach due to the inherent uncertainty of the event. Then, participants are required to assess the causal attribution using a 7-point, fully labeled, scale that ranges from "completely incidental" (equal to 1) to "completely intentional" (equal to 7) and then to indicate their level of confidence in their assessment using a 7-point, fully labeled, confidence scale that ranges from "not confident at all" (equal to 1) to "very confident" (equal to 7). Causal attribution

[13] Eutsler and Lang (2015) find that a fully labeled 7-point scale provides the greatest benefits to researchers. They argue that labeling results in many benefits, such as reduced response bias, maximization of variance, maximization of power, and minimization of error. They provide evidence that variance is maximized when using 7-point scales.

then equals the points allocated to the causal attribution question times the participant's level of confidence in their assessment.[14]

Results

Manipulation Checks and Review Questions

To test the effectiveness of the manipulation of disclosure timeliness, I ask participants about their agreement with the following statement: "Aplus Insurance disclosed the breach in a timely manner."15 I find that participants in the timely condition (mean=5.71) agree to a greater extent that Aplus Insurance disclosed the breach in a timely manner, ($F=236.800$, $p<0.001$) compared to participants in the not timely condition (mean=2.07). In addition, to test the manipulation of plausibility, I ask participants about their agreement with the following two statements: "Aplus Insurance's justification for the timing of the disclosure is credible" and "Aplus Insurance's justification for the timing of the disclosure is believable". I find that participants in the not timely/not plausible condition perceived justifications as less plausible (mean=2.89) that participants in the not timely/plausible condition (mean=3.125) but the difference between conditions is not statistically significant. Likewise, participants in the timely/plausible condition assessed justificantions as more plausible (mean=5.375) than participants in the timely/not plausible condition (5.214) but the difference between groups is not statistically significant. This analysis suggest that participants perceived timely disclosures as more plausible and less timely disclosures as less plausible, regardless of the context of justifications (plausible/implausible) manipulated between participants.

[14] The measure of causal attribution is scaled by seven (7) to use 7-point scales in the analysis consistently.
[15] The participants use a 7-point, fully labeled, scale that ranges from "strongly disagree" (equal to 1) to "strongly agree" (equal to 7).

Testing of Hypotheses

Hypothesis 1

H1 predicts that less (more) timely disclosure of a cybersecurity incident leads to a greater (lower) likelihood that jurors will find the company liable. Panel A of Table 1 presents descriptive statistics for the participant's liability assessments. I tested H1 using analysis of variance (ANOVA), and the results are tabulated in Panel B of Table 1.

As indicated in Table 1, I find support for the hypothesized relationship between disclosure timeliness and liability assessments. Consistent the predictions, liability assessments are lower in the timely condition than in the not timely condition ($F=28.161$, $p<0.001$). Two additional measures of liability assessments are also captured. The first measures a juror's verdict, which is a dichotomous variable equal to one (1) if participants assess the defendant as liable, and that otherwise equals zero (0). The second measures the percentage of imposed damages on the company after the participant is informed that a majority of the jury found the company liable and therefore a determination of damages to be awarded needs to be made. The amount of potential damages to be awarded ranges from zero (0) percent to one-hundred (100) percent of the $10 Billion alleged loss. The result of the ANOVA (untabulated) using the two additional measures of liability assessments are qualitatively similar and consistent with the results of the main analysis.

Hypothesis 2

H2a predicts that less (more) timely disclosure of a cybersecurity incident leads to stronger (weaker) jurors' assessments of causal attribution. I present descriptive statistics for participants' assessments of causal attribution in Panel A of Table 2. The results of the analysis of variance (ANOVA), tabulated in Panel B of Table 2, support the hypothesized relationship

and indicate that delayed disclosure of a cyber-attack lead to stronger jurors assessments of causal attribution ($F=42.118$, $p<0.001$).

H2b predicts that jurors' liability assessments will increase (decrease) as jurors' assessments of causal attribution are stronger (weaker). Results of the mediation analysis, following Hayes (2017) process analysis are tabulated in Panel A and Panel B of Table 3.[16] As shown in Panel A of Table 3, I find a positive and significant relationship between delayed disclosures and assessment of causal attribution ($t=2.541$, $p=0.060$) and between assessments of causal attribution and liability assessments ($t=8.506$, $p<0.001$). Moreover, inspection of bootstrap confidence intervals for the analysis of indirect effects, included in Panel B of Table 3, confirms the hypothesized mediation.[17]

Hypothesis 3

H3 predicts that the plausibility of justifications moderates the strength of the effect of the timeliness of disclosure on jurors' beliefs about a company's intention to act opportunistically, such that implausible (plausible) justifications lead to stronger (weaker) jurors' beliefs about a company's intention to act opportunistically. I present descriptive statistics for participants' assessments of causal attribution in Panel A of Table 2. As shown in Panel B of Table 2 and Panel B and Panel C of Table 3, the results of ANOVA ($F=0.128$, $p=0.440$) and conditional Process analysis ($t=-0.082$, $p=0.467$) does not support the predicted interaction between disclosure timeliness and plausibility of justifications.

[16] I use Hayes (2017) Process model 7 to test moderated mediation.
[17] The analysis of bootstrap confidence interval does not include zero which denotes statistical significance (Hayes 2017).

Additional Analysis

Perceived Plausibility

Given the results, I conducted additional analysis to examine whether an ANOVA would be feasible by creating an alternative binary variable using the median cut-off of participants perceived plausibility. The analysis results in cell-sizes of 40 participants in the timely-plausible condition and 43 participants in the non-timely-implausible condition. In contrast, there are only 16 participants in the timely-implausible and 13 participants in the non-timely-plausible condition. The results suggest that disclosure timeliness is driving participants' perceived plausibility. The results of Chi-square test of independence are statistically significant (Chi-square=25.016, $p<0.001$) and confirm that perceptions of timeliness and plausibility are not independent.

Mercer's discussion of the impact of inherent plausibility on the credibility of management disclosures suggest that perceived plausibility is not objective and may not be necessarily related to the actual plausibility or credibility of a disclosure. In contrast, Mercer suggests that perceived plausibility depends on the extent to which information deviates from expectations and prior believes. As such. I conducted additional analysis to determine whether disclosure timeliness and jurors' preferences impact perceived plausibility and, in turn, jurors' assessments of causal attribution and liability. In particular, I collected data about participants' preference for accuracy (Prefer_Accuracy). Participants indicated their agreement with the following statement: "Aplus Insurance's should have emphasized more on disclosing comprehensive and accurate information about the cyber-attack than in disclosing the information on a timely manner". Then, I conducted mediation analysis using disclosure timeliness as the independent variable, plausibility, preference for accuracy, and the interaction

of plausibility and preference for accuracy with timeliness as covariates, perceived plausibility and causal attribution as mediators, and liability assessment as the dependent variable.

Descriptive statistics reveal that on average, participants have more preference for timeliness than for accuracy (mean=3.74). As shown in Panel A of Table 4 and as illustrated in Figure 4, I find that delayed disclosures and preference for accuracy lead to lower assessments of plausibility ($t=-6.368$, $p<0.001$ and $t=-2.598$, $p=0.005$, respectively). However, evidence of a negative and statistically significant interaction ($t=5.245$, $p<0.001$) between preference for accuracy and timeliness (delayed disclosures) confirms that participants preferences drive perceptions of plausibility. Specifically, this significant interaction suggests that participants in the more timely condition with higher preference for accuracy, over timeliness, perceived justifications as more plausible. The analysis also shows that higher perceptions of plausibility lead to lower assessments of causal attribution ($t=-11.543$, $p<0.001$). However, in contrast with the results of the main analysis, the relationship between causal attribution and liability assessments is only marginally significant ($t=1.268$, $p=0.103$). This finding, together with evidence from bootstrap analysis, as shown in Panel B of Table 4, suggest that the impact of timeliness on liability assessments is mediated by jurors' perceptions of justifications plausibility.

Perceived Timeliness

I collected additional data to capture how participants beliefs and expectations influence their perceptions of timeliness. First, I developed a four-item formative construct to capture participants' perceptions that delayed disclosures of cyber-attacks are acceptable (Delay_Acceptable). Using 7-point scales participants indicated their agreement with the following statements: 1) "delaying the disclosure of a cyber-attack is acceptable given the

increased sophistication of hacking techniques", 2) "delaying the disclosure of a cyber-attack is acceptable given the complexity of determining the scope of the breach", 3) "delaying the disclosure of a cyber-attack is acceptable to conduct required investigations", 4) "delaying the disclosure of a cyber-attack is acceptable even when there is loss of identifiable information from customers and employees".[18] Principal components analysis (PCA) confirms that all items load on the same construct with item loadings above the 0.5 threshold (Nunally 1978). Moreover, I confirmed that the VIF is below 3.3 (Diamantopoulos and Siguaw 2006) for all items.[19] As such, I use the average value of the four items as a single Delay_Acceptable measure for the analysis. Moreover, to capture participants perceptions of companies' incentives to delay disclosure (Delay_Incentive) participants indicated their agreement with the following statement: "managers have more incentives to disclose bad news on a timely basis than incentives to delay the disclosure of bad news".

Evaluation of the single items individually and the Delay_Acceptable formative construct reveal that the timeliness of disclosure is driving participants' perceptions that delayed disclosures of cyber-attacks are acceptable and perceptions of companies' incentives to delay disclosure. Specifically, timely disclosures lead to higher assessments that delayed disclosures are acceptable (mean=3.714) and that companies have more incentives to disclose bad news on a timely basis (mean=4.024), compared to delayed disclosures with means of 2.632 and 2.940, respectively. Although the additional data was collected to explore other potential determinants

[18] I developed this construct with formative items. In contrast with reflective constructs, in a formative construct causality flows from the items to the construct (Diamantopoulos and Siguaw 2006). The four items included measure whether delayed disclosures in the context of cybersecurity breaches are acceptable based on context specific complexities of cyber-attacks or personal preferences.

[19] For formative constructs, Petter, Strub, and Rai (2007) suggest using PCA, rather than traditional EFA, to assess construct validity and to assess collinearity (i.e., VIF < 3.3) to evaluate the construct's reliability.

of perceived timeliness, Chi-square test of independence (untabulated) is significant and shows that disclosure timeliness is not independent from perceptions that delayed disclosures of cyber-attacks are acceptable (Chi-square=37.55, p=0.021) and perceptions of companies' incentives to delay disclosure (Chi-square=19.222, p=.004).

Conclusion

The purpose of this study is to explore the impact of disclosure timeliness and the plausibility of management justifications on assessments of causal attribution and liability. I predict and find that more timely disclosure lead to more favorable assessments of causal attribution and liability and that assessments of causal attribution mediates the relationship between disclosure timeliness and liability. However, I was unable to find evidence that the use of justifications (plausible or implausible) help reduce liability.

This study has relevant implications for companies, investors, and analysts interested in understanding the cost of cybersecurity. In particular, the findings of this study suggest that a company's forthcomingness in disclosing the breach, even without disclosing all the facts, could help reduce the liability associated with cybersecurity breaches. Studying the cost of litigation in the context of cyber-security is pertinent considering that post data breach costs, including legal expenditures, represent one of the main cost drivers of cybersecurity incidents in the U.S. (Ponemon 2018). Having a broader understanding of the cost of cybersecurity could help companies to manage their cyber-risks effectively and help inform analysts and non-professional investors decisions. Also, this study provides evidence that suggests that jurors have difficulty assessing when justifications are plausible and implausible, and as such, justifications could be used opportunistically by companies trying to reduce their litigation risk. This finding is relevant for regulators and standard setters interested in promoting timely disclosure of cybersecurity.

This study also add to the literature on the use of remedial tactics to reduce litigation and provide evidence that such remedial tactics are not necessarily useful in reducing liability associated with delayed disclosure of cyber-attacks. Moreover, this study contributes to theory via the Litigation Reduction Hypothesis by developing and testing a more comprehensive model for explaining jurors' judgment and decisions making (JDM) processes. Specifically, I provide evidence of the significant influence of disclosure timeliness and perceived plausibility, based on participants beliefs and preferences, on assessments of causal attribution leading to final liability assessments.

The results should be evaluated in light of the inherent limitations. For instance, a limitation in studying the cost of litigation, using jurors' liability assessments, is that many times the plaintiff and the company try to reach a settlement. However, it is still important to study jurors' judgment and decision making given that the settlement outcomes are many times influenced by the potential outcomes of jury trial (Maksymov, Pickerd, Lowe, Peecher, and Reffett 2017). Moreover, it is possible that the results of this study may not be generalized to other type of participants, such as investors and analysts, given the differences in background and knowledge and individual preferences. As such, future research could explore the impact of disclosure timeliness in other contexts, such as judgments and decisions of financial statement users.

References

Arnold, V., and A. Triki. 2017. Use of student and online participants in behavioral accounting research. In *The Routledge Companion to Behavioral Research in Accounting,* edited by T. Libby and L. Thorne**,** forthcoming.

Bodin, L. D., L.A. Gordon, and M.P. Loeb. 2005. Evaluating information security investments using the analytic hierarchy process. *Communications of the ACM, 48*(2), 78-83.

Barton, J., and M. Mercer. 2005. To blame or not to blame: Analysts' reactions to external explanations for poor financial performance. *Journal of accounting and economics*, *39*(3), 509-533.

Boettrich, S., and S. Starykh. 2017. Recent Trends in Securities Class Action Litigation: 2016 Full-Year Review. *Nera Economic Consulting,* January 2017.

Brasel, K., M.M. Doxey, J.H. Grenier, and A. Reffett. 2016. Risk disclosure preceding negative outcomes: The effects of reporting critical audit matters on judgments of auditor liability. *The Accounting Review*, *91*(5), 1345-1362.

California Security Breach Information Act, CAL. CIV. CODE §§ 1798.29, 1798.82–.84 (West 2009)

Cornell, R. M., R.C. Warne, and M.M. Eining. 2009. The use of remedial tactics in negligence litigation. *Contemporary Accounting Research*, *26*(3), 767-787.

Diamantopoulos, A., and J.A. Siguaw, 2006. Formative versus reflective indicators in organizational measure development: A comparison and empirical illustration. *British Journal of Management*, 17(4), 263-282.

Donelson, D. C., J. M. McInnis, R. D. Mergenthaler, and Y. Yu. 2012. The timeliness of bad earnings news and litigation risk. *The Accounting Review*, *87*(6), 1967-1991.

Eutsler, J., and B. Lang. 2015. Rating scales in accounting research: The impact of scale points and labels. *Behavioral Research in Accounting*, *27*(2), 35-51.

Francis, J., D. Philbrick, and K. Schipper. 1994. Shareholder litigation and corporate disclosures. *Journal of accounting research*, 137-164.

Freifeld, K. 2014. U.S. companies allowed to delay disclosure of data breaches. *Reuters*, January 16, 2014.

Fung, B. 2017. The SEC is reportedly probing Yahoo over its data breaches. *The Washington Post*, January 23, 2017.

Gimbar, C., B. Hansen, and M.E. Ozlanski. 2015. Early Evidence on the Effects of Critical Audit Matters on Auditor Liability. *Current Issues in Auditing*, *10*(1), A24-A33.

Grenier, J. H., D.J. Lowe, A. Reffett, and R.C. Warne. 2015. The effects of independent expert recommendations on juror judgments of auditor negligence. *Auditing: A Journal of Practice & Theory*, *34*(4), 157-170.

Grenier, J., B. Pomeroy, and A. Reffett. 2012. Speak up or shut up? The moderating role of credibility on auditor remedial defense tactics. *Auditing: A Journal of Practice & Theory*, *31*(4), 65-83.

Grenier, J. H., A. Reffett, C. Simon, and R.C. Warne. 2017. Researching juror judgment and decision making in cases of alleged auditor negligence: methodological considerations. *Behavioral Research in Accounting*, Forthcoming.

Haselton T, and Y.N. Lee. 2017. Three Equifax executives sold $2 million worth of shares days after cyberattack. CNBC. Available at: https://www.cnbc.com/2017/09/07/equifax-cyberattack-three-executives-sold-shares-worth-nearly-2-million-days-after-data-breach.html

Hirst, D. E., K. E. Jackson, and L. Koonce. 2003. Improving financial reports by revealing the accuracy of prior estimates. *Contemporary Accounting Research*, *20*(1), 165-193.

Jones, E. E., and Davis, K. E. (1965). From acts to dispositions the attribution process in person perception. *Advances in experimental social psychology*, *2*, 219-266.

Jones, E. E., and K. E. Davis. 1965. From acts to dispositions the attribution process in person perception. *Advances in experimental social psychology*, *2*, 219-266.

Kadous, K. 2001. Improving jurors' evaluations of auditors in negligence cases. *Contemporary Accounting Research*, *18*(3), 425-444.

Kelley, H. H. 1973. The processes of causal attribution. *American psychologist*, *28*(2), 107.
Kimbrough, M. D., and I.Y. Wang. 2013. Are seemingly self-serving attributions in earnings press releases plausible? Empirical evidence. *The Accounting Review*, *89(2*), 635-667.

Koonce, L., M.G. Williamson, and J. Winchel. 2010. Consensus information and nonprofessional investors' reaction to the revelation of estimate inaccuracies. *The Accounting Review*, *85*(3), 979-1000.

Kothari, S. P., X. Li, and J. E. Short. 2009. The effect of disclosures by management, analysts, and business press on cost of capital, return volatility, and analyst forecasts: A study using content analysis. *The Accounting Review*, *84*(5), 1639-1670.

Maksymov, E. M., and M.W. Nelson. 2016. Malleable standards of care required by jurors when assessing auditor negligence. *The Accounting Review*, *92*(1), 165-181.

Maksymov, E.M., J. Pickerd, J.D. Lowe, M. Peecher, and A. Reffett. 2017. Toward a more complete theory of audit legal dispute resolution: insights from prominent attorneys. Working paper.

Mellers, B. A., A. Schwartz, K. Ho, and I. Ritov. 1997. Decision affect theory: Emotional reactions to the outcomes of risky options. *Psychological Science, 8*(6), 423-429.

Mercer, M. 2004. How do investors assess the credibility of management disclosures? *Accounting Horizons*, 18(3), 185-196.

New York State Department of Financial Services (NYSDFS). 2017. *Cybersecurity Requirements for Financial Service Companies.* 23 NYCRR 500. New York.
Nunnally, J. C. 1978. *Psychometric theory*, McGraw-Hill, New York.

Paolacci, G., J. Chandler, and P.G. Ipeirotis. 2010. Running experiments on amazon mechanical turk. *Judgment and Decision Making, 5*(5), 411.

Petter, S., D. Straub, and A. Rai. 2007. Specifying formative constructs in information systems research. *MIS Quarterly*, 31(4). 623-656.

Ponemon Institute. 2018. 2018 Cost of Data Breach Study: Global Overview. *Ponemon Institute Research Report*, July 2018.

Reffett, A. B. 2010. Can identifying and investigating fraud risks increase auditors' liability? *The Accounting Review, 85*(6), 2145-2167.

Reffett, A., B.E. Brewster, and B. Ballou. 2012. Comparing auditor versus non-auditor assessments of auditor liability: An experimental investigation of experts' versus lay evaluators' judgments. *Auditing: A Journal of Practice & Theory, 31*(3), 125-148.

Rennekamp, K., K.K. Rupar, and N. Seybert. 2015. Impaired Judgment: The Effects of Asset Impairment Reversibility and Cognitive Dissonance on Future Investment. *Accounting Review, 90*(2), 739-759.

Shepperd, J. A., and J.K. McNulty. 2002. The affective consequences of expected and unexpected outcomes. *Psychological Science, 13*(1), 85-88.

Skinner, D. J. 1994. Why firms voluntarily disclose bad news. *Journal of accounting research, 32*(1), 38-60.

Skinner, D. J. 1997. Earnings disclosures and stockholder lawsuits. *Journal of Accounting and Economics, 23*(3), 249-282.

U.S. Security and Exchange Commission Division of Corporation Finance (SEC). 2011. CF Disclosure Guidance: Topic No. 2 Cyber Security.

US. Security and Exchange Commission (SEC). 2018. Commission Statement and Guidance on Public Company Cybersecurity Disclosures. Available at https://www.sec.gov/rules/interp/2018/33-10459.pdf

STUDY TWO: INVESTORS' JUDGMENTS AND DECISIONS AFTER A CYBERSECURITY BREACH: UNDERSTANDING THE VALUE RELEVANCE OF CYBERSECURITY RISK MANAGEMENT ASSURANCE

Introduction

Cyber-breaches have drawn increased scrutiny due to their increasing frequency and magnitude of occurrence, and the associated financial impact on companies and investors. In response to these concerns, the American Institute of Certified Public Accountants (AICPA) is proposing new voluntary assurance services to address the information needs of users regarding company's cybersecurity activities and aiming to standardize associated reporting frameworks. Because use of the proposed services and the associated framework developed by the AICPA is voluntary, organizations' decision to engage in cybersecurity risk management assurance (CRM) is primarily risk-based. The AICPA acknowledges that it is the organization and its stakeholders who would drive the adoption of these services (AICPA 2017a). Prior research suggests that companies' underinvestment in cybersecurity may be a result of limited evidence regarding the benefits of such investments (Gordon, Loeb, Lycyshyn, Zhou 2015b). Consequently, this study answers a call for research by the AICPA (AAA 2017) to better understand the cost of cyber-security breaches, users' associated information needs, and how and why CRM assurance may be feasible and desirable for an organization.

The purpose of this study is twofold. First, I examine whether knowledge about a firm's engagement in voluntary CRM assurance, prior to a cyber-breach, affects non-professional investors' judgments and decisions, after the breach. Second, I investigate whether the changes in investors' judgments and decisions differ in magnitude depending on whether CRM assurance violates or conforms to industry norms. Although prior accounting research that explore the benefits of voluntary assurance document greater stock price assessments (Brown-Liburd and

Zamora 2014) and lower cost of capital (Dhaliwal, Zhen Li, Tsang, and Yang 2011), some studies suggest that the benefits of assurance are context specific and are only significant when the assured information is positive (Coram, Monroe, and Woodliff 2009) and relevant to the company (Cheng, Green, and Chi Wa Ko 2015). Thus, the value relevance of voluntary assurance in the context of cybersecurity is a very different proposition given that cyber-breaches, to some degree, are believed to be unavoidable. As such, I aim to explore whether the benefits of voluntary assurance hold in the context of CRM assurance when assurance fails to prevent liability. Moreover, in contrast with recent research that explores the effect of joint or separate provisioning of CRM assurance and cyber-breaches on investors' willingness to invest (Perols and Murthy 2018), I take a step back and assess the value relevance of voluntary CRM assurance in isolation by exploring investors' decision behavior given the presence or absence of assurance in light of market expectations.

The theoretical underpinnings for this study are drawn from Wallace's (1980) work on the economic demand for audits in free markets and the associated Insurance Hypothesis. The Insurance Hypothesis posits that the demand for audit services is driven by their use as a tool to manage a company's liability exposure. Drawing on the Insurance Hypothesis, I predict that CRM assurance is positively associated with investors' valuation judgments. Moreover, consistent with prior studies on investor judgment and decision making, I also predict that assessments of management credibility mediate the effects of CRM assurance on investors' valuation judgments.

A fundamental aspect affecting the value of assurance that is not captured in the voluntary assurance literature is the market expectations for assurance which may differ based on industry norms or other such characteristics creating expectations. Thus, I draw on Expectancy

Violations Theory (EVT) in predicting that the relationship between CRM assurance and assessments of management credibility will be stronger when expectations of a company engaging in assurance services are violated (do not conform to industry norms). Specifically, I predict that investors' assessments of management credibility will be more favorable for companies that engage in voluntary CRM assurance and are not expected to do so compared to companies that engage in voluntary CRM assurance as expected. In contrast, investors' assessments of management credibility will be less favorable for companies that do not engage in voluntary assurance and are expected to do so compared to companies that do not engage in voluntary assurance, but for which this is the norm.

I test the predictions using a 2 x 2 between-subjects experiment in which participants are required to make valuation judgments and to assess the credibility of management after a cyber-breach. The independent variables of interest are the presence or absence of CRM assurance and the expectancies regarding whether the company should engage in CRM assurance. Specifically, the presence of assurance is manipulated by informing participants that the company has a CRM program in place and operating effectively, and that the company engaged in voluntary assurance over their CRM program and received a clean opinion from the auditors. In contrast, participants in the no-assurance condition are informed that, although the company has not engaged in assurance over their CRM program, the company has a CRM program in place and operating effectively.[20] Moreover, the expectation on whether the company should engage in CRM assurance is operationalized by informing participants that engagement in CRM assurance is expected or not expected based on the behavior of other companies in the same industry. To test the predictions, participants assess the company's stock price value and management's

[20] This design is chosen after examining the trend of current cyber-breach disclosures. We noted that companies usually disclose that they have controls in place and operating effectively.

competence and trustworthiness (the two components of management credibility documented in prior research (e.g., Clor-Proell 2009; Mercer 2004; Mercer 2005; Rennekamp 2012)).

Consistent with the predictions, I find that voluntary CRM assurance, prior to the occurrence of a cyber-breach, results in more favorable investor valuation judgments after a cyber-breach is disclosed. I also find that this relation is mediated by management credibility assessments. The results also support the predicted moderated mediation and provide evidence that the indirect effect of assurance on valuation judgments, through assessments of management credibility, is conditional on whether firms' practices violate or conform-to-expectancies.

Additional analyses explore how investors' perceived benefits of assurance-as-insurance (AAI) and perceived accountants' cyber-expertise (ACE) impact investors' decision behavior. I find that the direct effect of CRM assurance is associated with higher valuation judgments only when users perceived higher benefits of AAI. Moreover, I find that expectancy violations only influence decision behavior for participants that perceived higher accountants' cyber-expertise. Using additional data collected to explore the impact of disclosure of companies' cyber-risk management practices, I find that investors reward (penalize) companies with (without) formal CRM programs in place.

This study has several relevant practical implications. The AICPA is promoting the use of the Trust Services Framework and Criteria, which was recently updated to address cyber-risk management, and is encouraging accounting professionals to use this framework to provide voluntary assurance over CRM. However, prior efforts in promoting similar voluntary assurance services, such as the WebTrust seal of assurance, have largely failed or as in the case of SysTrust morphed into primarily internal services for management (i.e., SOC II reports). As such, a more in-depth understanding of the potential reaction by investors to new assurance services over an

entity's cybersecurity activities is timely in providing additional evidence to the AICPA that may assist in maximizing the benefit of their cybersecurity initiatives. Moreover, the results of this study provide evidence of the perceived value of CRM assurance and shed light on the need for and benefit of such assurance. This evidence informs regulators (such as the SEC) and financial statement stakeholders, trying to promote further disclosure and assurance over companies' cyber-risk practices (AAA 2017; AICPA 2017a; Cohn 2018). The findings of the study suggest that organizations' stakeholders may be able to drive the demand for voluntary CRM assurance, particularly if voluntary CRM assurance becomes expected for specific industries. As such, to create the demand that justifies the cost of voluntary CRM assurance the profession may need to effectively market and promote SOC II and III CRM assurance services.

This study contributes to the literature on investor judgment and decision making. Specifically, this study addresses investors' judgments and decisions after cyber-breaches and adds context to the archival literature on cybersecurity events by aiding in understanding the underlying drivers behind investors decision-making. For instance, this study provides evidence that, in general, market participants value voluntary CRM assurance-as-insurance but the extent of the impact of CRM assurance depends on investors' perceived benefits of assurance-as-insurance and perceived cyber-expertise of auditors. Moreover, although prior research addresses investors' reactions to other types of negative news, these studies generally limit their focus to disclosures of negative financial performance (e.g., bad earnings news). In contrast, using the context of non-financial disclosures (such as cyber-breaches) sheds light on the factors likely driving market reaction towards other types of negative events and disasters.

I also add to the literature and theory that documents the demand for voluntary assurance (Wallace 1980). This study contributes to theory by examining Wallace's (1980) insurance

hypothesis within the investor JDM context. The context of this study enables testing of the insurance hypothesis and supports this theorized explanation of the demand for voluntary assurance in high litigation risk settings. Moreover, this study further contributes to theory by integrating EVT into the theoretical model underlying the insurance hypothesis. The theoretical model developed in this study highlight the role of market expectancies, based on industry norms, in explaining the magnitude of demand for voluntary assurance

The remainder of the paper proceeds as follows. The next section provides background and explains the theoretical motivations driving the predictions. Section III discuss the methods by providing a description of the participants, the task, and the main variables in the analysis. Section IV discusses the results of the hypotheses, and additional analysis and Section V concludes.

Background, Theory, and Hypothesis

The Cost of Cybersecurity Breaches

The incidence of cybersecurity incidents during the late 1990s and early 2000s and the conflicting views of their economic impact motivated early event studies to determine the cost of security breaches. Some of these event studies examine the impact of specific types of attacks, (such as Ettredge and Richardson 2003), while other studies consider a broader set of incidents (e.g., Campbell, Gordon, Loeb, and Zhou 2003 and Cavusoglu, Mishra, and Raghunathan 2004). Ettredge and Richardson (2003) focused on a single event, the DOS attack of internet companies in 2000, to study the market reaction to cybersecurity incidents. Interestingly, they found that there was an adverse market reaction toward companies that were attacked but also toward similar companies (within the same industry and size) that were not attacked. Other evidence gathered in the late 1990s from US corporations that disclosed an information security breach

suggest that there is a negative stock market reaction to cybersecurity incidents in general (Campbell et al. 2003). However, further analysis revealed that the negative market reaction was only associated with breaches that involved unauthorized access to confidential data (Campbell et al. 2003). The findings provide evidence that the nature of an event is a relevant piece of information for market participants. Those results are consistent with the results of Cavusoglu et al. (2004). Cavusoglu et al. (2004) reported an average 2.1 percent decrease in companies' market value within the two days surrounding the disclosure of a data breach. Additional cross-sectional analysis revealed that smaller companies and internet companies were more penalized than their counterparts and that the significant adverse market impact had been increasing over the years.

To reconcile mixed findings reported in early event studies regarding the impact of cybersecurity incidents on stock market returns and to explore a potential shift of investors' assessments over time, Gordon, Loeb, and Zhou (2011) analyzed evidence of stock returns over the 1995-2007 period. This study confirmed prior findings of significant negative stock market returns for companies that experienced a security breach, regardless of the type of breach. Also, their study found evidence of a downward shift in the impact of security breaches on stock market returns following the 9/11/2001 attacks. Two possible explanations may explain this downward shift: "1) more effective remediation and disaster recovery and 2) a perceived decrease in the tendency of customers to refrain from doing business with companies experiencing an information security breach" (Gordon et al. 2011, 33).

Cyber-risk Management

Concerns about the continued growth of cybersecurity incidents and the perceived failure of companies to adequately invest in cybersecurity, motivated the early accounting research on

cyber-risk management. These events and concerns lead to the development of economic models to determine the optimal investment in information security. For instance, the Gordon and Loeb (2002) model was developed to determine the optimal level of investment and resources that companies should allocate to secure their information. Their model proposed that increased vulnerability to data loss increases the optimal investment in information security; however, the model also acknowledged that for extreme levels of vulnerability the benefit of information security investment is minimal as the cost may overweight the benefits of the investment. Accordingly, the model established that the optimal investment in information security should be determined by evaluating the reduction in expected loss and not necessarily considering the vulnerability alone. Overall, the model proposed that the optimal investment in information security should not exceed 37% of the expected loss. The model was later extended as the authors acknowledged the importance of considering the cost of externalities to determine the optimal investment in information security (Gordon, Loeb, Lucyshyn, and Zhou 2015a).

Additional research on the economic aspects of preventing security breaches considers the use of cybersecurity insurance and information sharing in the discussion of information security investment practices. Gordon, Loeb, and Sohail (2003) discussed the importance of cyber-risk management to assess the optimal investment in information security but included the use of cybersecurity insurance as a relevant piece of information to be utilized for the cost-benefit analysis necessary to determine the optimal investment in cybersecurity following the Gordon and Loeb model. Gordon et al. (2003b) posited that to conduct this analysis requires companies to determine the dollar value of their information security risk exposure, after considering information security controls in place to reduce such exposure, and then to assess insurance coverage. Other factors to reduce the cost of preventing data loss were also examined.

For instance, Gordon, Loeb, and Lucyshyn (2003) documented the potential benefits of the federal government initiative, back in the early 2000s, of information sharing between companies about threats to computer security and the incidence of security breaches. Their analysis showed that information sharing lowered the cost of information security; however, the lack of incentives for companies to share information prevented the realization of such potential benefits (Gordon et al. 2003).

Models to determine the optimal investment in information security do address the qualitative factors and non-financial criteria that should be considered in evaluating the optimal information security investment. To illustrate, Bodin, Gordon, and Loeb (2005) proposed the use of an analytic hierarchy process as a tool to evaluate and compare relevant criteria for information security decisions. Bodin et al. (2005) emphasized the role of the Certified Information Security Officer (CISO) in evaluating the qualitative factors and non-financial criteria. Subsequently, Bodin, Gordon, and Loeb (2008) introduced a new risk metric to complement the analytic hierarchy process tool earlier proposed by Bodin et al. (2005). Over time, researchers have continued using new techniques to develop models to help companies assess their cybersecurity insurance needs (e.g., Mukhopadhyay, Chatterjee, Saha, Mahanti, and Sadhukhan 2013).

More recent literature highlights the top management team composition and their compensation structure as a relevant aspect of cyber-risk management. For instance, Kwon, Ulmer, and Tawei (2013) showed that the involvement of an IT executive in the top management team and the amount of compensation (fixed and variable) for the IT executive is negatively related to the incidence of information security breaches. This finding stresses the importance of

the involvement of IT experts for strategic decision making and cyber-risk management in organizations.

This body of research has significantly contributed to the development of risk management practices which are relevant to IT governance decision making (Debreceny 2013) and for compliance with regulatory requirements to disclose significant risk factors (SEC 2011, 2018). Furthermore, the objectives behind the early developed economic models for information security investment are still being applied and are consistent with current best practices, as well as the principles of risk assessment and risk response in the Enterprise Risk Management (ERM) framework developed by the Committee of Sponsoring Organizations' (COSO).

Assurance over Information Security

The Sarbanes-Oxley Act (SOX) act of 2002 requires management of public companies to assess the effectiveness of internal controls and requires auditors, under SOX section 404, to attest on management's assessment of internal controls (US 2002). Auditing Standard No. 5 (AS5) provides guidance for auditors to conduct an audit of management's assessment of the effectiveness of internal controls over financial reporting (ICFR) and establishes that, as part of the audit of internal controls, auditors should understand and evaluate the effectiveness of information technology general controls (PCAOB 2007). Accordingly, in connection with the audit of a company's ICFR, auditors are required to understand and evaluate controls over information security, such as controls to ensure that logical access to critical applications is restricted to only authorized users. Although there is an overlap between information security and cybersecurity controls, the scope of an audit of internal control is limited to controls relevant to financial reporting, as required by AS5, regardless of whether an application beyond the scope of the audit hosts critical data that could be the target of a cyber-breach.

Recent initiatives are being promoted to standardize the disclosure of companies' cybersecurity risk management and controls. For instance, early in 2017, the AICPA released an updated edition of the Trust Services Principles and Criteria (TSPC) and a newly developed cybersecurity risk management reporting framework. The TSPC was revised to better address an organization's cybersecurity risks and to align the prior version of the TSPC with the Committee of Sponsoring Organizations of the Treadway Commission's (COSO's) Internal Control Framework updated in 2013. The TSPC provides a mechanism for CPAs interested in performing attestation over the security, availability, processing integrity, confidentiality, and privacy of information systems in an organization.[21]

The cybersecurity risk management reporting framework was developed by the AICPA as a means for communicating relevant information about a company's cyber-risk management practices to stakeholders. CPAs are expected to use the framework to evaluate an organization's cyber-risk management practices and to report on the effectiveness of controls. The ultimate goal of this initiative is to promote the use of a uniform reporting framework and to increase stakeholders' confidence in a company's cybersecurity disclosures. In particular, the AICPA is promoting the use of a system and organization control (SOC) reporting framework for cybersecurity (AICPA 2017a). A SOC is an examination engagement that should be performed in accordance with AICPA attestation standards. The use of this reporting framework provides a uniform set of criteria for disclosure and the assessment of the effectiveness of a company's cyber-risk management practices. According to the AICPA (2017a), this reporting framework is meant to be voluntary and flexible to be suitable for organizations of varying sizes and

[21] More details of the AICPA cybersecurity initiative, the revised Trust Services Principles and Criteria, and the SOC over cybersecurity is provided at the AICPA's cybersecurity resource center. http://www.aicpa.org/InterestAreas/FRC/AssuranceAdvisoryServices/Pages/cyber-security-resource-center.aspx

industries. The AICPA is also developing other CRM assurance products, such as a SOC for cybersecurity specific for vendor supply chains (AICPA 2017b).

Despite the development of a new assurance framework to specifically focus on cybersecurity risks, it is not the first time that the accounting profession has tried to address concerns about the security, availability, processing integrity, confidentiality, and privacy of information systems. During the late 1990s and early 2000s, the AICPA and the Canadian Institute of Charter Accountants (CICA) developed SysTrust and WebTrust, which are a set of principles and criteria to assure the reliability of information systems and e-commerce transactions, respectively (Gendron and Barrett 2004). In contrast with current motivations associated with the increased incidence and magnitude of cyber-breaches, the development of SysTrust and WebTrust was motivated by the demand for assurance services to address system reliability (McPhie 2000) and the emergence of the internet and online transactions (Barett and Gendron 2006). SysTrust was initially designed to provide assurance over systems that support business activities and to focus specifically on the principles of availability, security, integrity, and maintainability (McPhie 2000). In contrast, WebTrust was developed to specifically address electronic commerce transactions and to focus on the principles of security, availability, business practices, and transaction integrity (Elliott 2002). The SysTrust and WebTrust principles and criteria were later merged into a single framework, the Trust Services Principles, and Criteria. This framework evolved into a more comprehensive framework that covers the principles of security, availability, processing integrity, confidentiality, and privacy and it is currently used by auditors to issue SOC 2 and SOC 3 reports.[22]

[22] There are three types of SOC reports. SOC 1 reports are used by auditors to provide assurance over internal controls over financial reporting (ICFR) to user organizations. In contrast, SOC 2 and SOC 3 are used to provide assurance over, all or any combination of, the Trust Services framework principles. The difference between the SOC 2 and SOC 3 reports is that SOC 2 reports are for restrictive use while SOC 3 reports are intended to meet the needs

The development of Web assurance services, in particular, the WebTrust seal, motivated early research on voluntary third-party assurance.[23] Overall, researchers found that Web assurance positively influenced consumers intentions to purchase online (Kovar, Burke, and Kovar 2000; Kaplan and Nieschwietz 2003) and that consumers could differentiate the quality of Web assurance seals (Lala, Arnold, Sutton, and Guan 2002). Although these initial findings seem to suggest that consumers valued third-party assurance, subsequent research failed to support the notion that external assurance results in incremental benefits for consumers. Specifically, Mauldin and Arunachalam (2002) found that Web assurance is only associated with higher intentions to purchase when consumers do not observe disclosures about internal assurance and are less familiar with the product. Bahmanziari, Odom, and Ugrin (2009) extended these findings, showing that external Web assurance did not impact consumers' trust or purchase intentions, neither on its own nor when interacting with internal assurance activities.

Although WebTrust was initially expected to be successful (Elliot 2002), the rate of companies engaging in Web assurance was lower than expected (Barrett and Gendron 2006). This triggered intrigue regarding the profession's behavior and researchers in accounting began to study WebTrust through the lenses of the professionalization of accounting (Gendron and Barrett 2004; Barett and Gendron 2006) and managerial decision-making (Boulianne and Cho 2009) to further develop an understanding of the factors that contributed to the development, adoption, and, eventually, the perceived failure of the WebTrust seal of assurance. By conducting field study research, Gendron and Barrett (2004) found that accountants perceived that organizations were skeptical about the potential of WebTrust to provide additional comfort

of users who desire assurance on the controls of a service organization but do not have the need of a SOC 2 report. (Singleton 2011).

[23] Companies that received an unmodified opinion in their WebTrust report were allowed to display the WebTrust seal on their websites.

and increase consumers trust. This finding was mainly attributed to the existence of competing products sponsored by large technology organizations and available at a lower cost. Further evidence revealed that the profession failed to properly allocate marketing resources to promote their proposed Web assurance service and companies perceived that the benefits were not sufficient to justify the necessary marketing cost (Boulianne and Cho 2009). Other researchers questioned whether the accounting profession was misguided to focus on assurance targeted to individual consumers (Sutton and Hampton 2003) and argued for a focus on business-to-business and supply chain related activities where accounting professionals had reputational advantages (Khazanchi and Sutton 2001; Sutton and Hampton 2003). The challenges faced by the accounting profession in establishing a reputation and demand for Web assurance resulted in the transformation of WebTrust into a set of principles and criteria (in particular, first used together with SysTrust and eventually merged with SysTrust into a single framework, the Trust Services principles and criteria) to be used for advisory and business-to-business assurance services (Gendron and Barrett 2004; Barret and Gendron 2006).

Theoretical Model

The theoretical model in this study is based on Wallace's (1980) Insurance Hypothesis and EVT ((Burgoon and Hale 1988; Burgoon 1993). The insurance hypothesis addresses why organizations may desire assurance irrespective of regulatory demands and provides a conceptual foundation for exploring sources of the demand for voluntary assurance over cybersecurity. The Insurance Hypothesis particularly argues that users value and demand voluntary assurance as an alternative to traditional insurance products used to control for litigation risk. As illustrated in Figure 5, the model predicts that CRM assurance is positively associated with investors' valuation judgments and that this relation is mediated by investors' perceptions of management

credibility. Then, drawing on EVT, I propose that expectancies should influence the strength of the demand modeled in the Insurance Hypothesis. In particular, I predict that expectancies of assurance will alter the strength of the relationship between voluntary assurance and perceived management credibility, which flows through to impact investors' valuation judgments. The theoretical model presented in this study incorporates these considerations to better explain why investors might expect a company to engage in such services and how these expectancies alter investors' assessments of management credibility and related valuation judgments.

Voluntary Assurance and the Insurance Hypothesis

Wallace (1980) explains the reasonableness behind using assurance services as insurance, relative or as a complement of using traditional insurance policies with four main arguments. First, the perceived need for auditors to substantiate professional care, which may be beneficial to argue against allegations of negligence in a litigation setting. These effects should also carry over to other company stakeholders that may have concerns related to perceptions of due care. Second, Wallace highlights how clients benefit from the auditors' sophisticated legal expertise which allows the use of the auditor as a powerful codefendant. Third, the client and auditor's shared interest and concern about their reputations ensures proper consideration of the impact of litigation. Last, Wallace argues that by engaging in assurance services companies can shift a portion of the blame and liability toward the auditor, as auditors are generally perceived as the guarantors of the accuracy of audited financial and non-financial information.

Findings from prior research show that voluntary assurance results in higher stock price assessments (Brown-Liburd and Zamora 2014) and lower cost of capital (Dhaliwal et al. 2011). In contrast, other research documents that the benefits of assurance are context specific. For instance, Coram et al. (2009) find that assurance of non-financial performance indicators

influence stock price estimates only when presenting positive indicators and Cheng et al. (2015) find that assurance of sustainability indicators increase willingness to invest when assured information is relevant to the company. I argue that the demand for CRM assurance, in the context of this study, is primarily motivated by Wallace's (1980) Insurance Hypothesis as among the main concerns regarding cyber-breaches are the litigation risks, company reputation, and the associated costs.[24]

In developing the baseline expectations, I consider the arguments that justify the use of voluntary assurance to mitigate potential legal damages and prior findings on the positive impact of voluntary assurance. As such, theoretically, companies that report a cyber-breach, but have previously engaged in voluntary CRM assurance, should receive less negative investors' valuation judgments. This leads to the first hypothesis:

> **H1:** Voluntary CRM assurance (no-assurance), prior to the occurrence of a cyber-breach, will result in less negative (more negative) investor valuation judgments after the disclosure of a cyber-breach.

Voluntary Assurance and Management Credibility

Findings from prior research suggest that companies engage in voluntary assurance services, mainly, to enhance their credibility and reputation (Simnett, Vanstraelen, and Chua 2009). For instance, Pflugrath, Roebuck, and Simnett (2011) find that assurance increased the credibility of CSR reports. I predict that management engagement in CRM assurance will result in more favorable assessments of management credibility, after the disclosure of a cyber-breach,

[24] We argue about the Insurance Hypothesis as the more likely source of demand for cybersecurity assurance considering the nature of cybersecurity threats. In particular, given the sophistication of cyber-breaches, companies may be unable to reduce the risk and potential loss associated with a cyber-breach through the implementation of internal controls alone. As such, the use of cybersecurity insurance is a likely resource that firms can use to share their cyber-risk, either as an alternative or complement to other potential controls to reduce or avoid cyber-risks. Besides, we expect that the information regarding the presence or absence of assurance after a cyber-breach will impact investors' judgments as the expected future loss will be lower given the use of assurance as insurance.

given two main reasons: 1) prior research establishes that audited disclosures are more credible than unaudited disclosures (e.g., Brown-Liburd and Zamora 2014; Dhaliwal et al. 2011; Mercer 2004), and 2) the benefits of using CRM assurance-as-insurance may lead to more favorable assessments of management competence given investors beliefs that management's decisions are in their best interest. Moreover, I predict that management credibility assessments will, in turn, impact valuation judgments. These arguments lead to the following hypotheses:

> **H2a:** Voluntary CRM assurance (no-assurance), before the occurrence of a cyber-breach, will result in less negative (more negative) investors' assessment of management credibility after the disclosure of a cyber-breach.
> **H2b:** Assessments of management credibility mediate the effects of CRM assurance on investors' valuation judgments.

Expectancy Violations Theory

Another aspect relevant to understanding the demand for CRM assurance is whether investors take into consideration the consensus use of such services (whether assurance is expected or not expected) by peer companies within the same industry. Prior research suggests that investors' evaluation of a company depends on whether the company's accounting choices conform to the industry norms (Clor-Proell 2009; Koonce, Miller, and Winchel 2015). Moreover, Mercer (2004, 192) argues that *"a disclosure that deviates significantly from investors' expectations will be less credible than one that does not."* This effect is conceptualized in expectancy violations theory (EVT) (Burgoon and Hale 1988; Burgoon 1993) which provides a theoretical basis for understanding why voluntary CRM assurance would have similar effects when engaging in such assurance services is considered an industry norm.

EVT establishes that individuals develop expectancies to assess communication outcomes and that these expectancies are influenced by the communicator characteristics, relationship factors, and context characteristics (Burgoon and Hale 1988; Burgoon 1993).

Expectancies are violated when the communication outcomes are not in conformity with expectations or preferences about social norms and known idiosyncrasies (Burgoon and Hale 1988). EVT posits that the impact of a violation depends on the violation valence, such that positive violations produce favorable communication consequences while negative violations are detrimental compared to outcomes that conform-to-expectancies. As such, it is expected that the arousal that is triggered by the violation results in an intensification of evaluations of the communicators.

As such, consistent with EVT, I predict that violation of expectancies will result in more extreme assessments of management credibility (see Figure 5, Panel B for predictions), such that positive violations (presence of assurance when it is not expected) result in more extreme positive assessments of management credibility and negative violations (absence of assurance when assurance is expected) result in more extreme negative assessments of management credibility. Moreover, I predict that investors' assessments of management credibility, based on whether the company violates or conforms to the expectations, will mediate the relationship between the presence (absence) of assurance and investor's assessments of future stock prices. This leads to the third set of hypotheses (as illustrated in Figure 5):

> **H3a:** The effect of CRM assurance on users' assessment of management credibility is more extreme in the presence of expectancy violations.
> **H3b:** Assessments of management credibility mediate the expectancies moderated effects of CRM assurance on investors' valuation judgments.

Methods

To test the research model, I use a 2 x 2 experimental design in which assurance (assurance versus no-assurance) and investors' expectations of the presence of assurance (violate-expectancies versus conform-to-expectancies) are manipulated between-participants. A

sample of non-professional investors are recruited to complete the experimental case in order to observe decision behavior. The focus of the experimental study is on how investor decision making changes in light of the presence or absence of assurance based on when company practices violate or conform-to-expectancies.

Participants

Participants are 168 individuals recruited through Amazon Mechanical Turk (MTurk) in exchange for either $1.00 or $2.50, based on their qualifications.[25] [26] [27] Participation is limited to MTurk workers that have completed at least 500 Human Intelligence Tasks (HITs) and with at least a 95 percent approval rate, or alternatively to participants designated as "Masters.[28] Research finds that MTurk workers are a source of reliable data (Buhrmester, Kwang, and Gosling 2011) and that it is an appropriate participant source for research on nonprofessional investors (Koonce et al. 2015).

---

[25] Data for the main analysis was collected concurrently with the data for additional analysis. Initially, I conducted a pilot test using Mturk participants that have at least 500 completed HITs and 95 percent approval rate. The initial desired sample size for pilot testing was 120 (20 participants per cell) participants. After eliminating invalid attempts to complete the survey, the total usable responses was 106. Then, I collected data intended to be used for the main analysis and participants were required to have the Mturk "Masters" qualification. The desired sample size was 180 (30 participants per cell) responses from Mturk Masters. However, I collected 146 usable responses. Given the failure to meet the desired sample size, I merged the responses from the pilot test and the main data collection and setup a Qualtrics quota to achieve equal cell sizes. There were 1,406 attempts to complete this study. From the 1,406 attempts, there were 252 usable responses (42 per cell), 274 incomplete surveys, 497 surveys in which participants failed to meet the qualification criteria, 343 incomplete surveys given that participants failed to pass the review questions or manipulation checks, and 38 surveys with either a duplicate IP address or Mturk ID.

[26] On average, participants spent about 12 minutes to complete the experiment. As such, compensation is deemed reasonable, considering MTurk workers' average hourly wage of $3.00 (Rennekamp, Rupar, and Seybert 2015). Compensation is based on the participant's Mturk qualifications as participants with more HITs completed and with higher approval rates are expected to receive greater compensation considering that these participants have higher approval rates and a low number of abandoned HITs (Farrell, Grenier, and Leiby 2017). Only participants who successfully completed the study and accurately answered all the review questions (including the attention check questions) and manipulation checks were compensated.

[27] The experiment in this study was approved by the Institutional Review Board (IRB) for Human Participants.

[28]" Specifically, 85 participants in the sample have at least 500 completed HITs and 95 percent approval rate and 83 participants that hold the Mturk "Masters" qualification. Amazon grants the "Masters" qualification to workers that consistently demonstrate a high degree of success in performing a wide range of HITs across a large number of requesters. All participants, regardless of their Mturk qualification, are required to meet the additional screening requirements. Participants' demographics are not significantly different between groups, including the time to complete the survey, and the inferences of the study are unchanged when controlling for participant's qualifications as a covariate in the analyses.

I conducted screening procedures to select only participants at least 18 years of age, United States citizens, and that are native English speakers. Also, consistent with prior research that uses MTurk as a source for non-professional investors (e.g., Rennekamp 2012; Koonce et al. 2015; Asay, Elliot, and Rennekamp 2017), participants are required to have taken at least two accounting or finance classes and have experience reading financial statements. On average, participants are 29 to 38 years old and full-time employed. About 60 percent of the participants are male, 72 percent of the participants have at least a bachelor's degree, and 90 percent of the participants have investment experience.[29]

Only participants who successfully completed the study and accurately answered all the review questions (including attention checks) and manipulation checks were compensated. In addition, to alleviate issues of repeated participation, access to the experimental materials is restricted to avoid duplicate responses from the same IP address (Arnold and Triki 2017).[30]

Task

The experimental task requires participants to evaluate a company, based on the information that is available. First, participants are provided with a brief description of the company. I use Aplus Auto Care to resemble a company in the car warranty and related solutions industry. After reading the description of the company, participants are required to make an initial valuation of the company's stock price.

Participants then receive a press release in which the company announces a data breach, along with information regarding the extent of the breach and a link to resources provided by the company to remediate the impact of the breach (e.g., dedicated Website, credit monitoring

[29] 65 percent of the participants have over three years of investment experience.
[30] Consistent with suggestions provided by Arnold and Triki (2017), a reminder about the importance of scientific research was also presented to discourage participants to participate a second time.

services). The format and content of the press release are consistent with press releases used to announce known data breaches, such as the Home Depot, TJ Maxx, and Target breaches. Participants also receive selected financial information about the company, background information on assurance over cybersecurity, and information about the presence or absence of assurance (manipulated between participants). After being provided with all the relevant case facts, participants updated their initial valuation of the company's stock price, answer additional case questions, answer manipulation check questions, and provide demographic information.

Independent Variables

The first independent variable is assurance. Assurance is operationalized by notifying participants whether the company engaged or not in CRM assurance for the fiscal year prior to the breach. For the assurance condition, participants learn that the company ***has*** a cybersecurity risk management program in place, controls are operating effectively, the company engaged in voluntary assurance over cybersecurity, and the auditors issued a clean audit opinion. In contrast, for the no-assurance condition participants will be notified that, although the company ***has not*** engaged in assurance over cybersecurity, the company has a cybersecurity risk management program in place and that controls are operating effectively. Before participants are informed about the presence or absence of CRM assurance, they receive general information about the risk of cyber-breaches and cyber-risk management and assurance. In particular, participants are notified about the AICPA initiative to develop a cybersecurity risk management program and are provided with a description of what a SOC for cybersecurity implies.

The second independent variable is expectancies of the presence or absence of assurance. Expectancy is operationalized by providing participants with information on whether the company's decision to engage (or the decision not to engage) in CRM assurance is consistent or

inconsistent with industry practices. This manipulation was adapted from Clor-Proell's (2009) work on expected and actual accounting choices and tailored to the context of CRM assurance. Consistent with Clor-Proell (2009), participants are first provided with information about the industry expectancies and then they receive information about the firm choice to engage or not engage in CRM assurance. Together, these two manipulations (assurance and expectancies) result in two violate-expectancies (there is assurance and assurance is not expected, or there is no-assurance and assurance is expected) and two conform-to-expectancies (there is assurance and assurance is expected, or there is no-assurance and assurance is not expected) conditions.

Dependent Variables

The dependent variable of interest is investors' perceived value of a company stock price (valuation judgments). The measure of valuation judgments is consistent with the measure used by Asay et al. (2017) that asks for participants' initial valuation judgments (before the manipulations) and for updated valuation judgments after participants are presented with additional information and the manipulations.[31] Valuation judgments are measured using a 7-point, fully labeled, scale that ranges from "very low" (equal to 1) to "very high" (equal to 7).[32] As such, valuation judgment represents a participant's updated valuation judgment using the initial valuation judgment as a covariate.

Management credibility is a mediator in the theoretical model. Consistent with prior research (e.g., Clor-Proell 2009; Mercer 2004; Mercer 2005; Rennekamp 2012), management credibility is measured using participants' assessment of management competence and trustworthiness, the two components of management credibility. To measure participants'

[31] Consistent with Asay et al. (2017), participants are anchored on the scale's mid-point to be able to use the initial valuation as a baseline to measure investor's reactions to the manipulations.
[32] Fully labeled 7-point scales are used consistent with recommendations from Eutsler and Lang (2015).

assessment of management competence and trustworthiness, I use a 7-point, fully labeled, scale that ranges from "very incompetent" (equal to 1) to "very competent" (equal to 7) and from "very untrustworthy" (equal to 1) to "very trustworthy" (equal to 7), respectively. In order to confirm the validity and reliability of the management credibility construct, I first conducted exploratory factor analysis (EFA) and generated the construct Cronbach's alpha. The results of EFA confirmed that assessment of management competence and assessment of management trustworthiness loads into a single construct with factor loadings of 0.790 and 0.784, respectively, while the construct's Cronbach's alpha is 0.934.[33] As such, I use the average value of these two measures as a single measure of management credibility for the analysis.

Results

Manipulation Checks and Comprehension Questions

The experimental materials were pre-tested with a similar participant pool to confirm the success of the study manipulations. Then, the final version of the experiment was released with three main manipulation check questions, three review questions, and one attention check. Only participants who answered all the main manipulation check questions, review questions, and attention checks were allowed to complete the experimental materials.

The two main manipulation check questions to test the manipulation of the presence or absence of assurance asks participants whether or not Aplus Auto Care engaged in CRM practices and CRM assurance, respectively, based on the case information. The main manipulation check question to test the manipulation of expectancies of assurance asks participants whether or not most firms in the industry choose to engage in CRM assurance

[33] Factor loadings and Cronbach's alpha were all above the recommended threshold of 0.50 and 0.70, respectively (Nunnally 1978).

practices, based on the case information. An additional question to test the manipulation of expectancies of assurance is included and asks participants about their agreement with the following statement: "Aplus Auto Care was expected to engage in CRM assurance before the data breach".34 I find that participants in the assurance-expected condition (mean=5.11) agree to a greater extent that Aplus Auto Care was expected to engage in CRM assurance (t=-4.090, p<0.001) compared to participants in the assurance-not-expected condition (mean=4.05).

Review questions are included to ensure that participants understand the information provided in the case. One review question is designed to confirm that participants understand the instructions and two review questions are included to ensure that participants understand the selected financial information presented. An attention check question is also included to ensure that participants are actively engaged in the task.

Testing of Hypotheses

Hypothesis 1

H1 predicts that voluntary CRM assurance (no-assurance), prior to the occurrence of a cyber-breach, results in less negative (more negative) investor valuation judgments after the disclosure of a cyber-breach. Panel A of Table 5 presents descriptive statistics for the participant's final valuation judgments adjusted for initial valuation judgments (initial valuation is a covariate in the model).[35] I tested this prediction using analysis of covariance (ANCOVA), and the results are graphically presented in Figure 6 and tabulated in Panel B of Table 5.

As indicated in Table 5, I find support for the hypothesized relationship between assurance and valuation judgments. Although I do not hypothesize an interaction of assurance

[34]" The participants use a 7-point, fully labeled, scale that ranges from "strongly disagree" (equal to 1) to "strongly agree" (equal to 7).
[35] Unadjusted means are not significantly different and in the same direction as adjusted means.

and expectancies, the analysis considers this interaction to determine the significance of the direct effect from assurance to valuation judgments. Consistent with the predictions, participants in the assurance condition assessed a higher stock value than participants in the no-assurance condition ($F=15.817$, $p<0.001$).

Hypothesis 2

H2a predicts that voluntary CRM assurance (no-assurance), before the occurrence of a cyber-breach, will result in less negative (more negative) investors' assessments of management credibility after the disclosure of a cyber-breach. I present descriptive statistics for participants' assessments of management credibility in Panel A of Table 6. The results of the analysis of variance (ANOVA), tabulated in Panel B of Table 6, support the hypothesized relationship and indicate that assurance is positively associated with assessments of management credibility ($F=54.489$, $p<0.001$). Moreover, H2b predicts that management credibility mediates the relationship of assurance and valuation judgments. Results of the mediation analysis, following Hayes (2017) process analysis, are graphically presented in Figure 7 and tabulated in Panel A and Panel B of Table 7.[36] Inspection of bootstrap confidence intervals for the analysis of indirect effects, included in Panel B of Table 7, confirms the hypothesized mediation.[37] The results suggest that the relationship of Assurance and Valuation Judgments is fully mediated by Management Credibility, as the coefficient of Assurance on Valuation Judgments is not significant ($p=0.797$) when including Management Credibility in the model.

[36] We use Hayes (2017) Process model 4 to test mediation.
[37] The analysis of bootstrap confidence interval does not include zero which denotes statistical significance (Hayes 2017).

Hypothesis 3

H3a predicts that the effect of CRM assurance on users' assessment of management credibility is more extreme in the presence of expectancy violations. As shown in Panel A of Figure 8, the graphical representation of the interaction of assurance and expectancy violations on management credibility is consistent with the predicted pattern. I present descriptive statistics for participants' assessments of management credibility in Panel A of Table 6. The results of the ANOVA, as presented in Panel B of Table 6, shows a significant interaction between assurance and expectancy violations ($F=9.820$, $p<0.001$). As such, I derive contrast weights to test the predicted disordinal interaction. The results of planned contrast analysis, as presented in Panel C of Table 6, confirm that assessments of management credibility are more extreme in the presence of expectancy violations for, both, positive and negative violations. In particular, contrast Weights to test the effect of positive violations on assessments of management credibility (0 for no assurance when assurance is expected, 0 for no assurance when assurances is not expected, -1 for assurance when assurance is expected, and +1 for assurance when assurance is not expected) is marginally significant ($t=1.562$, $p=.061$). Moreover, contrast weights to test the effect of negative violations on assessments of management credibility (-1 for no assurance when assurance is expected, +1 for no assurance when assurances is not expected, 0 for assurance when assurance is expected, and 0 for assurance when assurance is not expected) is significant ($t=2.747$, $p=.004$). Overall, the results support H3a and confirm that investor's expectancies moderate the effect of assurance on assessments of management credibility.

H3b predicts a moderated mediation in which expectancy violations moderate the effects of CRM assurance on investors' valuations through management credibility as a mediator. A graphical representation of the model is included in Panel 2 of Figure 8. To test the model, I

follow Hayes (2017) approach for conditional process analysis.[38] Results of the model estimation are consistent with the ANOVA conducted to test H1 and H2. In particular, there is evidence of a significant positive effect of assurance and the interaction of assurance and expectancy violations on management credibility, as shown in Panel A of Table 8. Inspection of bootstrap confidence intervals for the analysis of conditional indirect effects and the index of moderated mediation, included in Panel B and Panel C of Table 8, confirms the hypothesized moderated mediation.[39] Specifically, the analysis reveals that the effect of management credibility on valuation judgments is larger when expectancies are violated (effect = 0.8970) compared to when Assurance conforms to expectancies (effect = 0.3624) and that the difference in these effects is positive and significant.

Additional Analysis

Perceived Benefits of Assurance-as-Insurance – The Insurance Hypothesis

As discussed earlier, I use the Insurance Hypothesis to theoretically motivate the predicted effect of CRM assurance on investors' valuation judgments. This conceptualization is based on Wallace's four arguments for the insurance hypothesis to explain the demand for voluntary assurance as an alternative to traditional insurance products used to control for litigation exposure. Accordingly, I conducted additional analysis to test whether the perceived benefits of using CRM Assurance-as-Insurance (AAI) influence investors' behavior.

[38] Specifically, following Hayes (2017), the first stage moderation mediation is estimated to assess 1) the direct effect of assurance and the interaction of assurance and expectancy violations on management credibility (the mediator), and 2) the total effect of assurance and management credibility on valuation judgments (the dependent variable). Then, the conditional indirect effect is assessed as the product of the effect of assurance and the effect of the moderation of assurance and expectancy violations on management credibility and the effect of management credibility on valuation judgments, controlling for assurance. The difference between the conditional indirect effect at different values of the moderator (i.e., violate or conform to expectancies) represents the index of moderated mediation used to test the hypothesized relationship. We use PROCESS model 8.

[39] The analysis of bootstrap confidence interval does not include zero which denotes statistical significance (Hayes 2017).

First, I developed a four-item formative construct for participants' alignment with the insurance view of assurance, denoted AAI, based on a review of Wallace's (1980) arguments for the demand for assurance as posited through the insurance hypothesis. In particular, I ask participants about their agreement with beliefs that 1) "cybersecurity audits are necessary to substantiate professional care", 2) "cybersecurity audits are beneficial as they allow the auditor to be used as a codefendant", 3) "cybersecurity audits are beneficial as the auditor and the company shares an interest to protect both of their reputation in case of litigation", and 4) "cybersecurity audits are beneficial as the auditor shares a portion of the company's legal responsibility". To validate the construct's validity and reliability, I conducted principal components analysis (PCA) and tested the items for multicollinearity.[40] PCA corroborates that all items load on the same construct with item loadings above the 0.5 threshold (Nunally 1978). Also, test for multicollinearity shows that VIF is below 3.3 (Diamantopoulos and Siguaw 2006) for all items. Thus, I use the average value of the four items as a single measure of AAI.

I find that, on average, participants agree that CRM assurance is beneficial and can be used as an alternative for traditional insurance (mean=5.338). I used a median split based on the median value (5.375) of the AAI variable to generate a Hi/Low AAI dichotomous variable and then I split the sample and re-run all the hypotheses test for each group (Hi and Low perceptions group) to explore the impact of higher (versus lower) perceived benefits of AAI. I present the results, graphically, in Panel A and Panel B of Figure 9. The results of the ANCOVA, untabulated, shows that CRM only results in higher valuation judgments when investors have higher perceptions of the benefits of AAI. In contrast, CRM assurance is positively associated

[40] In contrast with reflective constructs, formative indicators do not reflect the same underlying constructs and as such multicollinearity is not desirable (Chin, Marcolin, and Newsted 2003). Petter, Strub, and Rai (2007) suggest using PCA, rather than traditional EFA, to assess construct validity and to assess collinearity (i.e., VIF < 3.3) to evaluate the construct's reliability.

with investors' assessments of management credibility for, both, the higher and lower AAI perception groups. On average, valuation judgments are higher for the Hi-AAI assurance (mean=4.37) group than for the Low-AAI assurance (mean=4.15), but not statistically significantly different (t=0.687, p=0.217). However, valuation judgments are significantly higher (t=3.340, p<0.001) for the Low-AAI no assurance (mean=3.93.) group than for the Hi-AAI no assurance group (mean=3.20). In addition, only negative violations remain significant for both groups. Last, the results (untabulated) of the mediation analysis and the mediated moderation analysis hold for both groups.

Altogether, the results suggest that investors' perceptions about the benefits of AAI influences valuation judgments. In particular, results of the ANOVA and inspection of mean valuation judgments between groups, suggest that investors with higher perceptions of the benefits of AAI reward firms that engage in voluntary CRM assurance and penalize firms with no assurance. Also, the results suggest that within these subgroups negative violations result in stronger negative reactions compared to the positive reaction of positive violations.

Perceived Accountant's Cyber-expertise

Prior studies (e.g., Gendron and Barrett 2004) reveal that the perceived accountants' lack of technology expertise may have contributed to the failure of the AICPA and CICA's Web assurance initiatives in the early 2000s. Therefore, I conducted additional analysis to explore participant's perceptions of accountant's cyber-expertise (ACE) and to explore how lower and higher perceptions of ACE affect the main analyses.

Accordingly, I developed a four-item formative construct, denoted ACE, adapted from Brazel and Agoglia's (2007) work on auditor's accounting information systems (AIS) expertise. Brazel and Agoglia's (2007) constructs include five items and is intended to capture aspects of

domain particular-experience and training, which are believed to be the main determinants of auditor expertise (Bonner 1990). While the items in Brazel and Agoglia's (2007) construct were developed as a self-reported measure of auditors' AIS expertise, in general, I adapted their items to capture participants' perceptions of accountant's specific cyber-expertise.41 In particular, I ask participants about their agreement with beliefs that 1) "accountants have significant experience auditing information security and cybersecurity controls", 2) "accountants spend a significant portion of their time auditing information security and cybersecurity controls", 3) "accountants receive significant combined informal and formal training in relation to information security and cybersecurity controls", and 4) "accountants have a high level of information security and cybersecurity controls expertise". Consistent with the analysis to test the validity and reliability of the AAI construct, I conducted PCA and confirmed that all items load in the same construct with item loadings above the 0.5 threshold (Nunally 1978) and also confirmed that VIF is below the 3.3 threshold (Diamantopoulos and Siguaw 2006) for all items. Thus, I use the average value of the four items as a single ACE measure for the analysis.

The analysis reveals that, on average, participants disagree that accountants have the sufficient level of domain particular-experience and training necessary to be considered cyber-experts (mean=3.770). I use a median split based on the median value (3.750) of the ACE variable to generate a Hi/Low ACE dichotomous variable and then I split the sample and re-run all the hypotheses test for each group (Hi and Low ACE) to explore the impact of higher (versus lower) perceptions of accountant's cyber-expertise. I present the results, graphically, in Panel A and Panel B of Figure 10. The analysis (untabulated) shows that assurance is positively associated with valuation judgments and assessments of management credibility, regardless of

[41] All items in Brazel and Agoglia's (2007) AIS expertise construct were included, except for an item that captures auditor's self-reported AIS experience (time) relative to peer auditors.

the level of perceived ACE. Nevertheless, I find that valuation judgments are significantly higher (t=2.109, p=0.018) when participants have higher perceptions of ACE and have assurance (mean=4.51) compared to valuations from the Low-ACE assurance group (mean =4.02). Further, assessments of management credibility for the Hi-ACE assurance group (mean=5.45) are marginally significantly higher (t=1.511, p=0.068) than for the Low-ACE assurance group (mean=5.14) but are not significantly different between the Hi and Low-ACE no assurance conditions. Moreover, the result of planned contrast analysis shows that the interaction of assurance and expectancy violations (both positive violations and negative violations) is only significant for the Hi-ACE group. Finally, the results of the mediation analysis (untabulated) hold for both groups, but the hypothesized mediated moderation is only significant for the Hi-ACE group.

Overall, the results indicate that perceived ACE explains investors' decision behavior when evaluating a firm's value and credibility, in light of information about the presence or absence of assurance and industry expectancies. In particular, the analysis suggests that in evaluating a firm's value and management credibility, participants place more Iight on their own perceptions of the ACE than on the industry consensus (peer firms behavior).

Disclosure of Cyber-risk Management Practices

I also conducted additional analysis to test whether disclosure of the existence (or lack) of management's CRM provides incremental rewards (penalties). In order to explore the value of management's CRM, I collected data for an additional experimental condition in which participants are informed that there is no risk management program and no assurance (84

additional participants were recruited through Mturk).[42] Given that in the main analysis participants in the assurance condition are notified that the firm engaged CRM and CRM assurance, and the participants in the no assurance condition are notified that the firm only engaged in CRM, the additional data collected yields a 3 x 2 experimental design with assurance/risk management (CRM assurance, CRM-only, and no-CRM) and expectancy violations manipulated between groups.

Mean values are graphically illustrated in Panel A and Panel B of Figure 11. Results of contrast Weights (untabulated) support that investors reward firms that disclose the existence of a CRM program. In particular, participants in the CRM-only conform-to-expectancies condition provided higher management credibility ratings (mean=4.40), compared to participants in the no-CRM conform-to-expectancies condition (mean 3.94) and also participants in CRM-only violate-expectancies condition provided higher management credibility ratings (mean=3.65), compared to participants in the no-CRM violate-expectancies condition (mean 3.34).[43] Although on average, valuation judgments for the CRM-only condition are higher than for the no-CRM condition, results do not support that there is a statistically significant difference in valuation judgments between groups in the CRM-only and no-CRM conditions.

Conclusion

This study provides theoretical and empirical evidence of the cost and benefits of voluntary CRM assurance. Specifically, I find that companies engagement in CRM assurance results in more favorable assessments of management credibility, leading to higher stock price

[42] Participant qualifications and screening are performed consistent with the main experiment. Also, participants were required to answer all the review questions (including the attention check questions) and manipulation checks to be allowed to complete the task.

[43] Contrast weights are significant (p=.027) for the assurance expected condition (-1,1,0,0,0,0) and marginally significant (p=.099) for the assurance not expected condition (0,0,-1,1,0,0).

valuations. Moreover, this study finds evidence of positive violations, such that investors reward companies that engage in CRM assurance when assurance is not expected, and negative violations, such that investors penalize companies that do not engage in CRM assurance when assurance is expected, in the context of assurance.

This study has relevant implications. First, this study is particularly informative to the AICPA as it provides evidence that investors knowledge about whether assurance is expected or not expected, based on industry norms, may help drive the demand for the proposed CRM assurance services. Moreover, additional analyses conducted highlights the importance of users perceptions of the benefits of assurance-as-insurance and their perceptions of accountant's cyber-expertise. These results provide insights to regulators expecting that the market will drive the demand for CRM assurance and CRM disclosures. Specifically, the results suggest, in general, it is users with higher perceived benefits of assurance and higher perceptions of accountant's cyber-expertise that primarily reward and penalize companies as initially hypothesized. As such, the results of this study may help better shape the underlying requirements of the AICPA proposed services and may provide insights on relevant aspects to address, such as marketing initiatives to inform users.

Second, this study informs financial statement stakeholders about the cost and incentives associated with voluntary CRM assurance. In addition to the results of the main analysis, additional analysis sheds light on the benefits of CRM disclosures. In particular, I provide evidence of the incentives associated with CRM practices as companies that disclose the existence of a CRM program receive more favorable investors' assessments of management credibility and stock price valuations, compared to companies that do not have a CRM program in place and operating effectively.

Third, this study contributes to the literature and theory on investor judgment and decision making and provides insights on the factors that explain the market reaction toward negative events and disasters, such as cyber-breaches, and the potential use of voluntary assurance to mitigate the damage on firms' value and credibility. In particular, this study provides evidence consistent with Wallace's (1980) insurance hypothesis and supports the benefits of voluntary assurance as a tool to control for litigation outcomes after negative events.

The results should be evaluated in light of the inherent limitations, which provide opportunities for future research. First, in order to explore how users' expectancies impact decision behavior, I operationalized expectancies by providing information about whether the firm's CRM assurance practices violate or conform-to-expectancies. However, whether investors are able to form expectancies, based on the industry cyber-risk, is a question beyond the scope of this study. As such, future research could explore whether the results hold without providing information about expectancies but instead by manipulating the type of industry (using industries with different levels of cyber-risk). Moreover, while in this study I hold constant the information provided about the source of the breach, recent research suggests that management responsibility acceptance influences investor's reactions to external breaches (Tan and Yu 2018). Thus, future research could further explore how managements' internal and external attributions influence the variables in the models and impact decision behavior.

References

American Accounting Association (AAA). 2017. Cybersecurity Risk Management Program Examination Engagements; Panelists: Chris Halterman, Amy Pawlicki, and Paul Steinbart. AAA Mid-Year Meeting of the AIS and SET Sections, January 19, 2017, Orlando, FL.

American Institute of Certified Public Accountants (AICPA). 2017a. SOC for cybersecurity: a backgrounder. Available at: https://www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/ downloadabledocuments/soc-for-cybersecurity-backgrounder.pdf.

American Institute of Certified Public Accountants (AICPA). 2017b. Getting ready for assurance has its benefits. Available at: http://blog.aicpa.org/2017/08/when-getting-ready-for-assurance-is-its-own-benefit.html#sthash.ouX8AaC1.dpbs

Arnold, V., and A. Triki. 2017. Use of student and online participants in behavioral accounting research. In *The Routledge Companion to Behavioral Research in Accounting*, edited by T. Libby and L. Thorne**,** forthcoming. Bodin, L. D., L.A. Gordon, and M.P. Loeb. 2005. Evaluating information security investments using the analytic hierarchy process. *Communications of the ACM*, 48(2), 78-83.

Asay, H. S., W.B. Elliott, and K. Rennekamp. 2016. Disclosure Readability and the Sensitivity of Investors' Valuation Judgments to Outside Information. *The Accounting Review*, *92*(4), 1-25.

Bahmanziari, T., M.D. Odom, and J.C. Ugrin. 2009. An experimental evaluation of the effects of internal and external e-Assurance on initial trust formation in B2C e-commerce. *International Journal of Accounting Information Systems*, 10(3), 152-170.

Barrett, M., and Y. Gendron. (2006). WebTrust and the "commercialistic auditor" The unrealized vision of developing auditor trustworthiness in cyberspace. *Accounting, Auditing & Accountability Journal*, 19(5), 631-662.

Bodin, L. D., L.A. Gordon, and M.P. Loeb. 2008. Information security and risk management. *Communications of the ACM*, *51*(4), 64-68.

Bonner, S. E. (1990). Experience effects in auditing: The role of task-specific knowledge. *Accounting Review*, 65(1), 72-92.

Boulianne, E., and C.H. Cho. 2009. The rise and fall of WebTrust. *International Journal of Accounting Information Systems*, 10(4), 229-244.

Brazel, J. F., and C. P. Agoglia. 2007. An examination of auditor planning judgments in a complex accounting information system environment. *Contemporary Accounting Research*, 24(4), 1059-1083.

Brown-Liburd, H., and V.L. Zamora. 2014. The role of corporate social responsibility (CSR) assurance in investors' judgments when managerial pay is explicitly tied to CSR performance. *Auditing: A Journal of Practice & Theory*, 34(1), 75-96.

Buhrmester, M., T. Kwang, and S.D. Gosling. 2011. Amazon's Mechanical Turk: A new source of inexpensive, yet high-quality, data?. *Perspectives on psychological science*, 6(1), 3-5.

Burgoon, J. K. 1993. Interpersonal expectations, expectancy violations, and emotional communication. *Journal of Language and Social Psychology*, 12(1-2), 30-48.

Burgoon, J. K., and J.L. Hale. 1988. Nonverbal expectancy violations: Model elaboration and application to immediacy behaviors. *Communications Monographs*, 55(1), 58-79.

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.

Chin, W. W., B. L. Marcolin, and P. R. Newsted. 2003. A partial least squares latent variable modeling approach for measuring interaction effects: Results from a Monte Carlo simulation study and an electronic-mail emotion/adoption study. *Information systems research*, 14(2), 189-217.

Cheng, M. M., W. J. Green, and J. Chi Wa Ko. 2015. The Impact of Strategic Relevance and Assurance of Sustainability Indicators on Investors' Decisions. *Auditing: A Journal Of Practice & Theory*, 34(1), 131-162.

Clor-Proell, S. M. 2009. The effects of expected and actual accounting choices on judgments and decisions. *The Accounting Review*, 84(5), 1465-1493.

Cohn, M. 2018. SEC recommends considering cyber threats to accounting controls. *Accounting Today*. Available at: https://www.accountingtoday.com/news/sec-recommends-companies-consider-cyber-threats-to-internal-accounting-controls

Coram, P. J, G. S. Monroe, and D. R. Woodliff. 2009. The value of assurance on voluntary nonfinancial disclosure: an experimental evaluation. *Auditing: A Journal of Practice & Theory*, 28 (1), 137-151.

Dhaliwal, D. S., O.Z. Li, A. Tsang, and Y.G. Yang. 2011. Voluntary nonfinancial disclosure and the cost of equity capital: The initiation of corporate social responsibility reporting. *The accounting review*, 86(1), 59-100.

Diamantopoulos, A., and J.A. Siguaw, 2006. Formative versus reflective indicators in organizational measure development: A comparison and empirical illustration. *British Journal of Management*, 17(4), 263-282.

Debreceny, R. S. 2013. Research on IT governance, risk, and value: Challenges and opportunities. *Journal of Information Systems*, *27*(1), 129-135.

Elliott, R. K. 2002. TInty-first century assurance. *Auditing: A Journal of Practice & Theory*, 21(1), 139-146.
Eutsler, J., and B. Lang. 2015. Rating scales in accounting research: The impact of scale points and labels. Behavioral Research in Accounting, 27(2), 35-51.

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.

Farrell, A. M., J.H. Grenier, and J. Leiby. 2017. Scoundrels or stars? Theory and evidence on the quality of workers in online labor markets. *The Accounting Review*, 92(1), 93-114.

Gendron, Y., and M. Barrett. 2004. Professionalization in action: Accountants' attempt at building a network of support for the WebTrust seal of assurance. *Contemporary Accounting Research*, 21(3), 563-602.

Gordon, L. A., and M.P. Loeb. 2002. The economics of information security investment. *ACM Transactions on Information and System Security*, *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, and T. Sohail. 2003. A framework for using insurance for cyber-risk management. *Communications of the ACM*, *46*(3), 81-85.

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

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

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. Externalities and the magnitude of cyber security underinvestment by private sector firms: a modification of the Gordon-Loeb model. *Journal of Information Security*, *6*(1), 24.

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

Kaplan, S. E., and R.J. Nieschwietz. 2003. A Web assurance services model of trust for B2C e-commerce. *International Journal of Accounting Information Systems*, 4(2), 95-114.

Khazanchi, D. and S.G. Sutton. 2001. Electronic Commerce Assurance Services: A Framework and Implications. *Journal of the Association for Information Systems*, 1(11), 1-54.

Koonce, L., J. Miller, and J. Winchel. 2015. The effects of norms on investor reactions to derivative use. *Contemporary Accounting Research*, 32(4), 1529-1554.

Kovar, S. E., K.G. Burke, and B.R. Kovar. 2000. Consumer responses to the CPA WEBTRUST™ assurance. *Journal of Information Systems*, 14(1), 17-35.

Kwon, J., J.R. Ulmer, and W. Tawei. 2013. The Association between Top Management Involvement and Compensation and Information Security Breaches. *Journal of Information Systems*, *27*(1), 219-236.

Lala, V., V. Arnold, S.G. Sutton, and L. Guan. 2002. The impact of relative information quality of e-commerce assurance seals on Internet purchasing behavior. *International Journal of Accounting Information Systems*, 3(4), 237-253.

Mauldin, E., and V. Arunachalam. 2002. An experimental examination of alternative forms of Web assurance for business-to-consumer e-commerce. *Journal of Information Systems*, 16(s-1), 33-54.

McPhie, D. 2000. AICPA/CICA SysTrust™ principles and criteria. *Journal of Information Systems*, 14(s-1), 1-7.

Mercer, M. 2004. How do investors assess the credibility of management disclosures? *Accounting Horizons*, 18(3), 185-196.

Mercer M. 2005. The fleeting effects of disclosure forthcomingness on management's reporting credibility. *The Accounting Review*, 80(2), 723-744.

Mukhopadhyay, A., S. Chatterjee, D. Saha, A. Mahanti, and S.K. Sadhukhan. 2013. Cyber-risk decision models: To insure IT or not?. *Decision Support Systems*, *56*, 11-26.

Nunnally, J. C. 1978. *Psychometric theory*, McGraw-Hill, New York.

Hayes A. 2017. *Introduction to mediation, moderation, and conditional process analysis: a regression-based approach*, Guilford Press, New York.

Perols, R., and U. Murthy. 2018. The Impact of Cybersecurity Risk Management Examinations and Cybersecurity Incidents on Investor Perceptions. Working Paper.

Petter, S., D. Straub, and A. Rai. 2007. Specifying formative constructs in information systems research. *MIS Quarterly*, 31(4). 623-656.

Pflugrath, G., P. Roebuck, and R. Simnett. 2011. Impact of assurance and assurer's professional affiliation on financial analysts' assessment of credibility of corporate social responsibility information. *Auditing: A Journal of Practice & Theory*, 30(3). 239-254.

Public Company Accounting Oversight Board (PCAOB). 2007. An Audit of Internal Control over Financial Reporting That Is Integrated with an Audit of Financial Statements. Auditing Standard No. 5. Available at: http://pcaobus.org/Standards/Auditing/Pages/Auditing_Standard_5.aspx

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

Rennekamp, K., K.K. Rupar, and N. Seybert. 2015. Impaired Judgment: The Effects of Asset Impairment Reversibility and Cognitive Dissonance on Future Investment. *The Accounting Review*, 90(2), 739-759.

U.S. Security and Exchange Commission Division of Corporation Finance (SEC). 2011. CF Disclosure Guidance: Topic No. 2 Cyber Security.

US. Security and Exchange Commission (SEC). 2018. Commission Statement and Guidance on Public Company Cybersecurity Disclosures. Available at https://www.sec.gov/rules/interp/2018/33-10459.pdf

Simnett, R., A. Vanstraelen, and W.F. Chua. 2009. Assurance on sustainability reports: An international comparison. *The Accounting Review*, 84(3), 937-967.

Singleton, T.W., 2011. IT audit basics: Understanding the new SOC reports. *ISACA Journal*, *2*, p.6.

Sutton, S.G. and C. Hampton. 2003. Risk Assessment in an Extended Enterprise Environment: Re-Defining the Audit Model. *International Journal of Accounting Information Systems*, 4(1), 57-74.

Tan, H. T., & Yu, Y. 2018. Management's Responsibility Acceptance, Locus of Breach, and Investors' Reactions to Internal Control Reports. *The Accounting Review*.

U.S. House of Representatives. 2002. The Sarbanes-Oxley Act of 2002. Public Law 107-204 [H. R. 3763]. Washington, DC: GPO.

Wallace, W. A. 1980. The economic role of the audit in free and regulated markets. *Open Education Resources*, 2. Available at: https://scholarworks.wm.edu/cgi/viewcontent.cgi?referer=https://www.google.com/&httpsredir=1&article=1000&context=oer

STUDY THREE: THE IMPACT OF DISCLOSURE TIMELINESS AND CYBERSECURITY RISK MANAGEMENT ASSURANCE ON INVESTORS JUDGMENTS AND DECISIONS

Introduction

As cyber-attacks become more sophisticated, companies increasingly struggle not only to prevent attacks but also to detect and disclose them in a timely fashion. After a cybersecurity incident is discovered, managers face competing incentives to delay or release bad news. Although managers have incentives to release bad news on a timelier basis to lower litigation costs (Skinner 1994, 1997), managers also have financial incentives to delay or obfuscate the disclosure of bad news (Kothari, Li, and Short 2009). In light of these competing incentives, it is important to understand the factors affecting how investors react to the timeliness of management disclosures. Moreover, one of the main cost drivers of cybersecurity incidents in the U.S. are the post data breach costs, including legal expenditures (Ponemon 2018). As such, understanding investors' reactions to the timeliness of disclosures is even more significant considering that the change in share value, in connection with the disclosure of bad news, is one of the main factors that influences litigation outcomes (Skinner 1994, 1997).

The purpose of this study is twofold. First, I aim to scrutinize how disclosure timeliness impacts investor's judgments and decisions. Second, I explore the use of voluntary cybersecurity risk management (CRM) assurance as a potential tool to mitigate the deleterious effects of delayed disclosures of cybersecurity incidents. This study helps further our understanding of how investors incorporate their perceptions of management's efforts to address complex disclosures in their investment decisions. This understanding is central to studying the impact of cybersecurity disclosures considering that the complexities of addressing cybersecurity breaches may impede company's ability to disclose a breach in a timely manner, and companies

may seek remedial tactics to mitigate potential adverse reactions toward both management and the company for their disclosure strategy. Moreover, this study is important as regulatory bodies, such as the SEC and the AICPA, are actively engaged in developing disclosure guidelines and CRM assurance products to address the increased risk of cyber-attacks. Understanding the value relevance of CRM assurance may help these regulatory bodies to understand and promote the related benefits.

The Litigation Reduction Hypothesis posits that timely disclosures are associated with a lower risk of litigation as a direct result of a reduced economic impact, given a shorter class period that results in a smaller class action, and also indirectly weakens any argument that management delayed the disclosure (Skinner 1994, 1997). Accordingly, drawing on the Litigation Reduction Hypothesis, I predict that the timeliness of disclosures is positively associated with investors' valuation judgments and assessments of management credibility. Consistent with prior research (e.g., Clor-Proell 2009; Mercer 2004; Mercer 2005; Rennekamp 2012), I also predict that assessments of management credibility mediate the effects of disclosure timeliness on investors' valuation judgments. Further, I also draw on the Insurance Hypothesis, which explains the demand for assurance as an alternative to traditional insurance (Wallace 1980), to predict that voluntary CRM assurance moderates the effect of disclosure timeliness on investors' assessment of management credibility.

I use a 2 x 2 between-subjects experiment, in which participants are required to make valuation judgments and to assess the credibility of management after a cybersecurity incident, to test the research model. The independent variables of interest are the timeliness of disclosure of a cybersecurity incident and the presence or absence of CRM assurance. The timeliness of the disclosure is manipulated by informing participants that the incident was disclosed *three days*

(for the more timely condition) or *three months* (for the less timely condition) after the company became aware of the incident. The presence of CRM assurance is manipulated by informing participants that the company engaged in voluntary assurance over CRM and received a clean opinion from the auditors. In contrast, participants in the no CRM assurance condition are informed that, although the company has not engaged in assurance over CRM, the company has a CRM program in place and operating effectively. To test the predictions, I collect participants valuations of the company's stock price and their assessment of management's competence and trustworthiness, the two components of management credibility documented in prior research.

Consistent with the predictions, I find that more timely disclosures lead to more favorable assessments of management credibility and more favorable valuation judgments. Moreover, I find that the relationship of disclosure timeliness and valuation judgments is mediated by perceptions of management credibility. Although I find a significant interaction between disclosure timeliness and CRM assurance, the analysis shows that the positive effect of CRM assurance on credibility assessments and valuation judgments is only significant when a breach is disclosed in a timely manner. Additional analysis reveals that perceptions of disclosure timeliness, in the context of cybersecurity breaches, is mainly driven by the actual timing of the disclosure. These perceptions are also influenced, however, by participants' perceptions of whether delayed disclosure of cybersecurity breaches is acceptable.

The results of this study inform regulators weighing appropriate mechanisms for cybersecurity risk management and disclosure. Specifically, this study sheds light on how the characteristics of cybersecurity disclosures, specifically the information about a company's disclosure timing strategy, is used by investors to assess stock price value. These findings shed light on the benefits of timely disclosures and could help regulators promote timely disclosures

of cybersecurity breaches. The results are also informative to the AICPA and assurance practitioners currently engaged in promoting System and Organization Controls (SOC) for Cybersecurity engagements. The results provide evidence that an important part of management's CRM process should include how communication of an identified breach will be made public to investors in a timely fashion. Thus, assurance practitioners should carefully consider this aspect of management's CRM process when providing CRM assurance.

This study contributes to the literature on market reactions to disclosure timeliness. The results of prior archival research suggest that companies successfully control for the reaction of market participants by delaying the disclosure of bad news and spreading the impact on stock prices over a longer period. Based on these findings researchers imply that, given the efficiency of markets, delayed news is not new information as investors are able to aggregate the information from other more timely sources. This study adds another component to this body of research by examining investors' reaction to the timeliness of disclosures when the facts about the timing are clearly disclosed. This study also contributes to the disclosure timeliness theory by testing both the litigation reduction hypothesis and the insurance hypothesis within the context of investors JDM.

The next section provides background, theory, and hypotheses. Section III discusses the methods by providing a description of the participants, the task, and the main variables in the analysis. Section IV discusses the results of the hypotheses, and additional analysis and Section V concludes.

Background, Theory, and Hypothesis

Disclosure Timeliness and Investment Decisions

The literature provides mixed evidence regarding the market reaction to the timeliness of disclosures. For instance, Givoly and Palmon (1982) found a stronger market reaction associated with earlier earnings announcements than the reaction to late announcements which suggests a decrease in the information content of delayed disclosures. Likewise, in studying the market reaction to dividend announcements, Kalay and Loewenstein (1986) report that delayed disclosures of bad news had a smaller price effect, compared to earlier disclosures of bad news. The authors suggest that market participants appear to set expectations about dividend announcements and then gradually adjust the price downward.

On the other hand, evidence suggests that the market imposes penalties on companies with delayed disclosures. BenYousset and Khan (2016) found that companies with longer restatement disclosure lags experience significantly stronger negative market reactions than companies with shorter disclosure lags. Moreover, research exploring whether managers delay disclosure of bad news, use the magnitude of the stock price reaction to proxy reporting timeliness under the assumption that there is a stronger negative reaction toward companies that withhold negative news (Kothari, Shu, and Wysocki 2009).

Although the archival literature provides some evidence of the impact of disclosure timeliness, only a handful of experimental studies indirectly address the market reaction associated with the timing of disclosures. Mercer (2005) establishes the timeliness of the disclosure as an important predictor of investors' perceived disclosure forthcomingness. Mercer (2005) provided evidence that management forthcomingness in disclosing bad news is positively associated with investors' assessments of management credibility. Libby and Tan (1999)

similarly report results that suggest that management forthcomingness, operationalized by warning participants about unexpected earnings, is positively associated with analysts' assessments of management credibility. Together these studies provide some evidence that suggests that more forthcoming, and perhaps more timely, disclosures may result in positive market reactions.

Further research is needed to explore gaps in the literature. Given that prior literature suggests that management credibility is positively associated with investment decisions, additional research could provide insight on how disclosure forthcomingness (i.e., timeliness) impacts investors' valuation judgments. These insights would add to the cumulative knowledge on disclosure forthcomingness by capturing the effect of disclosure timeliness. Isolating the effect of disclosure timeliness may shed light on how investors evaluate a company's disclosure strategy and provide clarity to the mixed findings reported in prior archival studies.

Disclosure Timeliness and the Litigation Reduction Hypothesis

Prior research on bad earnings news indicates that more timely disclosures are associated with lower settlement amounts (Skinner 1997) and overall lower incidences of litigation (Donelson, McInnis, Mergenthaler, and Yu 2012). These findings are attributed to the litigation reduction hypothesis which suggests that "more timely disclosure of bad news leads to lower expected legal costs" (Skinner 1997, 251). The legal rationale for this phenomena is explained, in the context of bad earnings news, using the SEC disclosure requirements which mandate prompt announcements of material facts regarding a company's financial condition and the timely disclosure of any material fact regarding a previous disclosure that has become misleading (Skinner 1997). Accordingly, the more timely disclosure of bad news is expected to deter litigation motivated by allegations of non-compliance with SEC-mandated disclosures.

Skinner (1997) challenges conflicting evidence reporting that pre-disclosure of bad earnings news does not deter litigation (Francis 1994) and finds that the timeliness of disclosures reduces the likelihood of stockholder litigation and for companies that undergo litigation, the magnitude of litigation outcomes is negatively related to the timeliness of disclosures. Skinner (1994, 1997) claims that timely disclosure of bad earnings news shortens the nondisclosure period and weakens the arguments that management failed to disclose the news resulting in fewer potential plaintiffs and legal damages and lower settlement cost. Further, pre-disclosure of poor performance is believed to reduce litigation risk considering that timelier disclosures "spread the stock price decline over multiple dates" (Healy and Palepu 2001) before the earnings announcement date; in turn, litigation motivated by a sudden stock price decline is less likely.

Consistent with federal securities laws, public companies are required to disclose timely, comprehensive, and accurate information about risks and events relevant to an investment decision (SEC 2011, SEC 2018). Although there are no specific disclosure requirements that address cybersecurity incidents, the Securities and Exchange Commission's (SEC) "Corporate Finance Disclosure Guidance: Topic No. 2" (U.S. 2011) highlights other mandated disclosures, such as the disclosure of significant events in the Management Disclosure and Analysis (MD&A) section of the annual report, that may require companies to disclose cybersecurity incidents if the cost and consequences represent a material event. As such, consistent with prior literature on timely disclosure of bad earnings news and considering that similar disclosure requirements will be applicable, I argue that more timely disclosure of cybersecurity incidents will deter litigation, leading to lower expected legal costs. The delayed disclosure of cybersecurity incidents should put investors at greater risk due to increased exposure to legal liability; in turn, the perceived failure of management to contain the damage results in investors'

lower performance expectations and lower valuation judgments. This leads to the first hypothesis:

> **H1:** More (less) timely disclosure of a cybersecurity incident, will result in more favorable (less favorable) investors' valuation judgments.

Disclosure Timeliness and Management Credibility

Prior research suggests that the observed negative impact of announcements of cybersecurity incidents on a company's market value may be due to investors' perceptions about the loss of reputation and consumer confidence. These expectations impact investors' estimation of future cash flows (Cavosuglu, Mishra, and Raghunathan 2004). Investors' perceptions of management forthcomingness may also explain prior findings that support the litigation reduction hypothesis. For instance, prior research documents a positive relationship between perceptions of disclosure forthcomingness and assessment of management credibility (Libby and Tan 1999; Mercer 2005). Libby and Tan (1999) examined disclosure forthcomingness by warning (or not warning in the case of less forthcomingness) analysts about adverse earnings; in their sample, analysts presented with more forthcoming disclosures assessed higher levels of management integrity compared to analyst presented with less forthcoming disclosures. Mercer (2005) similarly examined management forthcomingness and reported higher investors' assessments of management competence and trustworthiness when management is more forthcoming about bad news. Although the timeliness of disclosure was not a focus of the study, Mercer (2005) identifies disclosure timeliness as one of the factors, along with disclosure completeness and accuracy, which influence investors' perceptions of management forthcomingness. Accordingly, more timely disclosures of cybersecurity incidents should lead to more favorable investor assessment of management credibility.

The assumption that "timely disclosure may enhance managers' perceived competence or credibility, engendering a less severe negative stock price reaction" (Donelson et al. 2012, 1970) suggests that the timeliness of disclosures should impact investors' valuation judgments through investors' assessment of management credibility. As predicted in the first hypothesis, disclosure timeliness is expected to have a direct effect on investors' valuation judgments, but I also expect that investors' assessments of management credibility will mediate the relationship between disclosure timeliness and investors' valuation judgments. This leads to the second set of hypotheses:

> **H2a:** More (less) timely disclosure of a cybersecurity incident, will result in more favorable (less favorable) investors' assessment of management credibility.
> **H2b:** Investors' assessments of management credibility mediate the effects of disclosure timeliness on investors' valuation judgments.

Voluntary Assurance and the Insurance Hypothesis

The baseline hypotheses predict that the timeliness of disclosures will be positively associated with investors' assessments of management credibility and valuation judgments; these predictions are mainly motivated given the negative legal consequences of delayed disclosures of bad news which leads to investors' lower performance expectations and management credibility assessments. Management has competing incentives to delay or accelerate the disclosure of bad news. Although management may have a legitimate reason to delay the disclosure of a cybersecurity incident, research consistently highlights the deleterious impact of this practice. Findings from prior research suggest that companies engage in voluntary assurance services, mainly, to enhance their credibility and reputation (Simnett, Vanstraelen, and Chua 2009). This is explained theoretically by viewing the use of assurance as a remedial tactic. I build on Wallace's (1980) insurance hypothesis to explore the potential usefulness and value of voluntary

assurance as a mitigating factor that may help offset the negative impact of delayed disclosures of bad news.

Wallace (1980) provides four main reasons that explain the demand for audit services as a form of insurance: 1) the need for auditors to substantiate professional care, 2) the use of the auditor as a codefendant, considering the expertise that companies have developed to deal with liability suits, 3) the shared interests between the auditor and the client to protect both of their reputation and to lower any associated legal cost, and 4) the perception that auditors are the guarantor of the information release to investors, which shifts a portion of a company's legal liability to the auditor. Considering these factors, I argue that engaging in voluntary CRM assurance services may be even more valuable in the event of a cybersecurity incident. Considering the unique characteristics of these incidents, such as the complexity to assess damages and the uncertainty around these events, companies may find it challenging to disclose accurate and comprehensive information promptly.

Accordingly, although assurance over CRM should be valuable in any disclosure scenario (regardless the timeliness of disclosure), CRM assurance services should be even more valuable in circumstances where management is unable to make timely disclosures, as the higher the litigation risk, the more the need for insurance. Hence, perceptions about management competence in making decisions on behalf of investors that arise through prior acquisition of voluntary CRM assurance should result in more favorable management credibility assessments and will mitigate the negative impact of delayed disclosures of cybersecurity incidents. This leads to the third hypothesis (See Figure 12):

> **H3:** CRM assurance will have a more (less) positive effect on investor perceptions of management credibility in the presence of less (more) timely disclosures.

Methods

A 2 x 2 experimental design is used in which the timeliness of disclosure (more timely versus less timely) and CRM assurance (assurance versus no assurance) are manipulated between-subjects. A sample of non-professional investors is recruited to observe participants' decision behavior. Specifically, this study investigates how the timeliness of disclosure of a cybersecurity incident and the presence or absence of CRM assurance impact investors' valuation judgments and assessments of management credibility.

Design and Participants

I recruited 144 participants through Amazon Mechanical Turk. Prior research suggests that MTurk workers are a source of reliable data (Buhrmester, Kwang, and Gosling 2011) and that the participants drawn from this source are appropriate for research on nonprofessional investors judgment and decisions (Koonce et al. 2015).[44] As an additional control measure for the quality of the participant pool, only MTurk workers that have completed at least 1,000 human intelligence tasks (HITs) and have at least 98% approval rate over their HITs were recruited to complete the study. Also, additional screening was used to select only participants at least 18 years of age, United States citizens, fluent English speakers, that have taken at least two accounting or finance classes and have experience reading financial statements. These screening procedures are consistent with prior research that surveys non-professional investors' recruited from Amazon Mechanical Turk (e.g., Rennekamp 2012; Koonce, Miller, and Winchel 2015;

[44] Initially, the desired sample size was 120 (30 participants per cell) participants. To achieve equal cell sizes, the Qualtrics survey was set-up to randomly assign participants to one of the four experimental conditions. After gathering the data and eliminating invalid attempts to complete the survey, valid responses yield unequal cell-sizes. As such, I setup a Qualtrics quota to achieve equal cell sizes. There were 393 attempts to complete this study. From the 432 attempts, there were 144 usable responses (36 per cell), 35 incomplete surveys, 141 surveys in which participants failed to meet the qualification criteria, 65 incomplete surveys given that participants failed to pass the review questions, and 8 surveys with either a duplicate IP address or Mturk ID.

Asay, Elliot, and Rennekamp 2016). To alleviate issues of repeated participation, responses were screened to avoid duplicate responses from the same IP address or the same MTurk ID (Arnold and Triki 2017).[45]

On average, participants are 29 to 38 years old and full-time employed. About 62 percent of the participants are male, 80 percent of the participants have at least a bachelor's degree, and 91 percent of the participants have some investment experience.

Task

Participants are instructed to evaluate a company for stock price valuation, based on the information available. First, participants receive information about Aplus Insurance, described as a leading corporation in the health and well-being industry. After being provided with a brief description of the company, participants are instructed to make an initial valuation of the company's stock price. Participants then review a press release that announces a data breach. The press release includes information about the disclosure timeliness, the extent of the breach, and resources dedicated to help victims of the attack. Selected financial information and information about the presence or absence of CRM assurance is presented next. Participants are asked to reconsider their initial valuation judgments, and to answer additional case and demographic questions.

Independent Variables

The first independent variable of interest is disclosure timeliness. Timeliness is operationalized as the difference between the date when the company learned of the breach and the date the breach was disclosed. The information about the disclosure timeliness is presented

[45] Consistent with suggestions provided by Arnold and Triki (2017), a reminder about the importance of scientific research will be presented to discourage participants to participate a second time.

as part of the press release. Participants in the more timely condition are notified that the company disclosed the incident within three days, while in the less timely conditions participants are notified that the company disclosed the incident three months after discovery. Moreover, participants are informed whether the disclosure was considered timely or not timely, based on disclosure of similar cyber-attacks.

The second independent variable of interest is voluntary CRM assurance. In both conditions (assurance and no assurance), participants learn that the company has a CRM program in place and that controls are operating effectively. This variable is operationalized by notifying participants whether the company engaged or did not engage in CRM assurance in the fiscal year prior to the incident. Prior to the operationalization of this variable, participants receive information about the benefits of cybersecurity risk management, and are informed about the AICPA cybersecurity risk management guidelines and SOC for cybersecurity engagements.

Dependent Variables

The dependent variable is investors' perceived value of a company's stock price (valuation judgments). This variable is captured as participants' valuation judgments after they receive a description of the company but before the manipulations, and then again after the additional information is presented (after the manipulations).[46] The measure of valuation judgments is represented by the participant's updated valuation judgments, while their initial valuation judgment serves as a covariate. Valuation judgments are measured using a 7-point, fully labeled, scale that ranges from "very low" (equal to 1) to "very high" (equal to 7). [47]

[46]This is consistent with Asay et al.'s (2016) measure of investors' perceived value of a company's stock.
[47] Eutsler and Lang (2015) find that using a fully labeled 7-point scale result in reduced response bias, maximization of variance, maximization of power, and minimization of error.

Management credibility is a mediator in the model. Management credibility represents participants' assessment of management competence and trustworthiness, the two components of management credibility. Participants' assessment of management competence and trustworthiness are measured using 7-point, fully labeled, scales that range from "very incompetent" (equal to 1) to "very competent" (equal to 7) and from "very untrustworthy" (equal to 1) to "very trustworthy" (equal to 7), respectively. The average value of these two measures is used to assess the measure of management credibility.

Results

Manipulation Checks

To test the effectiveness of the disclosure timeliness manipulation, I gathered participants' perceptions of disclosure timeliness by asking participants to indicate the extent to which they agree that the company disclosed the breach on a timely manner using a 7-point, fully labeled, scale that ranges from "extremely disagree" (equal to 1) to "extremely agree" (equal to 7). I find that participants assessment of disclosure timeliness are higher for participants in the timely condition (mean=6.29) than for participants in the not timely condition (2.62). This difference is statistically significant ($F=289.077$, $p<0.001$) which confirms that timeliness was successfully manipulated between participants. Moreover, to confirm the successful manipulation of CRM assurance, I asked participants to indicate whether or not Aplus Insurance engaged in CRM assurance. Only participants that passed the manipulation check were allowed to complete the experiment.

Testing of Hypothesis

Hypothesis 1

H1 predicts that less (more) timely disclosure of a cybersecurity incident leads to more (less) favorable investors judgments. Panel A of Table 9 presents descriptive statistics for participant's final valuation judgments. I tested H1 using analysis of variance (ANOVA) and the results are presented in Panel B of Table 9. The results support the hypothesized relationship between timeliness and valuation judgments ($F=29.426$, $p<0.001$) and suggest that more timely disclosures lead to more favorable investor valuation judgments.

Hypothesis 2

H2a predicts that less (more) timely disclosure of a cybersecurity incident leads to more (less) favorable assessments of management credibility. Panel A of Table 10 presents descriptive statistics for participant's assessments of management credibility. The results of the ANOVA, as shown in Panel B of Table 10, support H2a, and indicate that disclosure timeliness is positively associated with management credibility assessments ($F=41.118$, $p<0.001$). The results are graphically presented in Figure 13.

H2b predicts that management credibility mediates the relationship between disclosure timeliness and valuation judgments. The results of the PROCESS mediation analysis, as shown in Panel A and Panel B of Table 11, confirm the results of the ANOVA and indicate that disclosure timeliness is positively associated with management credibility assessments ($t=3.487$, $p<0.001$) and confirms my expectation that more favorable assessments of management credibility leads to higher valuation judgments ($t=7.872$, $p<0.001$). Moreover, the analysis of the indirect effect of disclosure timeliness and valuation judgments, in particular the evidence from bootstrap confidence interval shown in Panel C of Table 11, confirm that management credibility

mediates the relationship between disclosure timeliness and valuation judgments. This result supports H2b.

Hypothesis 3

H3 predicts that a more (less) positive effect on investor perceptions of management credibility in the presence of less (more) timely disclosures. As shown in Panel A of Table 10, the mean management credibility assessments in the not timely/CRM assurance condition (mean=4.21) is higher than the mean in the not timely/not CRM assurance condition (mean=3.90) and the mean management credibility assessments in the timely/ CRM assurance condition (mean=5.64) is higher than the mean in the timely/no CRM assurance condition (mean=4.94). However, visual inspection of the interaction plot, as shown in Panel B of Figure 13, suggest that assurance has a greater positive impact on the favorability of credibility assessments for the timely condition than for the not timely condition. The simple effects analysis, reported in Panel C of Table 10, confirms a disordinal interaction between timeliness and CRM assurance but the moderation effect of the interaction is in the opposite direction of the hypothesis ($t=2.594$, $p<0.005$). Moreover, while the difference in management credibility assessments between the timely/CRM assurance and timely/no CRM assurance conditions is statistically significant ($t=2.547$, $p=0.006$), management credibility assessments are not statistically significantly different ($t=1.121$, $p=0.132$) between the not timely/CRM assurance and not timely/no CRM assurance. These results do not support H3 and suggest that CRM assurance enhances management credibility only when a breach has been timely disclosed.

Additional Analysis

Perceived Timeliness

To further the understanding of the determinants of perceptions of timeliness in the context of cybersecurity, I collected supplementary data to capture participants' 1) perceptions that delayed disclosures are acceptable (Delay_Acceptable), and 2) participants perceptions of the benefits of timely disclosures (Timely_Benefits). To gather participants perceptions that delayed disclosures are acceptable, participants indicated their agreement with the following statements: 1) "delaying the disclosure of a cyber-attack is acceptable given the increased sophistication of hacking techniques", 2) "delaying the disclosure of a cyber-attack is acceptable given the complexity of determining the scope of the breach", 3) 'delaying the disclosure of a cyber-attack is acceptable to conduct required investigations", 4) "delaying the disclosure of a cyber-attack is acceptable even when there is loss of identifiable information from customers and employees". Moreover, to gather participants perceptions of the benefits of timely disclosures, 1) "timely disclosure of a cybersecurity incident reduces the risk of litigation", 2) "timely disclosure of a cybersecurity incident reduces the risk of lost business", and 3) "timely disclosure of a cybersecurity incident is the right thing to do". Principal components analysis (PCA) confirms that the Delay_Acceptable and the Timely_Benefits are two different constructs and that all items load on a single construct with item loadings above the 0.5 threshold (Nunally 1978). Moreover, as expected for formative constructs, all items have a VIF below 3.3 (Diamantopoulos and Siguaw 2006).[48] As such, I created a Delay_Acceptable and a Timely_Benefits variable using the average of all items for each construct.

[48] PCA is desirable for formative constructs to assess construct validity (Petter, Strub, and Rai 2007).

I used the disclosure timeliness manipulated variable, the Delay_Acceptable variable, the Timely_Benefits variable, and their interaction with disclosure timeliness to explore how these variables impact perceptions of disclosure timeliness. The results of regression analysis, as shown in Table 12, show that there is a positive and statistically significant relationship between disclosure timeliness ($t=3.333$, $p<0.001$) and perceptions that delayed disclosures are acceptable ($t=8.755$, $p<0.001$) with participants' perceptions that the breach was disclosed in a timely manner. Moreover, a significant and negative interaction of disclosure timeliness and perceptions that delayed disclosures are acceptable ($t=-6.681$, $p<0.001$) suggests that delayed disclosures are considered more timely when perceptions that delayed disclosures are acceptable are higher. Overall, the analysis suggests that although the timing of the disclosure is the main determinant of perceived timeliness, there are context specific perceptions that also influence investors disclosure of timeliness and, in turn, influence investors judgments and decisions.[49]

Conclusion

This study explores the impact of the timeliness of cybersecurity breach disclosures and CRM assurance on investors' valuation judgments and management credibility assessments. I predict and find that more timely disclosure of a cybersecurity breach increases management credibility assessments and result in more favorable stock price valuations. I also find that the relationship between disclosure timeliness and valuation judgments is mediated by management credibility assessments.

The results of this study are important considering the evidence of the increasing cost of cybersecurity breaches and in particular the negative market reaction to cyber-attacks. My findings suggest that timely disclosures could help mitigate the negative stock price reaction associated

[49] I used the perceived timeliness variables as a disclosure timeliness measure for the main analysis and the results are consistent and qualitatively similar to the results using the manipulated variable for timeliness.

with the disclosure of cyber-attacks and that a combination of timely disclosure and prior CRM assurance provide the highest benefits. These results are relevant for companies interested in reducing the cost of cyber-attacks and also inform regulators and standard setters, such as the SEC and the AICPA, interested in promoting and developing guidance for cybersecurity disclosures.

I also find that CRM assurance leads to more favorable assessments of management credibility and valuation judgements only when the breach is disclosed in a timely fashion. This finding adds to the literature and theory on voluntary assurance and is relevant for the AICPA and audit practitioners given their current efforts to promote the SOC for cybersecurity. This study highlights the importance of management's ability to communicate a breach in a timely fashion as part of its CRM process and suggests that auditors should be attuned to this need when providing assurance over CRM processes.

Altogether, this study contributes to the literature and theory on the market reaction to disclosure timeliness. While prior archival research argues that there is not a negative market reaction to the timeliness of disclosures given the lack of information content of delayed disclosures (Givoly and Palmon 1982; Kalay and Loewenstein 1986), I provide evidence that timely disclosures are a strong signal that significantly impact investors judgments and decisions. Moreover, evidence from additional analysis suggest that there are context specific perceptions and expectations that drive perceptions of timeliness. This may help explain mixed findings documented in prior research on the market reaction to disclosure timeliness.

This study also brings opportunity for future research to further the understanding on remedial tactics for delayed disclosures. For instance, recent research suggests that management responsibility acceptance influences investor's reactions to external breaches (Tan and Yu 2018). Moreover, results from additional analysis suggest that perceptions that delayed disclosures are

acceptable influence perceptions of timeliness. As such, although the use of management justifications for their disclosure timing strategy is beyond the scope of this study, future research could explore whether management explanations and justifications could help influence perceptions of timeliness and in turn help mitigate the negative impact of delayed disclosures.

References

Arnold, V., and A. Triki. 2017. Use of student and online participants in behavioral accounting research. In *The Routledge Companion to Behavioral Research in Accounting,* edited by T. Libby and L. Thorne**,** forthcoming.

Bodin, L. D., L.A. Gordon, and M.P. Loeb. 2005. Evaluating information security investments using the analytic hierarchy process. *Communications of the ACM, 48*(2), 78-83.

Asay, H. S., W.B. Elliott, and K.M. Rennekamp. 2016. Disclosure Readability and the Sensitivity of Investors' Valuation Judgments to Outside Information. *The Accounting Review*.

Atiase, R. K., L.S. Bamber, and S. Tse. 1989. Timeliness of financial reporting, the firm size effect, and stock price reactions to annual earnings announcements. *Contemporary Accounting Research*, *5*(2), 526-552.

BenYoussef, N., and S. Khan. 2016. Timing of earnings restatements: CEO equity compensation and market reaction. *Accounting & Finance*.

Buhrmester, M., T. Kwang, and S.D. Gosling. 2011. Amazon's Mechanical Turk: A new source of inexpensive, yet high-quality, data?. *Perspectives on psychological science*, *6*(1), 3-5.

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.

Clor-Proell, S. M. 2009. The effects of expected and actual accounting choices on judgments and decisions. *The Accounting Review*, *84*(5), 1465-1493.

Donelson, D. C., J.M. McInnis, R.D. Mergenthaler, and Y. Yu. 2012. The timeliness of bad earnings news and litigation risk. *The Accounting Review*, *87*(6), 1967-1991.

Eutsler, J., and B. Lang. 2015. Rating scales in accounting research: The impact of scale points and labels. *Behavioral Research in Accounting*, *27*(2), 35-51.

Farrell, A. M., J.H. Grenier, and J. Leiby. 2017. Scoundrels or stars? Theory and evidence on the quality of workers in online labor markets. *The Accounting Review*, *92*(1), 93-114.

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

Givoly, D., and D. Palmon. 1982. Timeliness of annual earnings announcements: Some empirical evidence. *The Accounting Review*, 486-508.

Healy, P. M., and K.G. Palepu. 2001. Information asymmetry, corporate disclosure, and the capital markets: A review of the empirical disclosure literature. *Journal of Accounting and Economics*, *31*(1), 405-440.
Kalay, A., and U. Loewenstein. 1986. The informational content of the timing of dividend announcements. *Journal of Financial Economics*, *16*(3), 373-388.

Koonce, L., J. Miller, and J. Winchel. 2015. The effects of norms on investor reactions to derivative use. *Contemporary Accounting Research*, *32*(4), 1529-1554.

Kothari, S. P., X. Li, and J.E. Short. 2009. The effect of disclosures by management, analysts, and business press on cost of capital, return volatility, and analyst forecasts: A study using content analysis. *The Accounting Review*, *84*(5), 1639-1670.

Kothari, S. P., S. Shu, and P.D. Wysocki. 2009. Do managers withhold bad news? *Journal of Accounting Research*, *47*(1), 241-276.

Libby, R., and H.T. Tan. 1999. Analysts' reactions to warnings of negative earnings surprises. *Journal of Accounting Research*, *37*(2), 415-435.

Mercer, M. 2004. How do investors assess the credibility of management disclosures? *Accounting Horizons*, 18(3), 185-196.

Mercer M. 2005. The fleeting effects of disclosure forthcomingness on management's reporting credibility. *The Accounting Review*, *80*(2), 723-744.

Nunnally, J. C. 1978. *Psychometric theory*, McGraw-Hill, New York.

Petter, S., D. Straub, and A. Rai. 2007. Specifying formative constructs in information systems research. *MIS Quarterly*, 31(4). 623-656.

Ponemon Institute. 2018. 2018 Cost of Data Breach Study: Global Overview. *Ponemon Institute Research Report*, July 2018.

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

Rennekamp, K., K.K. Rupar, and N. Seybert. 2015. Impaired Judgment: The Effects of Asset Impairment Reversibility and Cognitive Dissonance on Future Investment. *The Accounting Review*, *90*(2), 739-759.

Simnett, R., A. Vanstraelen, and W.F. Chua. 2009. Assurance on sustainability reports: An international comparison. *The Accounting Review*, *84*(3), 937-967.

Skinner, D. J. 1994. Why firms voluntarily disclose bad news. *Journal of Accounting Research*, *32*(1), 38-60.

Skinner, D. J. 1997. Earnings disclosures and stockholder lawsuits. *Journal of Accounting and Economics, 23*(3), 249-282.

Wallace, W. A. (1980). The economic role of the audit in free and regulated markets. *Open Education Resources*, 2.

GENERAL CONCLUSION

The three studies in this dissertation explore the impact of cybersecurity disclosure and assurance. Study One investigates how jurors react to the timeliness of a cyber-attack announcement and to the plausibility of the explanations provided to justify the disclosure timing. In Study Two I explore whether voluntary CRM assurance, prior to a cyber-breach, affects non-professional investors' judgments and decisions, after the breach, and investigate whether the changes in investors' judgments and decisions differ when CRM assurance practices violate or conform to expectancies, based on industry norms. Study Three explores how disclosure timeliness and voluntary CRM assurance affect investor's assessment of management credibility and valuation judgments.

Findings from Study One confirm the prediction that more timely disclosure leads to more favorable assessments of causal attribution and liability and that assessments of causal attribution mediate the relationship between disclosure timeliness and liability. However, I was unable to find evidence that the use of justifications as a remedial tactic helps reduce liability. Additional anaysis reveals that more timely disclosures lead to greater beliefs that disclosures are plausisible and that perceptions of the acceptability of delayed disclosures also influence plausibility assessments and in turn affect causal attribution and liability assessments.

Evidence of the legal cost of delayed disclosure of cybersecurity breaches, as shown in Study One, informs companies and market participants. Moreover, these findings inform regulators and standard setters interested in promoting timely cybersecurity disclosures. Study One adds to the literature and theory on the use of remedial tactics to reduce litigation and suggests that the benefits of remedial tactics may be context specific. Moreover, this study

contributes to theory via the Litigation Reduction Hypothesis by developing and testing a more comprehensive model for explaining jurors' judgment and decision making (JDM) processes.

Study Two finds that CRM assurance results in more favorable assessments of management credibility and stock price valuations. Moreover, this study finds that investors reward companies that engage in CRM assurance when assurance is not expected and that investors penalize companies that do not engage in CRM assurance when assurance is expected. Evidence from additional analysis provides additional insights on the benefits of having a CRM program, even without the assurance component.

Study Two has relevant implications to practice as it informs the AICPA by providing evidence that investors' knowledge about whether assurance is expected or not expected, based on industry norms, may help drive the demand for voluntary CRM assurance, as currently being promoted with the SOC for cybersecurity engagements. This study also informs companies and shareholders about the cost and incentives associated with voluntary CRM assurance. Study Two also contributes to the literature and theory on investor judgment and decision making by providing insights consistent with Wallace's (1980) insurance hypothesis and is consistent with the usefulness of voluntary assurance as insurance to mitigate the damage to firms' value and credibility after a cyber-attack.

Findings from Study Three show that more timely disclosure of a cybersecurity breach leads to more favorable management credibility assessments and stock price valuations and that the relationship between disclosure timeliness and valuation judgments is mediated by management credibility assessments. I also find that CRM assurance increases credibility assessments and valuation judgments when a breach has been disclosed in a timely manner.

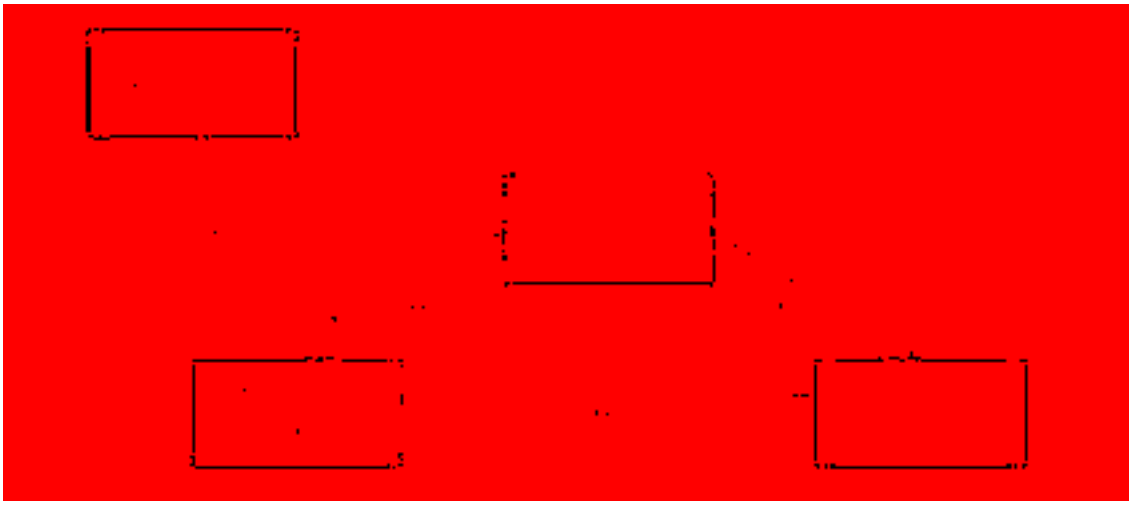
However, I am unable to support the prediction mitigating effect of CRM assurance on delayed disclosures.

The results of Study Three inform companies interested in reducing the cost of cyber-attacks by providing evidence that timely disclosures mitigate the negative stock price reaction associated with the announcement of a cyber-attack. These results are also relevant for regulators and standard setters currently working on cybersecurity disclosure guidance. The findings of Study Three close a breach in the accounting literature on disclosure timeliness by documenting context specific perceptions and beliefs that impact investors' perceptions of timeliness and may help explain mixed findings from prior research.

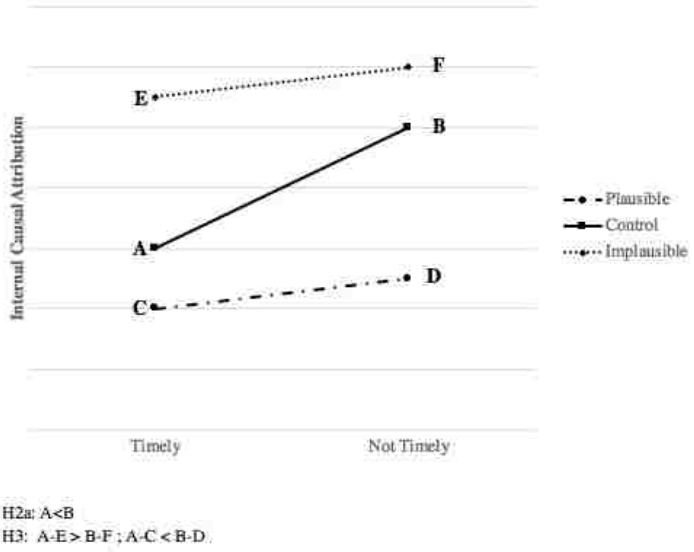
In summary, the results of the three studies have several implications for practice and for the accounting literature and theory. The findings of the thesis shed light on desirable CRM practices and mechanisms that can help reduce the cost of cyber-attacks. This evidence could be used by regulators and standard setters promoting cybersecurity disclosure and assurance. Altogether, these studies contribute to the judgment and decision making in accounting and provide initial insights into the impact of context specific aspects of cybersecurity that influence jurors' and investors' judgments.

APPENDIX A: STUDY ONE FIGURES

Panel A: Theoretical Model

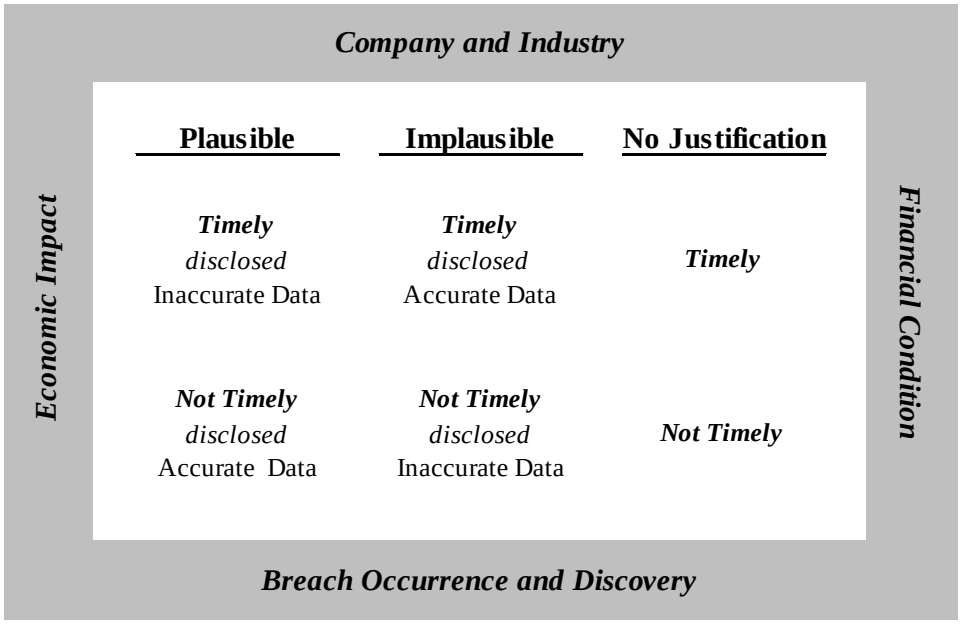


Panel B: Predicted Interactions



H2a: A<B
H3: A-E > B-F ; A-C < B-D

Figure 1 - Study 1: Model Predictions



*****The gray area represents fixed conditions between-subjects.

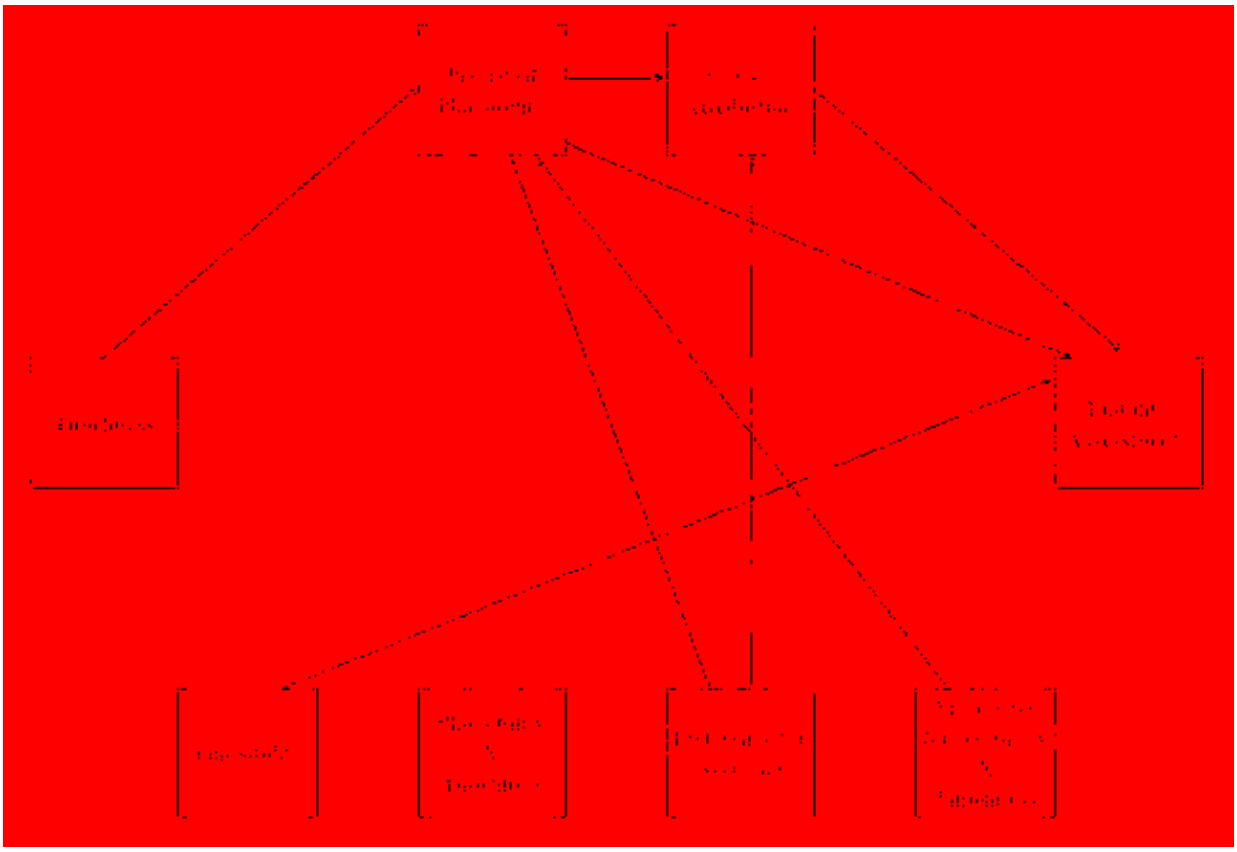
Figure 2 - Study 1: Experimental Conditions

	Timely		Not Timely	
	Plausible	**Implausible**	**Plausible**	**Implausible**
Case Information	On July 2016, Aplus Insurance announced that in **November** of 2015 hackers executed a sophisticated attack … The Class Period begins on **February 2016**, when Aplus Insurance filed an Annual Report on Form 10-K with the SEC, announcing the Company's financial and operating results for the year ended **December 31, 2015 (the "2015 10-K").**		On July 2016, Aplus Insurance announced that in **August** of 2015 hackers executed a sophisticated attack … The Class Period begins on **November 2015**, when Aplus Insurance filed a Quarterly Report on Form 10-Q with the SEC, announcing the Company's financial and operating results for the quarter ended **September 30, 2015 (the "Q3 2015 10-Q").**	
Plaintiff Arguments	The plaintiff also argues about the timing of Aplus Insurance's disclosures. The plaintiff presented evidence of the press-release, dated as of July 15, 2016, issued by Aplus Insurance in which the company acknowledges that the breach was discovered **three days before the announcement**, almost eight months after the attack.		The plaintiff also argues about the timing of Aplus Insurance's disclosures. The plaintiff presented evidence of the press-release, dated as of July 15, 2016, issued by Aplus Insurance in which the company acknowledges that the breach was discovered **three months before the announcement**, almost eight months after the attack.	
Defendant's Arguments	The defendant establishes that the incident was disclosed **three days** after it was discovered, in the most expedient time possible, and without unreasonable delay, as required by the regulations of the state of California.		The defendant establishes that the incident was disclosed **three months** after it was discovered, in the most expedient time possible, and without unreasonable delay, as required by the regulations of the state of California.	

	Timely		Not Timely	
	Plausible	**Implausible**	**Plausible**	**Implausible**
Plaintiff Closing Statement	The timeline presented shows that on average, it takes 47 days for a company to disclose a cybersecurity breach of a similar magnitude. However, in contrast with other firms that have disclosed a cyber-attack, Aplus Insurance disclosed the breach after **three days**. The disclosure was made 44 days **earlier** than the average disclosure. The plaintiff questions Aplus Insurance's disclosure timing as, **despite the incident being disclosed three days after it was discovered, it took them another three months to release comprehensive and accurate information about the extent of the breach.**	The timeline presented shows that on average, it takes 47 days for a company to disclose a cybersecurity breach of a similar magnitude. However, in contrast with other firms that have disclosed a cyber-attack, Aplus Insurance disclosed the breach after **three days**. The disclosure was made 44 days **earlier** than the average disclosure. The plaintiff questions Aplus Insurance's disclosure timing as **it is unlikely that a company would be able to gather comprehensive and accurate information and disclose the information within three days of discovery.**	The timeline presented shows that on average, it takes 47 days for a company to disclose a cybersecurity breach of a similar magnitude. However, in contrast with other firms that have disclosed a cyber-attack, Aplus Insurance disclosed the breach after **three months**. The disclosure was made 44 days **later** than the average disclosure. The plaintiff questions Aplus Insurance's disclosure timing as **it took them three months to disclose the incident and to release comprehensive and accurate information about the extent of the breach.**	The timeline presented shows that on average, it takes 47 days for a company to disclose a cybersecurity breach of a similar magnitude. However, in contrast with other firms that have disclosed a cyber-attack, Aplus Insurance disclosed the breach after **three months**. The disclosure was made 44 days **later** than the average disclosure. The plaintiff questions Aplus Insurance's disclosure timing as **it took them three months to disclose the incident and it took them another three months to release comprehensive and accurate information about the extent of the breach.**

	Timely		Not Timely	
	Plausible	**Implausible**	**Plausible**	**Implausible**
Defense Closing Statement	The attorney states that the Company made every effort to gather all the relevant facts of the impact of the breach. A press release was issued **quickly** to notify customers, so they could take actions to protect their identities. Given the initial uncertainties, management was unable to release accurate information about the extent of the breach **at the time of the announcement.** A dedicated website was established for customers to access additional information. **After gathering all the information, three months after the breach was disclosed,** the company issued additional press releases that included comprehensive and accurate information about the extent of the breach.	The attorney states that the Company made every effort to gather all the relevant facts of the impact of the breach. A press release was issued **quickly** to notify customers, so they could take actions to protect their identities. The press release included comprehensive and accurate information about the extent of the breach. A dedicated website was established for customers to access additional information.	The attorney states that the Company made every effort to gather all the relevant facts of the impact of the breach. Given the initial uncertainties, management was unable to release accurate information about the extent of the breach **when the breach was discovered**. However, a press release was issued in the most expedient time possible to notify customers, so they could take actions to protect their identities. The press release included comprehensive and accurate information about the extent of the breach. A dedicated website was established for customers to access additional information.	The attorney states that the Company made every effort to gather all the relevant facts of the impact of the breach. Given the initial uncertainties, management was unable to release accurate information about the extent of the breach **when the breach was discovered**. However, a press release was issued in the most expedient time possible to notify customers, so they could take actions to protect their identities. A dedicated website was established for customers to access additional information. **After gathering all the information, three months after the breach was announced,** the company issued additional press releases that included comprehensive and accurate information about the extent of the breach.

Figure 3 - Study 1: Operationalization of Plausibility



[a] Bold arrows are significant at the 0.10 level.

Variable definitions:
Liability assessment is the likelihood that participants find the defendant liable
Causal attribution is participants' assessment of causal attribution and participants' level of confidence in their assessment of causal attribution.
Perceived plausibility is the average of participants agreement that the justification is 1) plausible and 2) believable.
Timeliness is a dummy variable coded as one (1) if the company delayed the disclosure of the breach and zero (0) otherwise.
Plausibility is a dummy variable coded as one (1) if the company provided implausible justifications, two (2) if there is no justification provided, and three (3) if justifications are plausible.

Figure 4 - Study 1: Additional Analysis

APPENDIX B: STUDY ONE TABLES

Table 1 - Study 1: Test of H1

Liability Assessments

Panel A: Cell Means

	Timeliness					
	Timely			Not Timely		
Plausibility	**n**	**mean**	**S.D.**	**n**	**mean**	**S.D.**
Plausible	28	4.500	1.905	28	5.750	1.236
Control	28	4.321	1.949	28	5.429	1.451
Implausible	28	4.000	1.769	28	5.607	1.449

Panel B: Analysis of Covariance

Source	**d.f.**	**M.S.**	**F-value**	**p-value**[a]
Timeliness – ***H1***	1	73.339	28.161	<0.001
Plausibility	1	1.595	0.613	0.543
Timeliness * Plausibility	1	0.929	0.357	0.701
Error	162	2.604		

[a] Reported p-values are one-tailed for directional predictions.

Variable definitions:
Liability assessment is the likelihood that participants find the defendant liable
Timeliness is a dummy variable coded as one (1) if the company delayed the disclosure of the breach and zero (0) otherwise.
Plausibility is a dummy variable coded as one (1) if the company provided implausible justifications, two (2) if there is no justification provided, and three (3) if justifications are plausible.

Table 2 - Study 1: Test of H2a and H3

Assessment of Causal Attribution

Panel A: Cell Means

	Timeliness					
	Timely			Not Timely		
Plausibility	**n**	**mean**	**S.D.**	**n**	**mean**	**S.D.**
Plausible	28	2.490	1.547	28	4.388	1.788
Control	28	2.674	1.793	28	4.301	1.965
Implausible	28	2.740	1.919	28	4.694	1.901

Panel B: Analysis of Variance

Source	**d.f.**	**M.S.**	**F-value**	**p-value[a]**
Timeliness – ***H2a***	1	140.121	42.118	<0.001
Plausibility	1	1.236	0.371	0.345
Timeliness * Plausibility – ***H3***	1	0.427	0.128	0.440
Error	162	3.327		

[a]Reported p-values are one-tailed for directional predictions.

Variable definitions:
Causal attribution is participants' assessment of causal attribution and participants' level of confidence in their assessment of causal attribution.
Timeliness is a dummy variable coded as one (1) if the company delayed the disclosure of the breach and zero (0) otherwise.
Plausibility is a dummy variable coded as one (1) if the company provided implausible justifications, two (2) if there is no justification provided, and three (3) if justifications are plausible.

Table 3 - Study 1: Test of H2b and H3

Mediation and Moderated Mediation Analysis

Panel A: Test of Direct Effects

	Causal Attribution		Liability Assessment	
Variable	**Coefficient**	**p-value[a]**	**Coefficient**	**p-value[a]**
Timeliness	1.883	0.060	0.427	0.034
	(2.541)		(14.153)	
Plausibility	-0.125	0.303		
	(-0.515)			
Timeliness * Plausibility	-0.028	0.467		
	(-0.082)			
Causal Attribution			0.490	<0.001
			(8.506)	
Constant	2.884	<0.001	2.983	<0.001
	(5.506)		(8.506)	

Panel B: Conditional Indirect Effects of Timeliness on Liability Assessments

Mediator	**Expectancy**	**Effect**	**Boot SE**	**BootLLCI**	**BootULCI**
Implausible	1	0.9085	0.2881	**0.3937**	**1.5180**
Control	2	0.8948	0.2087	**0.5309**	**1.3357**
Plausible	3	0.881	0.2461	**0.4549**	**1.4052**

Panel C: Index of Moderated Mediation

Mediator	**Index**	**Boot SE**	**BootLLCI**	**BootULCI**
Plausibility	-0.0137	0.1681	-0.3582	0.3162

[a]Reported p-values are one-tailed for directional predictions.

T-values are reported in parenthesis. Bold confidence intervals are significant.

Variable definitions:

Liability assessment is the likelihood that participants find the defendant liable

Causal attribution is participants' assessment of causal attribution and participants' level of confidence in their assessment of causal attribution.

Timeliness is a dummy variable coded as one (1) if the company delayed the disclosure of the breach and zero (0) otherwise.

Plausibility is a dummy variable coded as one (1) if the company provided implausible justifications, two (2) if there is no justification provided, and three (3) if justifications are plausible.

Table 4 - Study 1: Additional Analysis

Panel A: Test of Direct Effects

	Perceived Plausibility			Causal Attribution			Liability Assessments		
Variable	**Coefficient**	**t-stat**	**p-value**[a]	**Coefficient**	**t-stat**	**p-value**[a]	**Coefficient**	**t-stat**	**p-value**[a]
Timeliness	-5.123	-6.368	<0.001	0.192	0.258	0.398	0.141	0.212	0.416
Plausibility	0.099	0.487	0.313	-0.056	-0.331	0.371	0.309	0.151	0.021
Timeliness * Plausibility	0.057	0.200	0.421	-0.026	-0.110	0.456	-0.154	-0.722	0.236
Prefer_Accuracy	-0.261	-2.598	0.005	-0.127	-1.498	0.068	0.023	0.303	0.381
Prefer_Accuracy * Timeliness	0.712	5.245	<0.001	-0.051	-0.420	0.338	-0.042	-0.388	0.349
Perceived Plausibility				-0.751	-11.543	<0.001	-0.620	-7.871	<0.001
Causal Attribution							0.090	1.268	0.103
Constant	6.2121	10.601	<0.001	7.281	11.536	<0.001	6.652	8.701	<0.001

Panel B: Analysis of Indirect Effects Assessments

Indirect effect	**Effect**	**Boot SE**	**BootLLCI**	**BootULCI**
Total	3.5386	0.6082	**2.3769**	**4.7595**
Timeliness -> Perceived Plausibility ->Liability Assessment	3.1770	0.8190	**1.9084**	**5.0790**
Timeliness -> Causal Attribution -> Liability Assessment	0.0172	0.0963	-0.2416	0.1674
Timeliness -> Perceived Plausibility -> Causal Attribution -> Liability Assessment	0.3444	0.3990	-0.3056	1.2740

[a]Reported p-values are one-tailed for directional predictions.

Bold confidence intervals are significant.

Variable definitions:

Liability assessment is the likelihood that participants find the defendant liable

Causal attribution is participants' assessment of causal attribution and participants' level of confidence in their assessment of causal attribution.

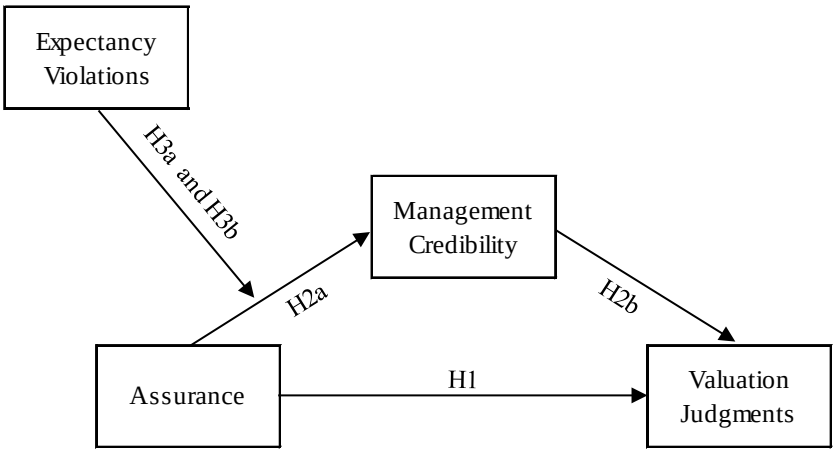
Perceived plausibility is the average of participants agreement that the justification is 1) plausible and 2) believable.

Timeliness is a dummy variable coded as one (1) if the company delayed the disclosure of the breach and zero (0) otherwise.

Plausibility is a dummy variable coded as one (1) if the company provided implausible justifications, two (2) if there is no justification provided, and three (3) if justifications are plausible.

APPENDIX C: STUDY TWO FIGURES

Panel A: Theoretical Model



Panel B: Interaction between CRM assurance and Conformity with Expectancies on Management Credibility

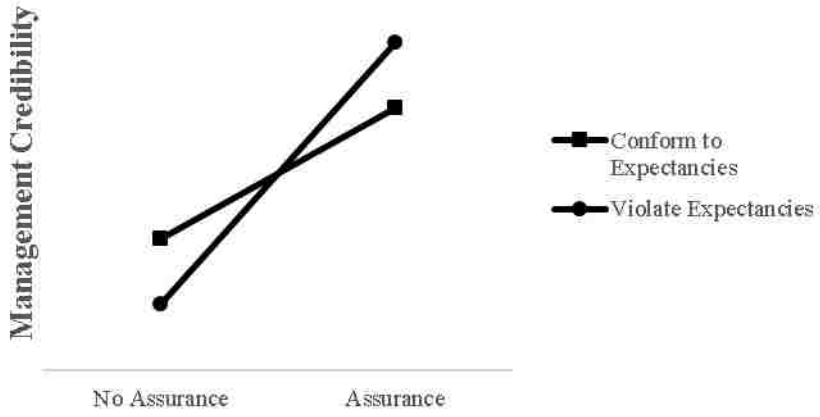


Figure 5 - Study 2: Model Predictions

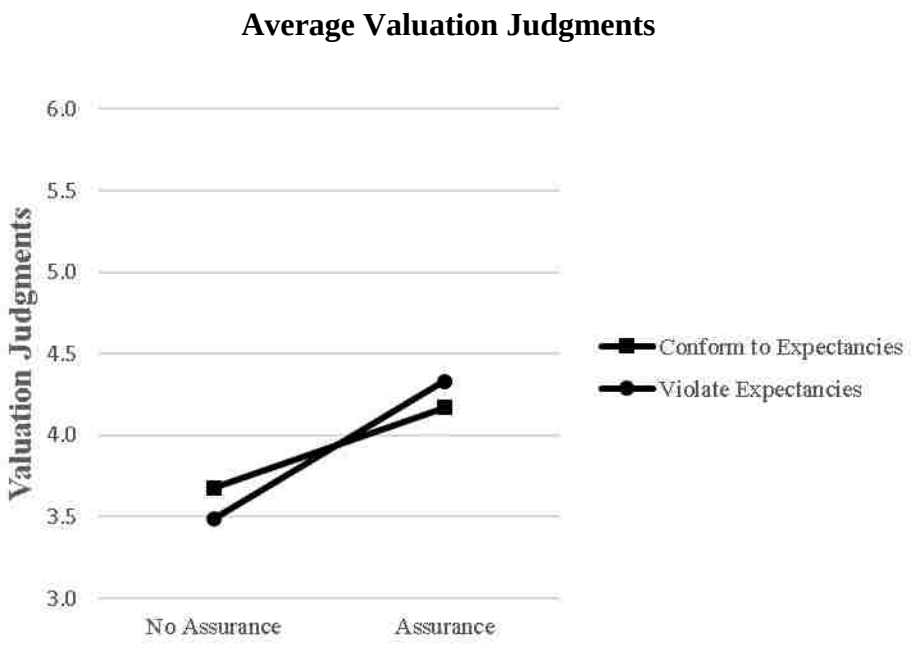
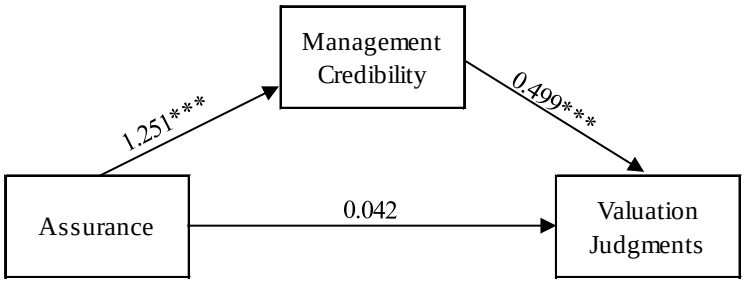


Figure 6 - Study 2: Test of H1

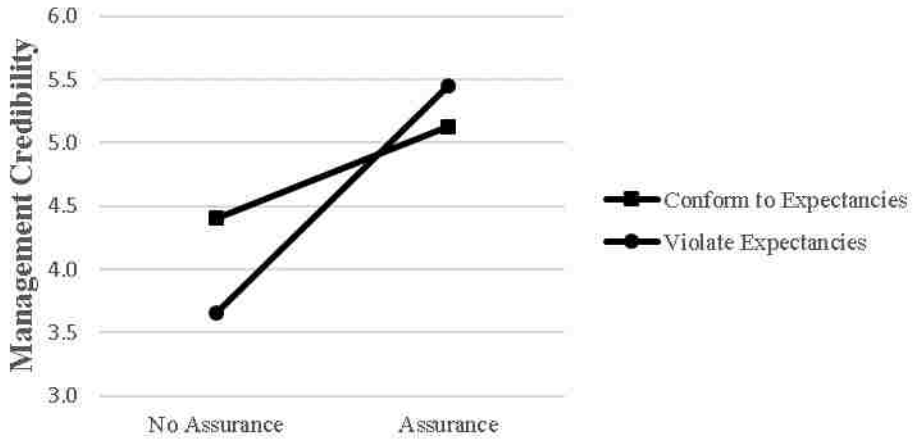
Mediation Analysis



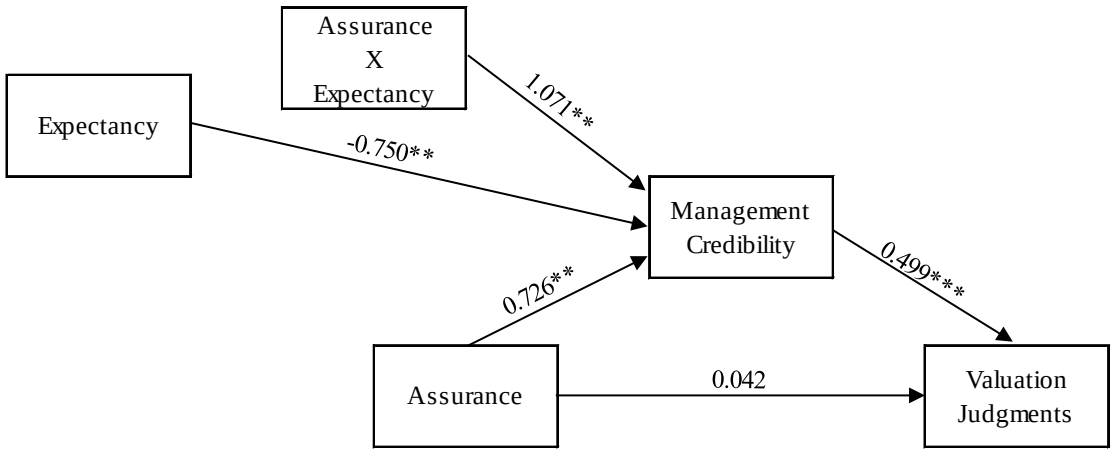
*, **, *** Indicate significance at $p < 0.10$, $p < 0.05$, and $p < 0.001$, respectively.
Variable definitions:
Assurance is a dummy variable coded as one (1) if the company engages in CRM assurance and zero (0) otherwise.
Management credibility is the participant's assessment of management competence and trustworthiness, measured using a scale that ranges from "very incompetent" (equal to 1) to "very competent" (equal to 7) and using a scale that ranges from "very untrustworthy" (equal to 1) to "very trustworthy" (equal to 7), respectively.
Valuation judgments is the participant's perceived value of a company stock price measured using a 7-point, fully labeled, scale that ranges from "very low" (equal to 1) to "very high" (equal to 7).

Figure 7 - Study 2: Test of H2

Panel A: Average Management Credibility Assessment – H3a



Panel B: Results of Mediated Moderation Analysis – H3b

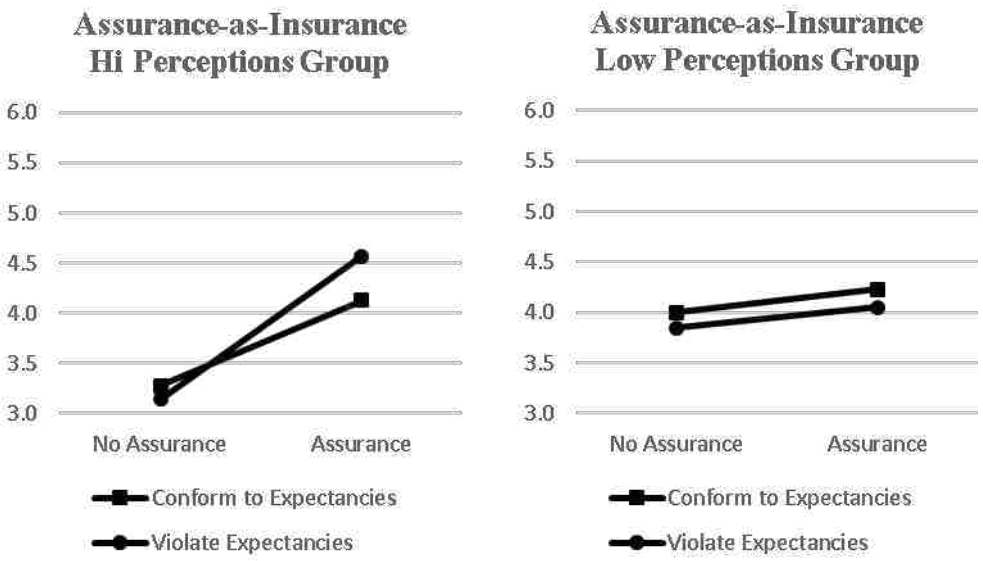


*, **, *** Indicate significance at $p < 0.10$, $p < 0.05$, and $p < 0.001$, respectively.
Variable definitions:
Assurance is a dummy variable coded as one (1) if the company engages in CRM assurance and zero (0) otherwise.
Expectancy is a dummy variable coded as one (1) if the company violates expectancies about CRM assurance practices and zero (0) otherwise.
Management credibility is the participant's assessment of management competence and trustworthiness, measured using a scale that ranges from "very incompetent" (equal to 1) to "very competent" (equal to 7) and using a scale that ranges from "very untrustworthy" (equal to 1) to "very trustworthy" (equal to 7), respectively.
Valuation judgments is the participant's perceived value of a company stock price measured using a 7-point, fully labeled, scale that ranges from "very low" (equal to 1) to "very high" (equal to 7).

Figure 8 - Study 2: Test of H3

Perceived Benefits of Assurance-as-Insurance

Panel A: Average Valuation Judgments



Panel A: Average Management Credibility Assessments

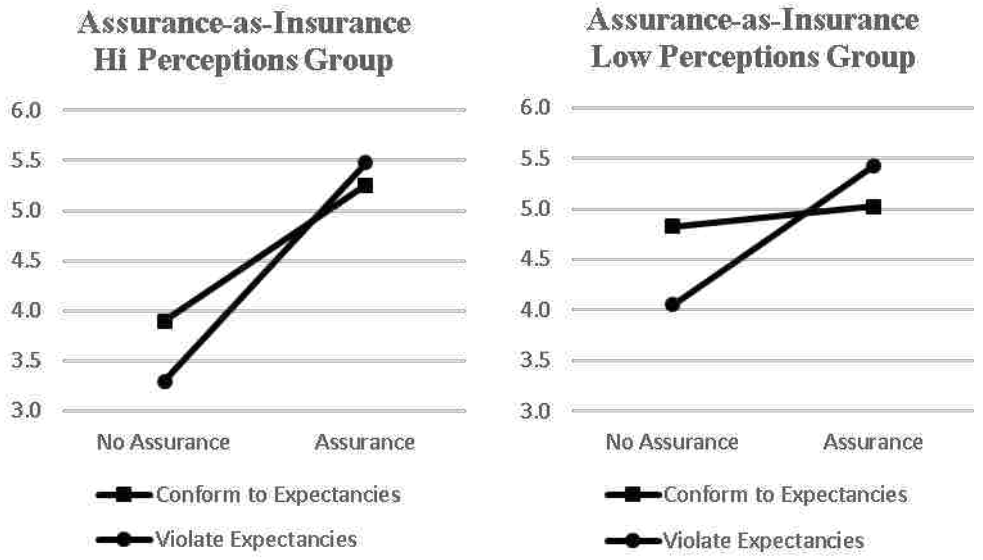
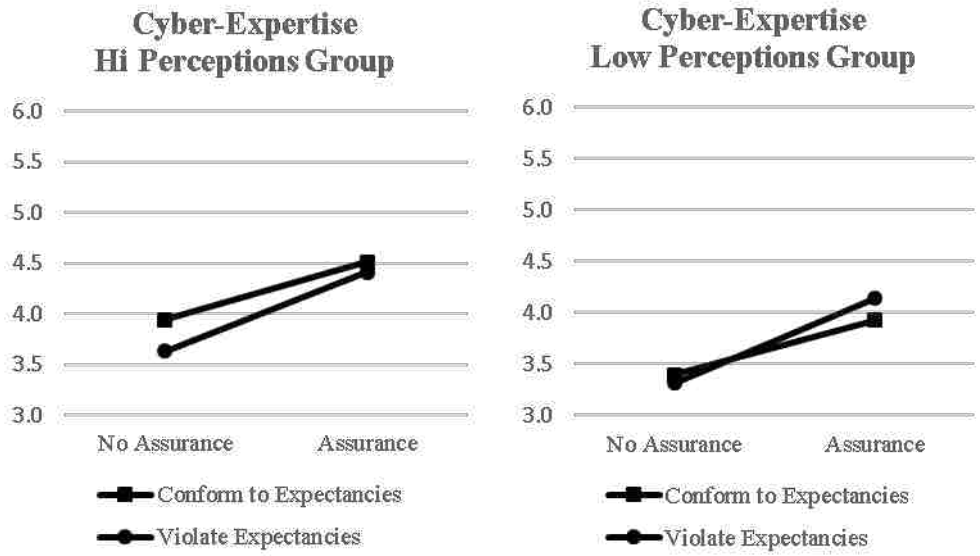


Figure 9 - Study 2: Additional Analysis

Perceived Accountants Cyber-Expertise

Panel A: Average Valuation Judgments



Panel A: Average Management Credibility Assessments

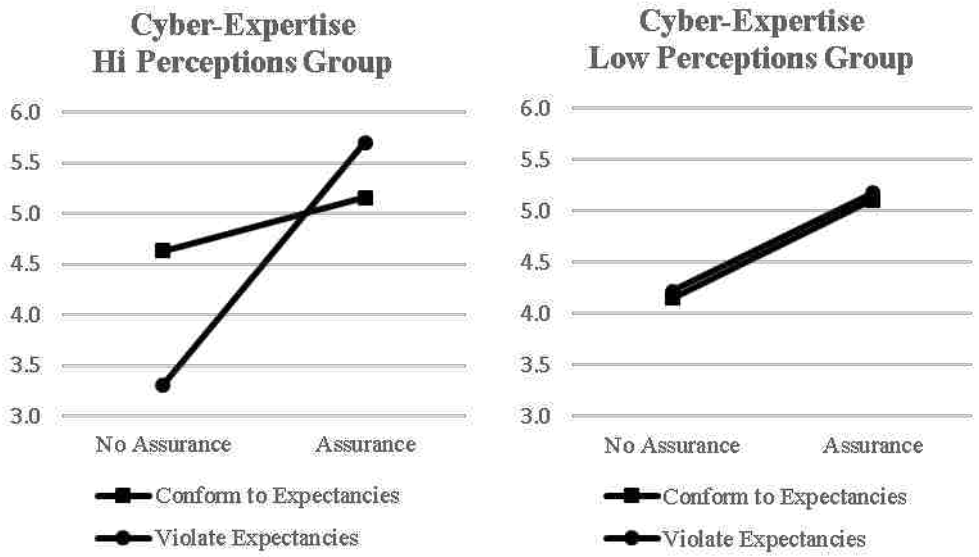
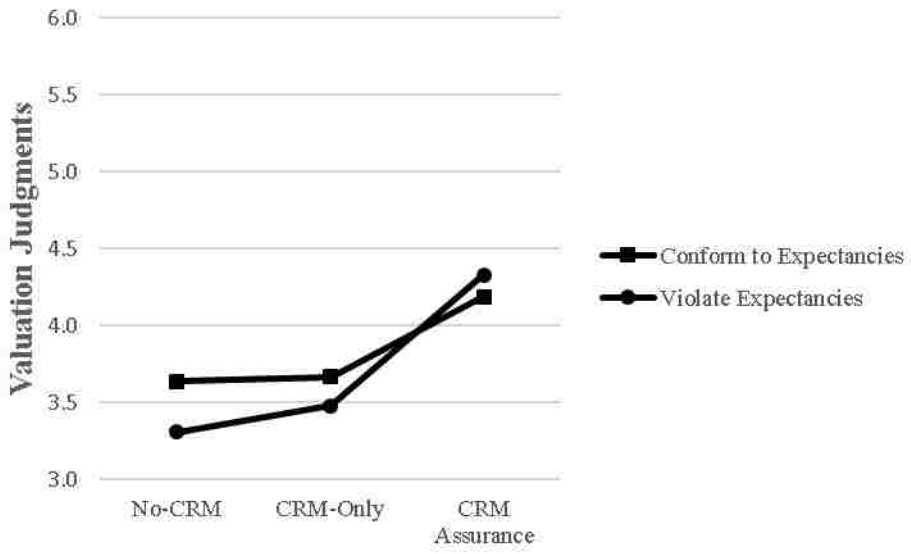


Figure 10 - Study 2: Additional Analysis

Disclosure of Cyber-risk Management Practices

Panel A: Average Valuation Judgments



Panel B: Average Management Credibility Assessments

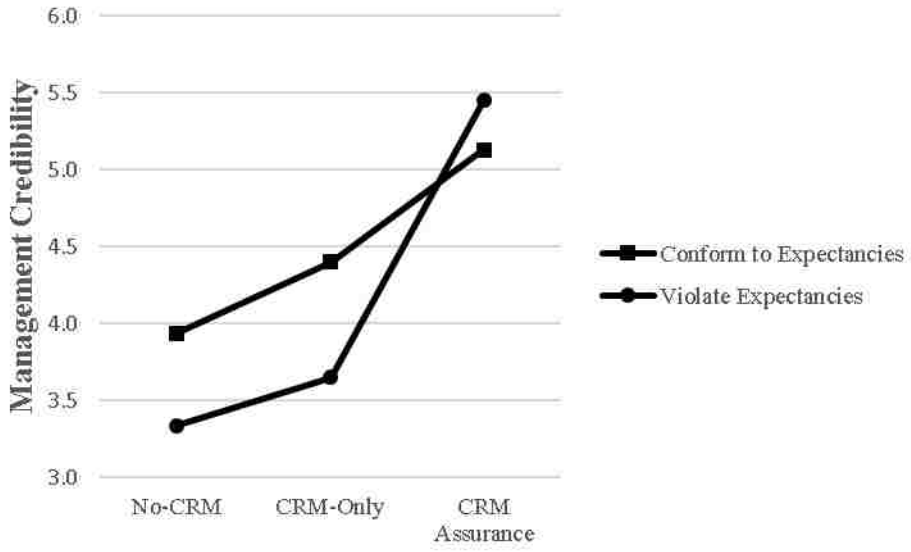


Figure 11 - Study 2: Additional Analysis

APPENDIX D: STUDY TWO TABLES

Table 5 - Study 2: Test of H1

Average Valuation Judgments

Panel A: Cell Means

	Assurance Expectancies [a]					
	Conform-to-expectancies			Violate-expectancies		
Assurance	**n**	**mean**	**S.D.**	**n**	**mean**	**S.D.**
Assurance	42	4.170	1.048	42	4.329	0.825
No Assurance	42	3.679	1.289	42	3.489	1.212

Panel B: Analysis of Covariance

Source	**d.f.**	**M.S.**	**F-value**	**p-value**[b]
Assurance – ***H1***	1	18.378	15.817	<0.001
Expectancy	1	0.010	0.009	0.926
Assurance * Expectancy	1	1.285	1.106	0.148
Initial Valuation	1	2.229	1.918	0.084
Error	163	1.162		

[a]Reported means are adjusted by initial valuations (mean=4.10). Unadjusted means are not significantly different and in the same direction.
[b]Reported p-values are one-tailed for directional predictions.
[c]The values attached are -1, 1, 0, 0 for the negative violation test; and 0, 0, -1, 1 for the positive violation test.
Variable definitions:
Valuation judgments is the participant's perceived value of a company stock price measured using a 7-point, fully labeled, scale that ranges from "very low" (equal to 1) to "very high" (equal to 7).
Assurance is a dummy variable coded as one (1) if the company engages in CRM assurance and zero (0) otherwise.
Expectancy is a dummy variable coded as one (1) if the company violates expectancies about CRM assurance practices and zero (0) otherwise.
Initial Valuation is the participant's valuation judgment before being presented with the manipulations.

Table 6 - Study 2: Test of H2a and H3a

Average Management Credibility Assessments

Panel A: Cell Means

	Assurance Expectancies					
	Conform-to-expectancies			Violate-expectancies		
Assurance	**n**	**mean**	**S.D.**	**n**	**mean**	**S.D.**
Assurance	42	5.131	1.048	42	5.452	0.825
No Assurance	42	4.405	1.289	42	3.655	1.212

Panel B: Analysis of Variance

Source	**d.f.**	**M.S.**	**F-value**	**p-value[a]**
Assurance – ***H2a***	1	66.881	54.489	<0.001
Expectancy	1	1.929	1.571	0.212
Assurance * Expectancy – ***H3a***	1	12.054	9.820	<0.001
Error	164	1.227		

Panel C: Test of Simple Effects – *H3a*

Simple effects[b]	**d.f.**	**M.S.**	**t-value**	**p-value[a]**
Negative Violation	164	0.750	2.747	0.004
Positive Violation	164	0.321	1.562	0.061

[a]Reported p-values are one-tailed for directional predictions.

[b] The values attached are -1, 1, 0, 0 for the negative violation test; and 0, 0, -1, 1 for the positive violation test.

Variable definitions:

Assurance is a dummy variable coded as one (1) if the company engages in CRM assurance and zero (0) otherwise.

Expectancy is a dummy variable coded as one (1) if the company violates expectancies about CRM assurance practices and zero (0) otherwise.

Management credibility is the participant's assessment of management competence and trustworthiness, measured using a scale that ranges from "very incompetent" (equal to 1) to "very competent" (equal to 7) and using a scale that ranges from "very untrustworthy" (equal to 1) to "very trustworthy" (equal to 7), respectively.

Table 7 - Study 2: Test of H2b

Mediation Analysis

Panel A: Test of Direct Effects

	Management Credibility		Updated Valuation	
Variable	**Coefficient**	**p-value[a]**	**Coefficient**	**p-value[a]**
Assurance	1.251	<0.001	0.0417	0.797
	(7.064)		(0.257)	
Management Credibility			0.499	<0.001
			(7.998)	
Initial Valuation	0.100	0.575	0.178	0.216
	(0.561)		(1.243)	
Constant	3.624	<0.001	0.839	0.185
	(4.939)		(1.332)	

Panel B: Indirect Effects of Assurance on Valuation Judgments

Mediator	**Effect**	**Boot SE**	**BootLLCI**	**BootULCI**
Management Credibility	0.624	0.131	**0.3903**	**0.8945**

[a]Reported p-values are one-tailed for directional predictions.

T-values are reported in parenthesis. Bold confidence intervals are significant.

Variable definitions:

Management credibility is the participant's assessment of management competence and trustworthiness, measured using a scale that ranges from "very incompetent" (equal to 1) to "very competent" (equal to 7) and using a scale that ranges from "very untrustworthy" (equal to 1) to "very trustworthy" (equal to 7), respectively.

Valuation judgments is the participant's perceived value of a company stock price measured using a 7-point, fully labeled, scale that ranges from "very low" (equal to 1) to "very high" (equal to 7).

Assurance is a dummy variable coded as one (1) if the company engages in CRM assurance and zero (0) otherwise.

Initial Valuation is the participant's valuation judgment before being presented with the manipulations.

Table 8 - Study 2: Test of H3b

Mediation and Moderated Mediation Analysis

Panel A: Test of Direct Effects

	Management Credibility		Updated Valuation	
Variable	**Coefficient**	**p-value[a]**	**Coefficient**	**p-value[a]**
Assurance	0.726	0.002	0.042	0.797
	(3.004)		(0.257)	
Expectancy	-0.750	0.002		
	(-3.102)			
Assurance * Expectancy	1.071	0.002		
	(3.134)			
Management Credibility			0.499	<0.001
			(7.998)	
Initial Valuation			0.178	0.216
			(1.243)	
Constant	4.405	<0.001	0.839	0.1846
	(25.766)		(1.332)	

Panel B: Conditional Indirect Effects of Assurance on Valuation Judgments

Mediator	**Expectancy**	**Effect**	**Boot SE**	**BootLLCI**	**BootULCI**
Management Credibility	0	0.3624	0.1419	**0.1156**	**0.6825**
Management Credibility	1	0.897	0.1666	**0.5849**	**1.2407**

Panel C: Index of Moderated Mediation

Mediator	**Index**	**Boot SE**	**BootLLCI**	**BootULCI**
Management Credibility	0.5347	0.1825	**0.2012**	**0.9209**

[a]Reported p-values are one-tailed for directional predictions.

T-values are reported in parenthesis. Bold confidence intervals are significant.

Variable definitions:

Management credibility is the participant's assessment of management competence and trustworthiness, measured using a scale that ranges from "very incompetent" (equal to 1) to "very competent" (equal to 7) and using a scale that ranges from "very untrustworthy" (equal to 1) to "very trustworthy" (equal to 7), respectively.

Valuation judgments is the participant's perceived value of a company stock price measured using a 7-point, fully labeled, scale that ranges from "very low" (equal to 1) to "very high" (equal to 7).

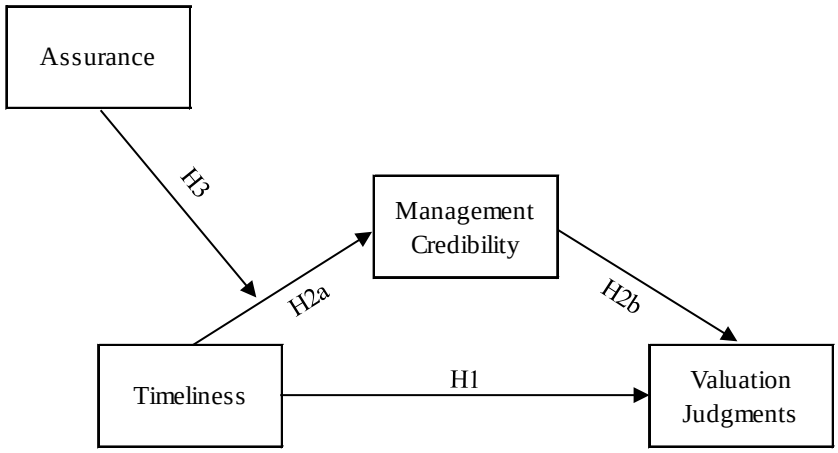
Assurance is a dummy variable coded as one (1) if the company engages in CRM assurance and zero (0) otherwise.

Expectancy is a dummy variable coded as one (1) if the company violates expectancies about CRM assurance practices and zero (0) otherwise.

Initial Valuation is the participant's valuation judgment before being presented with the manipulations.

APPENDIX E: STUDY THREE FIGURES

Panel A: Theoretical Model



Panel B: Interaction between CRM Assurance and Disclosure Timeliness on Management Credibility

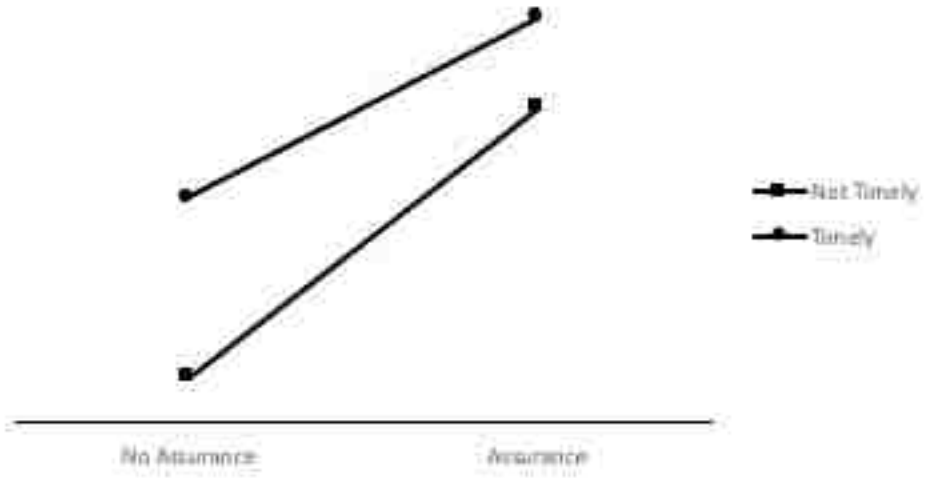
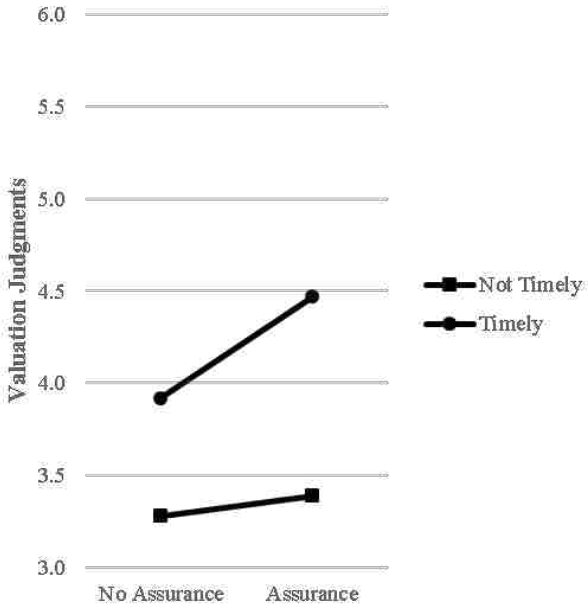


Figure 12 - Study 3: Model Predictions

Panel A: Average Valuation Judgments



Panel B: Average Management Credibility Assessments

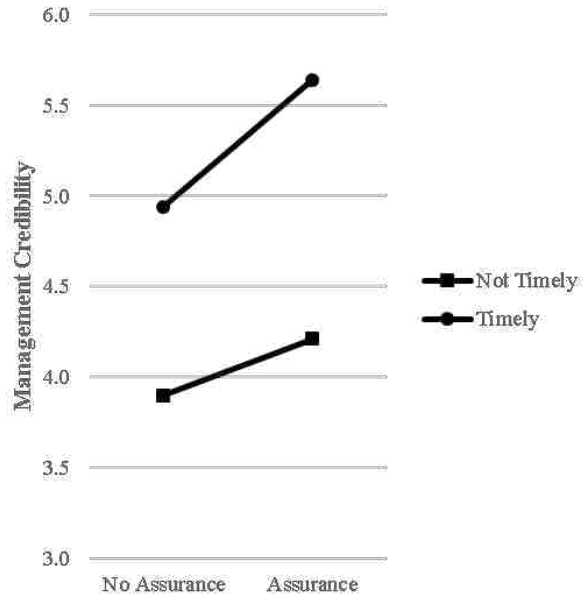


Figure 13 - Study 3: Test of H1 and H3

APPENDIX F: STUDY THREE TABLES

Table 9 - Study 3: Test of H1

Average Valuation Judgments

Panel A: Cell Means

	CRM Assurance					
	Assurance			No Assurance		
Timeliness	**n**	**mean**	**S.D.**	**n**	**mean**	**S.D.**
Timely	36	4.472	0.971	36	3.917	1.052
Not Timely	36	3.389	1.178	36	3.278	1.210

Panel B: Analysis of Variance

Source	**d.f.**	**M.S.**	**F-value**	**p-value**[a]
Timeliness – ***H1***	1	22.415	19.426	<0.001
Assurance	1	4.988	4.323	0.020
Timeliness * Assurance	1	2.705	2.344	0.064
Initial Valuation	1	11.120	9.638	0.001
Error	139	1.154		

[a] Reported p-values are one-tailed for directional predictions.

Variable definitions:

Valuation judgments is the participant's perceived value of a company stock price measured using a 7-point, fully labeled, scale that ranges from "very low" (equal to 1) to "very high" (equal to 7).

Timeliness is a dummy variable coded as one (1) if the company discloses the breach in three days and zero (0) if the company discloses the breach in three months.

Assurance is a dummy variable coded as one (1) if the company engages in CRM assurance and zero (0) otherwise.

Table 10 - Study 3: Test of H2a and H3

Average Management Credibility Assessments

Panel A: Cell Means

	CRM Assurance					
	Assurance			No Assurance		
Timeliness	**n**	**mean**	**S.D.**	**n**	**mean**	**S.D.**
Timely	36	5.639	0.825	36	4.944	1.241
Not Timely	36	4.208	1.197	36	3.903	1.303

Panel B: Analysis of Variance

Source	**d.f.**	**M.S.**	**F-value**	**p-value**[a]
Timeliness – ***H2a***	1	55.007	41.118	<0.001
Assurance	1	9.000	6.727	0.005
Timeliness * Assurance – ***H3***	1	1.361	1.017	0.157
Error	140	1.338		

Panel C: Planned Contrast

Contrast[b]	**d.f.**	**M.S.**	**t-value**	**p-value**[a]
Assurance	140	1.338	2.594	0.005

[a] Reported p-values are one-tailed for directional predictions.
[b] The values attached are -1, 1, -1, 1.
Variable definitions:
Management credibility is the participant's assessment of management competence and trustworthiness, measured using a scale that ranges from "very incompetent" (equal to 1) to "very competent" (equal to 7) and using a scale that ranges from "very untrustworthy" (equal to 1) to "very trustworthy" (equal to 7), respectively.
Timeliness is a dummy variable coded as one (1) if the company discloses the breach in three days and zero (0) if the company discloses the breach in three months.
Assurance is a dummy variable coded as one (1) if the company engages in CRM assurance and zero (0) otherwise.

Table 11 - Study 3: Test of H2b and H3

Moderated Mediation Analysis

Panel A: Test of Direct Effects

	Management Credibility		Valuation Judgments	
Variable	**Coefficient**	**p-value[a]**	**Coefficient**	**p-value[a]**
Timeliness	2.355	<0.001	0.185	0.125
	(3.487)		(1.073)	
Assurance	0.295	0.137		
	(1.098)			
Timeliness * Assurance	0.473	0.108		
	(1.241)			
Initial Valuation	0.379	0.028	0.264	0.024
	(2.321)		(2.002)	
Management Credibility – H2b			0.518	<0.001
			(7.872)	
Constant	2.355	<0.001	4.716	<0.001
	(3.395)		(13.834)	

Panel B: Conditional Indirect Effects of Timeliness on Valuation Judgments

Mediator	Plausibility	Effect	Boot SE	BootLLCI	BootULCI
Management Credibility	0	0.4902	0.1651	**0.1921**	**0.8250**
Management Credibility	1	0.7351	0.4344	**0.4344**	**1.0690**

Panel C: Index of Moderated Mediation

Mediator	Index	Boot SE	BootLLCI	BootULCI
Management Credibility – H3	0.2449	0.2085	-0.1417	0.6737

[a]Reported p-values are one-tailed for directional predictions.

T-values are reported in parenthesis. Bold confidence intervals are significant.

Variable definitions:

Valuation judgments is the participant's perceived value of a company stock price measured using a 7-point, fully labeled, scale that ranges from "very low" (equal to 1) to "very high" (equal to 7).

Management credibility is the participant's assessment of management competence and trustworthiness, measured using a scale that ranges from "very incompetent" (equal to 1) to "very competent" (equal to 7) and using a scale that ranges from "very untrustworthy" (equal to 1) to "very trustworthy" (equal to 7), respectively.

Timeliness is a dummy variable coded as one (1) if the company discloses the breach in three days and zero (0) if the company discloses the breach in three months.

Assurance is a dummy variable coded as one (1) if the company engages in CRM assurance and zero (0) otherwise.

Table 12 - Study 3: Additional Analysis

Regression Analysis for Determinants of Perceived Timeliness

	Perceived Timeliness		
Variable	**Coefficient**	**t-stat**	**p-value**
Timeliness	4.642	3.333	<0.001
Delay Acceptable	0.769	8.755	<0.001
Delay Acceptable * Timeliness	-0.858	-6.681	<0.001
Timely Benefits	0.181	1.302	0.195
Timely Benefits * Timeliness	0.238	1.124	0.263
Constant	-0.641	-0.698	<0.001
Observations	144		
R-Squared	0.797		

Variable definitions:
Perceived timeliness is participants agreement that the disclosure of the breach was made on a timely manner..
Timeliness is a dummy variable coded as one (1) if the company delayed the disclosure of the breach and zero (0) otherwise.
Delay Acceptable is participants perceptions that delayed disclosures of cyber-attacks are acceptable due to 1) the increased sophistication of hacking techniques, 2) the complexity of determining the scope of the breach, 3) need to conduct required investigations, 4) even when there is loss of identifiable information from customers and employees.
Timely benefits is participants perceptions that timely disclosure of cyber-attacks: 1) reduces the risk of litigation, 2) reduces the risk of lost business, and 3) is the right thing to do.

APPENDIX G: STUDY ONE EXPERIMENTAL MATERIALS

Comments to reviewers are made in Red, Bold, and Italics

Start of Block: Screening

Are you at least 18 years of age and a United States Citizen?

O Yes

O No

Have you ever worked for an insurance company or a health provider?

O Yes

O No

Have you worked as a lawyer or for a law firm?

O Yes

O No

Have you suffered financial loss due to identity theft?

O Yes

O No

What is your Mturk Worker ID?

_____

End of Block: Screening

Start of Block: Default Question Block

EXPLANATION OF RESEARCH

Title of Project: Jurors' liability assessments after cybersecurity breaches: the impact of disclosure timeliness and the plausibility of management justifications
Principal Investigator: Patricia Navarro-Velez
Faculty Supervisor: Steve G. Sutton

You are being invited to take part in a research study. Whether you take part is up to you.

The purpose of this study is to explore how jurors make liability assessments.

You will assume the role of a juror in a court case involving a group of shareholders and a corporation. In your role as a juror, you will read a summary of the trial testimony and answer questions regarding your opinions related to the case.

This study will be administered online. We expect that it will take you approximately 30 minutes to complete this experiment.

You must be 18 years of age or older to take part in this research study.

Study contact for questions about the study or to report a problem: If you have questions, concerns, or complaints contact Patricia Navarro-Velez, Doctoral Candidate, UCF Accounting Department at (407)823-5837 or Dr. Steve G. Sutton, Faculty Advisor, UCF Accounting Department at (407)823-5857.

IRB contact about your rights in the study or to report a complaint:
Research at the University of Central Florida involving human participants is carried out under the oversight of the Institutional Review Board (UCF IRB). This research has been reviewed and approved by the IRB. For information about the rights of people who take part in research, please contact: Institutional Review Board, University of Central Florida, Office of Research &

Only participants who answer Yes to screening question 1 and No to questions 2-4 are allowed to continue the survey.

Commercialization, 12201 Research Parkway, Suite 501, Orlando, FL 32826-3246 or by telephone at (407) 823-2901.

Continuing on to the following pages indicates your permission to take part in this research.

End of Block: Default Question Block

Start of Block: Task Description

Page Break

You must complete this task in a single sitting. The task will take about 30 minutes to complete. If you do not have approximately 30 minutes to complete the task right now, please do not start the study.

It is also critical that you do not complete this study twice or discuss this study with others. This is serious research of interest to financial regulators, and the results could be compromised or ruined by you discussing this material with others.

End of Block: Task Description

Start of Block: Task Instructions

In this case, you will first read background information. Second, you will assume the role of a juror in a court case involving a group of shareholders and a corporation. In your role as a juror, you will read a summary of the trial and answer questions regarding your opinions related to the case. There are no right or wrong answers to the case questions you will be asked.

It is important that you read all case materials carefully and answer the included questions thoughtfully and honestly. Throughout the case you will answer the following three types of questions:

Review Questions reflect whether you read and understand the presented material. These questions will not be difficult if you read the materials carefully.
Case Questions ask you for your judgments about the outcomes of the facts described in the case. **There are no right or wrong answers to these questions.**
Wrap-Up Questions ask you some miscellaneous and demographic questions.

IMPORTANT: YOU MUST ANSWER 100% OF THE REVIEW QUESTIONS CORRECTLY TO BE COMPENSATED.

Review Question:

To be compensated, I must answer at least:

O 50% of the review questions correctly.

O 75% of the review questions correctly.

O 100% of the review questions correctly.

End of Block: Task Instructions

Start of Block: FINANCIAL STATEMENTS BACKGROUND

Background Information – Disclosure of Cybersecurity Risks and Practices
The mission of the U.S. Securities and Exchange Commission (SEC) is to protect investors, maintain fair, orderly, and efficient markets, and facilitate capital formation. As such, the SEC requires public companies to disclose meaningful financial and other information to the public.

Companies prepare financial statements for investors, lenders, and other users. Thus, investors and lenders use financial statements to assess the financial "health" of the company to determine whether to invest in or loan money to the company. Although there are no specific SEC enforcements regarding cybersecurity disclosures, the federal securities laws require the disclosure of timely, comprehensive, and accurate information about material risks and events relevant to an investment decision. Information is considered material if there is a substantial likelihood that a reasonable investor would consider it important in making an investment decision. The SEC establishes that disclosures about material risks and events, including cybersecurity risks and incidents, may need to complement a company's financial statements and be included in the description of the company's risk factors, Management Discussion and Analysis (MD&A) section, or the disclosures (notes) to the financial statements.

When the disclosure of information about the company is in violation of securities laws investors who have suffered economic injury file lawsuits (securities class action) to seek compensation to recover the money they lost. When this occurs, jurors are chosen from the general public to evaluate if it is more likely than not that the allegations against the company are true. If the jury finds that it is more likely than not that the allegations against the company are true, the company is held responsible for compensating the plaintiff (i.e. the investors who lost money because of their reliance on the information disclosed). If the jury finds that it is not likely that the allegations against the company are true, the company is not required to pay any damages.

Review Questions:

Investors and lenders use a company's financial statements when making decisions about whether to invest in or loan money to that company.

O True

O False

Companies are required to disclose risks and events relevant to an investment decision.

O True

O False

Companies are required to disclose comprehensive and accurate information. However, the timeliness of the disclosure is not relevant for compliance with federal securities laws.

O True

O False

When a company fails to disclose relevant information for investment decisions, investors often sue the company to recover the money they lost.

O True

O False

Not Timely Condition

Start of Block: CASE INFORMATION

Case Information

Aplus Insurance is a publicly traded company listed on the New York Stock Exchange and is a leading health and well-being company headquartered in California. Aplus Insurance is one of the largest health benefits companies in the United States and delivers a variety of health solutions, such as health care, dental, and vision plans, along with other specialty products, such as life and disability insurance products. The 2015 financial statements for Aplus Insurance disclosed net revenue of $2.6 billion. Following the release of the 2015 financial statements, the stock price of the company continued on a positive trend.

On July 2016, Aplus Insurance announced that in August of 2015 hackers executed a sophisticated attack to gain unauthorized access to one of the company's IT systems and obtained personal information relating to customers and employees. The information accessed included unencrypted personal information, such as names, birthdays, social security numbers, street addresses, email addresses and employment information, including income data. According to Aplus Insurance, they became aware of the attack eight months after the incident and disclosed the incident three months afterward. Following this announcement, Aplus Insurance's share price fell $4.40, or 4.94%, to close at $84.6.

As a result of the cyber-attack on Aplus Insurance, the aggregate investor losses are estimated at $10 billion. Based on this, a securities class action lawsuit was filed by investors who bought or sold Aplus Insurance's securities within the class period. The Class Period begins on November 2015, when Aplus Insurance filed a Quarterly Report on Form 10-Q with the SEC, announcing the Company's financial and operating results for the quarter ended September 30, 2015 (the "Q3 2015 10-Q").

Timely Condition

Case Information

Aplus Insurance is a publicly traded company listed on the New York Stock Exchange and is a leading health and well-being company headquartered in California. Aplus Insurance is one of the largest health benefits companies in the United States and delivers a variety of health solutions, such as health care, dental, and vision plans, along with other specialty products, such as life and disability insurance products. The 2015 financial statements for Aplus Insurance disclosed net revenue of $2.6 billion. Following the release of the 2015 financial statements, the stock price of the company continued on a positive trend.

On July 2016, Aplus Insurance announced that in November of 2015 hackers executed a sophisticated attack to gain unauthorized access to one of the company's IT systems and obtained personal information relating to customers and employees. The information accessed included unencrypted personal information, such as names, birthdays, social security numbers, street addresses, email addresses and employment information, including income data. According to Aplus Insurance, they became aware of the attack eight months after the incident and disclosed the incident three days afterward. Following this announcement, Aplus Insurance's share price fell $4.40, or 4.94%, to close at $84.6.

As a result of the cyber-attack on Aplus Insurance, the aggregate investor losses are estimated at $10 billion. Based on this, a securities class action lawsuit was filed by investors who bought or sold Aplus Insurance's securities within the class period. The Class Period begins on February 2016, when Aplus Insurance filed an Annual Report on Form 10-K with the SEC, announcing the Company's financial and operating results for the year ended December 31, 2015 (the "2015 10-K").

Review Question:

The class action lawsuit against Aplus Insurance alleges investors' losses of $10 billion.

O True

O False

End of Block: CASE INFORMATION

Start of Block: Plaintiff Arguments

Not Timely Condition

Summary of the Plaintiff's Arguments

The Complaint alleges that, throughout the Class Period, defendants made materially false and misleading statements, as well as failed to disclose material adverse facts about the Company's business, operations, and prospects. Specifically, defendants made false and/or misleading statements and/or failed to disclose that: (i) Aplus Insurance failed to encrypt its users' personal information and/or failed to encrypt its users' personal data with an up-to-date and secure encryption scheme; (ii) consequently, sensitive personal account information from more than 70 million individuals was vulnerable to theft; (iii) a data breach resulting in the theft of personal customer data would foreseeably cause a significant drop in user engagement with Aplus Insurance services; and (iv) as a result, Aplus Insurance's public statements were materially false and misleading at all relevant times.

The plaintiff presented evidence of the annual (10K) and quarterly (10Q) reports released by Aplus Insurance during the class period. The evidence presented shows that Aplus Insurance failed to disclose the failure to encrypt its users' personal information and personal data with an up-to-date and secure encryption scheme.

The plaintiff argued that the disclosure of cybersecurity risks, within the annual and quarterly reports, was limited to the following statement of risk factors:

"Delays or disruptions to our service, or the loss or compromise of data, could result from a variety of causes, including cyber-attacks."

The plaintiff also argues about the timing of Aplus Insurance's disclosures. The plaintiff presented evidence of the press-release, dated as of July 15, 2016, issued by Aplus Insurance in which the company acknowledges that the breach was discovered three months before the announcement, almost eight months after the event.

Timely Condition

Summary of the Plaintiff's Arguments

The Complaint alleges that, throughout the Class Period, defendants made materially false and misleading statements, as well as failed to disclose material adverse facts about the Company's business, operations, and prospects. Specifically, defendants made false and/or misleading statements and/or failed to disclose that: (i) Aplus Insurance failed to encrypt its users' personal information and/or failed to encrypt its users' personal data with an up-to-date and secure encryption scheme; (ii) consequently, sensitive personal account information from more than 70 million individuals was vulnerable to theft; (iii) a data breach resulting in the theft of personal customer data would foreseeably cause a significant drop in user engagement with Aplus Insurance services; and (iv) as a result, Aplus Insurance's public statements were materially false and misleading at all relevant times.

The plaintiff presented evidence of the annual (10K) and quarterly (10Q) reports released by Aplus Insurance during the class period. The evidence presented shows that Aplus Insurance failed to disclose the failure to encrypt its users' personal information and personal data with an up-to-date and secure encryption scheme.

The plaintiff argued that the disclosure of cybersecurity risks, within the annual and quarterly reports, was limited to the following statement of risk factors:

"Delays or disruptions to our service, or the loss or compromise of data, could result from a variety of causes, including cyber-attacks."

The plaintiff also argues about the timing of Aplus Insurance's disclosures. The plaintiff presented evidence of the press-release, dated as of July 15, 2016, issued by Aplus Insurance in which the company acknowledges that the breach was discovered three days before the announcement, almost eight months after the event.

Page Break

Summary of the Defendant's Arguments

In response to the allegations of the plaintiff, the defendant, Aplus Insurance, responds that cyber-attacks have become an unavoidable business risk, and so Aplus Insurance discloses cyber-attacks as a risk factor in their annual and quarterly reports. In addition, Aplus Insurance presented evidence of actions taken to contain the damage promptly. Evidence included the disclosure of the incident, creation of a dedicated website established to provide additional information, including frequently asked questions, and provision of two years of free credit monitoring and identity protection services to customers and employees.

The defendant establishes that the incident was disclosed three days after it was discovered, in the most expedient time possible, and without unreasonable delay, as required by the regulations of the state of California.

Page Break

Plaintiff Closing Statement

The attorney for the plaintiff revisits the evidence and reviews the key arguments for the case, summarizing why Aplus Insurance should be held responsible for the class action financial losses. The plaintiff argues that the company presented misleading financial reports as Aplus Insurance failed to disclose its failure to encrypt users' personal information and personal data with an up-to-date and secure encryption scheme. The plaintiff alleges that Aplus Insurance's negligence resulted in aggregate investor losses estimated at $10 billion.

Timely/Plausible Condition

The plaintiff also presented the following timeline:

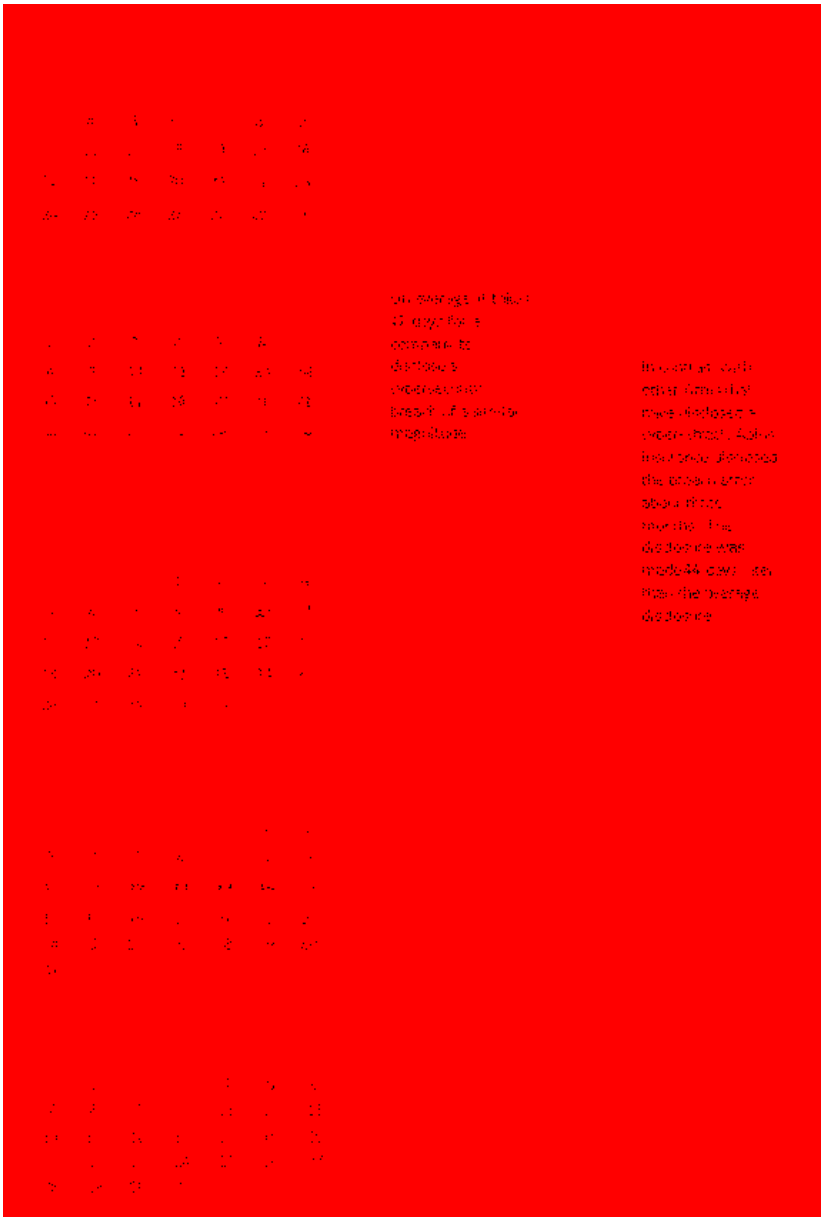
The timeline presented shows that on average, it takes 47 days for a company to disclose a cybersecurity breach of a similar magnitude. However, in contrast with other firms that have disclosed a cyber-attack, Aplus Insurance disclosed the breach after three days. The disclosure was made 44 days earlier than the average disclosure.

The plaintiff questions Aplus Insurance's disclosure timing strategy as, despite the incident being disclosed three days after it was discovered, it took them another three months to release comprehensive and accurate information about the extent of the breach.

The attorney for the plaintiff asks the jury to find for the plaintiff.

Not Timely/Plausible Condition

The plaintiff also presented the following timeline:



The timeline presented shows that on average, it takes 47 days for a company to disclose a cybersecurity breach of a similar magnitude. However, in contrast with other firms that have disclosed a cyber-attack, Aplus Insurance disclosed the breach after about three months. The disclosure was made 44 days later than the average disclosure.

The plaintiff questions Aplus Insurance's disclosure timing strategy as it took them three months to disclose the incident and to release comprehensive and accurate information about the extent of the breach.

The attorney for the plaintiff asks the jury to find for the plaintiff.

Timely/Implausible Condition

The plaintiff also presented the following timeline:

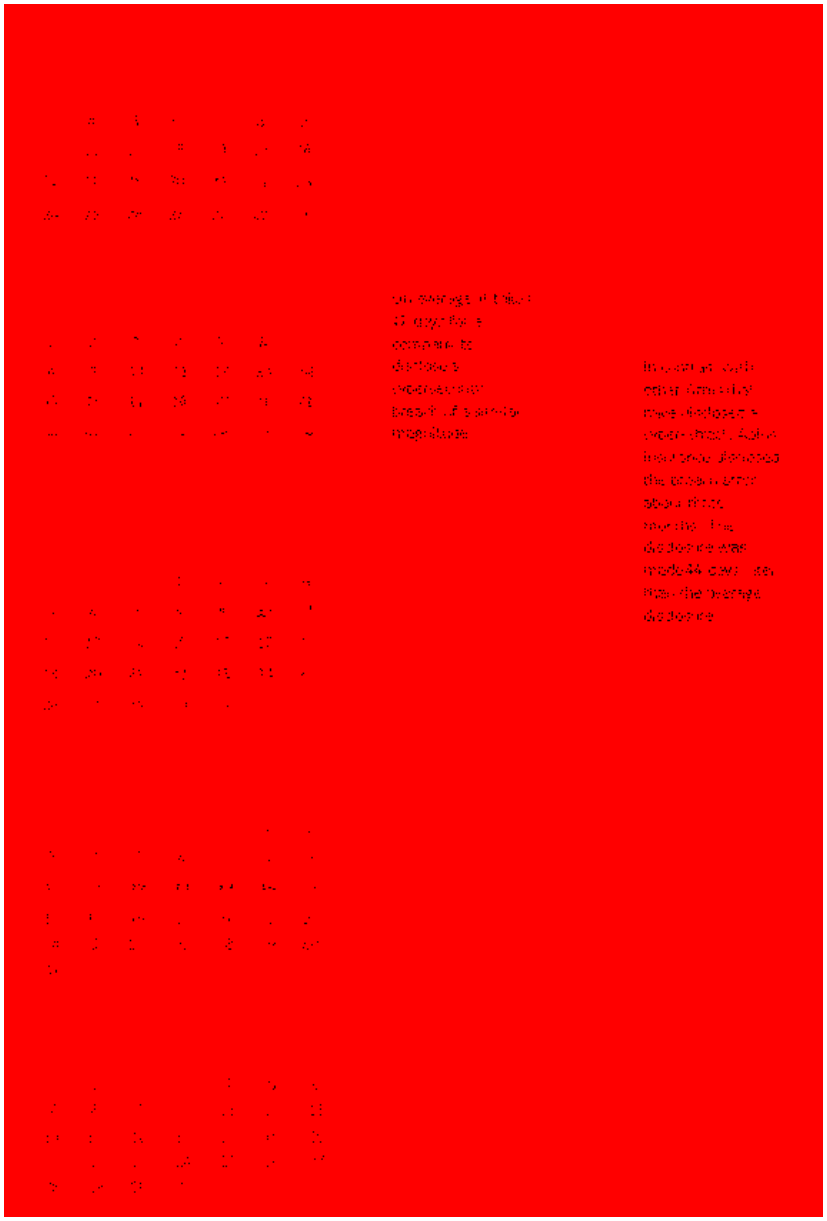
The timeline presented shows that on average, it takes 47 days for a company to disclose a cybersecurity breach of a similar magnitude. However, in contrast with other firms that have disclosed a cyber-attack, Aplus Insurance disclosed the breach after three days. The disclosure was made 44 days earlier than the average disclosure.

The plaintiff questions Aplus Insurance's disclosure timing strategy as it is unlikely that a company would be able to gather comprehensive and accurate information and disclose the information within three days of discovery.

The attorney for the plaintiff asks the jury to find for the plaintiff.

Not Timely/Implausible Condition

The plaintiff also presented the following timeline:



The timeline presented shows that on average, it takes 47 days for a company to disclose a cybersecurity breach of a similar magnitude. However, in contrast with other firms that have disclosed a cyber-attack, Aplus Insurance disclosed the breach after about three months. The disclosure was made 44 days later than the average disclosure.

The plaintiff questions Aplus Insurance's disclosure timing strategy as it took them three months to disclose the incident and it took them another three months to release comprehensive and accurate information about the extent of the breach.

The attorney for the plaintiff asks the jury to find for the plaintiff.

Timely/Control Condition

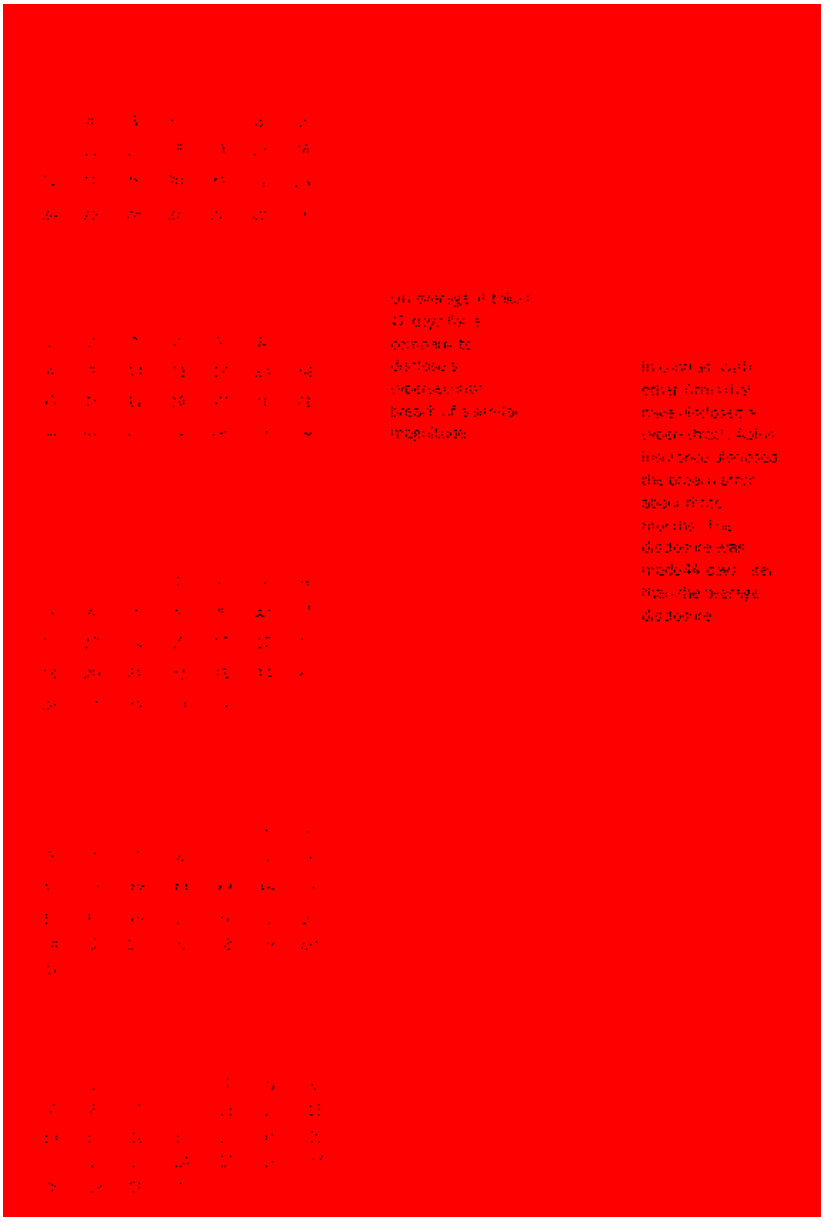
The plaintiff also presented the following timeline:

The timeline presented shows that on average, it takes 47 days for a company to disclose a cybersecurity breach of a similar magnitude. However, in contrast with other firms that have disclosed a cyber-attack, Aplus Insurance disclosed the breach after three days. The disclosure was made 44 days earlier than the average disclosure.

The attorney for the plaintiff asks the jury to find for the plaintiff.

Not Timely/Control Condition

The plaintiff also presented the following timeline:



The timeline presented shows that on average, it takes 47 days for a company to disclose a cybersecurity breach of a similar magnitude. However, in contrast with other firms that have disclosed a cyber-attack, Aplus Insurance disclosed the breach after about three months. The disclosure was made 44 days later than the average disclosure.

The attorney for the plaintiff asks the jury to find for the plaintiff.

Page Break

Timely/Plausible Condition

Defendant Closing Statement

The attorney for the defense revisits the evidence and reviews the key arguments for the case, summarizing why Aplus Insurance should not be held responsible for the class action financial losses. The attorney for the defense maintains that cyber-attacks have become an unavoidable business risk, and revisits evidence that shows that Aplus Insurance discloses cyber-attacks as a risk factor in their annual and quarterly financial reports.

In addition, the attorney for the defense argues that Aplus Insurance takes consumers' privacy very seriously and that the incident was disclosed in the most expedient time possible and without unreasonable delay.

The attorney states that the Company made every effort to gather all the relevant facts of the impact of the breach. A press release was issued quickly to notify customers, so they could take actions to protect their identities. Given the initial uncertainties, management was unable to release accurate information about the extent of the breach at the time of the announcement. A dedicated website was established for customers to access additional information. After gathering all the information, three months after the breach was disclosed, the company issued additional press releases that included comprehensive and accurate information about the extent of the breach.

The attorney for the defense asks the jury to find for the defendant, Aplus Insurance.

Timely/Implausible Condition

Defendant Closing Statement

The attorney for the defense revisits the evidence and reviews the key arguments for the case, summarizing why Aplus Insurance should not be held responsible for the class action financial losses. The attorney for the defense maintains that cyber-attacks have become an unavoidable business risk, and revisits evidence that shows that Aplus Insurance discloses cyber-attacks as a risk factor in their annual and quarterly financial reports.

In addition, the attorney for the defense argues that Aplus Insurance takes consumers' privacy very seriously and that the incident was disclosed in the most expedient time possible and without unreasonable delay.

The attorney states that the Company made every effort to gather all the relevant facts of the impact of the breach. A press release was issued quickly to notify customers, so they could take actions to protect their identities.

The press release included comprehensive and accurate information about the extent of the breach. A dedicated website was established for customers to access additional information.

The attorney for the defense asks the jury to find for the defendant, Aplus Insurance.

Not Timely/Plausible Condition

Defendant Closing Statement

The attorney for the defense revisits the evidence and reviews the key arguments for the case, summarizing why Aplus Insurance should not be held responsible for the class action financial losses. The attorney for the defense maintains that cyber-attacks have become an unavoidable business risk, and revisits evidence that shows that Aplus Insurance discloses cyber-attacks as a risk factor in their annual and quarterly financial reports.

In addition, the attorney for the defense argues that Aplus Insurance takes consumers' privacy very seriously and that the incident was disclosed in the most expedient time possible and without unreasonable delay.

The attorney states that the Company made every effort to gather all the relevant facts of the impact of the breach. Given the initial uncertainties, management was unable to release accurate information about the extent of the breach when the breach was discovered. However, a press release was issued in the most expedient time possible to notify customers, so they could take actions to protect their identities.

The press release included comprehensive and accurate information about the extent of the breach. A dedicated website was established for customers to access additional information.

The attorney for the defense asks the jury to find for the defendant, Aplus Insurance.

Not Timely/Implausible Condition

Defendant Closing Statement

The attorney for the defense revisits the evidence and reviews the key arguments for the case, summarizing why Aplus Insurance should not be held responsible for the class action financial losses. The attorney for the defense maintains that cyber-attacks have become an unavoidable business risk, and revisits evidence that shows that Aplus Insurance discloses cyber-attacks as a risk factor in their annual and quarterly financial reports.

In addition, the attorney for the defense argues that Aplus Insurance takes consumers' privacy very seriously and that the incident was disclosed in the most expedient time possible and without unreasonable delay.

The attorney states that the Company made every effort to gather all the relevant facts of the impact of the breach. Given the initial uncertainties, management was unable to release accurate information about the extent of the breach when the breach was discovered. However, a press release was issued in the most expedient time possible to notify customers, so they could take actions to protect their identities.

A dedicated website was established for customers to access additional information. After gathering all the information, three months after the breach was disclosed, the company issued additional press releases that included comprehensive and accurate information about the extent of the breach.

The attorney for the defense asks the jury to find for the defendant, Aplus Insurance.

Control Condition

Defendant Closing Statement

The attorney for the defense revisits the evidence and reviews the key arguments for the case, summarizing why Aplus Insurance should not be held responsible for the class action financial losses. The attorney for the defense maintains that cyber-attacks have become an unavoidable business risk, and revisits evidence that shows that Aplus Insurance discloses cyber-attacks as a risk factor in their annual and quarterly financial reports.

In addition, the attorney for the defense argues that Aplus Insurance takes consumers' privacy very seriously and that the incident was disclosed in the most expedient time possible and without unreasonable delay.

The attorney for the defense asks the jury to find for the defendant, Aplus Insurance.

End of Block: Plaintiff Arguments

Start of Block: Judge's Instructions

Judge's Instructions to the Jury:

Before allowing the jury to deliberate and determine a verdict, the Judge provides instructions to the jury:

It is your responsibility to determine the facts from the evidence presented to you. You will use these facts and the law given in these instructions to decide the case. You should consider the evidence in light of your observations and experiences in life. You may draw any reasonable inferences from the proven facts. Also, keep in mind that statements made by attorneys are not evidence.

The burden of proof lies with the plaintiff. The level of proof required is the preponderance of the evidence, which means that the allegations are more probably true than not true. To be successful in a claim of liability, the plaintiff must prove by a preponderance of evidence the allegations against Aplus Insurance. You should consider whether the defendant should be held liable for the plaintiff losses. If you decide that the defendant, Aplus Insurance, should not be held liable, you must find in its favor. If you decide that Aplus Insurance should be held liable, you must find for the plaintiff.

If you decide for the plaintiff, you must then determine the amount of money that will reasonably and fairly compensate the Class Members for its $10 billion loss resulting from the stock transactions. The amount of money that you determine must be based on the principle of proportional liability. The principle of proportional liability states that jurors must consider the

extent to which the defendant was responsible for the allegations relative to other responsible parties.

Review Question

It is my responsibility to determine the facts from the evidence presented to me. Statements made by attorneys are not evidence.

- O True
- O False

End of Block: Judge's Instructions

Start of Block: Case Questions

Case Questions

The following questions are intended to assess your views of the defendant's (Aplus Insurance's) level of liability for the plaintiff's alleged losses. ***There are no right or wrong answers - these questions ask for your personal views.*** Please answer the following response questions about the case openly and honestly.

Page Break

Assume that you are a juror on this case. Would you find Aplus Insurance (the defendant) liable with regards to shareholders' losses in connection with the cyber-attack to Aplus Insurance?

O Yes, Aplus Insurance is liable.

O No, Aplus Insurance is not liable.

How confident are you in your verdict?

	Not confident at all	Somewhat not confident	Slightly not confident	Neither not confident nor confident	Slightly confident	Somewhat confident	Very confident
	O	O	O	O	O	O	O

Page Break

DV1: Liability Assessment

How likely is it that Aplus Insurance is liable?

	Extremely Unlikely	Very Unlikely	Unlikely	Neither Unlikely nor Likely	Likely	Very Likely	Extremely Likely
	O	O	O	O	O	O	O

Page Break

Imagine that a majority of the jury has found Aplus Insurance liable and that you will be able to impose damages on Aplus Insurance to pay to compensate Class Members for their $10 billion loss. On the scale below, please indicate the percentage of damages, if any, you would be willing to require that Aplus Insurance pays Class Members? (Remember that the principle of proportional liability applies.)

	0%	10%	20%	30%	40%	50%	60%	70%	80%	90%	100%
	O	O	O	O	O	O	O	O	O	O	O

Page Break

Do you believe Aplus Insurance was grossly negligent in disclosing the cyber-attack (i.e., Aplus Insurance had extreme, reckless disregard for stakeholder's rights to be notified of material events)?

O Yes, Aplus Insurance was grossly negligent.

O No, Aplus Insurance was not grossly negligent.

Page Break

How likely is it that Aplus Insurance was grossly negligent?

	Extremely Unlikely	Very Unlikely	Unlikely	Neither Unlikely nor Likely	Likely	Very Likely	Extremely Likely
	O	O	O	O	O	O	O

Page Break

You may assess punitive damages beyond the recoverable damages up to another $20 billion on Aplus Insurance.
On the scale below, please indicate the percentage of punitive damages, if any, you would be willing to require that Aplus Insurance pays Class Members?

	0%	10%	20%	30%	40%	50%	60%	70%	80%	90%	100%
	O	O	O	O	O	O	O	O	O	O	O

Page Break

Attention Check

For this question ONLY, please choose 1.

	1	2	3	4	5	6	7
	O	O	O	O	O	O	O

Page Break

DV2: Causal Attribution

Based on the information that you have available, what do you think caused the delayed disclosure of the cyber-attack to Aplus Insurance?

Two potential reasons for the timing of Aplus Insurance's disclosure follow: 1) that the disclosure timing was intentional and caused by Aplus Insurance's intent to strategically disclose the cyber-attack to portray the company in a favorable light, or 2) that the disclosure timing was incidental and caused by Aplus Insurance's difficulty in estimating the extent of the breach due to the inherent uncertainty of the event.

On the scale below please indicate which reason is the most likely cause of the disclosure timing:

	Completely incidental	Somewhat more incidental than intentional	Slightly more incidental than intentional	Equally incidental than intentional	Slightly more intentional than incidental	Somewhat more intentional than incidental	Completely intentional
	O	O	O	O	O	O	O

How confident are you in your assessment?

	Not confident at all	Somewhat not confident	Slightly not confident	Neither not confident nor confident	Slightly confident	Somewhat confident	Very confident
	O	O	O	O	O	O	O

Page Break

To what extent do you believe the plaintiff (Class Members) must assume normal investment risks when making investments, and therefore is responsible for its loss?

	Completely Not Responsible for Loss	Not Responsible for Loss	Somewhat not Responsible for Loss	Neither not Responsible for Loss nor Responsible for Loss	Somewhat Responsible for Loss	Responsible for Loss	Completely Responsible for Loss
	O	O	O	O	O	O	O

Page Break

Block: Case Questions

Start of Block: Case Questions 2

To what extent do you agree or disagree with the following statements:

The order of the following questions is randomized

Class Members should have expected a cyber-attack.

	Strongly Disagree	Somewhat Disagree	Slightly Disagree	Neither Agree nor Disagree	Slightly Agree	Somewhat Agree	Strongly Agree
	O	O	O	O	O	O	O

Aplus Insurance cyber-attack was predictable by Class Members.

	Strongly Disagree	Somewhat Disagree	Slightly Disagree	Neither Agree nor Disagree	Slightly Agree	Somewhat Agree	Strongly Agree
	O	O	O	O	O	O	O

Companies in the health and well-being industry have a higher-risk of cyber-attack compared to companies in other industries.

	Strongly Disagree	Somewhat Disagree	Slightly Disagree	Neither Agree nor Disagree	Slightly Agree	Somewhat Agree	Strongly Agree
	O	O	O	O	O	O	O

Manipulation Check - Timeliness

Aplus Insurance disclosed the breach in a timely manner.

	Strongly Disagree	Somewhat Disagree	Slightly Disagree	Neither Agree nor Disagree	Slightly Agree	Somewhat Agree	Strongly Agree
	O	O	O	O	O	O	O

Manipulation Check - Plausibility

Aplus Insurance's justification for the disclosure timing is plausible.

	Strongly Disagree	Somewhat Disagree	Slightly Disagree	Neither Agree nor Disagree	Slightly Agree	Somewhat Agree	Strongly Agree
	O	O	O	O	O	O	O

Manipulation Check - Plausibility

Aplus Insurance's justification for the timing of the disclosure is believable.

	Strongly Disagree	Somewhat Disagree	Slightly Disagree	Neither Agree nor Disagree	Slightly Agree	Somewhat Agree	Strongly Agree
	O	O	O	O	O	O	O

Manipulation Check - Plausibility

Aplus Insurance's justification for the timing of the disclosure is credible.

	Strongly Disagree	Somewhat Disagree	Slightly Disagree	Neither Agree nor Disagree	Slightly Agree	Somewhat Agree	Strongly Agree
	O	O	O	O	O	O	O

Aplus Insurance's was more concerned about disclosing comprehensive and accurate information about the cyber-attack than in disclosing the information in a timely manner.

	Strongly Disagree	Somewhat Disagree	Slightly Disagree	Neither Agree nor Disagree	Slightly Agree	Somewhat Agree	Strongly Agree
	O	O	O	O	O	O	O

Aplus Insurance's should have emphasized more on disclosing comprehensive and accurate information about the cyber-attack than in disclosing the information in a timely manner.

	Strongly Disagree	Somewhat Disagree	Slightly Disagree	Neither Agree nor Disagree	Slightly Agree	Somewhat Agree	Strongly Agree
	O	O	O	O	O	O	O

Delaying the disclosure of a cyber-attack is acceptable given the increased sophistication of hacking techniques.

	Strongly Disagree	Somewhat Disagree	Slightly Disagree	Neither Agree nor Disagree	Slightly Agree	Somewhat Agree	Strongly Agree
	O	O	O	O	O	O	O

Delaying the disclosure of a cyber-attack is acceptable given the complexity of determining the scope of the breach.

	Strongly Disagree	Somewhat Disagree	Slightly Disagree	Neither Agree nor Disagree	Slightly Agree	Somewhat Agree	Strongly Agree
	O	O	O	O	O	O	O

Delaying the disclosure of a cyber-attack is acceptable to conduct required investigations.

	Strongly Disagree	Somewhat Disagree	Slightly Disagree	Neither Agree nor Disagree	Slightly Agree	Somewhat Agree	Strongly Agree
	O	O	O	O	O	O	O

Delaying the disclosure of a cyber-attack is acceptable even when a cyber-attack results in the loss of identifiable information from customers or employees.

	Strongly Disagree	Somewhat Disagree	Slightly Disagree	Neither Agree nor Disagree	Slightly Agree	Somewhat Agree	Strongly Agree
	O	O	O	O	O	O	O

Managers have more incentives to disclose bad news in a timely manner than incentives to delay the disclosure of bad news.

	Strongly Disagree	Somewhat Disagree	Slightly Disagree	Neither Agree nor Disagree	Slightly Agree	Somewhat Agree	Strongly Agree
	O	O	O	O	O	O	O

Compared to companies with lower risk of cyber-attacks, companies with higher risk of cyber-attacks are expected to have stronger controls for detecting and disclosing cybersecurity incidents in a timely manner.

	Strongly Disagree	Somewhat Disagree	Slightly Disagree	Neither Agree nor Disagree	Slightly Agree	Somewhat Agree	Strongly Agree
	O	O	O	O	O	O	O

End of Block: Case Questions 2

Start of Block: Thanks

Thanks for completing the task!
After completion of the following questionnaire you will receive a validation code to be used to process your payment.

End of Block: Thanks

Start of Block: Demographics

What is your gender?

- O Male
- O Female

What is your age?

- O 18 to 28 years
- O 29 to 38 years
- O 39 to 48 years
- O 49 to 58 years
- O 59 to 69 years
- O Over 70 years

Here is a 7-point scale on which the political views that people might hold are arranged from extremely liberal (left) to extremely conservative (right). Where would you place yourself on this scale?

	Extremely liberal	Somewhat liberal	Slightly liberal	Neither liberal nor conservative	Slightly conservative	Somewhat conservative	Extremely conservative
1	O	O	O	O	O	O	O

What is the highest level of school you have completed or the highest degree you have received?

- O Less than high school degree
- O High school graduate (high school diploma or equivalent including GED)
- O Some college but no degree
- O Associate degree in college (2-year)
- O Bachelor's degree in college (4-year)
- O Master's degree
- O Professional degree (JD, MD)
- O Doctoral Degree

If you studied beyond high school, what was your area of concentration?

_____

What is your current employment status?

- O Full-time employment
- O Part-time employment
- O Self-employed
- O Full-time student
- O Retired
- O Not currently employed, but looking for work
- O Not currently employed and not looking for work

Which of the following industries most closely matches the one in which you are employed?

- O Forestry, fishing, hunting or agriculture support
- O Real estate or rental and leasing
- O Mining
- O Professional, scientific or technical services
- O Utilities
- O Management of companies or enterprises
- O Construction
- O Admin, support, waste management or remediation services
- O Manufacturing
- O Educational services
- O Wholesale trade
- O Health care or social assistance
- O Retail trade
- O Arts, entertainment or recreation
- O Transportation or warehousing
- O Accommodation or food services
- O Information
- O Other services (except public administration)

O Finance or insurance

O Unclassified establishments

Information about income is very important to understand. Would you please give your best guess?Please indicate the answer that includes your entire household income in (previous year) before taxes.

O Less than $20,000

O $20,000 to $39,999

O $40,000 to $59,999

O $60,000 to $79,999

O $80,000 to $99,999

O $100,000 to $149,999

O $150,000 or more

Have you ever worked for an insurance company or a health provider?

O Yes

O No

Have you ever worked as a lawyer or for a law firm?

O Yes

O No

Have you been a victim of identity theft?

O Yes

O No

Have you been a victim of a cybersecurity attack?

O Yes

O No

Have you ever made personal investments in the common stock of a company?

O Yes

O No

Have you ever served on a jury before?

O Yes

O No

End of Block: Demographics

APPENDIX H: STUDY TWO EXPERIMENTAL MATERIALS

Comments to reviewers are made in Red, Bold, and Italics

Start of Block: Consent

EXPLANATION OF RESEARCH

Title of Project: Investors' judgments and decisions
Principal Investigator: Patricia Navarro-Velez
Faculty Supervisor: Steven G. Sutton

You are being invited to take part in a research study. Whether you take part is up to you.

The purpose of this study is to explore how investors make valuation judgments. You will receive one of several business contexts/situations.

You will assume the role of an investor to evaluate a company's stock value in light of some information that will be made available to you.

This study will be administered online. We expect that it will take you approximately 20 minutes to complete this experiment.

You must be 18 years of age or older to take part in this research study.

Study contact for questions about the study or to report a problem: If you have questions, concerns, or complaints contact Patricia Navarro-Velez, Doctoral Candidate, UCF Accounting Department at (407)823-5837 or Dr. Steve G. Sutton, Faculty Advisor, UCF Accounting Department at (407)823-5857.

IRB contact about your rights in the study or to report a complaint:
Research at the University of Central Florida involving human participants is carried out under the oversight of the Institutional Review Board (UCF IRB). This research has been reviewed and approved by the IRB. For information about the rights of people who take part in research, please contact: Institutional Review Board, University of Central Florida, Office of Research & Commercialization, 12201 Research Parkway, Suite 501, Orlando, FL 32826-3246 or by telephone at (407) 823-2901. search.

End of Block: Consent

Start of Block: Screening M Turk

Are you at least 18 years of age and a United States Citizen?

O Yes

O No

Are you a native English speaker?

O Yes

O No

Have you taken 2 or more Accounting or Financial courses at the college level?

O Yes

O No

Can you read and understand financial statements?

O Yes

O No

Have you ever made personal investments in the common stock of a company?

O Yes

O No

End of Block: Screening M Turk

Start of Block: Instructions

Only participants who answer Yes to screening question 1-4 are allowed to continue the survey.

You must complete this task in a single sitting. The task will take about 20 minutes to complete. If you do not have approximately 20 minutes to complete the task right now, please do not start the study.

It is also critical that you do not complete this study twice or discuss this study with others. This is serious research of interest to financial regulators, and the results could be compromised or ruined by you discussing materials with others.

End of Block: Instructions

Start of Block: Instructions 2

Your task today is to evaluate a company, in light of selected information that will be made available to you. The information you receive is not intended to include all the information that you might desire. However, do your best in light of the information provided and please base your answers to the questions on only the information provided. There are no right or wrong answers to the case questions you will be asked.

It is important that you read all case materials carefully and answer the included questions thoughtfully and honestly. Throughout the case you will answer the following three types of questions:

Review Questions reflect whether you read and understand the presented material. These questions will not be difficult if you read the materials carefully.
Case Questions ask you for your judgments about the outcomes of the facts described in the case. There are no right or wrong answers to these questions.
Wrap-Up Questions ask you some miscellaneous perception and demographic questions.

IMPORTANT: YOU MUST ANSWER 100% OF THE REVIEW QUESTIONS CORRECTLY TO BE COMPENSATED.

Review Question:

To be compensated, I must answer at least:

- O 50% of the review questions correctly.
- O 75% of the review questions correctly.
- O 100% of the review questions correctly.

End of Block: Instructions 2

Start of Block: Task 1

Some initial background information on the company is provided below:

About Aplus Auto Care:

Headquartered in San Diego, California, Aplus Auto Care is a leading American corporation in the car warranty and related solutions industry.

The company was founded in 1987 and serves over 74 million people throughout the United States.

End of Block: Task 1

Start of Block: Case Question

DV1a: Initial Valuation

Case Question 1:
(Note that case questions ask you for your judgments about the outcomes of the facts described in the case. There are no right or wrong answers to these questions.)

On the following scale, please indicate what you believe to be an appropriate common stock valuation for Aplus, ranging from very low to very high.

Given that you have very little information about Aplus up to this point, for now, you can assume that an "average" common stock valuation for Aplus is appropriate. In other words, for

this particular judgment, you should choose a value that is either at or very near '4' on the scale below.

	Very Low	Moderately Low	Slightly Low	Neither Low nor High	Slightly High	Moderately High	Very High
The appropriate common stock valuation for Aplus is:	O	O	O	O	O	O	O

End of Block: Case Question

Start of Block: Financial Information

Relevant Financial Information:

Below you are provided with selected financial information taken from the Annual Reports of Aplus Auto Care for the year ended December 31, 2016.

(in million dollars)

	2016	2015	2014
Net Assets	$65,083	$61,717	$61,676
Net Income	$2,569	$2,560	$2,469
Earnings per Share	5.56	4.82	4.76

Following the release of the 2016 financial statements in February 2017, the stock price of the company continued on a positive trend, and analysts considered this company to be a strong investment.

Review Questions

As reported in the tabulated information included in Aplus' annual report, there has been a consistent _____ trend in total Net Assets, Net Income, and Earnings per Share (EPS).

O Positive

O Negative

Following the release of the 2016 financial statements on February 2017, the stock price of the company continued on a _____ trend.

O Positive

O Negative

End of Block: Financial Information

Start of Block: Press Release Info

You also learned that a press release was issued by Aplus Auto Care. The press release that was provided by Aplus Auto Care is presented on the next page.

Please take the time to thoroughly review the press release in order to answer the questions that will follow. The success of this research depends on you paying careful attention to the task.

End of Block: Press Release Info

Start of Block: Press Release

Aplus Auto Care, Inc. Investigation on Data Breach

LOS ANGELES, July 1, 2017 /PRNewswire/ -- Statement regarding cyber-attack against Aplus Auto Care, Inc.

Cyber attackers executed a very sophisticated attack to gain unauthorized access to our parent company's IT systems and have obtained personal information relating to customers and employees. The information accessed includes names, birthdays, social security numbers, street addresses, email addresses and employment information, including income data. No credit card information was compromised, nor is there evidence at this time that any other information was targeted or obtained.

As soon as we learned about the attack, we immediately made every effort to close the security vulnerability, contacted authorities and began fully cooperating with their investigation.

Aplus Auto Care will individually notify current and former members whose information has been accessed. Credit monitoring and identity protection services will be provided free of charge so that those who have been affected can have peace of mind.

The company has established a dedicated website (www.apbreach.com) where members can access information, including frequently asked questions and answers.

We take consumers' privacy very seriously and are doing everything in our power to make our systems and security processes – and most importantly your data – more secure. In the meantime, as we learn more, we will continue to provide updates.

End of Block: Press Release

Start of Block: Assurance Info

Relevant Cyber-risk Management and Assurance Practices:

Upon further investigation, you find that, cyber-attacks are considered a business risk which organizations should address with a cybersecurity risk management program. You also find that, in response to the increased threat of cyber-attacks to organizations, the American Institute of Certified Public Accountants (AICPA) has developed a cybersecurity risk management reporting framework for organizations to provide users with information about the processes and controls they have implemented to mitigate cybersecurity risks (e.g. restricted access to unauthorized users). This framework is also used by Certified Public Accountants (CPAs) to evaluate the effectiveness of cybersecurity controls within an organization and to report the results in a Service Organization Controls (SOC) report.

A SOC over cybersecurity is a report that includes a description of the company's controls over cybersecurity and that also includes an independent audit opinion over the operating effectiveness of cybersecurity controls. For instance, a company describes how they restrict access to information systems to only authorized users and the independent auditor reports whether that control is operating effectively.

A clean opinion in a SOC report denotes that there is reasonable assurance that the cybersecurity controls are in place and operating effectively. This independent auditor's report is desirable for companies with high risk from cyber-attacks.

Page Break

Assurance Expected Condition

Additional Information:

You decided to do some additional research to find out about cybersecurity assurance practices in this industry.

You found that cybersecurity assurance is voluntary but that most firms in this industry **choose** to engage in cybersecurity assurance with an independent auditor.

Therefore, you expect that Aplus Auto Care, Inc. will choose to engage in cybersecurity assurance with an independent auditor.

Assurance Not Expected Condition

Additional Information:

You decided to do some additional research to find out about cybersecurity assurance practices in this industry.

You found that cybersecurity assurance is voluntary but that most firms in this industry **do not choose** to engage in cybersecurity assurance with an independent auditor.

Therefore, you expect that Aplus Auto Care, Inc. will not choose to engage in cybersecurity assurance with an independent auditor.

Page Break

Assurance/Conform to Expectancies Condition

Aplus Auto Care, Inc. Cyber-risk Management and Assurance Practices:

Aplus Auto Care reports that they have their own cybersecurity risk management program in place and operating effectively.

In addition, you noticed that, consistent with the rest of the firms in the industry, Aplus Auto Care voluntarily engaged an Independent Auditor to complete an examination to evaluate the effectiveness of Aplus' cybersecurity controls during 2016 (the year before Aplus Auto Care learned about the data breach).

Aplus Auto Care's auditor issued a clean opinion in their SOC report in January 2017 (before Aplus Auto Care learned about the data breach).

No Assurance/Conform to Expectancies Condition

Aplus Auto Care, Inc. Cyber-risk Management and Assurance Practices:

Aplus Auto Care reports that they have their own cybersecurity risk management program in place and operating effectively.

However, you noticed that, consistent with the rest of the firms in the industry, Aplus Auto Care has not engaged an Independent Auditor to complete an examination to evaluate the effectiveness of their cybersecurity controls.

Additional Analysis – No CRM/Conform to Expectancies Condition

Aplus Auto Care, Inc. Cyber-risk Management and Assurance Practices:

You noticed that, consistent with the rest of the firms in the industry, Aplus Auto Care does not have a cybersecurity risk management program in place and has not engaged an Independent Auditor to complete an examination to evaluate the effectiveness of their cybersecurity controls.

Additional Analysis – No CRM/Violate Expectancies Condition

Aplus Auto Care, Inc. Cyber-risk Management and Assurance Practices:

You noticed that, in contrast with the rest of the firms in the industry, Aplus Auto Care does not have a cybersecurity risk management program in place and has not engaged an Independent Auditor to complete an examination to evaluate the effectiveness of their cybersecurity controls.

No Assurance/Violate Expectancies Condition

Aplus Auto Care, Inc. Cyber-risk Management and Assurance Practices:

Aplus Auto Care reports that they have their own cybersecurity risk management program in place and operating effectively.

However, you noticed that, in contrast with the rest of the firms in the industry, which have engaged in cybersecurity assurance services, Aplus Auto Care has not engaged an Independent Auditor to complete an examination to evaluate the effectiveness of their cybersecurity controls.

Assurance/Violate Expectancies Condition

Aplus Auto Care, Inc. Cyber-risk Management and Assurance Practices:

Aplus Auto Care reports that they have their own cybersecurity risk management program in place and operating effectively.

In addition, you noticed that, in contrast with the rest of the firms in the industry, that have not engaged in cybersecurity assurance services, Aplus Auto Care voluntarily engaged an Independent Auditor to complete an examination to evaluate the effectiveness of their cybersecurity controls during 2016 (the year before Aplus Auto Care learned about the data breach).

Aplus Auto Care's auditor issued a clean opinion in their SOC report in January 2017 (before Aplus Auto Care learned about the data breach).

End of Block: Assurance Info

Start of Block: Case Questions

Case Questions:

(Note that case questions ask you for your judgments about the outcomes of the facts described in the case. There are no right or wrong answers to these questions.)

DV1b: Final Valuation

Considering the new information provided, please indicate what you believe to be an appropriate common stock valuation for Aplus, ranging from very low to very high.

	Very Low	Moderately Low	Slightly Low	Neither Low nor High	Slightly High	Moderately High	Very High
The appropriate common stock valuation for Aplus is:	O	O	O	O	O	O	O

DV2a: Management Credibility / Competence

How competent or incompetent do you believe the management of Aplus to be?

Very Incompetent	Incompetent	Somewhat Incompetent	Neither Incompetent nor Competent	Somewhat Competent	Competent	Very Competent
O	O	O	O	O	O	O

DV2b: Management Credibility / Trustworthiness

How trustworthy or untrustworthy do you believe the management of Aplus to be?

Very Untrustworthy	Untrustworthy	Somewhat Untrustworthy	Neither Untrustworthy nor Trustworthy	Somewhat Trustworthy	Trustworthy	Very Trustworthy
O	O	O	O	O	O	O

End of Block: Case Questions

The order of the following questions is randomized

Case Questions:

Please indicate the extent to which you agree with the following statements:

	Strongly Disagree	Somewhat Disagree	Slightly Disagree	Neither Agree nor Disagree	Slightly Agree	Somewhat Agree	Strongly Agree
"Independent cybersecurity audits are necessary to be able to substantiate professional care"	O	O	O	O	O	O	O
"Independent cybersecurity audits are beneficial, as the auditor can be used as a codefendant in case of litigation"	O	O	O	O	O	O	O
"Independent cybersecurity audits are beneficial, as the auditor and the company share an interest to protect both of their reputation in case of litigation"	O	O	O	O	O	O	O

“Independent cybersecurity audits are beneficial, as the auditor shares a portion of the company’s legal responsibility in case of litigation”	O	O	O	O	O	O	O
“Aplus Auto Care was expected to engage in cybersecurity assurance before the data breach.”	O	O	O	O	O	O	O
“I am worry about Aplus Auto Care's cybersecurity risks.”	O	O	O	O	O	O	O
“It is very difficult for Aplus Auto Care management to use their skill and diligence to control (limit) the company's cybersecurity risks.”	O	O	O	O	O	O	O
“Aplus Auto Care is a company with high cybersecurity.”	O	O	O	O	O	O	O

“Aplus Auto Care's cybersecurity risks are likely to be catastrophic.”	O	O	O	O	O	O	O
"Accountants have significant experience auditing information security and cybersecurity controls."	O	O	O	O	O	O	O
"Accountants spend a significant portion of their time auditing information security and cybersecurity controls.”	O	O	O	O	O	O	O
"Accountants receive significant combined informal and formal training in relation to information security and cybersecurity controls.”	O	O	O	O	O	O	O
"Accountants have a high level of information security and cybersecurity controls expertise.”	O	O	O	O	O	O	O

For this questions, select "4".	O	O	O	O	O	O	O

End of Block: Case Questions 2

Start of Block: Manipulation Checks

Review Questions:

Manipulation Check -CRM

Based on the case information, you learned that Aplus Auto Care has their own cybersecurity risk management program in place and operating effectively.

O True

O False

Manipulation Check - Assurance

Based on the case information, you learned that Aplus Auto Care voluntarily engaged an Independent Auditor to complete an examination to evaluate the effectiveness of their cybersecurity controls.

O True

O False

Manipulation Check – Assurance Expectancies

Based on the case information, most firms in the car warranty and related solutions industry choose to engage in cybersecurity assurance services with an independent auditor.

O True

O False

End of Block: Manipulation Checks

Start of Block: Thanks

Thanks for completing the task! After completion of the following questionnaire you will receive a validation code to be used to process your payment.

End of Block: Thanks

Start of Block: Demographics

What is your gender?

- O Male
- O Female

What is your age?

- O 18 to 28 years
- O 29 to 38 years
- O 39 to 48 years
- O 49 to 58 years
- O 59 to 69 years
- O Over 70 years

What is the highest level of school you have completed or the highest degree you have received?

- O Less than high school degree
- O High school graduate (high school diploma or equivalent including GED)
- O Some college but no degree
- O Associate degree in college (2-year)
- O Bachelor's degree in college (4 years)
- O Master's degree
- O Professional degree (JD, MD)
- O Doctoral degree

If you studied beyond high school, what was your area of concentration?

_____

What is your current employment status?

- O Full-time employment
- O Part-time employment
- O Self-employed
- O Full-time student
- O Retired
- O Not currently employed, but looking for work
- O Not currently employed and not looking for work

Which of the following industries most closely matches the one in which you are employed?

- O Forestry, fishing, hunting or agriculture support
- O Real estate or rental and leasing
- O Mining
- O Professional, scientific or technical services
- O Utilities
- O Management of companies or enterprises
- O Construction
- O Admin, support, waste management or remediation services
- O Manufacturing
- O Educational services
- O Wholesale trade
- O Health care or social assistance
- O Retail trade
- O Arts, entertainment or recreation
- O Transportation or warehousing
- O Accommodation or food services
- O Information
- O Other services (except public administration)

O Finance or insurance

O Unclassified establishments

Please indicate the answer that includes your entire household income in (previous year) before taxes.

O Less than $20,000

O $20,000 to $39,999

O $40,000 to $59,999

O $60,000 to $79,999

O $80,000 to $99,999

O $100,000 to $149,999

O $150,000 or more

Approximately, how many years of personal investment experience do you have?

O Less than one year

O More than one year but less than three years

O More than three years but less than five years

O More than five years

O No experience

Approximately, how many times have you purchased common stock of a company as a personal investment?

_____

End of Block: Demographics

APPENDIX I: STUDY THREE EXPERIMENTAL MATERIALS

Comments to reviewers are made in Red, Bold, and Italics

Start of Block: Screening M Turk

Are you at least 18 years of age and a United States Citizen?

O Yes

O No

Are you a native English speaker?

O Yes

O No

Have you taken 2 or more Accounting or Financial courses at the college level?

O Yes

O No

Can you read and understand financial statements?

O Yes

O No

Have you ever made personal investments in the common stock of a company?

O Yes

O No

Please provide your Mturk ID:

_____

Only participants who answer Yes to screening question 1-4 are allowed to continue the survey.

End of Block: Screening M Turk

Start of Block: Consent

EXPLANATION OF RESEARCH

Title of Project: Investors Valuation Judgments
Principal Investigator: Patricia Navarro-Velez
Faculty Supervisor: Steve G. Sutton, PhD

You are being invited to take part in a research study. Whether you take part is up to you.

Thank you for agreeing to participate in our research. Before you begin, please note that the data you provide may be collected and used by Amazon as per its privacy agreement. This agreement shall be interpreted according to United States law.

The purpose of this study is to explore how investors make valuation judgments. You will receive one of several business contexts/situations. You will assume the role of an investor to evaluate a company's stock value in light of some information that will be made available to you.

This study will be administered online. We expect that it will take you approximately 20 minutes to complete this experiment. After successful completion of the study, you will be compensated with $2.50. Compensation will be processed through your Mturk account.

You must be 18 years of age or older, a United States citizen, native English speaker that have taken two or more accounting or financial courses at the college level, and that can read and understand financial statements to take part in this research study. You must also have completed at least 1,000 Mturk HITs with over 98% approval rate.

Study contact for questions about the study or to report a problem: If you have questions, concerns, or complaints: Patricia Navarro-Velez, Doctoral Candidate, UCF Accounting Department at (407)823-5837 or Dr. Steve G. Sutton, Faculty Advisor, UCF Accounting Department at (407)823-5857.

IRB contact about your rights in this study or to report a complaint:
If you have questions about your rights as a research participant, or have concerns about the conduct of this study, please contact Institutional Review Board (IRB), University of Central

Florida, Office of Research, 12201 Research Parkway, Suite 501, Orlando, FL 32826-3246 or by telephone at (407) 823-2901, or email irb@ucf.edu.

End of Block: Consent

Start of Block: Instructions

You must complete this task in a single sitting. The task will take about 20 minutes to complete. If you do not have approximately 20 minutes to complete the task right now, please do not start the study.

It is also critical that you do not complete this study twice or discuss this study with others. This is serious research of interest to financial regulators, and the results could be compromised or ruined by you discussing materials with others.

End of Block: Instructions

Start of Block: Instructions 2

Your task today is to evaluate a company, in light of selected information that will be made available to you. The information you receive is not intended to include all the information that you might desire. However, do your best in light of the information provided and please base your answers to the questions on only the information provided. There are no right or wrong answers to the case questions you will be asked.

It is important that you read all case materials carefully and answer the included questions thoughtfully and honestly. Throughout the case you will answer the following three types of

questions:

Review Questions reflect whether you read and understand the presented material. These questions will not be difficult if you read the materials carefully.
Case Questions ask you for your judgments about the outcomes of the facts described in the case. There are no right or wrong answers to these questions.
Wrap-Up Questions ask you some miscellaneous perception and demographic questions.

IMPORTANT: YOU MUST ANSWER 100% OF THE REVIEW QUESTIONS CORRECTLY TO BE COMPENSATED.

Review Question:

To be compensated, I must answer at least:

- O 50% of the review questions correctly.
- O 75% of the review questions correctly.
- O 100% of the review questions correctly.

End of Block: Instructions 2

Start of Block: Task 1

Some initial background information on the company is provided below:

About Aplus Insurance:

Headquartered in San Diego, California, Aplus Insurance is a leading American corporation in the health and well-being industry.

The company was founded in 1987 and serves over 74 million people throughout the United States.

Page Break

End of Block: Task 1

Start of Block: Case Question

DV1a: Initial Valuation

Case Question 1:

(Note that case questions ask you for your judgments about the outcomes of the facts described in the case. There are no right or wrong answers to these questions.)

On the following scale, please indicate what you believe to be an appropriate common stock valuation for Aplus, ranging from very low to very high.

Given that you have very little information about Aplus up to this point, for now, you can assume that an "average" common stock valuation for Aplus is appropriate. In other words, for this particular judgment, you should choose a value that is either at or very near '4' on the scale below.

The appropriate common stock valuation for Aplus is:

	Very Low	Moderately Low	Slightly Low	Neither Low nor High	Slightly High	Moderately High	Very High
	O	O	O	O	O	O	O

End of Block: Case Question

Start of Block: Financial Information

Relevant Financial Information:

Below you are provided with selected financial information taken from the Annual Reports of Aplus Insurance for the year ended December 31, 2016.

(in million dollars)

	2016	2015	2014
Net Assets	$65,083	$61,717	$61,676
Net Income	$2,569	$2,560	$2,469
Earnings per Share	5.56	4.82	4.76

Following the release of the 2016 financial statements in February 2017, the stock price of the company continued on a positive trend, and analysts considered this company to be a strong investment.

Review Questions

As reported in the tabulated information included in Aplus Insurance's annual report, there has been a consistent _____ trend in total Net Assets, Net Income, and Earnings per Share (EPS).

O Positive

O Negative

Following the release of the 2016 financial statements on February 2017, the stock price of the company continued on a _____ trend.

O Positive

O Negative

End of Block: Financial Information

Start of Block: Press Release Info

You also learned that a press release was issued by Aplus Insurance. The press release that was provided by Aplus Insurance is presented on the next page.

Please take the time to thoroughly review the press release in order to answer the questions that will follow.

End of Block: Press Release Info

Start of Block: Press Release

Timely Condition

Aplus Insurance, Inc. Investigation on Data Breach

LOS ANGELES, July 15, 2017 /PRNewswire/ -- Statement regarding cyber-attack against Aplus Insurance, Inc.

On November 2016 cyber attackers executed a very sophisticated attack to gain unauthorized access to our parent company's IT systems and have obtained personal information relating to customers and employees. The information accessed includes names, birthdays, social security numbers, street addresses, email addresses and employment information, including income data. No credit card information was compromised, nor is there evidence at this time that any other information was targeted or obtained.

As soon as we learned about the attack, three days ago, on July 13, 2017, we immediately made every effort to close the security vulnerability, contacted authorities and began fully cooperating with their investigation.

Aplus Insurance will individually notify current and former members whose information has been accessed. Credit monitoring and identity protection services will be provided free of charge so that those who have been affected can have peace of mind.

The company has established a dedicated website (www.apbreach.com) where members can access information, including frequently asked questions and answers.

We take consumers' privacy very seriously and are doing everything in our power to make our systems and security processes – and most importantly your data – more secure. In the meantime, as we learn more, we will continue to provide updates.

Page Break

Not Timely Condition

Aplus Insurance, Inc. Investigation on Data Breach

LOS ANGELES, July 15, 2017 /PRNewswire/ -- Statement regarding cyber-attack against Aplus Insurance, Inc.

On August 2016, cyber attackers executed a very sophisticated attack to gain unauthorized access to our parent company's IT systems and have obtained personal information relating to customers and employees. The information accessed includes names, birthdays, social security numbers, street addresses, email addresses and employment information, including income data. No credit card information was compromised, nor is there evidence at this time that any other information was targeted or obtained.

As soon as we learned about the attack, three months ago, on April 15, 2017, we immediately made every effort to close the security vulnerability, contacted authorities and began fully cooperating with their investigation.

Aplus Insurance will individually notify current and former members whose information has been accessed. Credit monitoring and identity protection services will be provided free of charge so that those who have been affected can have peace of mind.

The company has established a dedicated website (www.apbreach.com) where members can access information, including frequently asked questions and answers.

We take consumers' privacy very seriously and are doing everything in our power to make our systems and security processes – and most importantly your data – more secure. In the meantime, as we learn more, we will continue to provide updates.

End of Block: Press Release

Start of Block: Assurance Info

Timely Condition

Relevant Cyber-risk Management and Assurance Practices:

Upon further investigation, you find that, Aplus Insurance disclosed the breach promptly, compared with other firms that have experienced a cybersecurity incident. You also find that cyber-attacks are considered a business risk which organizations should address with a cybersecurity risk management program. You also find that, in response to the increased threat of cyber-attacks to organizations, the American Institute of Certified Public Accountants (AICPA) has developed a cybersecurity risk management reporting framework for organizations to provide users with information about the processes and controls they have implemented to mitigate cybersecurity risks (e.g. restricted access to unauthorized users). This framework is also used by Certified Public Accountants (CPAs) to evaluate the effectiveness of cybersecurity controls within an organization and to report the results in a Service Organization Controls (SOC) report.

A SOC over cybersecurity is a report that includes a description of the company's controls over cybersecurity and that also includes an independent audit opinion over the operating effectiveness of cybersecurity controls. For instance, a company describes how they restrict access to information systems to only authorized users and the independent auditor reports whether that control is operating effectively.

A clean opinion in a SOC report denotes that there is reasonable assurance that the cybersecurity controls are in place and operating effectively. This independent auditor's report is desirable for companies with high risk from cyber-attacks.

Page Break

Not Timely Condition

Relevant Cyber-risk Management and Assurance Practices:

Upon further investigation, you find that, Aplus Insurance disclosed the breach late, compared with other firms that have experienced a cybersecurity incident. You also find that cyber-attacks are considered a business risk which organizations should address with a cybersecurity risk management program. You also find that, in response to the increased threat of cyber-attacks to organizations, the American Institute of Certified Public Accountants (AICPA) has developed a cybersecurity risk management reporting framework for organizations to provide users with information about the processes and controls they have implemented to mitigate cybersecurity risks (e.g. restricted access to unauthorized users). This framework is also used by Certified Public Accountants (CPAs) to evaluate the effectiveness of cybersecurity controls within an organization and to report the results in a Service Organization Controls (SOC) report.

A SOC over cybersecurity is a report that includes a description of the company's controls over cybersecurity and that also includes an independent audit opinion over the operating effectiveness of cybersecurity controls. For instance, a company describes how they restrict access to information systems to only authorized users and the independent auditor reports whether that control is operating effectively.

A clean opinion in a SOC report denotes that there is reasonable assurance that the cybersecurity controls are in place and operating effectively. This independent auditor's report is desirable for companies with high risk from cyber-attacks.

Page Break

Assurance Condition

Aplus Insurance, Inc. Cyber-risk Management and Assurance Practices:

Aplus Insurance reports that they have a cybersecurity risk management program in place and operating effectively. In addition, you noticed that during 2016 Aplus Insurance voluntarily engaged an Independent Auditor to complete an examination to evaluate the effectiveness of their cybersecurity controls during 2016 (the year before Aplus Insurance learned about the data breach). Aplus Insurance's auditor issued a clean opinion in their SOC report on January 2017 (before Aplus Insurance learned about the data breach).

No Assurance Condition

Aplus Insurance, Inc. Cyber-risk Management and Assurance Practices:
Aplus Insurance reports that they have a cybersecurity risk management program in place and operating effectively. However, you noticed that Aplus Insurance has not engaged an Independent Auditor to complete an examination to evaluate the effectiveness of their cybersecurity controls.

Page Break

End of Block: Assurance Info

Start of Block: Case Questions

Case Questions:
(Note that case questions ask you for your judgments about the outcomes of the facts described in the case. There are no right or wrong answers to these questions.)

DV1b: Final Valuation

Your initial stock valuation for Aplus was ***${DV1A/ChoiceGroup/SelectedAnswers}***.

Considering the new information provided, please indicate what you believe to be an appropriate common stock valuation for Aplus, ranging from very low to very high.

	Very Low	Moderately Low	Slightly Low	Neither Low nor High	Slightly High	Moderately High	Very High
	O	O	O	O	O	O	O

DV2a: Management Credibility / Competence

How competent or incompetent do you believe the management of Aplus to be?

	Very Incompetent	Incompetent	Somewhat Incompetent	Neither Incompetent nor Competent	Somewhat Competent	Competent	Very Competent
	O	O	O	O	O	O	O

DV2b: Management Credibility / Trustworthiness

How trustworthy or untrustworthy do you believe the management of Aplus to be?

	Very Untrustworthy	Untrustworthy	Somewhat Untrustworthy	Neither Untrustworthy nor Trustworthy	Somewhat Trustworthy	Trustworthy	Very Trustworthy
	O	O	O	O	O	O	O

End of Block: Case Questions

Start of Block: Manipulation Checks

Review Questions:

Based on the case information, you learned that Aplus Insurance has their own cybersecurity risk management program in place and operating effectively.

O True

O False

Manipulation Check: Assurance

Based on the case information, you learned that Aplus Insurance voluntarily engaged an Independent Auditor to complete an examination to evaluate the effectiveness of their cybersecurity controls.

O True

O False

End of Block: Manipulation Checks

Start of Block: Case Questions 2

Case Questions:
(Note that case questions ask you for your judgments about the outcomes of the facts described in the case. There are no right or wrong answers to these questions.)

Please indicate the extent to which you agree with the following statements:

The order of the following questions is randomized

“Independent cybersecurity audits are necessary to be able to substantiate professional care”

	Strongly Disagree	Somewhat Disagree	Slightly Disagree	Neither Agree nor Disagree	Slightly Agree	Somewhat Agree	Strongly Agree
	O	O	O	O	O	O	O

“Independent cybersecurity audits are beneficial, as the auditor can be used as a codefendant in case of litigation”

	Strongly Disagree	Somewhat Disagree	Slightly Disagree	Neither Agree nor Disagree	Slightly Agree	Somewhat Agree	Strongly Agree
	O	O	O	O	O	O	O

“Independent cybersecurity audits are beneficial, as the auditor and the company share an interest to protect both of their reputation in case of litigation”

	Strongly Disagree	Somewhat Disagree	Slightly Disagree	Neither Agree nor Disagree	Slightly Agree	Somewhat Agree	Strongly Agree
	O	O	O	O	O	O	O

“Independent cybersecurity audits are beneficial, as the auditor shares a portion of the company’s legal responsibility in case of litigation”

	Strongly Disagree	Somewhat Disagree	Slightly Disagree	Neither Agree nor Disagree	Slightly Agree	Somewhat Agree	Strongly Agree
	O	O	O	O	O	O	O

Manipulation Check - Timeliness

"Aplus Insurance disclose the breach on a timely manner."

	Strongly Disagree	Somewhat Disagree	Slightly Disagree	Neither Agree nor Disagree	Slightly Agree	Somewhat Agree	Strongly Agree
	O	O	O	O	O	O	O

"I am worry about Aplus Insurance's cybersecurity risks."

	Strongly Disagree	Somewhat Disagree	Slightly Disagree	Neither Agree nor Disagree	Slightly Agree	Somewhat Agree	Strongly Agree
	O	O	O	O	O	O	O

"It is very difficult for Aplus Insurance management to use their skill and diligence to control (limit) the company's cybersecurity risks."

	Strongly Disagree	Somewhat Disagree	Slightly Disagree	Neither Agree nor Disagree	Slightly Agree	Somewhat Agree	Strongly Agree
	O	O	O	O	O	O	O

"Aplus Insurance is a company with high cybersecurity risk."

	Strongly Disagree	Somewhat Disagree	Slightly Disagree	Neither Agree nor Disagree	Slightly Agree	Somewhat Agree	Strongly Agree
	O	O	O	O	O	O	O

“Aplus Insurance's cybersecurity risks are likely to be catastrophic.”

	Strongly Disagree	Somewhat Disagree	Slightly Disagree	Neither Agree nor Disagree	Slightly Agree	Somewhat Agree	Strongly Agree
	O	O	O	O	O	O	O

"Accountants have significant experience auditing information security and cybersecurity controls."

	Strongly Disagree	Somewhat Disagree	Slightly Disagree	Neither Agree nor Disagree	Slightly Agree	Somewhat Agree	Strongly Agree
	O	O	O	O	O	O	O

"Accountants spend a significant portion of their time auditing information security and cybersecurity controls.”

	Strongly Disagree	Somewhat Disagree	Slightly Disagree	Neither Agree nor Disagree	Slightly Agree	Somewhat Agree	Strongly Agree
	O	O	O	O	O	O	O

"Accountants receive significant combined informal and formal training in relation to information security and cybersecurity controls.”

	Strongly Disagree	Somewhat Disagree	Slightly Disagree	Neither Agree nor Disagree	Slightly Agree	Somewhat Agree	Strongly Agree
	O	O	O	O	O	O	O

"Accountants have a high level of information security and cybersecurity controls expertise.”

	Strongly Disagree	Somewhat Disagree	Slightly Disagree	Neither Agree nor Disagree	Slightly Agree	Somewhat Agree	Strongly Agree
	O	O	O	O	O	O	O

For this question, select "4".

	Strongly Disagree	Somewhat Disagree	Slightly Disagree	Neither Agree nor Disagree	Slightly Agree	Somewhat Agree	Strongly Agree
	O	O	O	O	O	O	O

"Delaying the disclosure of a cyber-attack is acceptable given the increased sophistication of hacking techniques."

	Strongly Disagree	Somewhat Disagree	Slightly Disagree	Neither Agree nor Disagree	Slightly Agree	Somewhat Agree	Strongly Agree
	O	O	O	O	O	O	O

“Delaying the disclosure of a cyber-attack is acceptable given the complexity of determining the scope of the breach.”

	Strongly Disagree	Somewhat Disagree	Slightly Disagree	Neither Agree nor Disagree	Slightly Agree	Somewhat Agree	Strongly Agree
	O	O	O	O	O	O	O

"Delaying the disclosure of a cyber-attack is acceptable to conduct required investigations."

	Strongly Disagree	Somewhat Disagree	Slightly Disagree	Neither Agree nor Disagree	Slightly Agree	Somewhat Agree	Strongly Agree
	O	O	O	O	O	O	O

"Delaying the disclosure of a cyber-attack is acceptable even when a cybersecurity attack results in the loss of identifiable information from customers or employees."

	Strongly Disagree	Somewhat Disagree	Slightly Disagree	Neither Agree nor Disagree	Slightly Agree	Somewhat Agree	Strongly Agree
	O	O	O	O	O	O	O

"Managers have more incentives to disclose bad news on a timely basis than incentives to delay the disclosure of bad news."

	Strongly Disagree	Somewhat Disagree	Slightly Disagree	Neither Agree nor Disagree	Slightly Agree	Somewhat Agree	Strongly Agree
	O	O	O	O	O	O	O

"Companies in the health and well-being industry have a higher-risk of cyber-attack compared to companies in other industries."

	Strongly Disagree	Somewhat Disagree	Slightly Disagree	Neither Agree nor Disagree	Slightly Agree	Somewhat Agree	Strongly Agree
	O	O	O	O	O	O	O

"Compared to companies with lower risk of cyber-attacks, companies with higher risk of cyber-attacks are expected to have stronger controls for detecting and disclosing cybersecurity incidents on a timely basis."

	Strongly Disagree	Somewhat Disagree	Slightly Disagree	Neither Agree nor Disagree	Slightly Agree	Somewhat Agree	Strongly Agree
	O	O	O	O	O	O	O

"Timely disclosure of a cybersecurity incident reduces the risk of litigation."

	Strongly Disagree	Somewhat Disagree	Slightly Disagree	Neither Agree nor Disagree	Slightly Agree	Somewhat Agree	Strongly Agree
	O	O	O	O	O	O	O

"Timely disclosure of a cybersecurity incident reduces the risk of lost business."

	Strongly Disagree	Somewhat Disagree	Slightly Disagree	Neither Agree nor Disagree	Slightly Agree	Somewhat Agree	Strongly Agree
	O	O	O	O	O	O	O

"Timely disclosure of a cybersecurity incident is the right thing to do."

	Strongly Disagree	Somewhat Disagree	Slightly Disagree	Neither Agree nor Disagree	Slightly Agree	Somewhat Agree	Strongly Agree
	O	O	O	O	O	O	O

End of Block: Case Questions 2

Start of Block: Thanks

Thanks for completing the task! After completion of the following questionnaire you will receive a validation code to be used to process your payment.

End of Block: Thanks

Start of Block: Demographics

What is your gender?

- O Male
- O Female

What is your age?

- O 18 to 28 years
- O 29 to 38 years
- O 39 to 48 years
- O 49 to 58 years
- O 59 to 69 years
- O Over 70 years

What is the highest level of school you have completed or the highest degree you have received?

- O Less than high school degree
- O High school graduate (high school diploma or equivalent including GED)
- O Some college but no degree
- O Associate degree in college (2-year)
- O Bachelor's degree in college (4 years)
- O Master's degree
- O Professional degree (JD, MD)
- O Doctoral degree

If you studied beyond high school, what was your area of concentration?

_____

What is your current employment status?

- O Full-time employment
- O Part-time employment
- O Self-employed
- O Full-time student
- O Retired
- O Not currently employed, but looking for work
- O Not currently employed and not looking for work

Which of the following industries most closely matches the one in which you are employed?

- O Forestry, fishing, hunting or agriculture support
- O Real estate or rental and leasing
- O Mining
- O Professional, scientific or technical services
- O Utilities
- O Management of companies or enterprises
- O Construction
- O Admin, support, waste management or remediation services
- O Manufacturing
- O Educational services
- O Wholesale trade
- O Health care or social assistance
- O Retail trade
- O Arts, entertainment or recreation
- O Transportation or warehousing
- O Accommodation or food services
- O Information
- O Other services (except public administration)

O Finance or insurance

O Unclassified establishments

Please indicate the answer that includes your entire household income in (previous year) before taxes.

O Less than $20,000

O $20,000 to $39,999

O $40,000 to $59,999

O $60,000 to $79,999

O $80,000 to $99,999

O $100,000 to $149,999

O $150,000 or more

Approximately, how many years of personal investment experience do you have?

O Less than one year

O More than one year but less than three years

O More than three years but less than five years

O More than five years

O No experience

Approximately, how many times have you purchased common stock of a company as a personal investment?

_____

Have you suffered financial loss due to a cybersecurity breach?

O Yes

O No

End of Block: Demographics

APPENDIX J: IRB APPROVALS

University of Central Florida Institutional Review Board
Office of Research & Commercialization
12201 Research Parkway, Suite 501
Orlando, Florida 32826-3246
Telephone: 407-823-2901 or 407-882-2276
www.research.ucf.edu/compliance/irb.html

Determination of Exempt Human Research

From: **UCF Institutional Review Board #1**
FWA00000351, IRB00001138

To: **Patricia Navarro Velez**
Date: **December 05, 2018**

Dear Researcher:

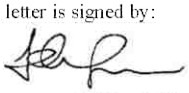
On 12/05/2018, the IRB reviewed the following activity as human participant research that is exempt from regulation:

Type of Review:	Exempt Determination
Modification Type:	Revisions to study instrument.
Project Title:	Jurors liability assessments
Investigator:	Patricia Navarro Velez
IRB Number:	SBE-17-13324
Funding Agency:	
Grant Title:	
Research ID:	N/A

This determination applies only to the activities described in the IRB submission and does not apply should any changes be made. If changes are made and there are questions about whether these changes affect the exempt status of the human research, please contact the IRB. When you have completed your research, please submit a Study Closure request in iRIS so that IRB records will be accurate.

In the conduct of this research, you are responsible to follow the requirements of the Investigator Manual.

This letter is signed by:



Signature applied by Adrienne Showman on 12/05/2018 01:39:40 PM EST

Designated Reviewer

University of Central Florida Institutional Review Board
Office of Research & Commercialization
12201 Research Parkway, Suite 501
Orlando, Florida 32826-3246
Telephone: 407-823-2901 or 407-882-2276
www.research.ucf.edu/compliance/irb.html

Determination of Exempt Human Research

From: **UCF Institutional Review Board #1**
FWA00000351, IRB00001138

To: **Patricia Navarro Velez**

Date: **April 13, 2018**

Dear Researcher:

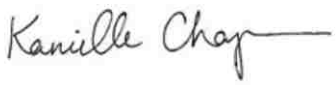
On 04/13/2018, the IRB reviewed the following activity as minor modifications to human participant research that is exempt from regulation:

Type of Review:	Exempt Determination
Modification Type:	Revised survey questions and extended timeline for the study. Revised Protocol and survey questions were uploaded in iRIS.
Project Title:	Jurors liability assessments
Investigator:	Patricia Navarro Velez
IRB Number:	SBE-17-13324
Funding Agency:	
Grant Title:	
Research ID:	N/A

This determination applies only to the activities described in the IRB submission and does not apply should any changes be made. If changes are made and there are questions about whether these changes affect the exempt status of the human research, please contact the IRB. When you have completed your research, please submit a Study Closure request in iRIS so that IRB records will be accurate.

In the conduct of this research, you are responsible to follow the requirements of the Investigator Manual.

This letter is signed by:



Signature applied by Kamille Chaparro on 04/13/2018 01:47:52 PM EDT

Designated Reviewer

UNIVERSITY OF CENTRAL FLORIDA

Institutional Review Board
FWA00000351
IRB00001138
Office of Research
12201 Research Parkway
Orlando, FL 32826-3246

EXEMPTION DETERMINATION

March 14, 2019

Dear Patricia Navarro Velez:

On 3/14/2019, the IRB determined the following submission to be human subjects research that is exempt from regulation:

Type of Review:	Initial Study, Category
Title:	Investors Valuation Judgments
Investigator:	Patricia Navarro Velez
IRB ID:	STUDY00000304
Funding:	None
Grant ID:	None

This determination applies only to the activities described in the IRB submission and does not apply should any changes be made. If changes are made, and there are questions about whether these changes affect the exempt status of the human research, please contact the IRB. When you have completed your research, please submit a Study Closure request so that IRB records will be accurate.

If you have any questions, please contact the UCF IRB at 407-823-2901 or irb@ucf.edu. Please include your project title and IRB number in all correspondence with this office.

Sincerely,

Adrienne Showman
Designated Reviewer